DOCUMENT COVER SHEET

DOCUMENT NO.	REVISION	PAGE	OPEN ITEMS
UKP-GW-GL-793NP	1	1 of 4401	N

DOCUMENT STATUS: **DES** | **AP1000** SAFETY CLASS: **NA**

LICENSING REVIEW STATUS: Not Required

PLANT APPLICABILITY:

☐ All **AP1000** Plants except:

☒ Only the following plants:
UKP

Westinghouse Acceptance of **AP1000** Design Partner Document by:

N/A
(Print Full Name)

(Signature/Date)

ALTERNATE DOCUMENT NUMBER: N/A

ORIGINATING ORGANIZATION: Westinghouse Electric Company LLC

TITLE: **AP1000** Pre-Construction Safety Report

DCP/DCA/SUPPLEMENTS/EDCR # INCORPORATED IN THIS DOCUMENT REVISION:
None

ATTACHMENTS:
F-UKP-GW-GAP-027-1.zip

PARENT DOCUMENT: UKP-GW-GL-793, Rev. 1

LEGAL REVIEW Colleen T. Grygier	SIGNATURE / DATE **(If processing electronic approval select option)** **Electronically Approved*** **
PATENT REVIEW Douglas E. Ekeroth	SIGNATURE / DATE **Electronically Approved*** **

ORIGINATOR(S) W2-6.1-100.pdf Paul E. Wick	SIGNATURE / DATE **(If processing electronic approval select option)** **Electronically Approved*** **	
REVIEWER(S) W2-6.1-100.pdf N/A	SIGNATURE / DATE	
VERIFIER(S) W2-6.1-100.pdf Helena K. Perry	SIGNATURE / DATE **Electronically Approved*** **	Verification Method: **Independent Review**
APPLICABILITY REVIEWER W2-6.1-100.pdf N/A	SIGNATURE / DATE	
RESPONSIBLE MANAGER* W2-6.1-100.pdf Jason J. Eisenhauer	SIGNATURE / DATE **Electronically Approved*** **	

**Approval of the responsible manager signifies that the document and all required reviews are complete, the appropriate proprietary class has been assigned, electronic file has been provided to the EDMS, and the document is released for use.*

****** Electronically approved records are authenticated in the electronic document management system. This record was final approved on Mar-17-2017. (This statement was added by the EDMS system to the quality record upon its validation.)***

******Electronically approved records are authenticated in the electronic document management system.***

DCP/DCA/SUPPLEMENTS/EDCR # INCORPORATED IN THIS DOCUMENT REVISION:

This document is the Non-Proprietary Class 3 version of UKP-GW-GL-793, Revision 1. Proprietary information has been marked with brackets and redacted from this version. See UKP-GW-GL-793, Revision 1 for DCP/DCA/Supplements/EDCR Incorporated.

AP1000® Pre-Construction Safety Report

UKP-GW-GL-793NP, Revision 1

Westinghouse Electric Company LLC
1000 Westinghouse Drive
Cranberry Township, PA 16066, USA

TABLE OF CONTENTS

TABLE OF CONTENTS

LIST OF TABLES

None.

LIST OF FIGURES

LIST OF ABBREVIATIONS AND ACRONYMS

ac	alternating current
ADS	automatic depressurisation system
ALARP	as low as reasonably practicable
ALWR	advanced light water reactor
BPM	best practical means
BSL	basic safety level
BSO	basic safety objective
C&I	control and instrumentation
CCS	component cooling water system
CDF	core damage frequency
CMT	core makeup tank
CNS	Civil Nuclear Security
CV	containment vessel
CVS	chemical and volume control system
DAC	Design Acceptance Confirmation
DAS	diverse actuation system
DBA	design basis accident
dc	direct current
DCD	Design Control Document
DiD	defence-in-depth
DOE	Department of Energy
EA	Environment Agency
ECS	main ac power system
EDS	Class 2 DC and Uninterruptible Power Supply System
EPRI	Electric Power Research Institute
GDA	generic design assessment
HSE	Health and Safety Executive
HVAC	heating, ventilation, and air conditioning
iDAC	interim Design Acceptance Confirmation
IDS	essential electrical supply system
iSoDA	interim Statement of Design Acceptability
IRWST	in-containment refueling water storage tank
LOCA	loss-of-coolant accident
LRF	large release frequency
LTOP	low-temperature overpressure protection
MCR	main control room
ND	Nuclear Directorate
NPP	nuclear power plant
ONR	Office for Nuclear Regulation
PCS	passive containment cooling system
PCSR	Pre-Construction Safety Report
PLS	plant control system
PMS	protection and safety monitoring system
PRHR	passive residual heat removal
PSA	probabilistic safety assessment
PWR	pressurised water reactor

LIST OF ABBREVIATIONS AND ACRONYMS (cont.)

PXS	passive core cooling system
RCS	reactor coolant system
RNS	normal residual heat removal system
RP	requesting party
SAP	safety assessment principle
SFW	startup feedwater system
SoDA	Statement of Design Acceptability
SSC	system, structure, or component
SWS	service water system
UK	United Kingdom
URD	Utility Requirements Document
US	United States
ZOS	onsite standby power system

1 INTRODUCTION

This chapter describes the contents of the Pre-Construction Safety Report (PCSR) for the Westinghouse AP1000 nuclear power plant (NPP or AP1000), submitted through the Office for Nuclear Regulation (ONR) and the Environment Agency (EA) generic design assessment (GDA) process. It provides an introduction to the GDA process, a summary of the content of the PCSR, and a high-level overview of the AP1000 design approach including its innovative safety features and capabilities.

The PCSR demonstrates that the AP1000 design, construction, operation and ultimate decommissioning fully meet United Kingdom (UK) regulatory requirements and fulfil the requirements of the ONR safety assessment principles (SAPs) (Reference 1.1).

1.1 BACKGROUND

The UK nuclear regulators, the ONR (previously the Health and Safety Executive-Nuclear Directorate [HSE-ND]), and the EA, have jointly established the UK GDA process (Reference 1.4), described in Section 2.3, to assess the safety, security, and environmental implications of particular generic reactor designs before an application is made for the permission to build a new nuclear reactor at a specific site. The complete licensing process is two phases, namely Phase 1 (GDA) and Phase 2 (nuclear site licensing). The GDA provides a coordinated approach by the regulators for the pre-licensing/pre-authorisation phase. If positive, the outcome of the GDA process will be the publication of a Design Acceptance Confirmation (DAC) and an EA Statement of Design Acceptability (SoDA) for the generic design. It is envisaged that the DAC and SoDA will form the basis of any application to build the corresponding reactor on a specific site.

Westinghouse is a requesting party (RP) in the GDA process, as it seeks the DAC from the ONR and a SoDA from the EA for its AP1000 standard design. Since the start of Phase 1, Westinghouse has submitted a number of documents to the ONR/HSE-ND and EA as required under the GDA. In summary, the submission and outcome of the four steps in Phase 1 are as follows:

- Step 1 (Q1 to Q3, 2007) was the preparatory design assessment process during which there were discussions to establish a full understanding of the requirements and processes that would be applied. A number of documents including, but not limited to, UK Compliance Document for AP1000 Design (Reference 1.5), UK AP1000 Safety and Environment Report (Reference 1.6), and the UK AP1000 Probabilistic Risk Assessment (Reference 1.7) were submitted for assessment by the HSE-ND and the EA. Step 1 was completed in August 2007, and the HSE-ND acknowledged (Reference 1.8) that the submission met the required criteria and was eligible for GDA.

- Step 2 (Q3, 2007 to Q2, 2008) was a review of the fundamental acceptability of the proposed reactor design concept within the UK regulatory regime to identify any aspects that could prevent the proposed design from being licensed in the UK. The HSE-ND Step 2 report (Reference 1.9) issued in March 2008 concluded that the HSE-ND did not find "any safety or security shortfalls that are so serious as to rule out at this stage eventual construction of the AP1000 on licensed sites in the UK. As a result of our assessment, we see no reason why the AP1000 should not progress to GDA Step 3."

- Step 3 (Q2, 2008 to Q4, 2009) required the RP to provide a generic PCSR to the HSE-ND and an environment report to the EA detailing the safety and environment aspects of the proposed reactor design. The general intention was to move from the

fundamentals of the previous step to an analysis of the design, primarily by examination at the system level and by analysis of the RP's supporting arguments. Westinghouse submitted PCSR Rev. 1 (Reference 1.10) in August 2009 and, following comments from the HSE-ND, PCSR Rev. 2 (Reference 1.11) in December 2009. The Step 3 report (Reference 1.12) concluded that the HSE-ND believed "that the AP1000 could be suitable for construction on licensed sites in the UK" subject to resolution of a number of issues in Step 4. It was also concluded that the HSE-ND had "not identified any significant issues, or significant design or safety case changes that could impact on radioactive waste arisings or have a significant negative environmental impact." During Step 3, Westinghouse submitted a technical report to the Office for Civil Nuclear Security that described the security measures for the AP1000 design. The Step 3 security assessment report (Reference 1.13) concluded "No significant issues have been identified so far that would preclude this design from being adequately secured against malicious capabilities."

- Step 4 (Q1, 2010 to Q4, 2011) is an in-depth assessment by the ONR/HSE-ND and EA of the safety case and generic site envelope submitted. The general intention of this step is to move from the system-level assessment of Step 3 to a fully detailed examination of the evidence, on a sampling basis, given by the safety analyses. The aim of this step is to do the following:

  – Confirm that the higher-level claims, such as system functionality, are properly justified.

  – Complete a sufficiently detailed assessment to allow the ONR/HSE-ND and EA to come to a judgement whether or not a DAC and Statement of Design Acceptability can be issued.

  At the end of Step 4, GDA Issues were identified that require the RP to resolve before the issuance of a DAC and SoDA.

  In December 2011, the ONR issued an interim Design Acceptance Confirmation (iDAC) (Reference 1.18) and the EA issued an interim Statement of Design Acceptability (iSoDA) (Reference 1.19) to Westinghouse.

Within the joint regulatory GDA process described above, the EA's process is based on two steps, consisting of a preliminary and a detailed assessment of the design. This is followed by a public consultation, which reflects its normal policy. Any comments received during the public consultation will be considered by the EA as part of any site authorisation process; they will not be considered during the GDA process.

In order to meet these requirements, Westinghouse has submitted this PCSR and other supporting documents, as defined in the GDA Master Document Submission List. The previous revisions of the PCSR presented the safety claims, arguments, and evidence at a level appropriate to the step of the GDA process. This revision reflects the developments since the iDAC and incorporates changes to the safety case identified in the closure phase.

1.2 UK NUCLEAR REGULATORY REGIME

The UK nuclear regulatory regime is based on the Nuclear Installations Act 1965 (as amended). The sections of this act relating to licensing and inspection of nuclear installations are relevant statutory provisions of the Energy Act 2013.

The ONR and EA developed the GDA process in response to a request from the UK government following its 2006 Energy Review. The following principal organisations are involved in the regulation of civil NPPs in the UK:

- **Office for Nuclear Regulation** (ONR) – Responsible for the regulation of nuclear safety and security across the UK.

- **Environment Agency** (EA) – Responsible for the regulation of discharges and radioactive waste disposals from nuclear power stations and to ensure their impact on air, water, and land is acceptable and minimised.

The regulatory regime in the UK is different from many other countries in that it is not based on compliance with prescriptive regulations apart from statutory radiological worker and public dose limits for normal operation. The UK approach is based on goal setting, and the ONR has published SAPs (Reference 1.1) that it uses to assess nuclear safety cases. The safety case is required to show that the design, construction, and operation of the plant is safe, and that the risk to the public, workforce, and environment is as low as reasonably practicable (ALARP).

1.3 AP1000 PRE-CONSTRUCTION SAFETY REPORT

This PCSR is a lead document in the submission by Westinghouse for the GDA process. The development of the PCSR and the way it fits within the suite of safety documentation that forms the safety case developed throughout the AP1000 plant life is discussed in Chapter 2.

This revision of the PCSR is specific to the close-out of the GDA process. It supersedes the earlier versions (Refs. 1.10 and 1.11) produced for GDA Steps 2, 3, and 4.

This PCSR provides the overall safety case for the AP1000 design, construction, commissioning, operation, maintenance, and decommissioning. The complete safety submission is described in Chapter 2, and consists of this PCSR and a number of supporting documents. The linkage of the PCSR with key supporting documents, including the Safety and Environment Report (Reference 1.6), is presented in the Plant Life Cycle Safety Report (Reference 1.14).

This PCSR is presented in the following six volumes:

- Volume 1 – Executive Summary and Safety Case Management

- Volume 2 – Engineering Principles and Plant Overview

- Volume 3 – Faults and Accident Assessment

- Volume 4 – Engineering Substantiation

- Volume 5 – Radiation Protection, Emergency, Accident, and Waste Management

- Volume 6 – Conclusions

Acronyms used within the chapters are defined at the start of each chapter and consolidated for the whole of the PCSR in Appendix 1A.

1.3.1 Volume 1, Executive Summary and Safety Case Management

Chapter 1, Introduction – Describes the contents of the PCSR submitted under Phase 1, Step 4 of the GDA process. It also provides a high-level overview of the AP1000 design approach together with an introduction to its innovative safety features and capabilities.

Chapter 2, Safety Case – Presents the structure, content and overall logic of the safety case. The safety case itself is developed in the subsequent chapters.

Chapter 3, Management of Safety – Deals with the management of safety and quality relating to this safety case and how it provides key inputs into the site-specific safety cases required for construction, commissioning, operation, maintenance and ultimate decommissioning and how the safety case will be developed throughout the plant life.

Chapter 4, Generic Site Characteristics – Describes the UK generic site assumed in the assessment.

1.3.2 Volume 2, Engineering Principles and Plant Overview

Chapter 5, Engineering Principles – Describes the engineering principles applied within the PCSR and the approach to the classification of Safety Systems and equipment qualification and reliability.

Chapter 6, Plant Description and Operation – Presents a comprehensive, detailed description of the AP1000 plant including the primary and auxiliary systems, the passive safety systems and the civil structures.

Chapter 7, Life Cycle Engineering and Safety – Describes the approach to engineering and safety during the complete lifecycle of the reactor from design control, construction, commissioning and operation through to decommissioning. The requirements for examination, maintenance, inspection and testing and taking due cognisance of ageing and degradation are also presented.

1.3.3 Volume 3, Faults and Accident Assessment

Chapter 8, Fault and Accident Analysis – Presents the methodology for fault and consequence assessment, identification of the design basis faults and development of the fault schedule. A composite fault list that covers the full set of initiating faults addressed throughout the safety justification is provided in Appendix 8A.

Chapter 9, Internally Initiated Faults – Describes the internally initiated faults that could lead to core damage or could lead to a release of nuclear material.

Chapter 10, Reactor Faults Probabilistic Safety Assessment and Severe Accident Analysis – Presents a summary of the Probabilistic Safety Assessment (PSA) for the AP1000 design, its links to design basis accident (DBA) fault sequence groups and the approach to risk reduction and the ALARP principle.

Chapter 11, Internal Hazards – Presents the internal hazards identified for the AP1000 design including but not limited to fire, flood, explosions and missiles, dropped loads and release of toxic material. The safety case for each hazard is provided.

Chapter 12, External Hazards – Presents the identified external hazards including, but not limited to, earthquake, extreme wind and rainfall. The safety case for each hazard is provided.

Chapter 13, Human Factors – Provides a summary of the human factors input to the design and safety process including error identification methodology and classification, the screening of errors and the ALARP arguments.

Chapter 14, Results and Conclusions – Fault Analysis – Presents the results and conclusions of the analyses presented in Chapters 8 to 13 with an overall ALARP assessment demonstrating that the plant is safe to operate.

1.3.4 Volume 4, Engineering Substantiation

Chapter 15, Engineering Substantiation – Describes the approach to engineering substantiation and a summary of the Engineering Schedule.

Chapters 16, Civil Engineering – Describes the civil engineering aspects of the plant and presents evidence that the engineering provision meets the safety requirements of normal operation, fault and hazard conditions and ageing.

Chapter 17, Mechanical Engineering – Describes the mechanical engineering aspects of the plant and presents evidence that the engineering provision meets the safety requirements of normal operation, fault and hazard conditions and ageing.

Chapter 18, Essential Electrical Systems – Describes the essential electrical systems of the plant and presents evidence that the engineering provision meets the safety requirements of normal operation, fault and hazard conditions and ageing.

Chapter 19, Control and Instrumentation – Describes the control and instrumentation (C&I) engineering aspects of the plant and presents evidence that the engineering provision meets the safety requirements of normal operation, fault and hazard conditions and ageing.

Chapter 20, Structural Integrity – Describes the structural integrity aspects of the plant and presents evidence that the engineering provision meets the safety requirements of normal operation, fault and hazard conditions and ageing.

Chapter 21, Reactor Chemistry – Describes the reactor chemistry aspects of the plant and presents evidence that the engineering provision meets the safety requirements of normal operation, fault and hazard conditions and ageing.

Chapter 22, Fuel System, Nuclear and Thermal Hydraulic Design – Describes the fuel design and presents evidence that the engineering provision meets the safety requirements of normal operation, fault and hazard conditions and ageing.

Chapter 23, Containment and Nuclear Ventilation Systems – Describes the containment and ventilation aspects of the plant and presents evidence that the engineering provision meets the safety requirements of normal operation, fault and hazard conditions and ageing.

1.3.5 Volume 5, Radiation Protection, Emergency, Accident, and Waste Management

Chapter 24, Radiation Protection – Summarises the radiological hazards under normal and accident conditions and the protection measures to mitigate consequences of the identified hazards.

Chapter 25, Accident Management – Describes general arrangements, facilities and equipment to assist the management of emergencies currently included in the AP1000 design basis.

Chapter 26, Radioactive Waste Management – Summarises the arrangements for handling wastes arising from normal operations, the approach to waste minimisation and the approach to the segregation of wastes. The chapter draws on information provided, in particular in the Environment Report and the Integrated Waste Strategy, for the management and details of all radioactive waste and non-radioactive waste arising during operations and decommissioning.

Chapter 27, Decommissioning and End-of-Life Aspects – Presents the decommissioning strategy that demonstrates that the generic AP1000 design can be safely decommissioned at the end of its operational life. Demonstration that dose management through decommissioning will result in doses that are ALARP, and that waste volumes and activities have been minimised by design, are also presented.

1.3.6 Volume 6, Conclusions

Chapter 28, Conclusions – Draws together the overall conclusions from the previous chapters.

1.4 THE AP1000 DESIGN

1.4.1 AP1000 Design Philosophy

The Westinghouse AP1000 design is an advanced and passively safe pressurised water reactor (PWR) with an output capacity of approximately 1100 MWe (actual power output depends on site-specific conditions) and a design service life of 60 years.

The most significant aspect of the AP1000 design philosophy, and the one that sets the design apart from existing PWRs, is the use of passive means of protecting against faults. These passive safety features rely solely on natural mechanisms such as natural convection and driving forces derived from stored energy (gravity, batteries, and compressed gases) rather than active pumped systems; therefore, safety is substantially enhanced.

In comparison with PWR plants in operation today, the AP1000 design represents considerable simplifications that enhance nuclear safety and facilitate construction, operation, maintenance, and decommissioning. A general arrangement is presented in Figure 1-1.

The AP1000 design is the combination of proven design concepts and is the result of operational experience from existing PWR plants applied to a defined set of functional requirements in the most simple, effective way practicable.

The design is founded on adherence to the following inviolate principles:

- The systems providing the principal means of delivering the following safety functions will not require alternating current (ac) power:
  - Shutting down the nuclear reaction
  - Removing decay heat, which uses only natural mechanisms such as natural circulation, conduction, convection, evaporation, and condensation
  - Maintaining the reactor coolant water inventory
  - Containment isolation

  - Maintaining other safety functions such as spent fuel pool cooling, main control room (MCR) habitability, and severe accident mitigation features

- Active Class 2 systems minimise demand on passive systems and provide defence in depth.

- Multiple barriers exist to prevent release of fission products. The function of containment of radioactive materials is provided by a hierarchy of barriers, one within another. The initial barrier is the cladding of the fuel; each fuel element is clad in a tube made from a zirconium alloy. The integrity of this cladding is ensured by adequate transfer of heat to the coolant. The reactor core is contained in a high-integrity steel pressure vessel (the reactor vessel) that, together with the primary circuit, provides the next barrier. The containment building provides a final barrier and retains radioactive material in the event that the primary circuit is breached; for example, in a loss-of-coolant accident (LOCA).

- Calculated core damage frequency (CDF) and large release frequency (LRF) are minimised by eliminating failure modes by design rather than providing mitigation features. This approach ultimately results in a plant design that is safe because it has the design objective that the risk to the operators and the public is ALARP.

- Simplification of the plant with respect to design, licensing, construction, operation, inspection, and maintenance.

- Tolerance to faults by means of reducing possible faults by design and by the provision of reliable, passive, automatic mitigating systems.

1.4.2 Evolution of the AP1000 Design

1.4.2.1 Design Evolution

Westinghouse has been involved with PWRs since the early days of commercial nuclear power in the 1950s. Westinghouse has designed and delivered more than 100 commercial NPPs and nearly 50 percent of the world's 440 nuclear plants are based on Westinghouse technology. The AP1000 design is the culmination of this design, build, and operating experience. Eight AP1000 plants are currently under construction in the United States (US) and China, with dozens more planned around the world.

The AP1000 design is an evolution of the AP600 design originally developed by Westinghouse during the 1980s and early 1990s as part of the cooperative US Department of Energy (DOE) and Electric Power Research Institute (EPRI) advanced light water reactor (ALWR) programme. The purpose of the programme was to design a new plant with levels of safety that were significantly improved over existing plants by using the lessons learned from the operating experience gained over the previous three decades.

Designed to satisfy the standards defined in the ALWR Utility Requirements Document (URD) (Reference 1.15), the Westinghouse AP600 design is a combination of innovative passive safety systems that rely on dependable natural forces and proven conventional technology. The ALWR URD contains a large number of design improvements for safety and reliability, many of which were implemented or improved upon in the AP600 design. The implementation of some features exceeded the URD requirements; for example, post-accident reliance on ac power is eliminated rather than just reduced. Following a DBA, the passive safety systems and equipment are sufficient to automatically establish and maintain core cooling and containment integrity indefinitely, by reliance exclusively on natural forces and stored energy (see Section 1.4.2.3).

When the AP600 design received US Design Certification, it was the safest, simplest, and lowest-cost nuclear reactor on the market. However, this also coincided with a period of relatively low oil and gas prices that made the AP600 design uneconomic in comparison with a fossil fuel plant.

Making a significant reduction in the cost of the AP600 design was not possible by making small system and component improvements. The solution was to increase the power output of the plant which would reduce the cost per megawatt below that of a natural gas plant; this would require some components to increase in size/capacity however the cost increase was much less than power increase. The power increase was achieved by increasing the height of the reactor vessel and the containment structure such that the general arrangement of the plant did not have to change. Other changes included a larger turbine and other plant equipment as appropriate to provide the larger power output and to maintain safety margins. This new design, capable of generating over 1000 MWe, is the AP1000 design. The AP1000 design primary circuit components are shown in Figure 1-2.

The AP1000 design maintains the large safety margins of the AP600 design. No new concepts or changes to fundamental principles were introduced to the proven components chosen for the AP600 design. The test data obtained for the AP600 design were shown to be applicable to the AP1000 design. The changes to the AP600 Design Control Document (DCD) were minimised and the AP1000 design retains compliance with the US utilities' requirements as expressed in the ALWR URD (Reference 1.15). The AP1000 design safety analysis is documented Chapter 9 and the risk to the public is documented in the probabilistic safety assessment (PSA) (Chapter 10), which together demonstrates that large safety margins are maintained for the AP1000 design. It also shows that the AP1000 design improves on the probability of large release goals for advanced reactor designs in the event of a severe accident scenario retaining the molten core within the reactor vessel.

1.4.2.2 Use of Proven Components and Technology in the AP1000 Design

The use of proven components and technology greatly facilitates the construction, operation, and maintenance of the AP1000 design. The AP1000 core and major reactor internal components are designs proven by their use in currently operating PWRs supplied by Westinghouse:

- The AP1000 core uses a design for the fuel used in current Westinghouse reactors.
- The control rod drive mechanisms are the same as in existing Westinghouse reactors.
- The AP1000 steam generator design is based on 30 years of operating experience, including design features incorporated in the latest Westinghouse replacement steam generator designs.
- Construction materials for components in the AP1000 design have been selected based on lessons learned from operating experience in existing plants.
- The development of digital C&I systems for back-fitting to currently operating plants has allowed such systems to be incorporated into the AP1000 design with a level of safety proven by practical experience and extensive computer software verification and validation.

Furthermore, several important enhancements, all based on existing technology, improve the safety performance characteristics of the design relative to currently operating PWRs:

- The AP1000 reactor coolant pumps do not have seals. Their design is based on proven seal-less motor pump technology that has been used in naval PWRs and various non-nuclear commercial applications. This eliminates the potential for LOCAs due to seal failure, enhancing safety by removing the major contributor to small LOCAs.

- The AP1000 design reactor coolant system (RCS) piping with an outside diameter of 10 cm or more has been designed to reduce the probability of their gross failure. Evaluations have concluded that elimination many of the pipe whip restraints is ALARP considering improvements in the ability to perform in-service inspection and also reduces operators' radiation exposures associated with such inspections. The number of welds in the primary circuit has been reduced in comparison with earlier designs.

- The number of containment penetrations has been reduced by half and the containment isolation valves have been replaced by types that are less likely to leak than those used on previous PWRs.

- The AP1000 design features an advanced MCR, as required by the ALWR URD (Reference 1.15). Incorporating human factors assessment in the design and testing of the MCR reduces the likelihood of the operators either inadvertently causing initiation of a fault sequence or performing the wrong actions during a fault sequence.

1.4.2.3 Use of Innovative Safety Features and Capabilities in the AP1000 Design

The distinguishing safety enhancement of the AP1000 design over existing PWR technology is the adoption of passive protective safety measures, which operate during fault sequences in the event that normal duty systems have failed. These systems are regarded as passive because they rely on natural physical processes for their operation with no reliance on active components such as pumps, fans, or diesel generators; and they are designed to function without Class 1 support systems such as ac power and component cooling water. The only requirement for initiating these passive systems is the one-time realignment of valves which can be achieved with high reliability.

These passive systems provide a means of controlling reactivity and removing decay heat for the first 72 hours in design basis accident scenarios.

- The core makeup tanks (CMTs) provide borated water by gravity feed to provide additional coolant and to control reactivity.

- The automatic depressurisation system (ADS) depressurises the primary circuit to allow for safety injection. The accumulators are connected to the primary circuit with non-return valves and contain water under pressure from compressed gas. They provide additional coolant automatically once the primary pressure drops below the gas pressure that forces the borated water through the non-return valves.

- The passive residual heat removal (PRHR) system uses a heat exchanger in the in-containment refuelling water storage tank (IRWST) to remove heat from the primary circuit by natural circulation.

- The passive containment cooling system (PCS) uses water flowing under gravity and natural circulation of air to cool the outside of the containment vessel (CV). Heat is transferred to the CV from the reactor by evaporation of water that condenses on the inside of the CV and then runs back to the IRWST.

- The PCS and passive core cooling system (PXS) provide means for long-term core cooling and containment heat removal.

The operation of these passive systems has been verified using highly developed thermal-hydraulic computer codes, which in turn are verified against real systems tests and extensive rig testing. Computer simulations using these codes have enabled the AP1000 design to demonstrate that these innovative passive features substantially enhance its nuclear safety capability. A summary of the technical support documents that support the AP1000 design are presented in Chapter 2.

The PXS shown in Figure 1-3 comprises the CMTs, ADS, accumulators, IRWST, and PRHR system. The PCS is shown in Figure 1-4.

The primary means of satisfying Category A safety functions is using passive Class 1 systems, structures, or components (SSCs). In addition to the passive systems outlined above, a number of Class 1 and Class 2, SSC's support the passive components and provide defence in depth by adding additional redundancy and diversity to the AP1000 design.

For C&I systems:

- The protection and safety monitoring system (PMS) provides detection of abnormal conditions and actuation of the appropriate Class 1 systems necessary to achieve and maintain the plant in a safe shutdown condition.

- The diverse actuation system (DAS) is a Class 2 system that provides diverse backup actuation of the Class 1 passive features. The DAS also provides manual actuation capability for a number of systems.

- The plant control system (PLS) provides Class 2 actuation of the active defence-in-depth (DiD) systems.

- The essential electrical supply system (IDS), referred to as the essential power supply in this PCSR, consists of four static battery-backed divisions. The IDS provides reliable power for the Class 1 equipment required for the plant instrumentation, control, monitoring, and other vital functions needed for shutdown of the plant. In addition, the IDS provides power to the normal and emergency lighting in the MCR and the remote shutdown workstation.

For mechanical systems:

- The plant Class 1 passive features such as the PRHR HX, CMTs and PCS.

- For more frequent events, other Class 1 passive features provide backup to these passive features such as passive feed and bleed (ADS, Accumulators, IRWST injection and containment recirculation)

- A number of active Class 2 systems provide additional backup for frequent events.

    - The startup feedwater system (SFW) supplies feedwater to the steam generators during plant startup, hot standby, and shutdown conditions.

    - The chemical and volume control system (CVS) consists of two centrifugal makeup pumps providing makeup flow to the reactor primary circuit.

- The normal residual heat removal system (RNS) removes heat from the core and RCS and provides RCS low-temperature overpressure protection (LTOP) at reduced RCS pressure and temperature conditions after shutdown.

- The component cooling water system (CCS) is a closed-loop cooling system that supports the RNS during fault conditions.

- The service water system (SWS) supplies cooling water to remove heat from the CCS heat exchangers in the turbine building.

- The Class 2 dc and Uninterruptible Power Supply System (EDS) provides dc and uninterruptible ac electrical power to the Class 2 components above.

- The main ac power system (ECS) provides electrical ac power to the Class 2 components above.

- The onsite standby power system (ZOS) consists of two onsite Class 2 standby diesel generator units and support systems that support EDS functions.

The quality assurance requirements associated with the Class 1 and Class 2 SSCs outlined above are presented in Chapter 5.

1.4.3 Standardisation of the AP1000 Design

The evolution of the AP1000 design has been built on the design philosophy which emphasised safety and simplicity. Another important aspect of the AP1000 plant design approach is standardisation across multiple sites around the world. This approach of using a standard design has been welcomed in the U.S. and around the world in applications to other regulatory authorities. Standardisation brings large benefits in the minimization of the chance of design, analysis, licensing, construction, and operation errors by advoiding repetition of design activities and sharing operational experience amongst licensing agencies and operating utilities in the future.

The Design Reference Point document (Reference 1.17) defines the UK design reference point for the AP1000 design that is relevant to the GDA application. Further discussion on the AP1000 design reference point is presented in Chapter 6 together with a detailed description of the plant and operation.

Following initial approval, design documentation is placed under configuration control. Once under configuration control, changes to the design documentation can only be made through the design change proposal process (Reference 1.17). Design change control is discussed further in Chapter 7.

1.5 KEY SAFETY ATTRIBUTES

In many respects, the AP1000 design is a conventional PWR. However, the implementation of passive safety features and the simplification of the design significantly contribute to the improved safety and reliability of the plant. A summary of the key safety attributes is presented here, with the full detail covered in the remainder of the PCSR:

- The use of proven technology and evolutionary design means plant operation is highly reliable in all plant operating modes (startup, power operation, standby, and refuelling) and throughout plant life (construction, commissioning, operation, maintenance, and

decommissioning) with the fault rates for many types of common or anticipated faults being significantly lower than for existing plants.

- Passive systems are available to supply all essential safety functions following a fault, with more conventional systems providing defence in depth. This makes the AP1000 design and operation extremely tolerant to faults with risk to the public, workers, and environment being significantly reduced over existing plants and being reduced to levels that are ALARP; for example, CDF and LRF are several orders of magnitude lower than existing plants.

- The use of modular construction techniques means that the construction process is safer, simpler, and more predictable, leading to higher quality construction. This form of construction also aids decommissioning.

- All design basis and probabilistic targets are met using passive Class 1 safety systems backed up by other Class 1 systems and also by active Class 2 systems providing defence in depth.

- Separation, segregation, redundancy, and diversity provided by the design minimise the effects of internal and external hazards and human errors.

- Simplifications in the design mean that operator doses are significantly reduced during operation, maintenance, and inspection activities. Operational release of activity is well within the authorised limits, and doses will be kept below the basic safety level (BSL), the legal limit, and, where practicable, the basic safety objective (BSO), and ALARP; e.g., targets 1, 2, and 3 of the ONR SAPs (Reference 1.1). Best practicable means (BPM) are used to minimise discharges to the environment and to minimise radioactive wastes arisings, including those from operations, maintenance, decommissioning, and site restoration.

- Simplification of the design will have a major impact on decommissioning. Compared with similarly sized NPPs, the AP1000 design has roughly 50 percent fewer valves; 35 percent fewer pumps; 80 percent less piping; and 80 percent fewer heating, ventilation, and air conditioning (HVAC) systems. Therefore, the decommissioning phase of the AP1000 design is expected to be shorter, and decommissioning activities are expected to produce less activated or contaminated material, resulting in simpler strategies and lower funding requirements.

1.6 SUMMARY

This PCSR is one of the lead documents in the safety submission for the AP1000 design, construction, operation, and maintenance. Subject to obtaining a successful DAC, and a SoDA from the EA, the PCSR will be updated with site-specific licensing requirements for Nuclear Site Licensing. The complete safety submission is described in Chapter 2, and consists of this PCSR and a number of supporting documents.

The safety case detailed in subsequent chapters demonstrates that the AP1000 design, construction, and operation meet UK licensing requirements and safety principles; have safety levels in excess of nuclear plants currently in operation; and have levels of public, worker, and environmental risk that are ALARP.

1.7 REFERENCES

1.1 "Safety Assessment Principles for Nuclear Facilities," Rev. 0, Office for Nuclear Regulation, 2014.

1.2 Not Used.

1.3 Not Used.

1.4 ONR Document ONR-GDA-GD-001, Rev. 2, "New Nuclear Reactors, Generic Design Assessment, Guidance to Requesting Parties," June 2016.

1.5 Westinghouse Report UKP-GW-GL-710, Rev. 0, "UK Compliance Document for AP1000 Design," August 2007.

1.6 Westinghouse Report UKP-GW-GL-790, Rev. 6, "UK AP1000 Environment Report," January 2017.

1.7 Westinghouse Report UKP-GW-GL-022, Rev. 0, "UK AP1000 Probabilistic Risk Assessment," May 2007.

1.8 Letter from HSE 2007/152059, "Generic Design Assessment – Agreements," October 7, 2007.

1.9 "Public Report on the Generic Design Assessment of New Nuclear Reactor Designs, Westinghouse Electric Company LLC AP1000 Nuclear Reactor, Conclusions of the Fundamental Safety Overview of the AP1000 Nuclear Reactor (Step 2 of the Generic Design Assessment Process)," Health and Safety Executive, March 2008.

1.10 Westinghouse Report UKP-GW-GL-732, Rev. 1, "Pre-Construction Safety Report," October 2009.

1.11 Westinghouse Report, UKP-GW-GL-732, Rev. 2, "Pre-Construction Safety Report," December 2009.

1.12 Report of the System Design and Security Review of the AP1000 Nuclear Reactor June 2008 – October 2009 (Step 3 of the Generic Design Assessment Process), November 2009.

1.13 HSE-ND Division 5 Assessment Report No. AR 09/042-P, "Step 3 Security Assessment of the Westinghouse AP1000," Health and Safety Executive, Nuclear Directorate.

1.14 Westinghouse Report UKP-GW-GL-737, Rev. 2, "Plant Life Cycle Safety Report," March 2011.

1.15 "Advanced Light Water Reactor Utilities Requirements Document," Volumes I, II, and III, Rev. 8, Electric Power Research Institute, March 1999.

1.16 Not Used.

1.17 Westinghouse Report UKP-GW-GL-060, Rev. 10, "AP1000 Design Reference Point for UK GDA," January 2017.

1.18 Letter from ONR 2011/606827, "New nuclear power stations: Generic Design Assessment Interim Design Acceptance Confirmation for the AP1000® Reactor," December 2011.

1.19 Letter from EA, "Generic assessment of candidate nuclear power plant designs interim statement of design acceptability for the AP1000® design submitted by Westinghouse Electric Company LLC," December 2011.

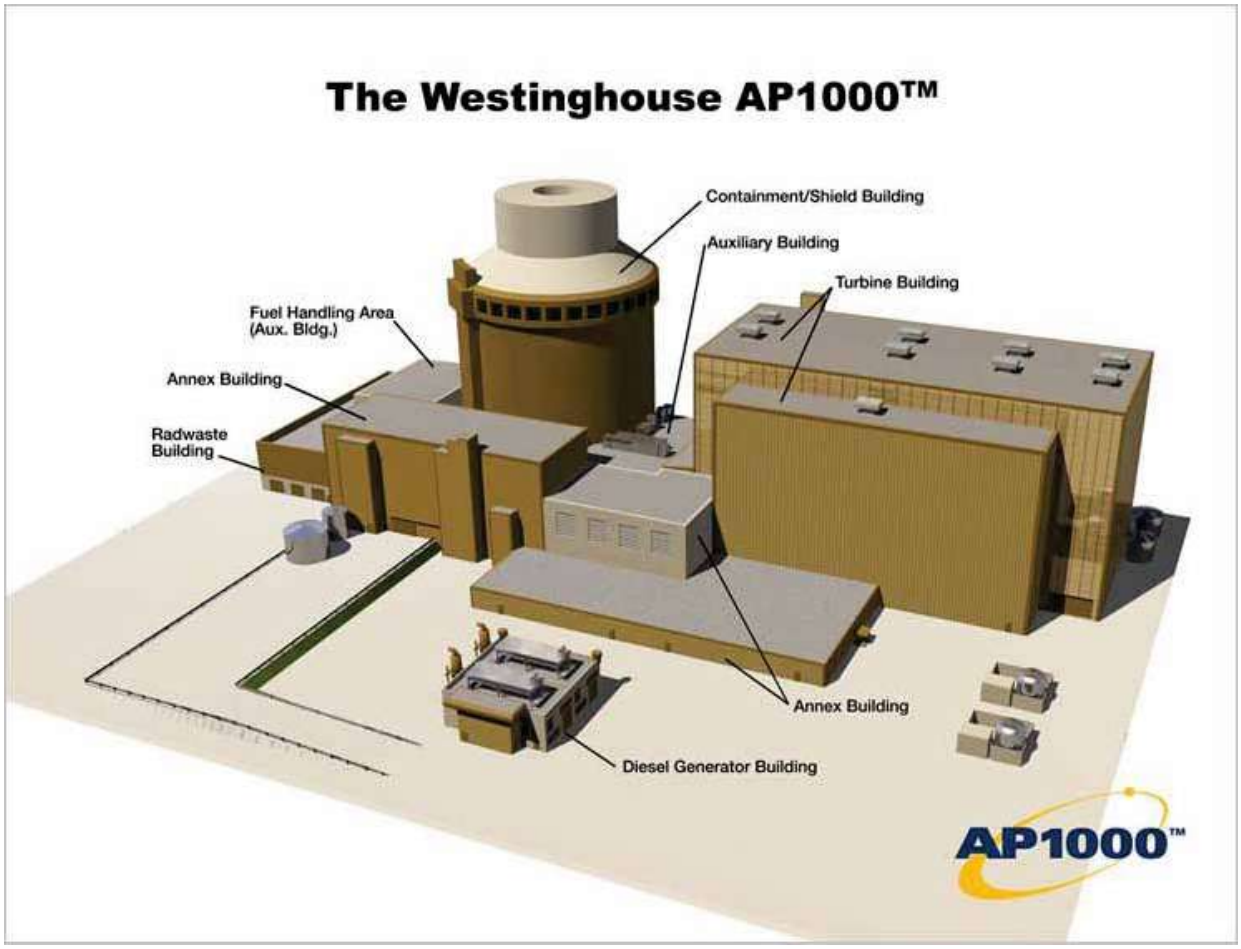


Figure 1-1. General Arrangement of an AP1000 Pressurised Water Reactor

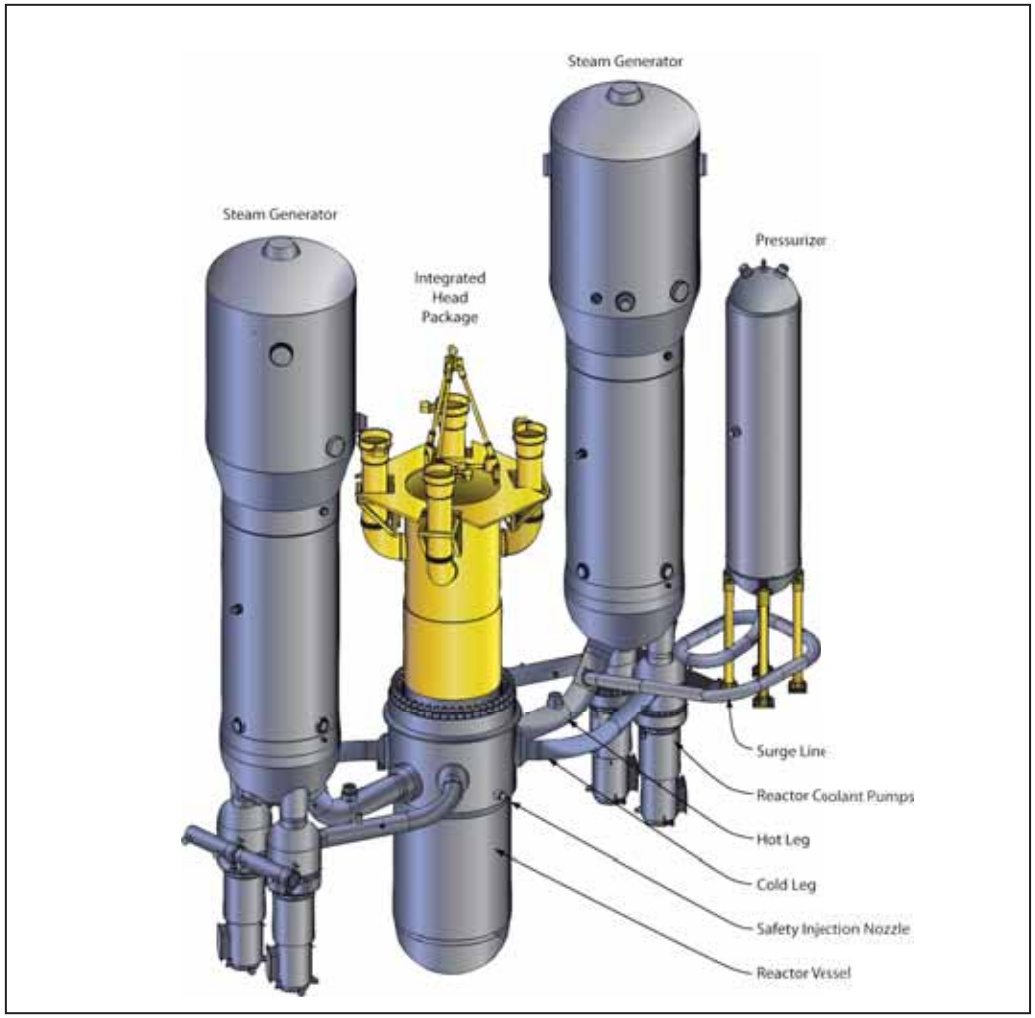


Figure 1-2. AP1000 Design Primary Circuit Components

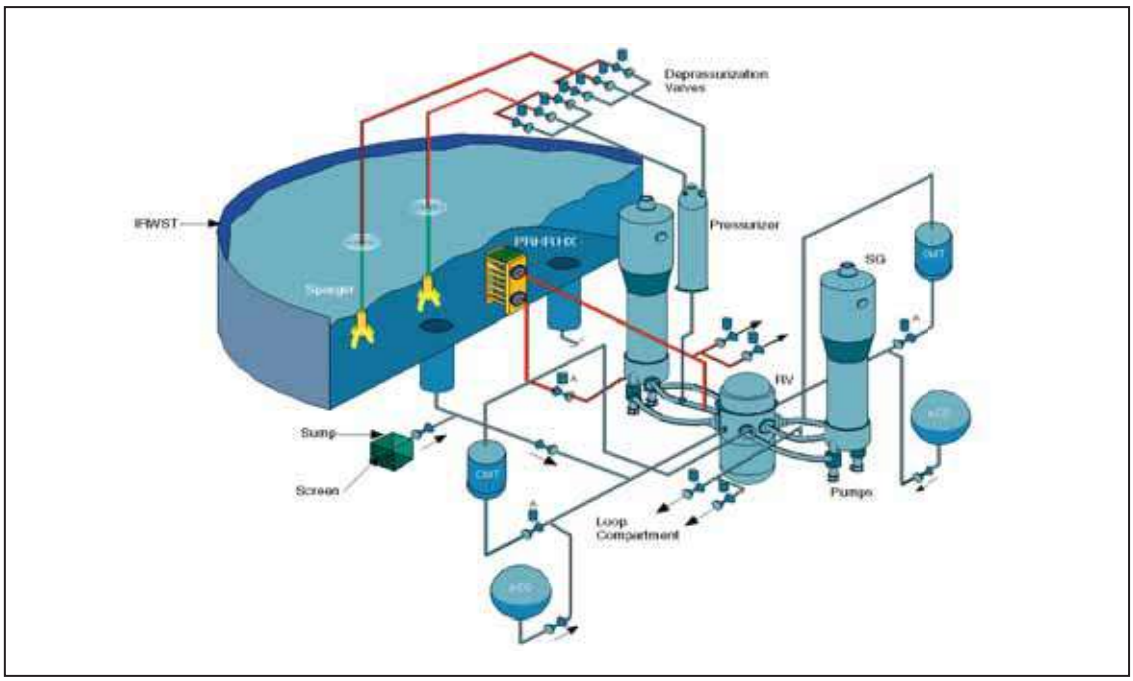


Figure 1-3. AP1000 Passive Core Cooling System Components

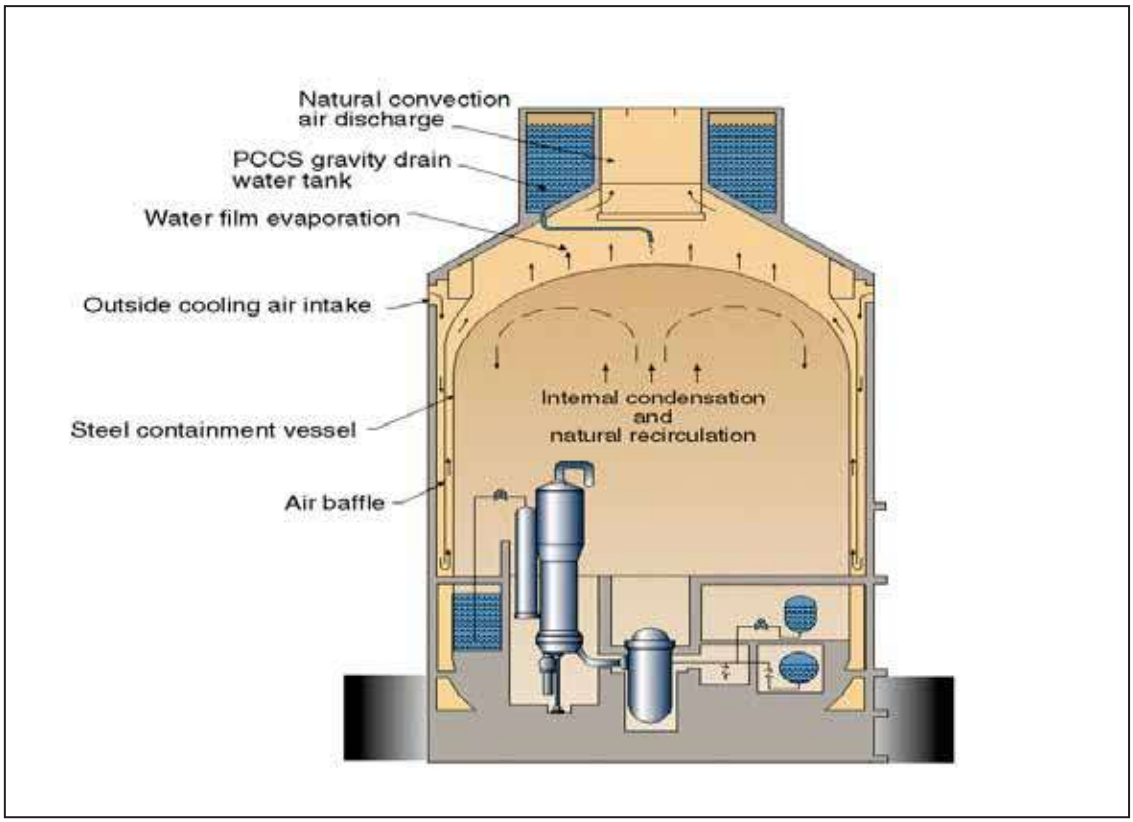


Figure 1-4. AP1000 Passive Containment Cooling System

APPENDIX 1A
TRADEMARKS

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

None.

LIST OF ABBREVIATIONS AND ACRONYMS

ALARP	as low as reasonably practicable
BSC	Basis of Safety Case
DA	design authority
DAC	Design Acceptance Confirmation
DAS	Diverse Actuation System
DDS	Data Displays and Processing System
DRP	design reference point
EA	Environment Agency
EFQM	European Foundation for Quality Management
GDA	generic design assessment
IAEA	International Atomic Energy Agency
IC	intelligent customer
INR	independent nuclear review
IRR	Ionising Radiations Regulations
IRR99	Ionising Radiations Regulations 1999
ISO	International Organisation for Standardisation
ONR	Office for Nuclear Regulation
PCSR	Pre-Construction Safety Report
PLS	Plant Control System
PMS	Protection and Safety Monitoring System
PQP	Project Quality Plan
PSA	probabilistic safety assessment
PWR	pressurised water reactor
QA	quality assurance
QMS	quality management system
RQ	Regulatory Query
SAP	safety assessment principle
SFAIRP	so far as is reasonably practicable
SLC	site licence condition
SMA	safety management arrangements
SoDA	Statement of Design Acceptability
SSC	system, structure, or component
UK	United Kingdom

2 SAFETY CASE

2.1 INTRODUCTION

This chapter gives an overview of the safety case presented in this Pre-Construction Safety Report (PCSR) for the AP1000 design within the context of the United Kingdom (UK) regulatory regime in general and the generic design assessment (GDA) process in particular.

2.2 UNITED KINGDOM REGULATORY REGIME

The UK nuclear regulatory regime is described in Chapter 1 whereby the onus is on the licensee to demonstrate that the design, construction, commissioning and operation of the plant is safe and that the risk to the public, workforce and the environment is as low as reasonably practicable (ALARP). The Office for Nuclear Regulation (ONR) safety assessment principles (SAPs) (Reference 2.1) are used to assess applications from licensees.

2.3 GENERIC DESIGN ASSESSMENT PROCESS

The GDA provides a coordinated approach by the safety, security, and environmental regulators for the pre-licensing/preauthorisation phase. The complete licensing process has been split into the following two phases:

- **Phase 1: GDA** – The assessment of the safety case for a generic design, leading to the issue of a Design Acceptance Confirmation (DAC) and an Environment Agency (EA) Statement of Design Acceptability (SoDA) if the outcome is positive. Phase 1 has four steps, which are explained in detail in Section 1.1.

- **Phase 2: Nuclear site licensing** – The assessment of the application for a nuclear site licence, which is site, reactor design, and operator specific.

This PCSR and its supporting documentation constitute Westinghouse's submission under GDA Closeout and the basis for the development of the site-specific safety cases that will be presented in Phase 2 of the licensing process. The safety case is currently owned by Westinghouse, the requesting party for GDA. A key feature is that once the DAC and the SoDA are received, the operating organisations that become the licensees will own the safety case and will be responsible for any changes and future reviews of that design, and Westinghouse will transition to the role of responsible designer and continue to support the licensee.

The safety case presented in this PCSR for submission under GDA Closeout is for a generic site which is described in Chapter 4. It is based on the design reference point (DRP) (Reference 2.4), which is described in Chapter 6. The DRP lists the design documentation that specifies the AP1000 plant's detailed design that forms the basis of this PCSR.

2.4 AP1000 DESIGN SAFETY CASE OVERVIEW

2.4.1 AP1000 Design Safety Case

This section provides an overview of the scope and purpose of the safety case and how the safety case is developed throughout the life of the AP1000 plant. Throughout the various phases of the AP1000 project, the safety case will be reviewed and revised and will consider at each stage the relevant safety, engineering, and management information. It is understood that the regulatory bodies, the ONR or the EA, may specify regulatory "hold points" beyond

which the licensee may not proceed without regulatory agreement or consent. Westinghouse would expect that the safety case at each stage will demonstrate the safety of the design prior to the conclusion of the phase. The expected phases of the AP1000 project and the purpose of the associated safety reports are provided below, starting with this PCSR.

2.4.1.1 Pre-Construction Safety Report

According to the Plant Life Cycle Safety Report (Reference 2.5), the purpose of this PCSR is to do the following:

- Demonstrate prior to non-active construction that the detailed design proposal will meet regulatory dose-frequency targets and that risks are as low as reasonably practicable.
- Specify generic safety functions and design requirements for all structures, systems and components important for safety and provide evidence to substantiate the design.
- Demonstrate that the plant can be built to an appropriate quality and that it can be operated safely and within safe operating limits throughout life, including decommissioning.

2.4.1.2 Site-Specific Pre-Construction Safety Report

The main purpose of the site-specific PCSR is similar to that of this PCSR, but it is also to address any site-specific issues that were not specifically covered by this PCSR. The site-specific PCSR will be required by the potential licensee as part of the licensing phase of the project.

2.4.1.3 Pre-Commissioning Safety Report

This may be split into two separate phases of inactive and active commissioning. The purpose of the pre-inactive commissioning phase is to do the following:

- Demonstrate that the plant as built will meet the safety criteria and standards set in the PCSR and show that it can be operated safely.
- Define the extent of the inactive commissioning and that it will demonstrate the proper functioning of safety systems, procedures, and equipment via safety commissioning schedules.
- Justify the safety of nonactive commissioning operations.

The pre-active commissioning phase will do the following:

- Sentence any shortfalls revealed during inactive commissioning.
- Demonstrate that the inactive commissioned plant continues to meet relevant safety criteria and is capable of safe operation.
- Demonstrate that the active commissioning activities can and will be carried out safely and that the operating procedures for commissioning are supported by the safety case.
- Enable the production of a programme of safety commissioning activities that will demonstrate the proper functioning of systems, procedures, and equipment.
- Demonstrate that all identified aspects of safety have been demonstrated prior to active commissioning.
- Identify limits and conditions necessary in the interest of safety.
- Demonstrate compliance with the legal duty to reduce risks to workers and the public (so far as is reasonably practicable (SFAIRP).

2.4.1.4 Pre-Operational Safety Report

The main purpose of the pre-operational safety report is to do the following:

- Demonstrate that the plant (as built and commissioned) meets the safety standards and criteria set down in the PCSR.
- Demonstrate that detailed analysis has been undertaken to provide support of the safety case.
- Demonstrate that all necessary pre-operational actions have been completed, validated, and implemented.
- Identify limits and conditions necessary in the interest of safety.
- Demonstrate compliance with the legal duty to reduce risks to workers and the public SFAIRP.

2.4.1.5 Plant Operational Safety Report

The main purpose of the plant operational safety report is to do the following:

- Demonstrate operation of the plant meets the safety standards and criteria set down in the PCSR.
- Demonstrate compliance with the legal duty to reduce risks to workers and the public SFAIRP.
- Take account of experience to review and changes that have been necessary, and that the safety case is still valid.

- Review the safety adequacy of the plant in light of its current and projected conditions and against modern safety standards and expectations.

- Take a strategic look forward to consider facility lifetime and contingency requirements.

As part of the transfer of information from Westinghouse to the licensees, any assumptions made in the safety case documentation will be highlighted. These aspects will form part of the training of licensee personnel. The aim of the knowledge transfer process is to ensure that potential licensees have the capability to secure and maintain safety of the facility and that, where necessary, the licensee has the means to perform as an intelligent customer (IC). The knowledge transfer process is described in detail in Chapter 7 of this PCSR.

Arrangements for future safety case production, approval, independent nuclear safety assessment, and periodic review will be part of the licensee's own arrangements.

2.4.2 Development of the AP1000 Design Pre-Construction Safety Report

This PCSR is one of the lead documents in the submission to the ONR and the EA for DAC. It provides the overall safety case for AP1000 design, construction, and operation.

For the AP1000 design, the intent is that its lifetime should consist of design, construction, commissioning, and 60 years of operations followed by decommissioning and long-term storage of spent fuel. Ageing considerations are presented in Chapter 7.

The safety case developed in this PCSR has a number of elements to demonstrate that the AP1000 design as constructed and operated meets statutory dose limits in normal operation, that it meets specified dose targets in design basis fault conditions, and that the risks to workers, the public, and the environment are ALARP in all normal operational and fault conditions and throughout plant life.

Volume 1: Safety is managed throughout the plant life cycle.

Chapter 1 is the overall introduction to the PCSR, and Chapter 2 (this chapter) gives an overview of the safety case. Chapter 3 lays out the principles and processes underlying the management of safety. These principles and processes ensure that safety important information is passed on from the design stage, through construction and commissioning to power operation and ultimately to decommissioning. The principles and processes also describe Westinghouse's expectations of the licensees' systems that will be in place during operation to ensure continuity from the design process throughout the life cycle of the plant.

The safety management process described ensures that design, construction, commissioning, operation, and decommissioning fully meet UK licensing standards and best practices, specifically that the levels of safety exceed those of most currently operating nuclear plants, and that the public, worker and environmental risks associated with all phases of the plant's life cycle are ALARP.

The safety case described in this PCSR is based on a generic site, which is described in Chapter 4. The information presented there will form the starting point for the development of site-specific PCSRs required for site licensing in the future.

Volume 2: Safety is achieved through simple, passive design and defence in depth.

The basic engineering principles that underlie the design process are described in Chapter 5 with the major systems, structures, and components (SSCs) that make up the AP1000 design described in Chapter 6. The significant difference between the AP1000 design and other existing pressurised water reactors (PWRs) is in the use of Class 1 passive safety systems; that is, safety systems that rely solely on natural phenomena such as gravity, natural convection cooling, or the energy stored in pressurised gases. The AP1000 design passive systems are also significantly simpler than the active protection systems in conventional PWRs.

The implementation of passive safety features and simplification of the design significantly contribute to the improved safety and reliability compared with existing plants.

Design simplification also contributes to the reliability, extended design life of the plant, and reduced decommissioning efforts. Chapter 7 describes the engineering processes that are in place to maintain high levels of reliability throughout the plant's life and to protect against the effects of ageing.

Volume 3: Design and operation are tolerant to faults and risks are ALARP.

During the development of the AP1000 design, design choices have been made that reduce fault frequencies, thereby removing some faults common to existing plants altogether. The fault analysis presented in this volume shows that the passive design of the protection systems significantly improves the response of the plant to faults with the risks to the public, workforce and environment being considerably reduced over those associated with existing plants.

Chapter 8 describes the methodology used in the identification and assessment of faults, as well as provides a list of all the faults identified and the grouping used to analyse them. Chapter 9 provides the design basis assessment, and Chapter 10 provides the probabilistic assessment that allows the design to be compared with UK dose and risk targets. Chapters 11 and 12, respectively, provide the corresponding analysis of internal and external hazards. Human factors and the tolerance of the plant to human errors are presented in Chapter 13.

The analysis presented in Volume 3 leads to the identification of safety functions that are required to maintain safety in all of the identified life cycle phases and operating conditions, and the SSCs of the design that provide them.

Chapter 14 consolidates the results of the previous chapters to demonstrate that design targets are met with considerable margin. Chapter 14 also demonstrates that, throughout the development of the AP1000 design, the designers have systematically sought means of further reducing risk. The designers have also used available tools such as the probabilistic safety assessment (PSA) and severe accident assessment to identify risk-reduction measures. Many design decisions and design changes have been implemented as a result, which contribute to the overall risk being ALARP.

Volume 4: Engineering solutions are fully substantiated. The SSCs of the design are fully able to satisfy the claims made on them and are able to provide the safety functions identified in the fault analysis.

Chapter 15 lists the sources of claims on SSCs in the safety case and the requirements on SSC performance that are implied by them. The evidence that the SSCs fulfil these requirements is presented in Chapters 16 to 23 of this PCSR.

Volume 5: Radiological releases are minimised in normal and abnormal operating conditions.

Chapter 24 demonstrates that simplifications in the design mean that operator doses during normal operations and during fault conditions are significantly reduced over those from existing PWRs. Chapter 25 Describes general arrangements, facilities and equipment to assist the management of emergencies currently included in the design basis for the AP1000. Chapter 26 demonstrates that operator doses and routine releases to the environment from radioactive waste management on the site are minimised, and Chapter 27 shows that decommissioning activities are expected to produce less activated or contaminated material than for existing plants.

Volume 6: Conclusions.

Chapter 28 is the only chapter in this volume. It draws together the overall conclusions from the previous chapters and makes general conclusions relating to regulatory targets and risk that is ALARP.

2.4.3 Compliance with Dose and Frequency Targets

The ONR SAPs have a number of dose and frequency targets for normal operation, including legal limits, and for accident conditions. The targets are addressed in this PCSR as follows:

Target 1	Doses and legal limits for normal operation – any person on the site	Chapter 24
Target 2	Doses for normal operation – any group on the site	Chapter 24
Target 3	Doses and legal limits for normal operation – any person off the site	Chapter 24
Target 4	Frequency dose targets for design basis sequences – any person	Chapters 9 and 14
Target 5	Individual risk of death – any person on the site	Chapters 10 and 14
Target 6	Frequency dose targets for any single accident – any person on the site	Chapter 14
Target 7	Individual risk of death – any person off the site	Chapters 10 and 14
Target 8	Frequency dose targets for any single accident – any person off the site	Chapters 10 and 14
Target 9	Total risk of 100 or more fatalities	Chapters 10 and 14

2.5 AP1000 DESIGN GENERIC DESIGN ASSESSMENT DOCUMENTATION

The safety submission provided for the GDA process consists of this PCSR and a number of supporting documents. Supporting documents are included in the reference section for each PCSR Chapter. The principal supporting documents are summarised in this section.

2.5.1 Topic Reports

- Internal Hazards

  The following Internal Hazards Topic Reports support Chapter 11:

  - Flooding Topic Report, UKP-GW-GLR-107 (Reference 2.21), presents the safety case in determining the effects to SSCs resulting from a flood within the AP1000 plant.
  - Dropped Loads Topic Report, UKP-GW-GLR-110 (Reference 2.22), presents the safety case in determing the effects to SSCs resulting from a dropped load.
  - Fire Protection Topic Report, UKP-GW-GLR-111 (Reference 2.23), presents the safety case in determining the effects to SSCs resulting from a fire within the AP1000 plant.
  - Internal Missiles Topic Report, UKP-GW-GLR-108 (Reference 2.24), presents the safety case in determining the effects to SSCs resulting from an internally generated missile within the AP1000 plant.
  - Pressure Part Failure Topic Report, UKP-GW-GLR-114 (Reference 2.25), presents the safety case in determining the effects to SSCs resulting from the failure of pressure-retaining fluid systems within the AP1000 plant.
  - Explosions Topic Report, UKP-GW-GLR-109 (Reference 2.26), presents the safety case in determining the effects to SSCs resulting from an explosion within the AP1000 plant.
  - Combined Hazards Topic Report, UKP-GW-GLR-036 (Reference 2.27), presents the safety case in determining the effects to SSCs resulting from combined hazards.

2.5.2 Basis of Safety Case Documents

- Control and Instrumentation

The following Basis of Safety Case (BSC) documents support Chapter 19:

- Plant Control System (PLS) BSC, UKP-PLS-GLR-001 (Reference 2.28)
- Data Display and Processing System (DDS) BSC, UKP-DDS-GLR-001 (Reference 2.29)
- Diverse Actuation System (DAS) BSC, UKP-DAS-GLR-001 (Reference 2.30)
- Protection and Safety Monitoring System (PMS) BSC, UKP-PMS-GLR-001 (Reference 2.31)

- BEACON Core Monitoring System BSC, UKP-GW-GL-162 (Reference 2.32)

- Electrical

  - Electrical BSC, UKP-GW-GL-163 (Reference 2.33), supports Chapter 18.

2.5.3 Other Supporting Documents for United Kingdom Safety Case

- AP1000 Design Reference Point for UK GDA

  UKP-GW-GL-060 (Reference 2.4) specifies the documents that define the DRP to which this safety case applies. The DRP is dated 31st March 2016, and any design changes subsequent to that date are subject to design change control with respect to this safety case (Section 6.1.1).

- Categorisation and Classification Methodology

  UKP-GW-GL-044 (Reference 2.9) describes the scheme adopted for the AP1000 design in the UK for the categorisation of safety functions and the classification of SSCs. This is summarised in Chapter 5.

- Classification of SSCs

  Appendix 15A lists the safety classification for each SSC claimed in the safety case, together with an outline of its functional and reliability requirements and applicable design codes and standards.

- Equivalence/Maturity Study of US Codes and Standards

  UKP-GW-GL-045 (Reference 2.11) provides evidence for the suitability of the codes and standards used in the AP1000 design as compared to current European codes and standards.

- Human Factors

  The Human Factors Qualitative Error Analysis Report (Reference 2.7) provides evidence for the substantiation of the AP1000 plant human factors safety case and demonstrates an appropriate human error analysis process.

- Limits and Conditions

  The Limits and Condition Process Description (Reference 2.35) describes the operating rules, the methodology for development, and the process for transition into the operating phase.

  The Generic Technical Specifications (Reference 2.36) are a dynamic set of plant parameters, associated limits and conditions for plant operation, and associated SSCs, including high integrity items, that provide the delivery of important safety functions for the AP1000 plant.

- Plant Life Cycle Safety Report

The Plant Life Cycle Safety Report (Reference 2.5) describes the safety programmes to support plant owners throughout the design, construction, and operation of the AP1000 reactor. Chapter 7 discusses the plant life cycle.

- Environment Report

  The Environment Report (Reference 2.13) consolidates and summarises the environmental information to demonstrate that the AP1000 design meets the environmental requirements of the GDA process. Chapter 4 discusses the environmental aspects of the safety case.

- Structural Integrity Classification

  The Structural Integrity Classification Report (Reference 2.20) describes the process used to determine the structural integrity classification of the AP1000 plants components which was used in the development of the safety case presented in Chapter 20.

- ALARP

  APP-GW-GER-005 (Reference 2.17) is the main supporting document that demonstrates the derivation of the low-risk AP1000 design. This is discussed in detail in Appendix 6A.

In addition to the documents listed above, there are a number of other documents produced in support of the Environment Report, which are listed in the AP1000 DRP document together with a further list of detailed design documents (Reference 2.4).

2.6 WESTINGHOUSE QUALITY MANAGEMENT SYSTEM

To control the process for submission of the PCSR, Westinghouse operates a Quality Management System (QMS) that assures, maintains, and improves all areas of critical support operations such as safety, health, environmental, quality, technical, operational, and commercial, combining all functional requirements into one corporate framework. It extends from high-level policy documentation and regulatory compliance processes to detailed guidance documents and others, incorporating detailed work instructions and taking full cognisance of recognised standards throughout all corporate disciplines.

The QMS is based on the model devised by the European Foundation for Quality Management (EFQM) Excellence Model, certified to International Organisation for Standardisation (ISO) 9001:2008, and designed to work in tandem with specific external required processes, which include but are not limited to the following:

- ISO 9001:2008 Quality Management Systems – Requirements
- ISO 10006 Guidelines for Quality Management
- ISO 19011 Guidelines for Quality and Environmental Management Systems Auditing
- ISO 90003 Software Engineering Quality Management Standard
- GQAS General Quality Assurance Specifications
- BS OHSAS 18001 Occupational Health and Safety

- BS 7000 series Design Management Systems
- ANSI/ASME NQA-1 Quality Assurance Requirements for Nuclear Facilities
- IAEA GS-R-3 The Management System for Facilities and Activities
- IAEA GS-G-3.1 Safety Guide
- IAEA SF-1 Fundamental Safety Principles

The Westinghouse QMS provides an approach that is consistent with the ONR SAPs (Reference 2.1), the Ionising Radiations Regulations (IRRs) (Reference 2.18), and the site licence condition (SLC) requirements through a documented assessment programme. The following SLCs are considered:

- SLC 6 Documents, Records, Authorities and Certificates
- SLC 12 Duly Authorised and Other Suitably Qualified and Experienced Persons
- SLC 14 Safety Documentation
- SLC 15 Periodic Review
- SLC 17 Management Systems
- SLC 19 Construction or Installation of New Plant
- SLC 20 Modification to Design of Plant Under Construction
- SLC 23 Operating Rules
- SLC 36 Organisational Capability

The role of the QMS is not only to ensure full control of the contents the PCSR and the process of its submission to governing bodies, but also to ensure that the highest levels of communication, innovation, performance management, and teamwork are being comprehensively delivered. Among the benefits of the QMS are the increased confidence that requirements will be met, greater assurance that processes are under control, and evidence that a culture of continuous improvement is in place. These assurances are reached by following robust procedures. Those procedures that are relevant to the PCSR are included in Table 2-1.

2.6.1 Control of the Development of the Safety Case

In respect of any operation that may affect nuclear safety, it is a requirement to make and implement adequate arrangements for the production and assessment of all documentation relating to the safety case. This safety case justifies and documents safety at all phases of the life cycle including design, manufacture, construction, commissioning, operation and decommissioning.

The safety case comprises the complete safety justification for the operation within the scope of this case. This safety case is considered to be the totality of claims, arguments, and evidence that substantiates the safety of the plant, activity, operation, or modification in question.

Prior to commencement of safety case development, a Project Quality Plan (PQP) (Reference 2.14) was produced. This detailed the scope, boundary, and interfaces of the PCSR and how it is intended to produce and manage the safety case.

The PQP and supporting procedures held within the QMS ensure that the proposed design can meet regulatory safety requirements and that the safety case is supported with all the

documentary evidence that is needed to be able to construct, maintain, and operate the plant in accordance with the intent assumed in the safety case. The nuclear site licence holder will ensure the safety of all facilities and activities on the site. The interface between Westinghouse and the utilities is described in more detail in Chapter 3.

This PCSR provides a baseline for configuration management against which all future phases of the plant life cycle can be measured; suitable audit trails are maintained throughout all phases of the life cycle (see Chapter 7 for more detail on the plant life cycle). The Westinghouse QMS provides an approach that is consistent with the ONR SAPs, SLCs, International Atomic Energy Agency (IAEA) GS-R-3 (Reference 2.19), and Ionising Radiations Regulations 1999 (IRR99) (Reference 2.18) requirements through a robust and documented assessment programme. During the GDA process, if there is a requirement to update safety case documentation that can impact the site-specific PCSR, then where there are potential licensees, they will be invited to be part of that review process. In moving to an operational regime, the safety case will be owned by the licensee, and an operational safety case will be required.

Safety documentation is classified according to safety significance and is to be subject to the prescribed due process for UK licensing, including independent nuclear review (INR). Once approved, no alteration or amendment must be made to the safety case unless the verification process has approved such alteration or amendment.

The safety case provides deterministic safety arguments and design substantiations against the range of hazards identified. These are supported by appropriate ALARP justifications. In particular, the Westinghouse QMS gives assurance that the safety case does the following:

- Demonstrates that there is a benefit from affecting the operation or operating the plant that outweighs the risks arising from the activity.
- Confirms that all relevant standards have been met and that risks have been reduced to levels that are ALARP.
- Presents the bases and assumptions used in estimating risks and ensures that they are defined and maintained during the plant life cycle, including emergency arrangements.
- Demonstrates that suitable safety management arrangements (SMAs) are in place or are credibly planned to affect the various activities required during the plant life cycle.

The safety case demonstrates that the AP1000 plant can be operated such that the risks to the operators, site workers, public, and environment are ALARP.

All stages of the development of the safety case consider interactions with interfacing safety justifications and other stakeholder systems if deemed necessary, e.g., transport, fire and conventional hazards. The flow of information across all identified boundaries is managed throughout the plant life cycle (see Chapter 3).

The complete safety case is presented to and accepted by the ONR prior to implementation; and, once produced the adequate arrangements are to be put in place by the licensee for its periodic and systematic review and reassessment.

2.6.2 Control of the Quality of the Pre-Construction Safety Report Production

A safety case is mandatory for all operations required to be performed throughout the plant life cycle. The development of a safe design is an iterative process involving complex

interactions between safety, design, and safety case documentation (see Section 2.6.1). It is imperative that the scope of the safety case is clearly defined at the commencement of any project. This requires definition of the physical (e.g., system/equipment) boundaries of the safety case, organisational boundaries, and the provenance and appropriateness of information that crosses such boundaries.

The function of the safety case is to demonstrate that the plant can be operated safely throughout the plant life cycle. Additionally, it must balance the functional requirement of the design with the requirement to deliver the function safely. The safety case must recognise that the optimum design may be a balance between nuclear safety and other constraints, such as conventional health and safety or environmental issues. This applies whether considering new designs, modifications to existing or as yet unbuilt designs, or on modifications to extant plant.

Due to the size and complexity of PCSR production, detailed planning was considered at the start of the production process to facilitate the presentation of the safety case in a clear, well-structured, and logical manner.

Implicit in the production of the PCSR is a requirement that Westinghouse, as the design authority (DA), has the responsibility for, and the requisite knowledge to support maintenance of the design integrity and the overall basis for safety of its nuclear facilities over its entire life cycle, from design to decommissioning. The DA also has responsibility to maintain the design intent of the AP1000 plant throughout its life cycle. At a suitable point, the DA role will be handed over to the licensee, and Westinghouse will become the responsible designer while continuing to support the licensee.

Robust documented procedures contained within the Westinghouse QMS (Chapter 3) detail those requirements that enable the ONR to gain adequate confidence that the AP1000 design is being designed, procured, constructed, and commissioned to meet the design intent, including the fuel and the neutron sources, and thus operate safely. These procedures do the following:

- Comply with the fundamentals of nuclear safety to be applied to safety cases, derived with due cognisance to the IAEA guidance.
- Ensure that the resulting designs are acceptable when judged against the SAPs and complementary safety case methodologies that assist authors and technical leads in the production of safety cases to the required standards. They also ensure that the resulting safety cases present the key elements normally expected in any safety case and facilitate the production of a case compliant with relevant principles.
- Provide prescription and guidance on the purpose, content, and structure of a safety case including the PCSR, and describe each of the reports that may be employed to present the AP1000 design safety case throughout the design and build project stage.
- Mandate the classification of all documentation comprising the safety case (including the PCSR) and prescribe the AP1000 design approval route.

2.6.3 Control of the Quality of Safety Case Documentation

The Westinghouse QMS contains arrangements specifying particular skills and experience required of individuals to deliver key roles in the organisation and the project delivery framework. Management is responsible for determining the necessary personnel competencies in terms of skill, education, and experience requirements for the activities affecting quality, and the supply chain is carefully monitored through a rigorous audit procedure to ensure competence levels are met, maintained, and exceeded.

Documented arrangements, along with a full suite of training and competency records, are held within the QMS to give assurance and confidence to the ONR that the safety case is of the required quality. These complement the records that will be kept by the licensee later in the process to ensure the suitability of staff who construct, commission, operate, examine, maintain, inspect, test, and modify the SSCs that make up the plant.

Fundamental to complying with SLC 12 is the ability to demonstrate to the ONR that Westinghouse has suitable and sufficient SMAs in place to ensure that only suitably qualified and experienced persons conduct functions that may have an effect on nuclear or radiological safety during the production of the PCSR.

Compliance with SLC 12 ensures that the licensee applies quality assurance to all activities associated with the design, construction, manufacture, commissioning, operation, and decommissioning of the installations on the site, including the preparation and review of safety documentation. The licensee's arrangements are expected to include the provision of a quality assurance (QA) function to oversee the specification, audit and review of QA arrangements.

2.7 REFERENCES

2.1 "Safety Assessment Principles for Nuclear Facilities," Rev. 0, Office for Nuclear Regulation, 2014.

2.2 Not Used.

2.3 Not Used.

2.4 Westinghouse Report UKP-GW-GL-060, Rev. 10, "AP1000 Design Reference Point for UK GDA," January 2017.

2.5 Westinghouse Report UKP-GW-GL-737, Rev. 2, "Plant Life Cycle Safety Report," March 2011.

2.6 Not Used.

2.7 Westinghouse Report UKP-GW-GL-126, Rev. 0, "United Kingdom AP1000 Human Factors Qualitative Error Analysis," June 2016.

2.8 Not Used.

2.9 Westinghouse Report UKP-GW-GL-044, Rev. 1, "AP1000 UK Safety Categorisation and Classification Methodology," April 2010.

2.10 Not Used.

2.11 Westinghouse Report UKP-GW-GL-045, Rev. 2, "AP1000 Equivalence/Maturity Study of the U.S. Codes and Standards," September 2011.

2.12 Not Used.

2.13 Westinghouse Report UKP-GW-GL-790, Rev. 6, "UK AP1000 Environment Report," January 2017.

2.14 Westinghouse Report UKP-GW-GAH-001, Rev. 6, "Project Quality Plan for the UK AP1000 Generic Design Assessment (GDA) Issue Resolution," October 2016.

2.15 Not Used.

2.16 Not Used.

2.17 Westinghouse Report APP-GW-GER-005, Rev. 1, "Safe and Simple: the Genesis and Process of the AP1000 Design," August 2008.

2.18 UK Statutory Instrument No. 3232, "Ionising Radiations Regulations," 1999.

2.19 IAEA GS-R-3, "The Management System for Facilities and Activities," International Atomic Energy Agency, 2006.

2.20 Westinghouse Report UKP-GW-GLR-004, Rev. 3, "AP1000 UK Structural Integrity Classification," January 2017.

2.21 Westinghouse Report UKP-GW-GLR-107, Rev. 1, "UK AP1000 Internal Hazards – Flooding Topic Report," January 2017.

2.22 Westinghouse Report UKP-GW-GLR-110, Rev. 1, "UK AP1000 Internal Hazards Topic Report – Dropped Loads," January 2017.

2.23 Westinghouse Report UKP-GW-GLR-111, Rev. 1, "UK AP1000 Internal Hazards Topic Report – Fire Protection," January 2017.

2.24 Westinghouse Report UKP-GW-GLR-108, Rev. 1, "UK AP1000 Internal Hazards Topic Report – Internal Missiles," January 2017.

2.25 Westinghouse Report UKP-GW-GLR-114, Rev. 1, "UK AP1000 Internal Hazards Topic Report – Pressure Part Failure," January 2017.

2.26 Westinghouse Report UKP-GW-GLR-109, Rev. 1, "UK AP1000 Internal Hazards Topic Report – Explosions," January 2017.

2.27 Westinghouse Report UKP-GW-GLR-036, Rev. 0, "UK AP1000 Internal Hazards Topic Report – Combined Hazards," August 2016.

2.28 Westinghouse Report UKP-PLS-GLR-001, Rev. 1, "United Kingdom AP1000 Plant Control System (PLS) Basis of Safety Case," December 2016.

2.29 Westinghouse Report UKP-DDS-GLR-001, Rev. 1, "United Kingdom AP1000 Data Display and Processing System (DDS) Basis of Safety Case," December 2016.

2.30 Westinghouse Report UKP-DAS-GLR-001, Rev. 2, "Basis of Safety Case for the Diverse Actuation System," December 2016.

2.31 Westinghouse Report UKP-PMS-GLR-001, Rev. 2, "United Kingdom AP1000 Protection and Safety Monitoring System Safety Case Basis," December 2016.

2.32 Westinghouse Report UKP-GW-GL-162, Rev. 1, "UK AP1000 BEACON Core Monitoring System Basis of Safety Case," October 2016.

2.33 Westinghouse Report UKP-GW-GL-163, Rev. 2, "United Kingdom AP1000 Electrical Basis of Safety Case," December 2016.

2.34 Not Used.

2.35 Westinghouse Report UKP-GW-GL-500, Rev. 0, "AP1000 UK Limits and Condition Process Description," December 2015.

2.36 Westinghouse Report UKP-GW-GL-501, Rev. 0, "AP1000 UK Generic Technical Specifications," January 2016.

Table 2-1. PCSR Level 2 and Level 3 Procedures

W2-1.3-100	Management System and Procedure Management Process
W2-1.3-102	Quality Manuals, Quality Plans and Interface Agreements
W2-2.5-100	Competence, Awareness, and Training
QA-2.8	Qualification of Audit Personnel
W2-6.1-100	Document Control
W2-5.1-100	Westinghouse Corrective Action Program
W2-5.1-107	Corrective Action Review Board
W2-6.2-100	Quality Assurance Records
W2-4.2-101	Internal Quality Assurance Audits
W2-5.1-301	Self-Assessments
UKP-GW-GAH-001	Project Quality Plan for the UK Generic Design Assessment (GDA) Issue Resolution
UKP-GW-GAP-011	Preparation of UK Licensing Documentation – Regulatory Submission
UKP-GW-GAP-012	The Receipt and Processing of Regulatory Queries (RQs) from the UK Regulators
UKP-GW-GAP-013	The Processing of Outgoing Correspondence to the UK Joint Programme Office
UKP-GW-GAP-014	The Receipt and Processing of Incoming Correspondence from the UK Joint Programme Office
UKP-GW-GAP-016	The Procedure for the Creation, Handling and Processing of Protectively Marked Documents
UKP-GW-GAP-027	Pre-Construction Safety Report (PCSR) Approval Process
APP-GW-GAP-425	Preparation and Control of AP1000 Calculation and System Specification Supplements
APP-GW-GAP-102	AP1000 Document Management Process Work Instructions

TABLE OF CONTENTS

LIST OF TABLES

None.

LIST OF FIGURES

None.

LIST OF ABBREVIATIONS AND ACRONYMS

ALARP	as low as reasonably practicable
DA	design authority
DAC	Design Acceptance Confirmation
D-RAP	Design Reliability Assurance Programme
DRP	design reference point
EA	Environment Agency
EHS-MS	Environmental, Health, and Safety Management System
FP	fundamental principle
GDA	generic design assessment
IC	intelligent customer
ITP	initial test programme
ONR	Office for Nuclear Regulation
ONR CNS	ONR Civil Nuclear Security
PCmSR	Pre-Commissioning Safety Report
PCSR	Pre-Construction Safety Report
QA	quality assurance
QMS	Quality Management System
RI	regulatory issue
RO	regulatory observation
RQ	regulatory queries
SAP	safety assessment principle
SLC	site licence condition
SQEP	suitably qualified and experienced person
SSC	system, structure, or component
Tech Spec	technical specification
TQ	technical query
UK	United Kingdom
WGMS	Westinghouse Global Management System

3 MANAGEMENT OF SAFETY

3.1 INTRODUCTION

Safety is paramount within the Westinghouse management system, overriding all other demands. All levels of Westinghouse management and workforce are focused on achieving a high level of safety and ensuring Westinghouse remains a high-reliability organisation. This is facilitated through the Westinghouse Global Management System (WGMS) (Reference 3.47). The main aim of the management system is to achieve and enhance safety by doing the following (Reference 3.2):

- Bringing together in a coherent manner all the requirements for managing the organisation.
- Describing the planned and systematic actions necessary to provide adequate confidence that all these requirements are satisfied.
- Ensuring that health, environmental, security, quality, and economic requirements are not considered separately from safety requirements, to help preclude possible negative impact on safety.

The WGMS ensures that documented quality and safety procedures are in place; that they are followed; and that they are robust, managed, and monitored in accordance with statutory, legal, and regulatory requirements. The AP1000 design has in place a robust safety management framework that meets the requirements of United Kingdom (UK) and international regulations and good practices (References 3.2, 3.3, and 3.4).

During the design phase, the safety case is owned by Westinghouse, the requesting party for Phase 1 of the UK New Build licensing process; i.e., the generic design assessment (GDA) process. During the life cycle of the AP1000 plant, safety responsibilities will transfer from Westinghouse to the site licensee who will have prime responsibility for safety when the plant is operational. Once the Design Acceptance Confirmation (DAC) is received, the operating organisations that become licensees will own the safety cases and will be responsible for any changes and future reviews of that design, albeit with input from Westinghouse where deemed appropriate by both parties. Westinghouse will implement its safety and quality management systems:

- Up to the end of the UK New Build licensing process, phase 2; i.e., Nuclear Site Licensing
- During subsequent plant construction
- During the commissioning phase prior to product acceptance handover to the operating organisation’s licensee

The function of the WGMS is to define the safety and quality management framework, ensure that safety and quality management arrangements are adhered to, and ensure that an effective safety culture is maintained. The WGMS also ensures that Westinghouse safety management arrangements are appropriately transferred and integrated into the safety and quality management systems of the licensee.

The scope of this chapter is to do the following:

- Describe the WGMS structure applied to the AP1000 project, and the safety fundamentals, safety requirements, and safety guides that it addresses.

- Specify the details of the quality assurance programme (Reference 3.5) that Westinghouse will use to meet its stated objectives for providing the necessary technical information and documentation for the Office for Nuclear Regulation (ONR) and Environment Agency (EA) to conduct a complete GDA of the AP1000 design.

3.2 SAFETY MANAGEMENT FRAMEWORK

3.2.1 General Arrangements

Westinghouse operates its WGMS (Reference 3.47) in order to manage, maintain, and continuously improve all areas of safety, including technical, operational, commercial, and management. The quality policy of Westinghouse is:

> *To provide products and services that fully satisfy customer and regulatory requirements.*

Among the benefits of the WGMS are the following:

- Increased confidence that requirements will be met.

- Greater assurance that processes are appropriately managed.

- Motivation to recognise opportunities for improvement, with a high degree of importance being placed upon nuclear safety issues, error reporting, feedback, and lessons learned.

The WGMS comprises high-level policy documentation, procedures, and guidance documents (incorporating detailed work instructions), and takes full account of the required standards in all disciplines. The three QMS levels follow:

- Level 1: QMS, Westinghouse Quality Management System Manual (Reference 3.1); EHS-MS, Environmental, Health, and Safety Management System (Reference 3.48)

- Level 2: Westinghouse and Operational Organisation Policies and Procedures

- Level 3: Function/Department/Plant Procedures and Work Instructions

The Westinghouse QMS is certified to ISO 9001:2008 and is designed to be fully compatible and work in juxtaposition with specific externally required processes, as detailed throughout this chapter. Section 5.4 explains the levels of quality assurance (QA) required in relation to the equipment classification and the associated codes and standards.

Each level of the WGMS is populated with policies and procedures. The arrangements for those are detailed in the Westinghouse Management System Document Administration document (Reference 3.6), which identifies compliance, implementation, processes, and work instructions that have been developed and implemented. These procedures are focused on the following:

- Ensuring safety is considered as the key aspect in all activities
- Ensuring effectiveness and improvement through a process- and risk-based approach
- Ensuring a robust safety culture is embedded
- Conducting projects according to a specific project quality plan
- Delivering a quality product safely

The maintenance and continual improvement of Westinghouse procedures and processes are achieved through a comprehensive audit programme that acts as a catalyst for driving safety improvement and that is operated under Westinghouse procedures for quality assurance audits (Reference 3.7), self-assessments (Reference 3.8), and control of purchased items and services (Reference 3.9). Using suitably qualified and experienced quality auditors (Reference 3.10), the findings from these audits are actioned in accordance with documented procedures for corrective actions (References 3.11 and 3.12). The Westinghouse quality assurance records procedure (Reference 3.13) explains the method by which the creation of, validation of, and changes to Westinghouse documents are managed.

The audit process allows the organisation to discern clearly its strengths and areas in which safety and quality improvements can be made, and culminates in planned improvement actions that are then monitored for progress. A Westinghouse management review (Reference 3.14) assesses how the performance and outcomes compare with processes, procedures, and targets that were set. This assessment then demonstrates the suitability, adequacy, and effectiveness of the WGMS.

The audit process ensures that the most important controls are in place and that the root causes of errors, problems, and areas of weakness are fully addressed and corrected. It also ensures that the potential problems are identified before they become an issue. Emphasis is placed on preventive action and the trending process included in the Westinghouse procedure for the corrective action program (Reference 3.11), root cause analysis (Reference 3.16), and apparent cause analysis (Reference 3.17).

The function of the WGMS within this project is not only to ensure adherence to the requirements of governing bodies and Westinghouse procedures but also to ensure that communication, innovation, performance management, and safety culture are integrated into the safety and quality management systems of the licensee in order to help the licensee produce a robust QMS that maintains and improves upon safety and international good practices.

There are eight fundamental principles (FP.1 through FP.8) within the ONR safety assessment principles (SAPs) (Reference 3.19). Together with SAP MS.1, meeting the expectations of these SAPs is essential for the licensee to produce an acceptable, robust QMS that maintains and improves upon safety and international good practices. These SAPs will be used by the ONR to judge the acceptability of the design during the plant life cycle and therefore must be considered by both Westinghouse during design and construction and the site licensee during plant operation. The SAPs follow:

- FP.1 – Responsibility for Safety
- FP.2 – Leadership and Management for Safety
- FP.3 – Optimisation of Protection
- FP.4 – Safety Assessment
- FP.5 – Limitation of Risks to Individuals
- FP.6 – Prevention of Accidents
- FP.7 – Emergency Preparedness and Response
- FP.8 – Protection of Present and Future Generations
- MS.1 – Leadership

The control of the WGMS is the responsibility of the Westinghouse management, and changes are reviewed and approved by Westinghouse in accordance with management review procedures (Reference 3.14 and Reference 3.6).

Site licensees will be required to demonstrate that similar arrangements are in place for all above aspects of their management system prior to acceptance handover.

3.2.2 Arrangements Specific to the Generic Design Assessment Process

The current quality management system arrangements for the AP1000 GDA project are detailed in the Project Quality Plan for the UK GDA (Reference 3.5). The purpose of the project quality plan is to specify how the quality objectives for the GDA are met. This quality plan also details the QA programme for the GDA and makes reference to UK guidance documents used throughout the GDA, together with Westinghouse Level 2 policies and procedures, and Westinghouse Level 3 procedures specific to the UK GDA.

The Plant Life Cycle Safety Report (Reference 3.20) outlines the safety programmes developed by Westinghouse to support plant owners throughout the design, construction, commissioning, operation, and decommissioning of the AP1000 plant, and sets out the following safety philosophy policy statement:

> *It is the Westinghouse policy to design, produce, market, and distribute our products and services and to conduct our operations in an environmentally sound and socially responsible manner. Westinghouse considers the impact our actions may have on the environment and the health and safety of our employees, subcontractors, customers, and public.*

Section 3.4 discusses the management of safety through the plant life cycle in more detail.

As part of the GDA assessment process, the ONR has raised regulatory queries (RQs), regulatory issues (RIs), regulatory observations (ROs), and technical queries (TQs). These have been processed, and responded to in accordance with Westinghouse procedures (References 3.24, 3.25, and 3.49).

3.3 ARRANGEMENTS FOR THE INTERFACE WITH UTILITIES

3.3.1 Key Roles in the Project Life Cycle

The nuclear site licence holder (Reference 3.26) ensures the safety of all facilities and activities on the site, in part, by assuming the responsibility of the intelligent customer (IC) for the purchase of all equipment and services associated with it. Prior to the issuance of a site licence, the IC is also responsible for ensuring that the aspects of the pre-work impacting nuclear safety and environmental protection are brought together with the same rigour as if a site licence had been in place.

Westinghouse, as design authority (DA) for the AP1000 design, has assumed the position of IC for the purposes of the GDA. Ownership of the IC role will change during the life cycle of the plant. At some time during the licensing process the licence holder will take on the role. In addition, the role of DA will also transfer from Westinghouse to the licensee. The interfaces between Westinghouse, the utilities, and other stakeholders (e.g., contractors) over the life cycle of the plant are described in detail in Chapter 7.

3.3.2 Interfaces between Westinghouse and the Utilities

Westinghouse has worked with potential utility licensees during the GDA process concerning submissions to the UK regulators with the purpose of ensuring that an acceptable safety case has been made for the AP1000 design. A formal interface exists with potential utilities, which is covered in the Project Quality Plan (Reference 3.5). This ensures that the safety of the AP1000 design is understood and maintained during its life cycle, and that a systematic approach has been undertaken to ensure the competency of the utilities at technical, operational, and managerial levels.

Representatives from the utilities attend regular GDA progress meetings. This ensures concerns raised throughout the review process by all parties are promulgated, addressed, and discussed. This should also facilitate any future licensing application for construction and operation of AP1000 reactors.

Fundamental to the success of the interface between Westinghouse and the utilities is for all parties to implement safety requirements appropriate to their role at each phase of the project. This includes the management of contractors and development (and delivery) of appropriate integrated safety standards.

Steps have been taken to build confidence that there is a robust interface with stakeholders on the Pre-Construction Safety Report (PCSR). The Project Quality Plan (Reference 3.5) requires that all employees performing work on the UK GDA project be responsible for the quality of their own work and comply with Westinghouse policies, procedures, and work instructions.

In accordance with SLC 36, Organisational Capability (Reference 3.26), a strong nuclear safety culture is being developed between Westinghouse and the utilities, the aim of which is to ensure a common understanding of the key aspects of nuclear safety within their respective organisations. This will aid the formal demonstration to the regulatory bodies that procedure compliance has been achieved.

Each utility manager or appointed person designated to determine plant safety will ensure that a strong safety culture is developed within their section/department in order to establish, maintain, and continually improve the safety management system requirements in accordance with those identified by the IC and in accordance with regulatory requirements and SLCs. Strong emphasis will be placed on continuous improvement and ensuring that lessons learned are implemented, monitored, and fully documented.

3.3.3 Security Arrangements

The GDA process and safety case submissions will require the transfer of detailed knowledge in document form between Westinghouse, vendors, stakeholders, and utilities, the confidentiality of which is paramount. The procedure for creating, handling, and processing protectively marked documents (Reference 3.27) ensures that all documents are marked appropriately with the correct level of security classification and handled in accordance with ONR Civil Nuclear Security (ONR CNS) requirements (Reference 3.28).

3.4 MANAGEMENT OF SAFETY THROUGH THE PLANT LIFE CYCLE

The management of safety in the plant life cycle begins with the design process (Reference 3.20). The input to the design process incorporates safety principles, assessments, codes, and standards that will continue through the life of the plant. Regulations require the management of safety to be fully documented. Design, construction, commissioning, operation, and decommissioning phases will each have appropriate documentation in order to demonstrate how the regulations are intended to be implemented, managed, and monitored.

Westinghouse will be the DA until at a suitable point, this role will be transitioned over to the licensee, and Westinghouse will become the responsible designer. Westinghouse will provide support to the licensee until agreed otherwise, and formal procedures will be established between Westinghouse and the licensee to define the responsibilities throughout the development of the AP1000 design, procurement, construction, installation, and commissioning phases.

Chapter 7 discusses the plant life cycle in more detail with reference to the Plant Life Cycle Safety Report (Reference 3.20). The key aspects of the safety management of each project phase are discussed in the following sections.

3.4.1 Design

The fundamental principles of plant design ensure that the design meets the required specification, is capable of delivering and maintaining required safety functions, is fit for purpose, and all mitigating risks have been identified and reflected in the design. The involvement of suitably qualified and experienced persons (SQEPs) from the IC, utilities, and other stakeholders should ensure that all aspects of the specification are fully reviewed prior to incorporation in the design.

Well-established procedures within Level 2 and Level 3 of the WGMS regulate the design process and ensure compliance with regulatory requirements and those of the potential utility. These procedures are subject to audit in accordance with internal quality assurance audits procedure (Reference 3.7) and reviewed if necessary during GDA progress meetings.

To ensure a well-established design process is formally documented and implemented, the following examples of Westinghouse procedures have been reviewed in the preparation of the Project Quality Plan (Reference 3.5):

- Design and Development (Reference 3.29)
- Safety Classification (Reference 3.30)
- Design Analysis (Reference 3.31)
- Design Reviews (Reference 3.32)
- Safety Analysis Reports (Reference 3.33)
- Functional Specifications (Reference 3.34)
- Design Specifications (Reference 3.35)

In accordance with the WGMS (Reference 3.47), training records of the Westinghouse design management team are required to confirm the competence of SQEPs and to identify relevant training when required (Reference 3.36). Contracted key personnel used by Westinghouse during the GDA process have been confirmed as SQEPs; their records of qualification have been verified. Processes aligned to the requirements of SLC 36, Organisational Capability (Reference 3.26), have been adhered to following changes to personnel. The knowledge transfer process associated with the transfer of the IC role to the site licensee will involve incorporation of this PCSR into the licensee safety case and acceptance of a joint suite of procedures that define clearly the ongoing roles and responsibilities of both parties. These procedures will be fully documented within both the site licensee and the WGMS. During the design, construction, and commissioning phases when Westinghouse is the DA, some elements may be assigned to other responsible designers. However, the responsibility of the overall design integrity will remain with Westinghouse, which has sufficient in-house knowledge to understand the impact of subcontracted work. The formal arrangements will be addressed in the appropriate level of the WGMS. The licensee will also be required to have suitable arrangements to maintain design integrity. When the site licence has been granted, any changes will be carried out in accordance with the licensee's arrangements for making modifications, under SLC 20, Modification to Design of Plant Under Construction (Reference 3.26). Section 7.3 describes in more detail the management of design change control with reference to the plant life cycle (Reference 3.20).

The AP1000 design has been reviewed to determine safety classification of systems, structures, and components (SSCs) based on the safety function of the SSC. The safety class dictates the level of integrity required of that system or equipment (often expressed as a specified reliability or probability of failure on demand), and Chapter 5 discusses the UK equipment classification scheme in detail. Such information is useful early in the design process as it can facilitate the choice of design options and, where necessary, assist in the procurement of long-lead items.

The GDA process recognised that the implied reliability and safety margins were developed using standards from outside the UK/Europe. The governing AP1000 codes and standards document (Reference 3.37) was, therefore, reviewed to take account of those codes and standards that have been applied during the design of the AP1000. The AP1000 Equivalence/Maturity Study of the U.S. Codes and Standards (Reference 3.38) has been produced by Westinghouse to ensure the UK SSC requirements have been met. This is discussed in more detail in Section 5.3.

Westinghouse has also introduced a design reference point (DRP) document (Reference 3.39), that is used to define a known (baseline) status for every document and activity associated with the design, against which the GDA can be carried out. The GDA process will result in the issuance of a DAC for the generic AP1000 design that will comprise the DRP and other supporting documentation. The identification and assessment of any future safety-significant changes with regard to the DAC will be referenced in an application and issuance of any nuclear site licence for the construction and operation of the AP1000 design in the UK.

3.4.2 Construction

The modular design of the AP1000 plant allows a portion of construction to be undertaken in a factory environment. This allows quality and safety to be more closely monitored within a more securely controlled environment than in a traditional build approach. It also reduces the potential environmental risks associated with large civil construction.

Westinghouse will work closely with the licensee during the construction stage and ensure that technical information is provided to the licensee; e.g., for verification purposes. Account will be taken of the requirements of the licensee set out in SLC 19, Construction or Installation of New Plant (Reference 3.26).

The prime construction contractor will be required to have a fully functional site safety manual that includes a safety policy statement covering all aspects of site safety, e.g., fire protection, accident reporting and feedback, planning, and training.

Controls of purchased items and services are established to ensure that applicable technical and quality requirements are met by subcontractors (Reference 3.9). Procurement activities are controlled through documented procedures and instructions that include requirements for bid evaluation, selection and qualification of suppliers, communication of requirements to suppliers, evaluation of supplier performance, and resolution of nonconformances. Where Westinghouse has procured services outside their organisation, under the Westinghouse procedure for control of purchased items and services (Reference 3.9), they remain wholly responsible for the control and provision of SQEPs to ensure output is delivered efficiently and the appropriate level of safety management is used. Westinghouse will perform surveillance activities at a supplier's facility during manufacturing, inspection, testing, and release of items, as appropriate and as specified in procurement documents in accordance with the Westinghouse supplier oversight procedure (Reference 3.40) and quality oversight at resident facilities (Reference 3.41). The management of nonconformances is executed in accordance with Reference 3.42.

A construction verification process (which includes information on inspections, tests, analyses, and acceptance criteria to demonstrate the condition of the plant) is aligned with the intended design, which is identified as an essential component of plant safety (Reference 3.20). The process requires that the prime construction contractor provides evidence that processes are established to ensure that build quality is in accordance with the design intent. It also requires demonstration that modifications during the build are controlled and approved. When the build is complete, the constructor or consortium is required to produce appropriate documentation giving a detailed demonstration that the plant has been built to meet the design intent.

The overall build programme (material procurement, component manufacture, construction, and commissioning) for the plant is controlled by a series of hold points, where the preceding activity is examined for completion/adequacy before the activity in the following phase is permitted. An element of this permission is demonstrating that the plant build complies with the design intent. Hold points will also be applied throughout the design and build phase to assist in the management of risks. Hold points are typically set at stages where there are significant changes in the levels of risk associated with the project, e.g., where the foreclosure of options occurs, or where the design baseline can be set to facilitate configuration management. Hold point control documents define the hold point logic for the project and present the nuclear-safety-implicated activities associated with each hold point, together with the criteria and deliverables for release.

Management of the construction process and an overview of the construction verification process and its objectives are discussed in Section 7.4.

3.4.3 Commissioning

The overall objective of commissioning is to demonstrate that the plant has been constructed as designed, that the systems perform in a manner consistent with the plant design, and that activities culminating in operation at full power, including initial fuel load, initial criticality, and power ascension, are performed in a controlled and safe manner.

Westinghouse has established an initial test programme (ITP) that will be further developed to incorporate the expectations of a Pre-Commissioning Safety Report (PCmSR), which will address both inactive and active commissioning. Its primary purpose is to present firm evidence that the plant has been constructed in accordance with the design intent and that sufficient and appropriate tests will be conducted to support the future operational safety case.

The ITP demonstrates that the construction and installation test programmes, pre-operational test programmes, and startup test programmes have been developed in sufficient detail to allow the commissioning tests to be carried out without undue risk to operators, site workers, and the public, and in accordance with statutory health and safety requirements. This implies that the future operating infrastructure must be in place and approved, at least for active commissioning, and demonstrates that the commissioning trials will not compromise the future safe operation of the plant.

During commissioning the licensee has the responsibility under SLC 21, Commissioning (Reference 3.26), to have in place and implement adequate arrangements to ensure safety. In accordance with SLC 20, Modification to Design of Plant under Construction (Reference 3.26), the licensee is required to ensure that management arrangements are in place in order to maintain design integrity and to define a baseline statement for the safety of the plant through the remaining life cycle of the facility.

A detailed description of the commissioning phases of the project is discussed in Section 7.5.

3.4.4 Operation

During operation, the responsibility for the safety of the plant lies with the licensee. The licensee must demonstrate that adequate management arrangements are in place, and that examination, inspection, monitoring, and testing of the plant and assets, through a series of comprehensive and systematic audit process of safety assessments, are fully documented.

Westinghouse will supply technical and operational information, through specifications as detailed within the Plant Life Cycle Safety Report (Reference 3.20), that prescribes the manner with which the licensee will operate the plant. The supplied technical and operational information will include or will provide input to:

- Technical specifications and operating limits,
- Examination, maintenance, inspection, and testing schedules,
- Procedures for normal operation, emergency conditions, and accident management,
- Training programmes,
- Radiation protection arrangements for operators, and
- Emergency preparedness

This ensures that the requirements of the safety case, and the assumptions on which the safety case is based, are captured and communicated to operating utilities and incorporated into the operating regime.

The AP1000 Technical Specifications (Tech Specs) compile the equipment conditions, signals, and operational requirements from all of the identified accident conditions. Each requirement within the Tech Specs comprises the limiting condition for operation and the surveillance requirements.

Westinghouse may have a DA capability within the licensee's organisation (dependent upon the licensee), under which any design changes must undergo due process in accordance with SLC 22, Modification or Experiment on Existing Plant (Reference 3.26), and SLC 23, Operating Rules (Reference 3.26). The general principles of design change control as detailed in the ONR technical assessment guide Design Safety Assurance (Reference 3.43) are as follows:

- Recognition of change
- Understanding the safety impact of change
- Agreement of change at the correct authority level
- Controlled implementation and communication of change
- Update of necessary documentation

3.4.5 Decommissioning

The licensee has a requirement to produce a decommissioning safety case to give confidence to the governing bodies that the decommissioning of the plant will be in accordance with regulatory requirements and under the auspices of a robust set of management arrangements. The safe decommissioning of the plant has been taken into account since the initial planning stage, the dismantling of the structure and the removal of hazardous material has been reviewed, and the risks to the general public and the environment have been identified and reduced to a level that can be demonstrated to be as low as reasonably practicable (ALARP) at all stages of decommissioning.

Westinghouse involvement will be determined through due process as either a design consultant or an external contractor, and in accordance with the licensee's requirements, with any such involvement being documented in the decommissioning safety case. High-level information on decommissioning is available from the design work to date, which is reflected in the detailed liaison requirements for Westinghouse and the potential licensees, to ensure that due process for the plant end of life is fully considered. The level of detail in this PCSR is proportionate with the current stage of the AP1000 design.

Management and disposal of waste is described more fully in the integrated waste strategy (Reference 3.44) and supporting documents (References 3.45 and 3.46).

A detailed description of the decommissioning stages of the project is discussed in Section 7.9 and in Chapter 27.

3.5 ROLE PROFILES

The safety of the plant is dependent on the abilities and attitudes of the individuals who design, construct, commission, operate, examine, maintain, inspect, test, and modify the SSCs that make up the plant. Management is responsible for determining the necessary personnel competencies in terms of skills, education, and experience requirements for the activities affecting quality.

Westinghouse has produced a procedure regarding individual training and competency requirements (Reference 3.36).

Top-level management within Westinghouse has the ultimate responsibility for the training and development of competent persons, and to ensure that procedures implemented within the WGMS are managed, maintained, and continuously improved in accordance with regulatory requirements and company quality policies. Westinghouse will liaise closely with utilities and licensees to ensure these levels are met and maintained within their organisations.

Where Westinghouse has procured services outside their organisation, under the Westinghouse procedure for control of purchased items and services (Reference 3.9), they remain wholly responsible for the control and provision of adequate SQEPs to ensure that output is delivered efficiently and that safety management controls are in place.

3.6 DESIGN RELIABILITY ASSURANCE PROGRAMME

Westinghouse has implemented the Design Reliability Assurance Programme (D-RAP), which gives confidence that through-life reliability is designed into the AP1000 plant. The D-RAP comprises the following three phases:

Phase 1 Identifies and evaluates risk-significant SSCs

Phase 2 Post-Design Certification process that develops component maintenance recommendations for plant operation

Phase 3 Relates to advice to the licensee on plant operation

Section 5.9.1.2.1 discusses the D-RAP programme in more detail.

3.7 REFERENCES

3.1 Westinghouse QMS, Rev. 7, “Westinghouse Electric Company Quality Management System,” August 2013.

3.2 IAEA GS-R-3, “The Management System for Facilities and Activities,” International Atomic Energy Agency, 2006.

3.3 75-INSAG-3, Rev. 1, “Basic Safety Principles for Nuclear Power Plants,” International Nuclear Safety Advisory Group, October 1999.

3.4 UK Statutory Instrument No. 3232, "Ionising Radiations Regulations," 1999.

3.5 Westinghouse Report UKP-GW-GAH-001, Rev. 6, "Project Quality Plan for the UK AP1000 Generic Design Assessment (GDA) Issue Resolution," October 2016.

3.6 Westinghouse Level 2 Procedure W2-1.3-101, (latest revision), "Management System Document Administration,"[1]

3.7 Westinghouse Level 2 Procedure W2-4.2-101, (latest revision), "Internal Quality Assurance Audits,"[1]

3.8 Westinghouse Level 2 Procedure W2-5.1-301, (latest revision), "Self-Assessments,"[1]

3.9 Westinghouse Level 2 Procedure W2-9.4-101, (latest revision), "Control of Purchased Items and Services,"[1]

3.10 Westinghouse Level 2 Procedure QA-2.8, (latest revision), "Qualification of Audit Personnel,"[1]

3.11 Westinghouse Level 2 Procedure W2-5.1-101, (latest revision), "Corrective Action Program Procedure,"[1]

3.12 Westinghouse Level 2 Procedure WEC W2-5.1-107, (latest revision), "Corrective Action Review Board,"[1]

3.13 Westinghouse Level 2 Procedure WEC W2-6.2-100, (latest revision), "Quality Assurance Records,"[1]

3.14 Westinghouse Level 2 Procedure W2-4.3-100, (latest revision), "Management Review,"[1]

3.15 Not used.

3.16 Westinghouse Level 2 Procedure W2-5.1-103, (latest revision), "Root Cause Analysis,"[1]

3.17 Westinghouse Level 2 Procedure W2-5.1-104, (latest revision), "Apparent Cause Analysis,"[1]

3.18 Not used.

3.19 ONR, "Safety Assessment Principles for Nuclear Facilities," Rev. 0, November 2014.

3.20 Westinghouse Report UKP-GW-GL-737, Rev. 2, "Plant Life Cycle Safety Report," March 2011.

3.21 Not used.

3.22 Not used.

3.23 Westinghouse Report UKP-GW-GL-790, Rev. 6, "UK AP1000 Environment Report," January 2017.

1. This forms part of the Westinghouse Quality Management System (Reference 3.1).

3.24 Westinghouse Report UKP-GW-GAP-018, Rev. 0, "The Receipt and Processing of Regulatory Observations (ROs) and Regulatory Observation Actions (ROAs) from the UK Regulator," March 2010.

3.25 Westinghouse Report UKP-GW-GAP-012, Rev. 2, "Receipt and Processing of Technical Queries (TQs) from the UK Regulators," March 2011.

3.26 Office for Nuclear Regulation, "Licence condition handbook", January 2016.

3.27 Westinghouse Report UKP-GW-GAP-016, Rev. 2, "The Procedure for the Creation, Handling and Processing of Protectively Marked Documents," January 2011.

3.28 Office for Civil Nuclear Security, "The Management of Sensitive Nuclear Information during the Generic Design Assessment of Nuclear Technologies," Health and Safety Executive, February 2008.

3.29 Westinghouse Level 2 Procedure WEC W2-8.1-101, (latest revision), "Design and Development,"[2]

3.30 Westinghouse Level 2 Procedure WEC W2-8.2-102, (latest revision), "Safety Classification,"[2]

3.31 Westinghouse Level 2 Procedure W2-8.3-101, (latest revision), "Design Analysis,"[2]

3.32 Westinghouse Level 2 Procedure W2-8.4-101 (latest revision), "Design Review," [2]

3.33 Westinghouse Level 2 Procedure WEC W2-8.3-104, (latest revision), "Safety Analysis Reports,"[2]

3.34 Westinghouse Level 2 Procedure WEC W2-8.2-198, (latest revision), "Field Service – Equipment and Process Functional Specifications,"[2]

3.35 Westinghouse Level 2 Procedure WEC W2-8.2-199, (latest revision), "Design Specifications,"[2]

3.36 Westinghouse Level 2 Procedure W2-2.5-100, (latest revision), "Competence, Awareness, and Training,"[2]

3.37 Westinghouse Report APP-GW-G1X-001, Rev. 8, "Governing AP1000® Design Codes and Standards," June 2014.

3.38 Westinghouse Report UKP-GW-GL-045, Rev. 2, "AP1000 Equivalence/Maturity Study of the U.S. Codes and Standards," September 2011.

3.39 Westinghouse Report UKP-GW-GL-060, Rev. 10, "AP1000® Design Reference Point for UK GDA," January 2017.

3.40 Westinghouse Level 2 Procedure W2-9.5-104, (latest revision), "Supplier Oversight,"[3]

2. This forms part of the Westinghouse Quality Management System (Reference 3.1).

3 This forms part of the Westinghouse Quality Management System (Reference 3.1).

3.41 Westinghouse Level 2 Procedure W2-9.5-103, (latest revision), "Resident QA Oversight at Asian Supplier and Construction/Customer Sites,"[3]

3.42 Westinghouse Level 2 Procedure 2 W2-9.4-102, (latest revision), "Deviation Notices,"[3]

3.43 ONR Nuclear Safety Technical Assessment Guide NS-TAST-GD-057, Rev. 3, "Design Safety Assurance," November 2014.

3.44 Westinghouse Report UKP-GW-GL-054, Rev. 1, "UK AP1000 Integrated Waste Strategy," March 2011.

3.45 Westinghouse Report UKP-GW-GL-055, Rev. 2, "UK AP1000 Radioactive Waste Management Case Evidence Report for Intermediate Level Waste," March 2011.

3.46 Westinghouse Report UKP-GW-GL-027, Rev. 2, "UK AP1000 Radioactive Waste Arising, Management and Disposal," March 2011.

3.47 Westinghouse Global Management System Description Document, WGMS-DD-001, Rev. 0.0, 8 January 2016.

3.48 Westinghouse Environmental, Health, and Safety Management System, EHS MS, Rev. 1, 15 January 2013.

3.49 Westinghouse Report UKP-GW-GAP-012, Rev. 5, "Receipt and Processing of Regulatory Queries (RQs) from the UK Regulators," September 2016.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

None.

LIST OF ABBREVIATIONS AND ACRONYMS

COMAH	Control of Major Accident Hazards
CWS	Circulating Water System
EA	Environment Agency
GDA	generic design assessment
NPS	National Policy Statement
ONR	Office for Nuclear Regulation
SSA	Strategic Siting Assessment
SSC	system, structure, or component
SWS	Service Water System
UK	United Kingdom

4 GENERIC SITE CHARACTERISTICS

4.1 Introduction

The UK generic design assessment (GDA) process requires that the suitability of the AP1000 plant for application to sites in the UK be assessed before a specific location for such a plant has been identified. This includes an early assessment of the potential impact of the AP1000 design to members of the public and the surrounding environment. To allow such assessments to be undertaken, a UK generic site has been defined. This generic site does not represent any particular location in the UK, but rather reflects a conservative set of conditions for a credible UK site. Early consideration of the characteristics of a UK generic site is important for the following reasons:

- The assessment of radiological risk to the local population depends on the location and characteristics of that population as well as those local factors that affect the dispersion of activity released into the environment.

- It is important to understand and, if necessary, mitigate those hazards over which an operator has no effective control. These "external hazards" could have an impact on the safe construction or operation of the plant.

- It is essential to assess the suitability of a site to support the engineering and infrastructure requirements of the design.

The intention of this chapter is primarily to provide confidence that the generic site characteristics in the UK will not lead to materially increased radiological risk to people from the AP1000 design throughout the life cycle of the nuclear site. A detailed assessment of external hazards can be found in Chapter 12. An assessment of the engineering and infrastructure requirements can be found in Volume 4. The impact of the AP1000 plant on the wider environment is described in the UK AP1000 Environment Report (Reference 4.1, Section 5.3). This includes the consideration of nonhuman species and sensitive habitats.

This chapter has the following structure.

UK Strategic Siting Assessment

In parallel with the GDA process, and independent of it, in 2010 the UK government undertook a process to identify strategically suitable sites for possible new build. This process is known as the Strategic Siting Assessment (SSA). As part of this process a number of strategically suitable sites for possible new build were identified. The SSA process is described in Section 4.2.

UK Generic Site Characteristics

For the purpose of carrying out radiological impact assessments for the GDA process, a generic UK site was defined. The characteristics of that generic site are summarised in Section 4.3.

Design Parameter Assessment against Generic Site Characteristics

The AP1000 plant is a standardised nuclear power plant designed for construction and operation at sites meeting a broad range of parameters (see Table 4-9). The site design parameters relevant in the context of this chapter are presented in Section 4.4 to demonstrate

that potential UK sites are acceptable for the operation of an AP1000 plant from a radiological perspective.

Monitoring of Site-Specific Parameters

The outline of a suitable monitoring programme of site-specific parameters is given in Section 4.5.

The siting characteristics are covered here from a generic UK perspective. A number of the siting criteria discussed in this chapter are dependent on local conditions of a specific site. In such cases, detailed assessments are expected to form part of any future site licence application.

4.2 Strategic Siting Assessment

Details of the SSA process undertaken by the UK government are provided in the National Policy Statement (NPS) for Nuclear Power Generation (Reference 4.3). As part of the SSA process, criteria have been developed against which the strategic suitability of possible sites can be judged. These criteria relate to nuclear safety, environmental protection, societal issues, and operational requirements, and are presented in Part 5 of the NPS for Nuclear Power Generation (Reference 4.3).

The conclusion of the SSA is that ten of the nominated sites are potentially suitable for the deployment of new nuclear power stations. The sites are listed and details provided in the NPS for Nuclear Power Generation (Reference 4.3).

The GDA generic site assessment, as the focus of this chapter, is not geared towards any particular candidate site in the UK. Nevertheless, a consideration of the general characteristics of the candidate sites identified through the SSA process is useful. For example, the site boundaries for the SSA-nominated sites enclose areas of between 75 hectares (185 acres) and 298 hectares (714 acres). Of the ten potential sites, eight are located adjacent to existing nuclear power stations (either operational or in a decommissioning phase). The other two nominated sites are located on the west coast of Cumbria, within the wider locality of Sellafield. All ten sites are located on the UK seacoast or on major estuaries.

4.3 UK Generic Site Characteristics

4.3.1 Introduction

The GDA process requires that the suitability of the AP1000 design for application to sites in the UK be assessed. This necessitates some assumptions be made on the local environment surrounding the AP1000 plant. To allow for such assessments to be undertaken in the absence of a specific location for the plant, a UK generic site has been defined. The UK generic site has a number of characteristics that relate to the distribution of population centres and parameters that influence the dispersion of radionuclides in the environment. The UK generic site characteristics are based on data obtained from a number of existing coastal nuclear power stations in the UK and are given in the following subsections. It has generally been assumed that the generic site characteristics remain constant over the life cycle of the nuclear plant. Details on the impact of a future climate change on meteorological and hydrological data are discussed in Chapter 12.

A number of the UK generic site characteristics data are taken from an Environment Agency (EA) assessment method report (Reference 4.4). This includes exposure group characteristics as well as atmospheric and marine dispersion conditions. Other UK generic data have been

derived from the environmental data from five existing UK nuclear power station sites: Dungeness, Hartlepool, Heysham, Hinkley, and Sizewell. These include the distribution of population centres, topography, geology, meteorology, flooding, tidal ranges, and coastal water depths. The values derived for the UK generic site from data for those sites are normally conservative values, represented by maximum and minimum values, or 80 and 20 percentile values. More details on how these site characteristics were derived can be found in the UK Generic Site Report (Reference 4.5). Details on the environmental assessments undertaken to support the AP1000 build in the UK are presented in the UK AP1000 Environment Report (Reference 4.1).

4.3.2 Human Population

It has been assumed that the population centres of a given size are located at the nearest distance recorded for the five existing nuclear power stations. The density of population centres is based on the 80 percentile distribution for the five sites. Population centres are present within 2 km (1.2 mi), 10 km (6.2 mi), and 20 km (12.4 mi) of the site; individual properties/farms are also present within 2 km (1.2 mi) of the UK generic site. Details are shown in Table 4-1.

Members of the public who have the potential to receive an offsite dose of radioactive discharges from the operation of a nuclear power plant can only be characterised on a site-specific basis. For a general assessment of the impact of radioactive discharges at a generic coastal site the default methodology is to consider the following potential exposure groups: a local resident family and a fisherman family. The local resident family represents members of the public primarily exposed to atmospheric releases through external exposure to activity in the plume and deposited to the ground, inhalation of activity in the plume, and ingestion of activity transferred to terrestrial foodstuffs. The fisherman family represents members of the public primarily exposed to liquid releases through external exposure to activity in beach sediments and ingestion of marine seafood. Habit data for the local resident and fisherman families are shown in Tables 4-2 and 4-3, respectively.

4.3.3 Water Environment

The nearby foreshore and marine environment supports a fishery, wildfowl, and seabirds. It has been assumed that the intertidal zone of the generic site contains a wide range of substrates within 10 km (6.2 mi) of the site. These may include sand, gravel, mud, rocky outcrops, and made ground.

Tidal ranges are shown in Table 4-4. This UK generic site data is based on five existing nuclear sites and assumes the 80 percentile value for high tides and the 20 percentile value for low tides. Limiting water depths off the coast of five existing nuclear sites are shown in Table 4-5. The UK generic site is assumed to have the shallowest depth.

For the purpose of radiological impact assessments, a conservative volumetric water exchange rate of 130 m^3/s (2.1E6 gpm) has been adopted to characterise the flushing of the local marine water compartment. This is based on the lowest value at existing UK coastal nuclear sites. A low value leads to higher activity concentrations in beach sediments and marine biota in the local compartment and hence to higher doses to members of the relevant exposure group.

4.3.4 Terrestrial Environment

Within the five existing nuclear sites, the highest ground elevation within 2 km (1.2 mi) of the UK generic site is 30 m (98 ft), and within 10 km (6.2 mi) is 358 m (1,174 ft). Land cover

within 5 km (3.1 mi) includes arable and grassland, dune vegetation, and some woodland. A surface roughness length of 0.3 m (1 ft) is applicable for atmospheric dispersion modelling purposes. It is assumed that the land is stable and that the presence of faults is minimal.

4.3.5 Meteorological Data

Ranges of temperature, wind speed, and rainfall for the UK generic site are shown in Table 4-6. These data are based on five existing nuclear sites. They do not represent extreme weather conditions in the whole of the UK and are therefore not directly comparable with the meteorological data considered in the external hazard assessment (Chapter 12).

The distribution of atmospheric stability categories and atmospheric deposition rates for the generic site are given in Tables 4-7 and 4-8, respectively.

4.4 Design Parameter Assessment against Generic Site Characteristics

4.4.1 Introduction

This section provides a demonstration that the natural environmental conditions for a generic site in the UK are consistent with the safe operation of the AP1000 plant and will not lead to elevated risk to people. Consideration is also given to anthropogenic factors that could have an impact on the safety features of the AP1000 plant.

A review of relevant criteria has been carried out. These are based on site characteristics considered in the AP1000 human risk assessment reported in the UK AP1000 Environment Report (Reference 4.1, Section 5.2). Consideration has also been given to external hazard criteria relevant to human risk assessments in Chapter 12 and the SSA criteria considered in the NPS for Nuclear Power Generation (Reference 4.3). The relevant parameters can be grouped as follows:

- Meteorological conditions
- Geological and hydrogeological conditions
- Topography
- Hydrological conditions
- Access to suitable sources for cooling
- Human populations
- Potentially hazardous man-made installations or hazardous human activities
- Site dimension

The impacts of meteorological, geological, hydrogeological, and hydrological conditions encountered in the UK as well as the potential impact of hazardous installations or activities on the safe operation of the AP1000 standard plant have been assessed in detail in Chapter 12. The AP1000 plant design parameters relevant to the criteria assessed here are shown in Table 4-9.

Generally, in the context of siting, the site-specific characteristics of natural and man-made external hazards need to be confirmed in detail at the site-licensing stage to ensure that the safe operation of the AP1000 plant at a specific location is not compromised. As demonstrated by the assessments reported in Chapter 12, the AP1000 design incorporates adequate and sufficient defences to ensure that the delivery of Category A safety functions are not compromised by the potential effects of the range of external hazards that are likely to be encountered at a candidate site in the UK.

In addition to ensuring that the characteristics of a specific site do not compromise the safe operation of the AP1000 plant, a number of other site-specific parameters need to be established at the detailed site investigation stage. This includes an investigation into historical land use (to determine whether there could be any existing contamination in the ground), protected or sensitive habitats, and the presence of archaeological remains.

A summary comparison between the bounding design parameters of the AP1000 plant and the ranges of naturally occurring environmental conditions in the UK, as well as the potential impacts from man-made installations or activities, is presented in the following subsections. In addition the AP1000 plant design parameters are compared to the characteristics of the UK generic site defined in Section 4.3.

4.4.2 Meteorology

Extreme ranges of temperature, wind, snow, and rainfall in the UK and their potential impact on the AP1000 plant are presented in Chapter 12, where it is demonstrated that the safe operation of the plant would not be compromised. This includes an assessment of the likely impact of a climate change on these parameters over the expected lifetime of the plant.

Comparing the meteorological design parameters for temperature and wind shown in Table 4-9 with those of the UK generic site shown in Table 4-6 shows that the AP1000 plant design parameters encompass the UK generic site conditions for those parameters.

Meteorological parameters that influence the atmospheric dispersion of aerial emissions are not related to plant design, but are based on the atmospheric conditions prevalent at a specific site. Therefore, these must be considered further at the site-specific planning phase in conjunction with detailed site-specific modelling of gaseous radioactive emissions. A generic assessment of the dispersion of operational atmospheric emissions and related doses to the public is summarised in the UK AP1000 Environment Report (Reference 4.1, Section 5.2). This assessment is based on the meteorological parameters assumed for the GDA generic site, as described in Section 4.3. The conclusion from the assessment of the impact of atmospheric emissions is that applying UK generic site dispersion factors results in very low doses to the local exposure group.

The AP1000 plant is suitable for the range of meteorological conditions likely to be encountered at sites in the UK.

4.4.3 Geology and Hydrogeology

The potential impact of seismic hazards on Class 1 systems, structures, and components (SSCs) is considered in Chapter 12. The effects of drought and associated changes in groundwater levels on the stability of foundations and the availability of water for plant systems and fire protection are also considered. It is concluded that for conditions that can be expected in the UK the safety features of the AP1000 plant would not be compromised.

The AP1000 plant is designed for a normal groundwater elevation to within 0.6 m (2 ft) of the plant grade elevation (see Table 4-9). For the UK generic site, groundwater is assumed to occur at 2 m (6.6 ft) below the surface (Reference 4.5). As a result the AP1000 plant design parameter is more conservative than the UK generic site characteristics.

Geotechnical engineering parameters for soils (e.g., bearing capacities) to support the generic design are considered in Chapter 16. Foundation design will need to be considered further at the site-specific design stage, including the definition of appropriate ground engineering

options. This will require geotechnical ground investigation to determine soil types and their engineering properties and will include investigation of groundwater level and variability.

Possible coastal erosion and other landscape changes over the lifetime of the plant, including long-term fuel storage after operations have ceased, have to be assessed on a site-specific basis.

In addition, the following site-specific geological, seismological, and geophysical information will need to be considered at the site licensing stage:

- Structural geology of the site
- Seismicity of the site
- Correlation of earthquake activity with seismic sources
- Seismic wave transmission characteristics of the site
- Geological history
- Evidence of paleoseismicity
- Site stratigraphy and lithology
- Engineering significance of geological features
- Site groundwater conditions
- Dynamic behaviour during prior earthquakes
- Zones of alteration, irregular weathering, or structural weakness
- Unrelieved residual stresses in bedrock
- Materials that could be unstable because of mineralogy or unstable physical properties
- Effect of human activities in the area (e.g., mining, drilling)

4.4.4 Topography

The local topography around a nuclear site can influence the extent and characteristics of local transport routes. This needs to be considered for the initial construction of the plant, for the normal operations of the plant (e.g., movement of goods to and from the site), in the context of emergency responses (e.g., evacuation routes, movement of emergency response units), as well as for future decommissioning activities. A detailed analysis of access from a site to local transport routes and of any restrictions imposed on transport routes by the local topography needs to be carried out at the site licensing stage.

In addition, the topography around a nuclear plant can influence the dispersion of radionuclides emitted from the plant. For example aerial effluents can become trapped in local valleys in certain atmospheric conditions and the topography can influence the local wind field.

4.4.5 Hydrology

Ranges of external flooding from elevated rivers and sea levels, high tides, storm surges, and tsunamis in the UK and their potential impact on the AP1000 plant are presented in Chapter 12. This includes an assessment of the likely impact of a climate change on the sea level rise over the anticipated lifetime of the plant in Section 12.7.

This assessment demonstrates that the design of the plant prevents the loss of key safety functions in any credible inundation event. Further confirmation that this is the case will be provided by site-specific flood risk assessments required at the site licensing stage. These assessments will include defining maximum predictable flood levels, taking into account local coastal defences already in place. In addition, site-specific issues will be identified that could lead to local flooding such as surface run-off and upstream dam failure.

For such issues site-specific flood protection beyond that provided by the AP1000 standard plant may need to be provided.

A number of local water body characteristics that are not related to plant design may influence the dispersion of liquid emissions and the radiological impact on the local population. This includes seawater volumetric exchange rates for the local area, tidal range, water depth, characteristics of the bed sediments, and details of aquatic biota. A generic assessment of liquid effluents and related doses to the public is presented in the UK AP1000 Environment Report (Reference 4.1, Section 5.2). This assessment was carried out based on parameters assumed for the GDA generic site, as described in Section 4.3.

The characteristics of the marine environment of the UK generic site were based on an analysis of conditions at existing nuclear sites in the UK with the most conservative chosen for this assessment.

The conclusion from the assessment of the liquid emissions impact is that the characteristics of the UK generic site do not adversely affect the radiological risk to the local population. Therefore, it can be established that the AP1000 standard plant is suitable for the range of hydrological conditions likely to be encountered at sites in the UK.

4.4.6 Sources of Cooling

The generic site has access to seawater for balance of plant heat removal. This is consistent with the preliminary conclusions of the SSA, as shown in Section 4.2. The AP1000 standard design for the UK is based on indirect cooling of the circulating water system (CWS) and service water system (SWS) where nonradiological water is passed through cooling towers and water vapour is discharged to the atmosphere. Water can also be used to provide direct cooling of the CWS and SWS in which the same cooling water for the plant is discharged back to the marine environment.

An assessment of the generic impact of cooling water discharge on the marine environment is provided in the generic assessment of the impacts of cooling options (Reference 4.6).

Historically, a cooling water problem encountered by plants in coastal locations using seawater cooling has been due to marine organisms blocking the cooling water inlet screens. The potential external hazard associated with biological fouling of cooling water inlets is considered in Chapter 12. Protective features of the air and water inlet systems have been designed to resist biological fouling. These features will need to be supplemented with routine inspections and surveillance by the operators.

Considering the factors discussed above, it can be established that seawater cooling presents a viable option for the AP1000 design in the UK. Further consideration of the cooling water system will be necessary at the site-specific planning and design stages.

The circulating water system is not required to be used as the ultimate heat sink in response to an accident.

4.4.7 Human Populations

It is important that the characteristics of the population of a site be taken into account to ensure that an appropriate response can be made to an emergency extending beyond the boundaries of the site. It must be possible to apply emergency offsite measures on an appropriate timescale. As these measures may include evacuation, it is necessary to make particular arrangements to cover institutions housing significant numbers of relatively immobile people.

The characteristics of the population local to the site need to be considered in detail at the site licensing stage. Regarding the UK generic site, individual dwellings and small population centres are present within a couple of kilometres of the UK generic site, with larger towns typically situated further afield (see Table 4-1).

From this perspective, there are significant advantages in locating AP1000 plants on candidate sites adjacent to existing nuclear facilities. The emergency arrangements for the existing plants will have been agreed by the Office for Nuclear Regulation (ONR) and the relevant statutory consultees. There will have been regular exercises to test the arrangements. The offsite civil agencies will have been involved in these exercises. Further consideration will be necessary at the site-specific planning and design stages, particularly in response to external hazards that could simultaneously impact neighbouring sites.

4.4.8 Potentially Hazardous Installations or Activities

A number of installations and activities should be considered, including:

- Hazardous industrial facilities for example those that fall under the Control of Major Accidents and Hazards (COMAH) Regulations (Reference 4.7)
- Proximity to other nuclear installations
- Proximity to civil aircraft movements
- Proximity to military installations or operations
- Transport of hazardous materials

There are two aspects to the consideration of nearby potentially hazardous installations or activities. First, these could present hazards to the safe operation of the nuclear facility. These hazards are primarily either physical (resulting, for example, from fire, explosion, or impact) or chemotoxic (resulting from the release of gases or vapours). Second, the neighbouring hazardous installations and activities might be affected by an incident at the nuclear facility. Careful consideration of potentially hazardous installations is important for complex sites, where several facilities exist close to one another.

The potential impact of physical and chemotoxic hazards on the safety functions of the AP1000 design are considered in detail in Chapter 12 with the conclusions outlined in the following sections.

External Explosions

For the AP1000 plant, all SSCs required for nuclear safety are located on the robust reinforced concrete nuclear island structure which provides a level of protection from explosions outside of the nuclear island. The AP1000 site security system is designed to protect the AP1000 nuclear island from credible external explosions.

Accidental Aircraft Crash

Civil aircraft movements can present a hazard in the case of an accidental aircraft crash (see Section 12.8). UK legislation restricts flying in the vicinity of UK nuclear sites. The predicted frequency of an accidental aircraft crash away from flight paths and airfields has been calculated for a range of aircraft types. Malicious aircraft crashes are outside the scope of this review due to their sensitive nature. It should be confirmed on a site-specific basis that accidental aircraft crash frequencies and UK legislation that restricts flying in the vicinity of existing UK nuclear sites is applicable to the specific site under consideration.

External Fire

The AP1000 standard plant will withstand the effects of external smoke, heat, or fumes caused by external fires to an extent that is sufficient to ensure that they would not compromise either the control of core reactivity or the removal of heat from the core, and would not, therefore, result in the uncontrolled dispersion of radioactivity or the uncontrolled exposure of plant personnel or the public to radiation.

External Toxic Gases

Any smoke or toxic gases that penetrate the AP1000 site boundary are considered in the context of internal or external hazards (Chapter 11 or 12, respectively). The AP1000 plant main control room is designed to provide isolation from toxic smoke and gases generated onsite. The main control room is pressurised to a positive pressure using compressed air for a period of 72 hours which prevent toxic gases from entering.

Further consideration of these issues will be necessary to confirm that the assumptions and data presented in Chapters 11 and 12 remain applicable on a site-specific basis. In addition an assessment will need to be undertaken on whether any hazardous installations in the vicinity could be affected by an incident at the AP1000 plant.

4.4.9 Site Dimension

The required land area for the construction, operation, and decommissioning of the AP1000 plant needs to be considered and compared with available sites in the UK.

A typical layout for the AP1000 standard plant is presented in Chapter 6. With the exception of the parking area, the entire facility is contained within a perimeter fence that encloses approximately 10 hectares (2.5 acres). The site boundaries for the SSA-nominated sites enclose areas between 75 hectares (185 acres) and 298 hectares (714 acres) (Section 4.2). Hence, all of the nominated sites have sufficient land area available for at least one AP1000 nuclear power station.

The finalised layout will need to accommodate both generic and site-specific requirements and meet with the approval of the regulators. As part of that, the finalised layout will need to ensure that the constructed AP1000 plant can be operated in a safe and secure manner, with access to the site and nuclear materials strictly controlled.

4.4.10 Grid Connection

A distinguishing feature of the AP1000 plant is that it is designed to be able to achieve a safe shutdown without site ac power supplies or standby diesel generators. The grid connection type and reliability for the UK generic site do not adversely affect the radiological risk to the local population. As a result, redundant grid connections are not required.

4.5 Monitoring of Site-Specific Parameters

The monitoring of site-specific parameters is part of the environmental management system for environmental protection purposes. With regard to the site-specific criteria noted in this chapter, the parameters to be monitored on a site-specific basis should include, but not be restricted to the following:

- Meteorological conditions and tidal cycles/height (both in advance and to identify any longer-term changes)
- Groundwater levels
- Signs of coastal erosion
- Structural integrity and effectiveness of any flood protection systems at the plant

In addition changes in the characteristics of the local populations, in infrastructure and in neighbouring industries, are likely during the life cycle of the plant. As a result these data need to be monitored periodically and the safety case updated if necessary.

Monitoring will begin prior to construction in order to develop a baseline against which to judge any changes that occur. The collation of baseline data is required as part of an environmental impact assessment to support an application for planning consent.

As the development programme moves into the construction phase, any changes in the baseline will need to be identified and an assessment made of whether revisions of either plant design or construction methodologies are required. Likewise, monitoring will be continued throughout the licensing period, to include the operational phase and decommissioning phases, to identify whether any revisions are necessary to operational procedures or facility engineering.

More details on the environmental management system can be found in the UK AP1000 Environment Report (Reference 4.1, Section 6.2).

Throughout the full life cycle of the plant, the operating organisation and other responsible parties that will vary throughout the life cycle (e.g., during decommissioning) will be required to keep themselves appraised of any developments in the vicinity of the plant that could affect plant safety or emergency planning arrangements. For example, any new housing developments in the vicinity of the plant could affect the emergency planning assumptions.

4.6 Conclusions

In this chapter, an overview is given on general siting topics and how they apply to the AP1000 plant. The foremost intent of this chapter is to establish that characteristics of a generic UK site will not lead to increased risks to the population from the AP1000 design.

This chapter's overview provides confidence that the generic site characteristics in the UK will not lead to materially increased radiological or other risks from the AP1000 design throughout the life cycle of the nuclear site. The evaluations forming this confidence are based on the assessment of relevant AP1000 plant parameters against UK generic site data, with consideration of the following critical areas as forming the basis for defining a UK generic site:

- Meteorological conditions
- Geological and hydrogeological conditions
- Topography
- Hydrological conditions
- Access to suitable sources for cooling
- Human populations
- Potentially hazardous man-made installations or hazardous human activities
- Site dimension

Additionally, supporting detailed assessment of site external hazards can be found in Chapter 12, including an assessment of the potential impact of a future climate change. The influence and interactions of the AP1000 plant on the wider environment is described in the UK AP1000 Environment Report (Reference 4.1, Section 5.3), including consideration of nonhuman species and sensitive habitats.

From these assessments, assurance is provided that the natural environmental conditions for a generic site in the UK are consistent with the safe operation of the AP1000 plant and will not lead to elevated risk to either the human population or local environs.

Further, a set of key site environmental parameters associated with the UK generic site has been presented. This chapter then sets out the arguments that establish that the UK generic site concept is a suitable basis for a generic assessment of the AP1000 design and will form a sound basis for any future specific site licensing.

4.7 References

4.1 Westinghouse Report UKP-GW-GL-790, Rev. 6, "UK AP1000 Environment Report," January 2017.

4.2 Not Used.

4.3 Department of Energy and Climate Change, "National Policy Statement for Nuclear Power Generation (EN-6)," July 2011.

4.4 Environment Agency Report SC030162/SR2, "Initial Radiological Assessment Method – Part 2, Methods and Input Data," May 2006.

4.5 Westinghouse Report UKP-GW-GL-025, Rev. 1, "Generic Site Report," January 2010.

4.6 Westinghouse Report UKP-GW-GL-034, Rev. 1, "Generic Assessment of the Impacts of Cooling Options for the Candidate Nuclear Power Plant AP1000," February 2010.

4.7 UK Statutory Instrument No. 483, "The Control of Major Accident Hazards Regulations," 2015.

Table 4-1. Number of Population Centres within 20 km (12.4 mi) of the UK Generic Site

Population	<1 km[1] (0.6 mi)	<2 km[1] (1.2 mi)	<10 km[1] (6.2 mi)	<20 km[1] (12.4 mi)	Closest to Site Boundary[1]
>100,000	–	0	0	1	8.5 km (5.3 mi)
>20,000	–	1	3	5	5.2 km (3.2 mi)
>5000	–	1	1	6	3.0 km (1.8 mi)
>1000	–	0	3	14	3.5 km (2.2 mi)
≤1000	–	0	0	0	–
Farms/properties	50	100	–	–	80 m (260 ft)

Note:
1. From Reference 4.1

Table 4-2. Habit Data of Local Resident Family Exposure Group

Food Consumption Rates (kg/yr)	Infant (1 yr)[1]	Child (10 yr)[1]	Adult[1]
Green vegetables	15	35	80
Root vegetables	45	95	130
Fruit	35	50	75
Sheep meat	3	10	25
Sheep liver	2.75	5	10
Cow meat	10	30	45
Cow liver	2.75	5	10
Milk	320	240	240
Breathing rates (m^3/hr)	0.22	0.64	0.92
Occupancy at habitation (h/yr)	8760	8760	8760
Fraction of time spent indoors	0.9	0.8	0.5
Cloud shielding factor	0.2	0.2	0.2
Shielding factor for deposited radionuclides	0.1	0.1	0.1

Note:
1. From Reference 4.1

Table 4-3. Habit Data of Local Fisherman Family Exposure Group

Food Consumption Rates (kg/yr)	Infant (1 yr)[1]	Child (10 yr)[1]	Adult[1]
Fish	5	20	100
Crustaceans	0	5	20
Molluscs	0	5	20
Occupancy on the beach (hr/yr)	30	300	2000

Note:
1. From Reference 4.1

Table 4-4. Tidal Range at the UK Generic Site

Tide	Generic Site Value[1]
Highest astronomical tide	11.17 m (36.65 ft)
Mean high water springs	10.06 m (33.01 ft)
Mean high water neaps	7.75 m (25.43 ft)
Mean low water springs	1.72 m (5.64 ft)
Mean low water neaps	0.67 m (2.20 ft)
Lowest astronomical tide	-0.06 m (-0.20 ft)

Note:
1. From Reference 4.1

Table 4-5. Bathymetry at the UK Generic Site

Distance from Generic Site	Depth (Max/Min)	Depth[1]
1 km (0.6 mi)	Max	5 m (16.4 ft)
	Min	-15 m (-49.2 ft)
2 km (1.2 mi)	Max	5 m (16.4 ft)
	Min	-15 m (-49.2 ft)
10 km (6.2 mi)	Max	15 m (49.2 ft)
	Min	-15 m (-49.2 ft)

Note:
1. Admiralty chart datum from Reference 4.1

Table 4-6. Meteorological Data for the UK Generic Site

Parameter		Unit	Generic Site Value[1]
Temperature	Max	°C (°F)	37.7 (99.9)
	Min	°C (°F)	-6.9 (19.6)
	Average	°C (°F)	11.8 (53.2)
Wind speed	Max	m/s (mph)	33.6 (75.2)
	Min	m/s (mph)	3.1 (6.9)
	Average	m/s (mph)	6.5 (14.5)
Wind speed	Gust	m/s (mph)	46.0 (102.9)
Wind direction	Average	Deg	200.5
	Gust	Deg	241.9
	Maximum fraction of time in any one 30-degree sector	–	0.25
Rainfall (annual)	Max	mm/yr (in/yr)	998.5 (39.3)

Note:
1. From Reference 4.1. UK generic site values have been derived from the worst-case maximum and minimum data and the average data from the five sites.

Table 4-7. Atmospheric Conditions at the UK Generic Site

Pasquill Stability Category	Frequency of Occurrence (%)[1]	Wind Speed at 10 m (32.8 ft) Height [1]
A	1	1 m/s (2.2 mph)
B	9	2 m/s (4.5 mph)
C	21	5 m/s (11.1 mph)
D	50	5 m/s (11.1 mph)
E	8	3 m/s (6.7 mph)
F	10	2 m/s (4.5 mph)
G	2	1 m/s (2.2 mph)

Note:
1. From Reference 4.5

Table 4-8. Atmospheric Deposition Rates at the UK Generic Site

Parameter		Unit	Generic Site Value[(1)]
Dry deposition velocity	Default	m/s (ft/s)	0.001 (0.002)
	Iodine isotopes (as inorganic compounds)	m/s (ft/s)	0.01 (0.02)
	Noble gases	m/s (ft/s)	0 (0)
Washout coefficient	Default	s^{-1}	0.0001
	Noble gases	s^{-1}	0

Note:
1. From Reference 4.1

Table 4-9. AP1000 Standard Site Design Parameters

Air Temperature	
Maximum safety[a]	46.11°C (115°F) dry bulb/30.06°C (86.1°F) coincident wet bulb[g] 30.06°C (86.1°F) wet bulb (non-coincident)
Minimum safety[a]	-40°C (-40°F)
Maximum normal[b]	38.33°C (101°F) dry bulb/26.72°C (80.1°F) coincident wet bulb 26.72°C (80.1°F) wet bulb (non-coincident)[d]
Minimum normal[b]	-23.33°C (-10°F)
Wind Speed	
Operating basis	64.82 m/sec (145 mph) (3-second gust); importance factor 1.15 (Class 1), 1.0 (non-Class 1); exposure C; topographic factor 1.0
Tornado	134.11 m/sec (300 mph)
Seismic	
Certified seismic design response spectra	0.30g peak ground acceleration [c]
Fault displacement potential	No potential fault displacement considered beneath the Seismic Category I and Seismic Category II structures and immediate surrounding area. The immediate surrounding area includes the effective soil-supporting media associated with the Seismic Category I and Seismic Category II structures.
Soil	
Average allowable static bearing capacity	The allowable bearing capacity, including a factor of safety appropriate for the design load combination, shall be greater than or equal to the average bearing demand of 426.1 kPa (8900 lb/ft²) over the footprint of the nuclear island at its excavation depth.
Dynamic bearing capacity for normal plus safe shutdown earthquake	The allowable bearing capacity, including a factor of safety appropriate for the design load combination, shall be greater than or equal to the maximum bearing demand of 1675.8 kPa (35000 lb/ft²) at the edge of the nuclear island at its excavation depth. or Site-specific analyses demonstrate a factor of safety appropriate for normal plus safe shutdown earthquake loads.
Shear wave velocity	Greater than or equal to 304.8 m/sec (1000 ft/s) based on minimum low-strain soil properties over the footprint of the nuclear island at its excavation depth.

Table 4-9. AP1000 Standard Site Design Parameters (cont.)

Soil (cont.)	
Lateral variability	Soils supporting the nuclear island should not have extreme variations in subgrade stiffness. This may be demonstrated by one of the following: 1. Soils supporting the nuclear island are uniform in accordance with Regulatory Guide 1.132 if the geologic and stratigraphic features at depths less than 36.58 m (120 ft) below grade can be correlated from one boring or sounding location to the next with relatively smooth variations in thicknesses or properties of the geologic units. 2. Site-specific assessment of subsurface conditions demonstrates that the bearing pressures below the nuclear island do not exceed 120% of those from the generic analyses of the nuclear island at a uniform site. 3. Site-specific analysis of the nuclear island basemat demonstrates that the site-specific demand is within the capacity of the basemat. As an example of sites that are considered uniform, the variation of shear wave velocity in the material below the foundation to a depth of 36.58 m (120 ft) below finished grade within the nuclear island footprint and 12.19 m (40 ft) beyond the boundaries of the nuclear island footprint meets the criteria in the case outlined below: Case 1: For a layer with a low strain shear wave velocity greater than or equal to 762 m/sec (2500 ft/s), the layer should have approximately uniform thickness, should have a dip not greater than 20 degrees, and should have less than 20% variation in the shear wave velocity from the average velocity in any layer.
Liquefaction potential	No liquefaction considered beneath the Seismic Category I and Seismic Category II structures and immediate surrounding area. The immediate surrounding area includes the effective soil-supporting media associated with the Seismic Category I and Seismic Category II structures.
Minimum soil angle of internal friction	Greater than or equal to 35 degrees below footprint of nuclear island at its excavation depth.
Missiles	
Tornado	1814.4 kg (4000 lb) automobile at 46.94 m/sec (105 mph) horizontal, 33.1 m/sec (74 mph) vertical 124.7 kg (275 lb), 203.2 mm (8 in) shell at 46.94 m/sec (105 mph) horizontal, 33.1 m/sec (74 mph) vertical 25.4 mm (1 in) diameter steel ball at 46.94 m/sec (105 mph) horizontal and vertical

Table 4-9. AP1000 Standard Site Design Parameters (cont.)

Flood Level	Less than plant elevation 100.0 m (100 ft)
Ground Water Level	Less than plant elevation 99.39 m (98 ft)
Plant Grade Elevation	Less than plant elevation 100.0 m (100 ft) except for portion at a higher elevation adjacent to the annex building
Precipitation	
Rain	525.8 mm/hr (20.7 in/hr) [1-hr 2.6 km^2 (1-mi^2)PMP]
Snow/ice	3.6 kPa (75 lb/ft^2) on ground with exposure factor of 1.0 and importance factors of 1.2 (Class 1) and 1.0 (non-Class 1)
Atmospheric Dispersion Values - χ/Q(e)	
Site boundary (0 – 2 hr)	$\leq 5.85 \times 10^{-4}$ sec/m^3
Site boundary (annual average)	$\leq 2.0 \times 10^{-5}$ sec/m^3
Low population zone boundary 0 – 8 hr 8 – 24 hr 24 – 96 hr 96 – 720 hr	 $\leq 2.2 \times 10^{-4}$ sec/m^3 $\leq 1.6 \times 10^{-4}$ sec/m^3 $\leq 1.0 \times 10^{-4}$ sec/m^3 $\leq 8.0 \times 10^{-5}$ sec/m^3
Population Distribution	
Exclusion area (site)	0.8 km (0.5 mi)

Notes:

(a) Maximum and minimum safety values are based on historical data and exclude peaks of less than 2 hours duration. Class 1 SSCs are designed for maximum and minimum safety values.

(b) The maximum normal value is the 1 percent seasonal exceedance temperature. The minimum normal value is the 99 percent seasonal exceedance temperature. The minimum temperature is for the months of December, January, and February in the northern hemisphere. The maximum temperature is for the months of June through September in the northern hemisphere. The 1 percent seasonal exceedance is approximately equivalent to the annual 0.4 percent exceedance. The 99 percent seasonal exceedance is approximately equivalent to the annual 99.6 percent exceedance.

(c) See Chapter 16.

(d) The noncoincident wet bulb temperature is applicable to the cooling tower only.

(e) For the AP1000 plant, the terms “site boundary” and “exclusion area boundary” are used interchangeably. Thus, the χ/Q specified for the site boundary applies whenever a discussion refers to the exclusion area boundary.

(f) Not Used.

(g) The containment pressure response analysis is based on a conservative set of dry bulb and wet bulb temperatures. These results envelop any conditions where the dry bulb temperature is 46.11°C (115°F) or less and the wet bulb temperature of less than or equal to 30.06°C (86.1°F).

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS AND ACRONYMS

ac	alternating current
ACI	American Concrete Institute
ADS	automatic depressurisation system
ALARP	as low as reasonably practicable
ANSI	American National Standards Institute
AOP	abnormal operating procedure
ARP	alarm response procedure
ASME	American Society of Mechanical Engineers
C&I	control and instrumentation
CCF	common-cause failure
C-I	Category I
C-II	Category II
CM	corrective maintenance
CMT	core makeup tank
COLR	core operating limits report
DAS	diverse actuation system
DB	design basis
DBA	design basis accident
DBE	design basis event
dc	direct current
DID	defence in depth
DNBR	departure from nucleate boiling ratio
D-RAP	design reliability assurance programme
EMC	electromagnetic compatibility
EMI	electromagnetic interference
EMIT	examination, maintenance, inspection, and testing
EOP	emergency operating procedure
EQDP	equipment qualification data package
EU	European Union
GAC	general availability controls
GDA	generic design assessment
GNS	general non-safety
GOP	general operating procedure
HI	high integrity
HSS	high safety significance
IDS	essential electrical supply system
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
ILRT	integrated leak rate test
IRWST	in-containment refuelling water storage tank
ISI	in-service inspection
IST	in-service testing
I-131 (135)	Iodine-131 (135)
LC	licence condition
LCO	limiting conditions for operation
LLRT	local leak rate test

LIST OF ABBREVIATIONS AND ACRONYMS (cont.)

MCR	main control room
MOV	motor-operated valve
NDE	non-destructive examination
NEMA	National Electrical Manufacturers Association
NNS	non-nuclear seismic
NSL	nuclear site licensing
NUREG	Nuclear Regulatory Commission technical report designation
ODCM	offsite dose calculation manual
ONR	Office for Nuclear Regulation
OPRAA	operational phase reliability assurance activity
O-RAP	operational reliability assurance programme
OR	operating rule
OTS	operating technical specifications
PCS	passive containment cooling system
PCSR	Pre-Construction Safety Report
PCT	peak clad temperature
PdM	predictive maintenance
PM	preventative maintenance
PRHR	passive residual heat removal
PSA	probabilistic safety assessment
PSI	pre-service inspection
PT	periodic testing
PTLR	pressure/temperature limits report
PWR	pressurised water reactor
QA	quality assurance
RAP	reliability assurance programme
RCS	reactor coolant system
SI	Système Internationale (metric units)
SOP	system operating procedure
SP	setpoint programme
SQEP	suitably qualified and experienced person
SR	surveillance requirement
SSC	system, structure, or component
TRM	technical requirements manual
TS	technical specifications
UK	United Kingdom
US	United States
VFTP	ventilation filter testing programme
Xe-133	Xenon-133

5 ENGINEERING PRINCIPLES

5.1 Introduction

Chapter 6 describes the systems that make up the AP1000 design. The design is based on sound engineering principles and extensive operating experience with similar plants.

The purpose of this chapter is to describe the measures used to demonstrate that the systems, structures, or components (SSCs) provided by the AP1000 design are fit for purpose – that they are designed, manufactured, installed, commissioned, maintained, and tested in accordance with their safety importance.

The safety importance of an SSC is determined by fault studies (see Chapter 8 & 9), probabilistic safety assessment (PSA) (see Chapter 10), Internal Hazards (see Chapter 11) and External Hazards assessments (see Chapter 12). These studies assign the functions provided by an SSC to a safety function category and the SSC itself to a safety class or assign the function and its SSCs as general non-safety (GNS). The categorisation and classification scheme used for the AP1000 plant in the United Kingdom (UK) is described in Section 5.2.

Codes and standards for design, manufacture, installation, commissioning, maintenance, and testing are specified as appropriate to each safety class. This is the mechanism that allows SSCs to be treated throughout their life in a way that is commensurate with their safety importance. Many of the SSCs in the AP1000 plant have been designed using United States (US) codes and standards. As part of the development of this Pre-Construction Safety Report (PCSR), an exercise has been undertaken to demonstrate that those codes and standards are appropriate to support the design, construction, manufacture and future safe operation of AP1000 reactor plants in the UK. Codes and standards are the subject of Section 5.3.

Required SSCs have to be able to meet their performance requirements (i.e., provide their safety functions) in both normal and abnormal conditions. The equipment qualification programme provides confidence that the relied upon SSCs can meet their performance requirements under normal operating conditions and in the environmental conditions expected to occur in a design basis event (DBE), including seismic events. The equipment qualification programme used for the AP1000 plant is described briefly in Section 5.8.

SSCs also need to perform reliably. The methodology used to assess the reliability of SSCs is described in Section 5.9. Particular attention is paid to passive systems in Section 5.10, since these are different from the systems normally associated with pressurised water reactors (PWRs).

The substantiation of the claims made against individual SSCs is the subject of Chapter 8 of this PCSR.

5.2 United Kingdom Categorisation and Classification Methodology

This section identifies the criteria used to classify the AP1000 plant SSCs that play an important part in ensuring nuclear safety in terms that are consistent with the ONR safety assessment principles.

Classification of SSCs defines the quality requirements placed on those SSCs during design, manufacture, and through life. In particular, the safety class of a given SSC is used to determine which codes, standards, and seismic design considerations are appropriate to the design and manufacture of that SSC.

The relevant ONR safety assessment principles for nuclear safety are used to categorise the safety functions required to maintain safety in the event of specific fault sequences by identifying which SSCs deliver these safety functions and classifying them accordingly.

5.2.1 Categorisation of Safety Functions

Relevant ONR safety assessment principles for nuclear safety recommend that the method for categorising safety functions takes the following into account:

- The consequence of failing to deliver the safety function, including both the direct consequence and the potential for a functional failure to initiate further faults or exacerbate the consequences of existing faults.
- The extent to which the function is required, either directly or indirectly, to prevent, protect against, or mitigate the consequences of initiating faults.
- The likelihood that the function will be called upon.

The categorisation of safety functions is functional. It is not affected by how the safety function is delivered by the design. Categorisation is also not affected by whether there is redundancy, diversity, or independence within the design.

The categorisation process for the AP1000 plant is performed by identifying the high-level safety function that the specific SSC delivers or supports. These safety functions are categorised A to C, based on the nuclear safety significance of delivery failure (Reference 5.2).

5.2.1.1 Category A Safety Functions

A Category A safety function is a principal means of maintaining nuclear safety. Category A safety functions are those utilised to achieve and maintain a nonhazardous, stable state for at least 72 hours following an initiating event. Category A safety functions are fulfilled by those systems analysed in the plant design basis accident (DBA) and those systems identified as having some importance to safety as discussed in Section 5.9.1. Failure to maintain a Category A safety function has the potential to result in significant core damage, radiation exposure >20 mSv to onsite personnel, or radiation exposure >1 mSv to the offsite population.

It should be noted that onsite personnel radiation exposure is affected by plant design, operation, and radiological access controls. These efforts form an integrated approach to minimising onsite personnel exposure and meeting Category A dose limits.

Examples of Category A safety functions include the following:

- Removing the nuclear core decay (or residual) heat from the reactor coolant during normal operations and accident conditions (including those SSCs that provide the heat sink for the removal of decay heat from the reactor coolant).
- Maintaining the integrity of the reactor coolant system (RCS) pressure boundary, including mitigating RCS overpressure during normal operations and accident conditions.
- Maintaining the integrity of the containment, thereby minimising the release of radioactive material from the containment.
- Controlling subcritical reactivity of the fuel in the reactor core and the spent nuclear fuel in the spent fuel pool and associated structures during normal operations and accident conditions.
- Maintaining reactor coolant inventory.
- Maintaining habitability of the main control room.
- Maintaining spent fuel integrity such that significant radioactive releases do not occur (as a result of impacts or overheating).
- Protecting SSCs from internal/external hazards that would directly and inevitably result in loss of a principal means of fulfilling a Category A safety function.
- Functions that prevent unacceptable consequences due to the failure or spurious actuation of an SSC and for which no other Category A function exists.
- Functions required to provide information and control capabilities that allow specified manual actions necessary to reach the nonhazardous stable state.
- Functions to warn personnel or to ensure personnel safety during or following events that involve or result in release of radioactivity, or risk of radiation exposure >20 mSv.
- Permanently installed structures used to provide shielding per the plant design basis to meet exposure requirements.

5.2.1.2 Category B Safety Functions

A Category B safety function is a significant contributor to nuclear safety. Category B safety functions are utilised to do the following:

- Maintain the nonhazardous stable state after 72 hours following an accident.
- Prevent radiological exposure to onsite personnel and the offsite population from exceeding the design basis limits.
- Mitigate beyond DBAs.

Alternatively, failure to maintain the safety function may reduce safety margins significantly, with radiation exposure less than Category A limits, but greater than normal operating limits.

Examples of Category B safety functions include the following:

- Preventing the release of radioactive waste material from onsite radioactive waste systems.
- Protecting against internal/external hazards that could, as part of a sequence of failures, result in the loss of one of the Category B safety functions, such as preventing the spread of fire such that the ability to deliver a specific Category B function is lost.
- Maintaining Category A safety functions after 72 hours following an accident.
- Controlling levels of radioactivity released into the environment.
- Functions that provide a backup or alternate actuation of a Category A safety function.
- Functions that considerably reduce the frequency of an initiating event, as identified by the DBA analysis.
- Functions provided to reach and maintain a stable state beyond DBAs, as specified in station operating procedures.
- Functions provided to minimise the consequences of severe accidents in accordance with the system design basis.
- Plant process control functions that maintain the main process variables within the limits assumed in the safety analysis. Failure of this function could lead directly to the actuation or operation of an SSC that delivers a Category A safety function.
- Functions that continuously monitor the availability of Category A safety functions for proper operation or alert control room staff of failures.

5.2.1.3 Category C Safety Functions

Category C safety functions are those safety functions that may make a contribution to nuclear safety, but are not categorised as Category A or Category B. Since the removal of nuclear heat during normal operation prevents reactor trips and the actuation of Category A and Category B functions, these normally operating duty systems are recognised as being important to safety.

Examples of Category C safety functions include the following:

- Removing nuclear heat from the reactor coolant during normal operation (including providing a heat sink for those systems involved in the removal of heat from the reactor coolant during normal operation). Failure of this function would result in a short-term power manoeuvre, thus affecting nuclear safety.
- Controlling reactivity to support normal power operation.
- Providing long-term support of Category A or B functions.

- Controlling the level of radioactivity within the reactor coolant.
- Monitoring radioactivity released into the environment.
- Functions that provide continuous or intermittent tests or monitoring of Category B functions to indicate their continued availability for operation and to alert control room staff to failures.
- Functions that monitor for the occurrence of, and alert personnel to take mitigating action following, internal hazards events (e.g., fire, flood).
- Functions that alert personnel of, or ensure personnel safety during or following, events that involve or result in the release of radioactivity, or the risk of radiation exposure <20 mSv.
- Functions that monitor for the occurrence of, and alert personnel to take mitigating action following, natural events (e.g., seismic disturbance, extreme wind).
- Functions that provide access control for the nuclear power plant.

5.2.2 Classification of Systems, Structures, and Components

Relevant ONR safety assessment principles require that the method for classifying the safety significance of an SSC be primarily based on deterministic methods, complemented where appropriate by probabilistic methods and engineering judgment, with account taken of factors such as the following:

- The category of safety function(s) to be performed by the SSC.
- The consequences of the failure of the SSC to perform its function.
- The probability that the SSC will be called upon to perform a safety function.
- The time following any initiating fault at which, or the period throughout which, the SSC will be called upon to operate.

Appropriately designed interfaces should be provided between SSCs of different categories and classes to ensure that any failure in a lower-class SSC will not propagate to an SSC of a higher class. SSCs providing the function to prevent the propagation of failures should be assigned to the higher class.

Auxiliary services that support components of a system important to safety should be considered part of that system and should be classified accordingly unless failure does not prejudice successful delivery of the safety function.

For the AP1000 plant, once a safety function category has been assigned to a specific SSC in line with the safety function it delivers (or supports the delivery of), the SSC is assigned a Safety Class between 1 and 3. The safety class takes the safety category into account, and considers the extent to which the SSC supports the safety function with which the safety category is associated. At this point, consideration is given to functional defence-in-depth, diversity, and redundancy in the plant design.

It should be noted the wherever an SSC satisfies the requirements of multiple categories and/or classes, that SSC may be separated into functional subcomponents. This approach will minimise the amount of conflicting or redundant classifications while allowing the appropriate safety classification to be applied based on the SSC's function.

Functions that do not satisfy the criteria defined in these subsections will be considered to have no impact on nuclear safety and as a result will be classified as GNS in system documentation.

5.2.2.1 Class 1 Systems, Structures, and Components

Class 1 SSCs provide the principal means of fulfilling a Category A safety function.

These SSCs are standby or normally operating SSCs required to protect against or mitigate the consequences of DBAs consistent with the design basis safety analysis. These SSCs provide the principal means for the protection of the health and safety of the public and workforce and are selected using deterministic methods. The reliability of these features is confirmed using a probabilistic safety analysis.

5.2.2.2 Class 2 Systems, Structures, and Components

A Class 2 SSC is a principal means of fulfilling a Category B safety function or a significant contributor to fulfilling a Category A safety function.

A significant contributor is defined as an SSC that provides a supplementary capability for those SSCs utilised in the principal response to DBAs. Class 2 SSCs are identified using the AP1000 plant reliability evaluations described in Section 5.9.

5.2.2.3 Class 3 Systems, Structures, and Components

Class 3 SSCs are all other SSCs not included in Class 1 or 2 that contribute to maintaining nuclear safety, and include SSCs identified to support the operation of Classes 1 and 2 SSCs.

5.2.2.4 General Non-Safety Systems, Structures, and Components

SSCs classified as GNS are those that do not contribute to maintaining nuclear safety, as determined by the safety case.

5.2.3 Summary of the UK Safety Categorisation and Classification Methodology

Table 5-1 illustrates the UK safety category and classification combinations that can be assigned to the AP1000 plant SSCs.

In addition, SSCs that do not contribute to nuclear safety in accordance with the AP1000 plant safety case are simply referred to as GNS and will not be categorised or classified separately.

5.3 Codes and Standards

The classification methodology described in Section 5.2 provides the rationale for the application of codes and standards appropriate for the safety importance of specific SSCs.

The AP1000 Equivalence/Maturity Study of the U.S. Codes and Standards (Reference 5.5) contains a fuller discussion of the codes and standards used for Class 1 and 2 SSCs. Application of codes and standards for electrical equipment, Control and Instrumentation are described in Chapter 18 and 19 and in Reference 5.19 respectively.

5.3.1 Codes and Standards for Class 1 Systems, Structures, and Components

Class 1 SSCs use recognised nuclear industry codes and standards. The majority of Class 1 SSCs are designed and manufactured to American Society of Mechanical Engineers (ASME) Code, Section III, Class 1, 2, or 3 for mechanical applications; International Electrotechnical Commission (IEC) codes and Institute of Electrical and Electronics Engineers (IEEE) Class 1E codes are used for electrical and control and instrumentation (C&I) applications.

In some instances, no nuclear standard has been identified because of the nature of the SSC. In these cases, "manufacturer's standards" are used, meaning the capability of the SSC is developed through engineering practice. Examples of Class 1 SSCs for which this is the case include the following:

- In-containment refuelling water storage tank (IRWST) gutter
- IRWST screens
- Control rod clusters

Table 5-22 provides a representation of relevant codes and standards associated with Class 1 SSCs. Application of codes and standards for electrical equipment, Control and Instrumentation are described in Chapter 18 and 19 respectively and in Reference 5.19.

5.3.2 Codes and Standards for Class 2 Systems, Structures, and Components

Class 2 SSCs use recognised Class 2 nuclear industry codes and standards where applicable. In some cases, based on applicability, no Class 2 nuclear industry codes or standards may be identified. In these cases, recognised industry codes and standards based on the type of SSC, or "manufacturer's standards" are used. The assessment for the use of recognised industry codes and standards is provided within Reference 5.28.

Table 5-3 presents a representation of relevant codes and standards associated with Class 2 SSCs. Application of codes and standards for electrical equipment, Control and Instrumentation are described in Chapter 18 and 19 respectively and in Reference 5.19.

5.3.3 Codes and Standards for Class 3 Systems, Structures, and Components

This classification uses the recognised non-nuclear industry codes and standards such as those shown in Table 5-4.

5.4 Quality Assurance

The three levels of safety classification are associated with the use of different levels of quality assurance (QA) requirements.

1. Recognized nuclear industry QA programme

2. Enhanced industry standard QA programme
3. Industry standard QA programme

Class 1 SSCs are designed and supplied in accordance with a recognised nuclear industry QA programme, whereas Class 2 SSCs are designed and supplied in accordance with an enhanced industry standard QA programme.

This enhanced QA is applicable to the Class 2 SSCs where the QA requirements will provide a reasonable assurance of improved SSC reliability. These SSCs are typically active (for example, pumps, fans, active valves, switchgears) and have been identified through deterministic and probabilistic methods.

For those components where the application of enhanced QA is not expected to result in an appreciable increase in reliability, the application of industry standard QA is acceptable. These are typically passive components (for example, piping, tanks, and heat exchangers) and are inherently rugged.

Class 3 SSCs are designed and supplied in accordance with an industry standard QA programme.

The requirements for the various QA programmes are given in Reference 5.2.

5.5 Seismic Categorisation

AP1000 plant SSCs are categorised with respect to the requirements to withstand the effects of an earthquake and are designated as seismic Category I (C-I), seismic Category II (C-II), and non-nuclear seismic (NNS) (Reference 5.2).

Seismic C-I applies to both function and integrity; seismic C-II applies only to integrity. NNS SSCs, whose collapse could result in a loss of function of Class 1 SSCs, must be designated as seismic C-II. Additionally, seismic C-II is applied to SSCs whose failure could incapacitate plant operators in the control room.

The three levels of safety classification are associated with the application of seismic categorisation of SSCs.

5.5.1 Seismic Categorisation of Class 1 Systems, Structures, and Components

Class 1 SSCs are designated as seismic C-I components. Since the seismic C-I designation applies to SSC function and integrity, the application of seismic C-I ensures that SSCs required to mitigate plant DBAs maintain their safety function following an earthquake and following exposure to environmental conditions that result from a DBA.

Conduit embedded in concrete does not perform a safety or seismic function. The purpose of embedded conduit is only to provide a channel for cables to pass through the concrete structure. The concrete structures themselves are qualified as Seismic C-I to withstand the appropriate seismic loads and hence allow the circuits to continue to perform their intended safety function.

5.5.2 Seismic Categorisation of Class 2 Systems, Structures, and Components

Class 2 SSCs are generally categorised as NNS; however, seismic C-II designations are applied in the following instances:

- Where a Class 2 SSC provides support for a Category A function after 72 hours following an accident. Note that SSCs stored offsite provide the primary capability for these functions. They will be stored far enough away from the site that they would not be subjected to the seismic loadings and still be transported to the site within 72 hours. As a result, the purpose of the installed post 72 hour SSCs is to provide reasonable assurance that they will be available within 72 hours of a seismic event and thereby reduce the need to resort to the offsite SSCs. The identification of the SSCs that require the seismic C-II designation has been performed using the deterministic and probabilistic methods described in Section 5.9. Because of this limited purpose the seismic C-II requirements are applied as follows:
    - For SSCs that are inherently rugged, such as pumps (Passive containment cooling system (PCS) recirculation pumps), diesel generators (Ancillary Diesel Generator), pressure vessels, or piping/valves, the only requirements are that their building is seismic C-II and the connection to the building is as strong as the building.
    - For less rugged SSCs such as large atmospheric storage tanks (Ancillary Water Storage Tank), the SSC itself will be classified as seismic C-II and will be analysed for the seismic loads.
- Where seismic C-II/I conditions exist, as described in Section 5.5.4.

5.5.3 Seismic Categorisation of Class 3 Systems, Structures, and Components

Class 3 SSCs are generally categorised as NNS; however, seismic C-II designations are applied where seismic C-II/I conditions exist, as described in Section 5.5.4.

5.5.4 Seismic Category II/I

If the failure of the integrity of an SSC in the event of a seismic event can result in an unacceptable interaction with a Class 1 SSC or an incapacitating injury to occupants of the control room, the SSCs are designated as seismic C-II/I (II over I).

Seismic C-II/I is associated with the support or anchorage of SSCs and assigned as a function of plant layout. Analyses are performed in accordance with the AP1000 Design Criteria for Protection from Seismic Interaction (Reference 5.3) on a system level and do not reflect SSC design requirements. Therefore, the application of the seismic C-II/I is not required to be reflected in SSC material and equipment specifications and procurement documentation other than the SSC supports or anchors themselves.

The requirements of seismic C-II/I are superseded by those of the seismic C-I designation, which applies to both integrity and functional requirements. Therefore, the seismic C-II/I designation does not apply to Class 1 SSCs.

5.6 Limits and Conditions

The design of the AP1000 plant includes consideration for a broad spectrum of plant-level

events to protect the health, safety, and welfare of the public to a level that is as low as reasonably practicable (ALARP). To ensure the operation of the plant is consistent with the safety case, limits and conditions are required. Application of the safety case limits and conditions will be completed during design and operating phases of plant life through the development and implementation of Operating Rules (ORs).
This section provides the description of the AP1000 ORs, the methodology for development, and the process for transition into the operating phase. ORs are a dynamic set of limits and conditions for plant operation that will be subject to plant-specific development and ongoing maintenance and upkeep over plant life. Therefore, this section does not present the final complement of ORs, as this will be the ultimate responsibility of the licensee during nuclear site licensing. Rather, this section will describe processes, identify key references and supporting documentation, and demonstrate adequacy of the AP1000 ORs for safe operation of the plant.

This section is intended to provide a high-level description of the considerations taken into account in the development of the AP1000 ORs. The content will be organised in the following manner; first the overall AP1000 limits and conditions methodology will be described, including process flow diagrams. Afterwards, each OR will be described in detail including:

- a general description
- detail of interfaces between ORs
- discussion of the interface between the generic design assessment (GDA) review and Licensee actions

This process will demonstrate adequate limits and conditions have been, or will be, developed by means of the creation of ORs for safe operation of the plant. It should be noted that many ORs are site-specific, or will be customised at the discretion of the Licensee; therefore, site considerations to the ORs will be developed as a part of the nuclear site licensing process.

The limits and conditions process is described in Reference 5.25.

5.6.1 Background

This development of the AP1000 ORs provides a link between the analysis documented in the UK AP1000 safety case and the eventual limits and conditions it implies and requires for the plant to be operated in accordance with the safety case by the licensee. The key construct within the AP1000 plant safety case is based on fault studies, in particular the design basis (DB) assessments that rely on transient and other analyses to demonstrate that the dose goals are met consistent with the likelihood of the event.

These analyses make a number of assumptions relating to normal plant conditions and to the performance and reliability of SSCs provided in the design to prevent or mitigate DB events. These assumptions relate to safety analyses for all plant operating modes (operating states) and to all major sources of radioactivity (i.e., the reactor, spent fuel, and Radwaste) and constitute the limits and conditions that must be observed in order for the analyses to remain valid and applicable during the lifetime of the plant.

Arrangements for moving the UK AP1000 safety case to an operating regime require that all limits and conditions assumed in the safety analysis are captured, consolidated, and

prioritised in documentation and procedures used for plant operation, thus providing the link between the analysis documented in the safety case and eventual limits and conditions identified so that the licensee can operate the plant in accordance with the safety case.

As an integral part of the development of the standard design of the AP1000 plant, limits and conditions for operation are identified, documented, and included in the arrangements for transfer of information between the vendor and licensee for licensing and operation. Limits and conditions for the standard AP1000 design are used to validate that the operating conditions of the systems and reactor are within those analysed in their respective plant operating mode (Table 5-5).

5.6.2 Methodology

The approach for defining the required limits and conditions for safe operation of the AP1000 plant involves a three staged approach.

- Demonstration of safety case
- Evaluation of plant characteristics
- Development of AP1000 operating rules

These stages provide the framework for the Design Phase of the AP1000 plant.

5.6.2.1 Demonstration of Safety Case

The Demonstration of Safety Case stage is mainly comprised of the claims from the AP1000 fault and accident analysis as documented in PCSR Volume 3, which include DBA and PSA insights. The output of this stage of the process is identification of design requirements necessary to satisfy safety and functional performance goals.

It should be noted that there are various disciplines and analysis inputs that comprise the assessment, and the evaluation of limits and conditions is not intended to promote fault and accident analysis as the ultimate review of the adequacy of these parameters. Rather, fault and accident assessment represents an integrated view of the plant response to DB events and provides a convenient path to identify those parameters of significance that will be evaluated for inclusion into the ORs.

5.6.2.2 Evaluation of Plant Characteristics

The Evaluation of Plant Characteristics stage reviews many different characteristics identified as design requirements; i.e., “Safety & Functional Requirements”. This multi-faceted review ultimately results in the identification of plant parameters that are included in the AP1000 ORs. Characteristics reviewed for incorporation into the ORs include:

- Plant Geometry; e.g., critical dimensions
- Initial Conditions
- Fuel Design and Performance Parameters
- C&I Functions and Setpoints

- System Performance Characteristics

The limits and conditions that arise from the safety case are attributed to four (4) distinct groups:

- Initial or Bounding Conditions for Transient or Accident Analyses
- Consequences of Abnormal Events
- SSC Performance
- SSC Availability or Integrity

Development of the AP1000 ORs necessitates the review of the plant characteristics with regard to each group for consideration.

5.6.2.2.1 Initial or Boundary Conditions for Transient or Accident Analyses

The transient analyses performed as part of the DB analysis and PSA make a number of assumptions concerning initial and boundary conditions. The validity of the safety case based on these analyses depends on the plant remaining within the operating envelope defined by these limits and conditions.

Examples of such limits and conditions are reactor pressure, containment temperature, etc.

5.6.2.2.2 Consequences of Abnormal Events

In some of the fault studies presented in the safety case, the assessed consequences make assumptions about such plant characteristics as activity levels in parts of the system or fuel cladding condition. The validity of the consequence calculations, and hence compliance with dose targets, relies on the plant being operated within the envelope defined by these implied limits and conditions.

Examples of such limits and conditions are primary circuit activity levels and fuel operating limits, such as reactor coolant flow, reactor coolant loop pressure, core power shape limits, peak cladding temperature (PCT), and departure from nucleate boiling ratio (DNBR). In addition, there are limits and conditions related to safety limits and accident management derived from the severe accident assessment (SAA) and documented in plant emergency operating procedures (EOPs).

5.6.2.2.3 SSC Performance

The DB fault analyses presented in the safety case specify the operation of various SSCs within their design parameters to mitigate the effects of the transient in view. These design parameters constitute limits and conditions on the operation of the identified SSCs.

Examples of such limits and conditions are the temperature, available volume, and boron concentration of the water in the core makeup tanks (CMTs), the available volume of water in the passive containment cooling water storage tank for containment cooling, or available water inventory in the spent fuel pool for spent fuel cooling.

5.6.2.2.4 SSC Availability or Integrity

The demonstration of compliance with probabilistic targets makes claims on the availability and integrity of risk-important SSCs identified in the safety case. Availability of SSCs is dominated by examination, maintenance, inspection, and testing (EMIT) activities and implies limits and conditions on such things as test intervals and repair times. Integrity is dominated by environmental effects such as load conditions, temperature, humidity, radiation levels, or chemistry effects such as pH or oxygen levels. The control of such environmental effects implies limits and conditions on the corresponding environmental parameters.

The latter consideration is particularly important for high integrity structural items such as the reactor pressure vessel. Limits and conditions relating to EMIT activities will provide the basis of the maintenance schedule for the plant.

5.6.2.3 Development of the AP1000 Operating Rules

The Development of the AP1000 ORs stage is grouped into six (6) categories that represent design phase products and ultimately facilitate transition to the operating phase. The ORs categories are:

- Design Transients (Loading Conditions)
- Fuel Design Requirements
- Operating Technical Specifications (OTS)
- Chemical and Radiochemical Specifications
- In-Service Inspection
- Periodic Testing (PT)

When evaluating any single plant parameter, it is possible that the parameter will apply to multiple groups since the operating phase controls may be representative of various functions, disciplines, or work streams. For example, the concentration of a hypothetical chemical parameter may be a consideration for fuel design and core operation (Fuel Design Requirements), require an administrative control in the main control room (MCR) OTS, and input into a chemistry programme trend or action level (Chemical and Radiochemical Specifications). It is expected that a plant parameter will apply to multiple OR categories with an increase in complexity or safety significance.

5.6.2.3.1 Interfaces Amongst Operating Rule Groups

As plant parameters may be applicable to multiple categories of the ORs as a function of their disciplinary interfaces and complexity, it is expected that these categories of the ORs formally interface to preserve these ties and reduce the likelihood of incomplete application of the associated limits and conditions. The OTS represent the primary operator interface document and thereby contains the majority of these programmatic controls.

Examples of these interfaces are listed below:

- Surveillance Requirements (SRs)

- Administrative Programs
- Maintenance Programme and Clearance Process
- Operating Procedures

5.6.3 Operating Technical Specifications (OTS)

5.6.3.1 AP1000 Plant Application

The AP1000 plant design applies passive safety design principles as the primary means to protect the health, safety, and welfare of the plant workers and the public. Active SSCs are also used in the plant design and provide first-actuation support prior to the operation of the passive features in completion of safety functions. Therefore, the development of the OTS for the AP1000 must reflect the application of passive and active technologies consistent with the plant safety case.

To reflect the distinction between primary SSCs (Class 1), and supporting SSCs (Class 2 and Class 3), the AP1000 OTS will be maintained by the Licensee in tiers:

- Tier 1 Technical Specifications (TS)
- Tier 2 Technical Requirements Manual (TRM)
- Tier 3 General Availability Controls (GAC)

While TS are typical of conventional applications, the TRM and GAC will be characterised by less restrictive action completion times and fewer surveillance requirements consistent with the role of these SSCs in the AP1000 plant safety case.

Criteria for the TRM will reflect a combination of deterministic and probabilistic methods and will include considerations for defence in depth (DID) functions, post-72 hour operations, and severe accident conditions.

Criteria for the GAC will reflect deterministic, probabilistic, programmatic, and operating experience-based methods and will include considerations for normal plant operational conditions and the operation of Class 3 SSCs.

Due to potential for overlapping scope, commonality between DID and normal operating systems, and the lack of a primary safety function or required support function within the scope, the Licensee may opt to physically locate the TRM and GAC content within the same volume for ease of use by operators.

5.6.3.2 General Principles

The OTS align with other portions of the ORs and typically serve the role of interface control with the MCR for critical functions or those with a high-level of complexity. The objective of OTS is to identify limits and conditions to ensure that normal operation of the reactor remains consistent with the safety case. Accordingly, the OTS are assembled with the following attributes:

- Normal operating limits and conditions for critical plant parameters and associated SSCs, referred to as Limiting Conditions for Operation (LCOs)

- Applicability of the operating limit or condition based on plant operating mode
- Action requirements applicable in the event a normal operating limit or condition is exceeded.
- SRs to ensure the corresponding LCO is satisfied.

5.6.3.3 Technical Specification Selection Criteria

As discussed in Section 5.6.2, plant parameters are screened for inclusion to the ORs. Subsequently, these parameters are reviewed for inclusion into the OTS. It should be clarified that a plant parameter that is selected for the ORs will be included in at least one of the OR categories; there is no general requirement that a plant parameter be present in the OTS as these parameters are subject to an application-specific criteria.

Application of the TS selection criteria allows for the identification of applicable parameters and those SSCs required to fulfil the operating requirements. The selection criteria is applied to each operating mode to cover the range of normal plant operation.

Criterion #1

Installed instrumentation that is used to detect, and indicate in the control room, a significant abnormal degradation of the reactor coolant pressure boundary.

Criterion #2

A process variable, design feature, or operating restriction that is an initial condition of a design basis fault or accident analysis that either assumes the failure of, or presents a challenge to, the integrity of a fission product barrier.

Criterion #3

A SSC that is part of the primary success path and which functions or actuates to mitigate a design basis fault or accident that either assumes the failure of, or presents a challenge to, the integrity of a fission product barrier.

Criterion #4

A structure, system, or component which operating experience or probabilistic safety assessment has shown to be significant to public health and safety.

5.6.3.4 Technical Requirements Manual Selection Criteria

TRM content is selected using a combination of deterministic and probabilistic criteria consistent with Appendix A of the AP1000 UK safety categorisation and classification methodology (Reference 5.2); this includes consideration of the assessment of non-Class 1 SSCs (Section 5.9.1.1) and the reliability assurance programme (Section 5.9.1.2). The criteria for TS is generally applicable, especially Criterion 4, to the selection of TRM controls, with a focus on the role of the SSC as a supporting function.

Attributes considered in the TRM selection include:

- Backup long-term plant shutdown support (Post-72 hour operation)
- SSCs that do not meet the TS risk-important criteria but do have some risk importance. This criteria applies to both core melt prevention and core melt mitigation functions.

5.6.3.5 General Availability Control Selection Criteria

GAC content is selected using a combination of deterministic, probabilistic, programmatic, and operating experience-based criteria. As the GAC is a supporting third-tier availability control, the rigour applied to the operating limitations, remedial actions, and surveillances is correspondingly reduced. Typically, GAC items consist of condition-based assessments (e.g., equipment availability) using a broad spectrum of surveillance techniques, such as instrumentation, alarms, routine EMIT tasks, and operator observations.

Examples of design features typical of GAC inclusion are:

- Fire protection programme availability controls
- Normal operating non-Class 1 ventilation functions; area temperature monitoring
- Operation of significant Class 3 SSCs
- Offsite emergency response facilities

5.6.3.6 Applicability of Limiting Conditions for Operation

The OTS criteria is applied to each plant operating mode consistent with the evaluation of DB events in the safety case. Operating modes are consistent across the plant design, as defined in Section 5.6.1.

Due to the physical nature of the plant design and the design attributes of the associated SSCs, many design features are not applicable to all operating modes; for example, passive residual heat removal (PRHR) requires a sufficient thermal gradient to produce the passive natural circulation, and therefore, is not applicable to operating modes with low temperature reactor coolant and the RCS open (e.g., refuelling).

5.6.3.7 Actions Required when Inoperable

Operability is defined as the capability of a SSC of performing its specified safety function(s). This definition considers the function of all necessary controls, instrumentation, normal or emergency electrical power, cooling and seal water, lubrication, and other auxiliary equipment that are required for the SSC to perform its specified safety function(s).

As a by-product of identifying LCOs for SSCs required to complete safety functions, the OTS process necessitates the identification of specific remedial actions in the case that the normal operating limits are exceeded; this condition is referred to as inoperable.

For each LCO, actions and completion times are defined. Actions and completion times are defined so that the plant can be maintained in a slightly degraded condition without compromising plant safety. Completion times are derived using deterministic and

probabilistic considerations. The speicified consequences of not meeting completion times varies with the safety significance of the OTS; for TS the plant is usually required to shutdown but for TRM and GAC the plant is allowed to continue operation.

For many functions, the allocation of redundant SSCs and completion time allocation is performed with consideration for regular EMIT activities. These considerations are maximized to the greatest extent practical to enable EMIT activities during normal operation and to minimize the number of activities required to be performed during shutdown operating modes.

5.6.3.8 Surveillance Requirements

SRs are requirements relating to monitoring, test, calibration, or inspections to ensure that the necessary quality of SSCs is maintained, that the facility operation will be within safety limits, and that the LCO will be met. Within the OTS, LCOs are provided with corresponding SRs that provide a prescriptive review of the plant condition for compliance with the associated LCO. Surveillances are discrete checks of compliance with the corresponding limit or condition. Failure of a surveillance indicates an inoperable condition and prompts application of the required actions.

Surveillances are used as a means of routine LCO compliance, with the frequency of the task based on the significance of the parameter, the predicted reliability of the SSC, and operating limitations imposed on the SSCs by the mode of plant operation.

Surveillances are not the sole means of inoperability identification. Operator indications, SSC performance, alarms, maintenance activities, plant conditions, and other viable sources of information are all means of entry into an LCO if the function of the SSCs can be affected.

SRs are considered a form of PT per Section 5.6.8.

5.6.3.9 Operating Technical Specifications Bases

Within the tiers of the OTS, the LCOs, SRs, remedial actions, and completion times should have a documented bases. Bases should at a minimum address the following considerations and appropriate references to support the control.

- What is the justification for the plant parameter’s inclusion into the OTS?
- What are the bases for each LCO?
- What are the reasons for the operating mode applicability of the LCO?
- What are the bases for each remedial action?
- What are the bases for each SR and the associated frequency?

The level of documentation for an OTS parameter is managed commensurate with the tier of the control.

5.6.3.10 Interfaces with other Operating Rules

Figure 5-2 shows the OTS OR Interfaces. The interfaces are described within this section.

5.6.3.10.1 Administrative Controls

The AP1000 plant design has placed selected administrative controls within the scope of the OTS due to the importance to the plant safety case (e.g., administrative programs) or to the formal operation of the plant and interface with the public and the regulator (e.g., responsibilities and organisation).

The key programs and reporting requirements:

- Offsite Dose Calculation Manual (ODCM)
- Radioactive Effluent Control Programme (RECP)
- Inservice Testing (IST) Programme
- Steam Generator (SG) Programme
- Secondary Water Chemistry Programme
- Containment Leakage Rate Testing Programme
- Component Cyclic or Transient Limit Programme
- System Level Operability Testing Programme
- Battery Monitoring and Maintenance Programme
- MCR Envelope Habitability Programme
- Ventilation Filter Testing Programme (VFTP)
- Core Operating Limits Report (COLR)
- RCS Pressure And Temperature Limits Report (PTLR)

Several of these controls are implemented by the plant operators within the MCR and under the direction of the OTS. These include:

- Safety Function Determination Programme (SFDP)

  The SFDP is an administrative control that directs the plant operators to assess the integral effect of unavailable or inoperable equipment on the plant by reviewing individual component failure for support system interactions with Class 1 functions. For example, the failure of a Class 1 direct current (dc) battery will yield the associated Class 1 SSCs unavailable to reposition if they do not fail to their safety state (i.e., motor-operated valves).

- Setpoint Programme (SP)

  The Setpoint Programme is the administrative mechanism for documentation and control of the limiting safety analysis limits, allocation of channel and setpoint statistical uncertainty, and nominal setpoint values applied to automatic Class 1 protection devices. The SP is the interface mechanism between fault and accident analysis, plant operation, and the site maintenance programme.

Finalisation and implementation of administrative controls are the responsibility of the Licensee. The OTS and associated administrative control procedures will comply with the relevant Licence Conditions (LCs).

5.6.3.10.2 Design Transients (Loading Conditions)

The OTS interfaces with the Design Transients OR through Administrative Controls.

- Component Cyclic or Transient Limit Programme

  The purpose of this administrative control is to catalogue the quantity of design transient (loading conditions) applied to Class 1 SSCs over the course of plant life to ensure the plant is continuously operated consistent with the Class 1 component design requirements and analyses.

- RCS Pressure And PTLR

  Consistent with the quantity of cycling imposed on Class 1 SSCs, consideration for material behaviours throughout the entire operating range of process conditions must be accounted for consistent with the SSC design analyses. The RCS pressure and PTLR formally documents operating limitations on the rate of change in temperature, the maximum operating pressure for a given system temperature, and the operating conditions of the low temperature overpressure protection devices to maintain compliance with ASME Code requirements.

5.6.3.10.3 Fuel Design Requirements

The OTS interfaces with the Fuel Design Requirements OR to maintain alignment between the nuclear and thermal-hydraulic design of the core design for each fuel cycle with the operating limits and controls applied in the OTS.

- COLR

  The COLR is an administrative control that is discussed in Section 5.6.5. The purpose of the COLR is to document those operating limits that must be incorporated into the OTS to ensure that the plant is operated consistent with the limiting fault and accident analyses for the duration of the fuel cycle to prevent fuel damage or DNBR. Since the core design changes each refuelling interval, the COLR is cycle-specific and the controlling operating limits must be reaffirmed reflecting the operating core configuration.

- Core Physics Testing

  To confirm the core analyses are valid, confirm refuelling activities are consistent with the cycle fuel design, and identify fuel anomalies and reactivity deviations, AP1000 plant reactor cores are subjected to physics testing during plant startup and following every refuelling operation. The completion of these physics tests do not reduce or challenge plant safety during execution and are reflected in the OTS so that the testing does not result in an inoperable condition.

Due to their unique nature, core physics testing is the subject of specific written procedures that address the required plant configuration and compliance with applicable OTS conditions.

5.6.3.10.4 Chemical and Radiochemical Specification

The OTS interfaces with the Chemistry and Radiochemistry Specifications OR to ensure the primary, secondary, and auxiliary fluid chemistries are maintained consistent with design requirements, best industry practices, and limiting fault and accident analysis assumptions.

- ODCM

  The ODCM contains the methodology and parameters used in the calculation of offsite doses resulting from radioactive gaseous and liquid effluents, in the calculation of gaseous and liquid effluent monitoring alarm and trip setpoints, and in the conduct of the radiological environmental monitoring programme. Additionally, the ODCM also contains the radioactive effluent controls and radiological environmental monitoring activities, and descriptions of the information that should be included in the site environmental and effluent reporting as required by site LCs.

- RECP

  The RECP is an administrative control applied to control radioactive effluents and for maintaining the doses to members of the public from radioactive effluents as low as reasonably achievable. The programme is contained in the ODCM, implemented by procedures, and includes remedial actions to be taken whenever the programme limits are exceeded.

  The RECP includes limitations on the capability of radioactive waste processing systems, limitations on radiological concentrations and dose, and the associated monitoring requirements.

- Secondary Water Chemistry Programme

  The secondary water chemistry programme is an administrative control applied to control and monitor secondary water chemistry to inhibit SG tube degradation and low pressure turbine disc stress corrosion cracking. Implementation of the programme includes defined process limits, monitoring provisions, and action requirements. The programme is consistent with process description and OR implementation discussed in Section 5.6.6.

- Radiation and Chemistry Limits

  The control and monitoring of both primary and secondary chemistry is a complex task that represents an interface between the OTS and the Chemical and Radiochemical Specifications categories of the ORs.

  Critical chemical input parameters used in the determination of dose assessment are contained in the OTS; e.g., primary and secondary specific activity levels. A broader scope of chemical and radiochemical controls are implemented through specific chemical and radiochemical specification documents, which are discussed in Section 5.6.6.

5.6.3.10.5 In-Service Inspection

The OTS interfaces with the In-service Inspection (ISI) OR to ensure the scope of the ISI reflects specific administrative requirements and that the overall plant conditions are acceptable for ISI activities.

- SG Programme

  The SG Programme is an administrative control applied to ensure that SG tube integrity is maintained, as the SG tube are a primary pressure boundary component. A specific control is required for the SG due to its unique nature, operating experience, and specialised inspection techniques. Inspection of SG tubes is performed as part of the ISI process.

- Plant Conditions for ISI

  The ISI OR is responsible for creation of procedures to control ISI tasks; these procedures shall consider the OTS for coordination of SSC accessibility and inspection technique selection, especially when ISI techniques require the SSCs being inspected to be inoperable. ISI is discussed in Section 5.6.7.

5.6.3.10.6 Periodic Testing (PT)

The OTS interfaces with the PT OR to coordinate required EMIT activities and ensure that the plant operation is maintained with operating limitations, even in alternate alignments or with SSCs taken out of service.

- IST Programme

  The IST programme is an administrative control applied to Safety Class 1 SSCs designed to Section III of the ASME Code. The administration of the IST programme is in accordance with the requirements of the ASME OM Code (Reference 5.21).

  Coordination is required with the OTS to ensure system alignments for IST activities do not unacceptably inhibit required safety functions. This is facilitated through alignment with the OTS SFDP as discussed above.

- Containment Leakage Rate Testing Programme

  A key assumption in the AP1000 plant fault and accident analyses are the integrity of the fission product barriers. The Containment integrity is especially critical in the calculation of worker and public doses for events that release activity into the containment. Therefore, the Containment Leakage Rate Testing Programme is required to routinely survey the Containment and its penetration assemblies to ensure that the leakage assumptions remain valid during plant life.

- Battery Monitoring and Maintenance Programme

  Due to the role and importance of the Class 1 batteries in the AP1000 plant fault and accident analyses, an administrative control is recommended to ensure the batteries are maintained consistent with governing codes and standards.

- MCR Envelope Habitability Programme

  MCR Envelope Habitability is required to protect the plant operators such that the MCR occupants can control the reactor safely under normal conditions and maintain it in a safe condition following a radiological event, hazardous chemical release, or a smoke challenge. The programme shall ensure that adequate radiation protection is provided to permit access and occupancy of the MCR under design-basis fault and accident analysis conditions without personnel receiving radiation exposures in excess of regulatory limits.

Coordination is required with OTS to ensure alignment of plant equipment for EMIT activities is consistent with the plant safety design and to verify assumptions made in normal operating OTS controls for MCR integrity.

- VFTP

  Consistent with the MCR Envelope Habitability Testing programme, the Class 1 MCR ventilation system is provided with filtration capability consistent with MCR operator accident dose assessments. Therefore, a EMIT function is required to test and replace these filters to maintain compliance with the governing assumptions.

- System-Level Operability Testing Programme

  Operability testing requirements in addition to component-level IST requirements are provided to verify that the passive safety features will operate consistent with their corresponding fault and accident analyses.

  The system level operability testing is coordinated with the OTS and documented as a SR for the affected safety functions, these include

  - Passive Containment Cooling
  - Passive Core Cooling
    - Accumulators
    - Core Makeup Tanks
    - PRHR
    - In-Containment Refuelling Water Storage Tank
    - Containment Recirculation (Long-term Core Cooling)
  - Main Control Room Habitability

- SRs

  As discussed in Section 5.6.3.7, each OTS LCO is identified with accompanying SRs, including actions and frequencies, that are implemented to provide a means of confirming the plant is being operated within the limits of the corresponding LCO. These SRs are considered periodic tests and are further discussed in Section 5.6.8.

- Plant Conditions for PT

  Coordination between the OTS and PT is required such that procedures to control PT activities account for SSC availability in accordance with applicable plant limits and conditions. This ensures that PT tasks are performed with the plant aligned with the AP1000 safety case. PT is discussed in Section 5.6.8.

5.6.3.10.7 GDA/Licensee Interface

The following items represent the interface between the scope of the AP1000 plant GDA and the Licensee submittal process for nuclear site licensing (NSL); it is anticipated that the licensee will adopt and develop these provisions in the implementation of site ORs.

- Generic plant parameters, associated limits and conditions, and associated SSCs comprising the Class 1 TS portion of the OTS will be presented to the Licensee (Reference 5.22). The Licensee will be responsible for the verification of the site application of the Class 1 TS and certification of the actions and completion times.
- Generic plant parameters, associated limits and conditions and associated SSCs comprising the Class 2TRM portion of the OTS will be presented to the Licensee (Reference 5.23). The Licensee is responsible for the verification of the site application of the Class 2 TRM and certification of the actions and completion times.
- Suggested administrative controls, programs, and reporting requirements are contained in the TS portion of the OTS. The final complement, development, and implementation of these administrative provisions are within the scope of the Licensee consistent with relevant License Conditions.
- The implementation of the OTS as described herein will be at the discretion of the Licensee and required to satisfy relevant License Conditions for the applicable units. Detailed development of the OTS and the interfacing documentation is within the scope of the Licensee.

5.6.4 Design Transients (Loading Conditions)

Pressurised Class 1 SSCs are designed in accordance with Section III of the ASME Boiler and Pressure Vessel Code (ASME Code, Reference 5.24), including consideration for evaluation of stress and fatigue behaviours (only Class 1 pressure boundaries are evaluated for fatigue on the AP1000 design). For these pressurised systems, five operating conditions are defined in the ASME Code and are considered for the design of the associated systems, including RCS components, auxiliary components, RCS component supports, and reactor internals. These five operating conditions follow:

- Level A Service Conditions – (Normal Conditions)
- Level B Service Conditions – (Upset Conditions, Incidents of Moderate Frequency)
- Level C Service Conditions – (Emergency Conditions, Infrequent Incidents)
- Level D Service Conditions – (Faulted Conditions, Limiting Faults)
- Testing Conditions

5.6.4.1 Interface with other Operating Rules

Figure 5-3 shows the Design Transients OR Interfaces. The interfaces are described within this section.

5.6.4.1.1 Fuel Design Requirements

The Design Transients interfaces with the Fuel Design Requirements OR in the form of a design input for core reload evaluation. The design of and operation of a fuel cycle is fundamentally limited by the nuclear and thermal-hydraulic capabilities of the fuel assemblies in response to normal, abnormal, and accident sequences. The Design Transient interface

provides required conditions and loading conditions for consideration in the reactor core design for compliance with the fault and accident analyses.

5.6.4.1.2 Operating Technical Specifications

Refer to Section 5.6.3.10.2

5.6.4.1.3 Chemical and Radiochemical Specifications

The interface with the Chemical and Radiochemical Specification OR is an input for programme planning and creation of procedures and processes. Changes in plant state typically result in, or require, a change in chemistry. These changes can be realised in the form of required modification to, or increased monitoring of, critical chemical parameters. Accordingly, the processing of fluids and changes in plant gaseous and liquid effluent may be affected.

5.6.4.1.4 In-Service Inspection (ISI)

The AP1000 plant ISI OR implements the provisions of Section XI of the ASME Code to pressure-retaining Class 1 SSCs. An interface with design transients is required as an input as the frequency of inspections, planning for ISI intervals, assessment of defects, and evaluation of repairs must consider the cyclic loading impact in the associated programme documentation and procedures.

5.6.4.1.5 Periodic Testing

There is no identified OR interface with Periodic Testing.

5.6.4.2 GDA/Licensee Interface

The Licensee will be provided an index of design transients and the associated number of occurrences considered in the mechanical design of the AP1000 plant Class 1 components. This index is consistent with those used in the evaluation of RCS Class 1 components in the AP1000 Structural Integrity assessment in Chapter 20.

The design transient document, coupled with the service conditions and component loading conditions constitute the interface documentation required for the Licensee to establish a cycle and transient monitoring programme for the purpose of recording the actual plant performance against the mechanical input assumptions used in the design of the Class 1 components and to ensure that the number of occurrences is not exceeded during plant life.

5.6.5 Fuel Design Requirements

The nuclear and thermal design of the AP1000 fuel is described in detail in Chapter 22.

- A detailed description of the AP1000 fuel system design consistent with the safety case is presented in Section 22.5.

- The process for the nuclear design of the AP1000 reactor core is described in Section 22.6
- The thermal-hydraulic design of the AP1000 reactor core is described in Section 22.7

Discussion in this section will be limited to the incorporation of the fuel design requirements into the operating phase and the coordination with the other ORs.

5.6.5.1 Operating Constraints

As summarised in Chapter 22, the AP1000 plant fuel system design is required to consider the broad scope of design basis events in the nuclear and thermal-hydraulic design of the core for each fuel cycle.

Specific operating limits and conditions that apply to the reactor directly interface with the OTS by means of the COLR, as required per the OTS Administrative Controls.

The COLR, along with the fuel management report for the associated cycle, document the operating limits that satisfy the plant safety analyses on a cycle-by-cycle basis; thereby validating the safety case.

5.6.5.2 Interface with other Operating Rules

Figure 5-4 shows the Fuel Design Requirements OR Interfaces. The interfaces are described within this section.

5.6.5.2.1 Design Transients (Loading Conditions)

Refer to Section 5.6.4.1.1

5.6.5.2.2 Operating Technical Specifications

Refer to Section 5.6.3.10.3

5.6.5.2.3 Chemical and Radiochemical Specifications

The Fuel Design Requirement OR section provides a critical input to the implementation of the Chemical and Radiochemical Specifications. Specifically, the design of the reactor core provides the following inputs:

- Primary Coolant Chemistry Requirements

  The design of the fuel assemblies account for nuclear and thermal-hydraulic effects, but the design must also consider the long-term chemical effects on the integrity of the first fission product barrier. Maximum chemical concentrations are identified in fuel performance documentation, which is supplier specific and finalised by the site Licensee.

- Fuel Management Report

  Accompanying the COLR, each reactor core is provided with a fuel management report that details design feature of the respective core design, including the cycle boron profile. The boron profile is used by plant operators to control the chemical content of the

primary circuit and verify operations are consistent with the reactor core design for the total fuel cycle.

5.6.5.2.4 In-Service Inspection

There is no identified OR interface with ISI.

5.6.5.2.5 Periodic Testing

Periodic testing encompasses an array of EMIT tasks that are applied to demonstrate the plant is operated and maintained in accordance with the plant safety case. EMIT activities include those that support refuelling, including fuel loading verification and core physics testing. These activities require input from the COLR and the fuel management report.

5.6.5.3 GDA/Licensee Interface

The Licensee will be provided a COLR and Fuel Management Report for the first cycle of each unit. These documents will be produced during the site licensing phase, as they are specific to a core design; it is anticipated that the licensee will adopt and develop these provisions in the implementation of site ORs.

The Licensee will be responsible for implementation of the COLR limits into the associated OTS.

5.6.6 Chemical and Radiochemical Specifications

5.6.6.1 Chemistry

The chemistry functions in the AP1000 plant are dealt with under three headings: primary system, secondary system, and auxiliary systems. The essential safety requirements of the chemistry, the various physical systems, and their design basis functions are described in Chapter 21.

Chapter 21 demonstrates compliance with the chemistry safety requirements for each operational mode of the AP1000 plant. This includes a description of the chemistry strategy and the standards that are applied. The chemical aspects of accident scenarios, the potential hazards and the hazard mitigation measures, are also discussed.

Pertinent PCSR sections that support this OR are:

- Primary Circuit (Section 21.5)
- Secondary Circuit (Section 21.6)
- Auxiliary Water Systems (Section 21.7)
- Operating Strategies (Section 21.8)
- Accident Chemistry (Section 21.9)

5.6.6.2 Radiochemistry

During normal operating conditions the following radiochemical control parameters are included in the OTS for alignment with fission product barrier design and dose assessment. Radiochemical analysis, monitoring provisions, and associated action levels are controlled by the programme outlined in Chapter 21.

5.6.6.2.1 Fuel Cladding (First Fission Product Barrier)

- Reactor coolant Iodine-131 (I-131) activity levels shall be controlled to a concentration, whereby, it would produce the committed effective dose equivalent to the quantity and isotopic mixture of iodine isotopes actually present in the coolant consistent with the safety case. This operating limit is imposed as Iodine isotopes contributed to the analysed onsite and offsite dose assessments.
- Levels of Xenon-133 (Xe-133) shall be less than a level that would produce the effective dose equivalent to the quantity and isotopic mixture of noble gases present in the reactor coolant consistent with the safety case. This operating limit is imposed as Xenon isotopes contributed to the analysed onsite and offsite dose assessments.
- The I-131 activity and ratio of I-131 and I-135 isotopes are applied as a practical approach to determine the health of the fuel cladding during normal power operation.

5.6.6.2.2 Reactor Coolant Pressure Boundary (Second Fission Product Barrier)

- The integrity of the RCS piping within the Containment (Third Fission Product Barrier) is ensured through the monitoring and limitation on leakage. Leakage is detected by diverse means of liquid collection and airborne radiation monitoring.
- RCS leakage into the secondary circuit through the SGs is continuously monitored and limited to reduce the consequences of plant transients. Leakage rates are applied in the determination of potential onsite and offsite dose assessments.
- SG dose equivalent I-131 levels shall be controlled to a concentration that consistent with the safety case and associated onsite and offsite dose assessments.

5.6.6.3 Interface with other Operating Rules

Figure 5-5 shows the Chemical and Radiochemical OR Interfaces. The interfaces are described within this section.

5.6.6.3.1 Design Transients (Loading Conditions)

Refer to Section 5.6.4.1.3

5.6.6.3.2 Fuel Design Requirements

Refer to Section 5.6.5.2.3

5.6.6.3.3 Operating Technical Specifications

Refer to Section 5.6.3.10.4

5.6.6.3.4 In-Service Inspection

There is no identified OR interface with In-Service Inspection.

5.6.6.3.5 Periodic Testing

The execution of the Chemical and Radiochemical Specifications require corresponding EMIT activities to be performed to verify compliance with prescribed chemical limits. Activities are comprised of:

- Routine sampling in accordance with the site chemistry programme
- Chemistry controls per approved chemistry procedures
- OTS SRs

5.6.6.4 GDA/Licensee Interface

In substantiation of AP1000 plant safety case claims, radiochemical limitations and fission product barrier integrity requirements will be defined. Generic AP1000 plant chemistry recommendations are provided as described in Chapter 21.

The Licensee is responsible for development and implementation of the plant Chemistry programme, a process that manages the monitoring and control of chemical parameters. The Chemistry programme will require procedures for chemical control, definition of action levels, and requisite completion times for when a threshold is exceeded.

5.6.7 In-Service Inspection (ISI)

The ISI OR is comprised of two facets; Pre-Service Inspection (PSI) of the plant prior to fuel load, and ISI of the plant during the operating life. The operation of the AP1000 plant requires inspection of Class 1 SSCs to confirm pressure boundary material conditions. The plant ISI programme provides the guidance for these examinations as well as processes for characterisation, repair, mitigation, and justification of defects identified by the inspection processes. An effective ISI programme ensures:

- The plant has been constructed consistent with the design requirements and that the integrity of Class 1 pressure retaining components is in alignment with the safety case.
- The safety of the plant is not adversely affected after the commencement of operation and throughout the operating lifetime of the plant.
- The levels of reliability and availability of all plant SSCs remain in accordance with the assumptions and intent of the design and, consequently, a cost effective electricity generation is guaranteed.

PSI is an ISI interval required to be completed prior to fuel load for the purpose of confirming acceptable material conditions prior to operation and in order to develop inspection baselines for lifetime ISI intervals.

ISI is a preventive maintenance inspection programme utilizing non-destructive examinations (NDE) for Class 1 pressure retaining SSCs.

5.6.7.1 Programme Requirements

The AP1000 plant ISI programme will be developed for the UK AP1000 plant in accordance with Section XI of the ASME Boiler and Pressure Vessel Code.

Additional considerations shall be incorporated in the development of the plant ISI programme based on the content of the AP1000 Structural Integrity assessment in Chapter 20; the Structural Integrity assessment imposes additional inspection and quality requirement for Class 1 SSCs classified as high-integrity (HI) or high safety significance (HSS).

5.6.7.2 Interface with other Operating Rules

Figure 5-6 shows the ISI OR Interfaces. The interfaces are described within this section.

5.6.7.2.1 Design Transients (Loading Conditions)

Refer to Section 5.6.4.1.4

5.6.7.2.2 Fuel Design Requirements

There is no identified OR interface with Fuel Design Requirements

5.6.7.2.3 Operating Technical Specifications

Refer to Section 5.6.3.10.5

5.6.7.2.4 Chemical and Radiochemical Specifications

There is no identified OR interface with Chemical and Radiochemical Specifications.

5.6.7.2.5 Periodic Testing

The execution of ISI activities are, by definition, EMIT activities. Although the programme planning, criteria, and procedures are contained within the ISI OR section, interface with Periodic Testing is required to ensure that work planning and the overall effect of the inspection activities on the plant are captured and controlled to within plant operating limits.

5.6.7.3 GDA/Licensee Interface

The safety case identifies the bases for the ISI programme (including PSI requirements) through adherence of Section XI of the ASME Code. The safety case confirms that equipment accessibility has been accounted for in the AP1000 design such that the required ISI is feasible. Finally, supplemental inspection requirements resulting from the AP1000 plant structural integrity assessment in Chapter 20 may be applicable to the scope of the ISI.

The detailed ISI programme will be defined by the Licensee during site licensing activities.

5.6.8 Periodic Testing

Periodic Tests are EMIT activities identified in the plant ORs and implemented in the plant operating documentation that provide assurance that the plant is operated consistent with the governing limits and conditions contained in the plant safety case.

5.6.8.1 General Principles

PTs are denoted in the AP1000 design and operating documentation as either of two (2) types:

- Surveillance Testing – Periodic tests performed to satisfy OTS SRs in order to demonstrate the plant is being operated within the LCO (See Section 5.6.3.8).
- Routine Testing – Periodic tests performed to satisfy the testing requirements of other ORs or plant programmes. Examples of routine tests may include; auxiliary system chemistry sampling, IST of active components, or ISI.

Considerations into the general requirements for PT are included in the plant design since the design of safety functions has a direct impact on the quantity, type, and frequency of PT activities. Furthermore, optimisation of the PT requirements aligned to the ORs has a direct effect on plant availability, potential worker radiation exposure requirements, and plant safety during PT operational alignments. General considerations applied to the plant design include:

- Reduction of the number of active SSCs through the application of passive safety technologies, thereby directly reducing the amount of PT required over plant life.
- Designing systems, where applicable, for PT during the power generation operating mode.
- Consolidation of ORs, where applicable, to reduce duplicate PT requirements; for example, the alignment of OTS SRs with the IST programme for active valves.
- Review of the PSA and industry operating experience for PT activities that create a greater potential for a plant-level fault to occur; for example, the testing of Safety Class 1 steam generator isolation valves are performed during refuelling outages in lieu of at power due to operating experience with valve control problems and the associated high-likelihood of a reactor trip event.
- Automation of PT sequences through the use of display and automation technologies.

AP1000 safety features acknowledged in the plant fault and accident analysis review (See Section 5.6.2) represent the scope of SSCs and parameters subject to PT. Consistent with this review, parameters subject to PT may be either functional (e.g., assurance an active component can perform its credited safety function) or conditional (e.g., tank volumes or ambient temperatures).

A safety feature is not subject to PT if the function is normally in operation and monitored consistent with its safety function; for example, the normally operating main feedwater and main steam systems.

The coordination between safety functions and PT is defined within the interfacing OR categories.

5.6.8.2 PT Frequency

The frequency of PT may be either time or condition-based. The differentiation is typically associated with the accessibility of the equipment.

- Condition-Based – PT activities specified based on the plant operating conditions such as, Cold Shutdown, a refuelling cycle basis, or an ASME in-service interval.
- Time-Based – PT assigned a recurring schedule independent of plant condition; e.g., hourly, daily, etc.

Assignment of the PT frequency is subject to an application-specific review and incorporates consideration for several properties; including alignment with an OR, conformance with a governing code or standard, application of operating experience with component types and specific manufacturers, licensing commitments and regulatory requirements, and probabilistic insights.

Over the course of plant life, the frequency of PT activities will be continuously subject to review and optimisation as part of the Maintenance Programme's effectiveness review requirements.

5.6.8.3 Interface with other Operating Rules

Figure 5-7 shows the OTS OR Interfaces. The interfaces are described within this section. A comprehensive review of OR interfaces with Periodic Testing can be obtained by a review of Sections 5.6.3 through 5.6.7.

5.6.8.4 GDA/Licensee Interface

The interface between the AP1000 plant designer and the licensee is established as follows:

- Generic SRs aligned to the TS will be provided. The application of the TS is subject to validation by the Licensee during site licensing and review of affected LCs.
- A set of analysis documentation will be made available to the Licensee for use in the identification of TRM SRs and other routine tests.
- The Licensee is responsible for the implementation of the PT process and transitioning design limits and conditions into operating documentation.
- The GDA review of the AP1000 design does not include PT frequencies as these may be site-specific based on equipment supplied and reliability assumptions applied in site analyses.

5.6.9 Inclusion of Limits and Conditions into Plant Operating Documents

The limits and conditions identified in the above process are required to transition into the Operating Phase for the plant in the form of operating documentation. This documentation will provide the basis for OTS, procedures, SRs and EMIT schedules. However, it is

recognised that these documents can only be finalised by the plant operator as they are a requirement of the site licence.

To this end, the AP1000 limits and conditions process outlines the overall documentation plan and transition process (Figure 5-8). This process provides a 'roadmap' showing how the identified limits and conditions will be included in operating documents and used in the development of EMIT schedules. The generic plant design process will stop short of producing the documents themselves as they are the ultimate responsibility of the site licensee.

Westinghouse will provide the licensee with SSC evaluations to ensure that only suitably qualified and experienced persons (SQEPs) are identified to perform work associated with the EMIT of any SSCs as per interfacing LCs.

5.6.9.1 Procedures

Consistent with the Administrative Controls accompanying the TS as generic recommended practices, written procedures shall be established, implemented, and maintained for the following functions/purposes:

- Administrative Procedures
- Normal Operating Procedures
    - General Operating Procedures (GOPs)
    - System Operating Procedures (SOPs)
- Alarm Response Procedures (ARPs)
- Abnormal Operating Procedures (AOPs)
- Emergency Operating Procedures (EOPs)
- Post-72 Hour Operating Procedures
- Severe Accident Mitigation Guidelines (SAMGs)
- EMIT Procedures
    - Surveillance Tests
    - Control/Calibration of Measuring and Test Equipment
    - Maintenance Procedures (Mechanical, Electrical, and C&I)
    - Refuelling Procedures
- Programme Procedures
    - Containment Local and Integrated Leakage Rate Testing (LLRT/ILRT) Procedures
    - Chemical and Radiochemical Control
    - ISI Procedures
    - Fire Protection Programme Procedures

- Effluent and Environmental Monitoring Procedures

The ORs are inputs to the preparation of the operating procedures so that plant component manipulations, sequences of operation, and response to alarm conditions are consistent with applicable limits and conditions of operation. These plant manipulations account for planned EMIT or programme functions, as controlled through their respective documentation. Procedure interfaces are depicted in Figure 5-1 and Figure 5-8.

During emergency operation, many operating limits are no longer a practical control since the plant is in a dynamic state. In this condition, AOPs and EOPs are provided to ensure the plant responds to the transient condition consistent with the safety analyses. When the exit conditions of AOPs and EOPs are satisfied, the plant will be in a safe and stable condition and ORs can be implemented during recovery.

5.6.9.2 Examination, Maintenance, Inspections and Testing

The plant EMIT schedules are responsible for the planning, execution, documentation, and review of the completion of plant activities, as directed by and consistent with interfacing ORs. EMIT interfaces are depicted in the limit and condition process flowchart (Figure 5-1), and the phase transition flowchart (Figure 5-8).

EMIT schedules will be developed by the Licensee, applying maintenance programme policies and practices developed to support operation. Plant maintenance is characterised by the application of predictive (PdM), preventative (PM), and corrective maintenance (CM) tasks, where the term “plant maintenance” is used to represent the spectrum of EMIT activities. EMIT schedules will be developed consistent with the site-specific SSC requirements consistent with Chapter 15, Appendix 15A.

Predictive tasks are routine condition assessment EMIT activities used to confirm compliance with ORs, ascertain SSC operating condition and readiness, and adjust EMIT schedules to optimise EMIT efficiency and equipment availability.

Preventative tasks are routine EMIT activities that are applied to confirm compliance with associated ORs and ensure SSC reliability and availability are consistent with fault and accident analysis assumptions.

Corrective tasks are reactive EMIT activities that respond to deficient conditions. Interface with ORs is essential in the execution of corrective tasks to confirm limits and conditions are satisfied and that safety functions are maintained.

Examples of predictive/preventative tasks that will be included in the EMIT schedule include:

- Surveillance Testing
- Chemical and Radiochemical Monitoring and Control
- ISI & PSI
- IST
- Containment LLRT and ILRT
- Battery Monitoring and Maintenance
- MCR Habitability Monitoring and Maintenance

- Ventilation System Filter Testing
- System-Level Operability Testing

5.7 Operator Actions

In some DBAs and other accidents, there is sometimes a requirement that operators should perform certain actions, either to manually initiate or realign a system (for example, manually activating feed and bleed cooling) or for their own protection (for example, to evacuate on the activation of an area activity alarm). Note that in the AP1000 plant, the use of passive Class 1 systems has reduced the number and the importance of such operator actions.

In both of these cases, the required operator action will be the subject of or form part of written operating procedures, supported by appropriate training and review. The importance of these actions for safety will vary in exactly the same way as the importance of different SSCs for safety.

In the case of an action to manually initiate or realign a Class 1 system providing a Category A safety function, the importance of the operator action will be the same as the corresponding SSC being actuated or realigned. The same applies to an action that would protect an operator from a radiation dose in excess of the design basis limit of 20 mSv. In both these cases, the operator action has an importance equivalent to a Class 1 SSC.

Similarly, operator actions to manually initiate or realign a Class 2 system supporting a Category

A safety function or providing a Category B safety function would have the same importance for safety as a Class 2 SSC. The same applies to an operating action that would protect an operator from a radiation dose in excess of normal operating radiation dose limits but below the design basis limit of 20 mSv.

The AP1000 plant uses symptom-based operating procedures that guide the operator through various actions depending on the state of the plant. There are three different types of operating procedures: emergency operating procedures, abnormal operating procedures, and normal operating procedures, the latter having some subdivisions. For the purpose of classification, emergency and abnormal operating procedures are considered more relevant. Both are made up of a number of actions with different importance for safety. Therefore, any given procedure may contain actions with different classifications.

5.8 Equipment Qualification

The SSCs of the AP1000 plant are designed to operate in different environmental conditions (temperature, pressure, humidity, radiation fields) depending on their duty. As part of the overall design and safety assessment, SSCs will be qualified where appropriate for the environments in which they are required to operate.

For mechanical systems, the five operating conditions defined in ASME Code, Section III are considered for the design of the RCS Class 1 components, auxiliary Class 1 components, RCS component supports, and reactor internals. These five operating conditions follow:

- Level A Service Conditions – (Normal Conditions)
- Level B Service Conditions – (Upset Conditions, Incidents of Moderate Frequency)

- Level C Service Conditions – (Emergency Conditions, Infrequent Incidents)
- Level D Service Conditions – (Faulted Conditions, Limiting Faults)
- Testing Conditions

Westinghouse Quality Management provides assurances for the dynamic testing and analysis and IST programmes relating to component qualification in these conditions. Chapter 18 describes the seismic and dynamic qualification of Seismic C-I mechanical and electrical equipment.

Class 1 electrical equipment is tested under the environmental conditions expected to occur in the event of a DBE. This testing provides a high degree of confidence in the Class 1 system performance under the limiting environmental conditions.

Three basic standards form the basis of the qualification requirements and methodology used for the AP1000 plant equipment qualification:

- IEEE Standard 323-1974 (Reference 5.6) provides revised standards for equipment qualification that are endorsed by the relevant US Regulatory Guide. In particular, IEEE Standard 323-1974 highlighted the concept of ageing and provided the basis for the development of ageing methods.

- IEEE Standard 344-1987 (Reference. 5.7) provides specific treatment of seismic qualification.

- IEEE Standard 627-1980 (Reference 5.8) generalises the principles and technical guidance of IEEE 323 and IEEE 344-1987 to the qualification of Class 1E electrical and safety-related mechanical equipment.

Compliance with IEEE Standard 323-1974 and 344-1987 requirements is the specific means of compliance with the intent of IEEE Standard 627-1980 for safety-related electrical and mechanical equipment.

The methodology adopted for the AP1000 plant equipment qualification addresses the expanded scope of IEEE Standard 627-1980 and is developed using a number of other standards; details are provided in chapter 18.

This methodology defines a number of qualification criteria, methods, and environmental conditions that comply with the above standards and applies to all Class 1 and seismic C-I electrical and mechanical equipment plus certain monitoring equipment. Class 1 electrical and mechanical equipment is typically qualified using analysis, testing, or a combination of these methods. The specific method or methods used depend on the safety-related function of the equipment type to be qualified. Class 1 mechanical equipment, such as tanks and valves, is typically qualified by analysis, with supplementary functional testing when functional operability is demonstrated only through testing, as is the case for active valves. Either testing or testing combined with analysis is the method used for environmental and seismic qualification of Class 1 electrical equipment.

Chapter 18 of this PCSR identifies qualification methods used for the AP1000 plant to demonstrate the performance of Class 1 electrical and mechanical equipment when subjected to abnormal and accident environmental conditions, including loss of ventilation systems; feedwater line, steam line, and main coolant system breaks; and seismic events, and provides the expected conditions for various locations in the AP1000 plant. General requirements for

the development of plans/procedures/reports are also provided. Application of codes and standards for electrical equipment is described in Chapter 18 and in Reference 5.19.

Performance during abnormal environmental conditions, while not specifically designated as an industry or a regulatory qualification requirement, is also addressed by the methodology. Performance during normal service conditions is demonstrated by tests and inspections addressed by the equipment specification. Electromagnetic interference (EMI) testing or analysis is not included in the qualification process and is addressed on an individual equipment basis, as necessary (e.g., if required by IEC standards and European Union (EU) directives).

AP1000 Plant Equipment Qualification Methodology document, APP-GW-G1-002 (Reference 5.20) provides guidelines, acceptable methods and procedures for the environmental, seismic, and electromagnetic compatibility (EMC) qualification of AP1000 Plant safety equipment and also provides seismic and EMC requirements that are applicable to safety-related equipment. This methodology document is applicable to the C&I. Qualification of safety and safety-related equipment for AP1000 applications is conducted in accordance with this document.

5.8.1 Equipment Qualification Data Package

The qualification methods described above are used to verify the environmental design basis and capability of the Class 1 electrical and mechanical equipment supplied for the AP1000 plant. The results of the verification, as well as the design basis for each item of equipment, are documented in an equipment qualification data package (EQDP).

The EQDP consists of the following elements:

- **Specifications** – Includes equipment identification, manufacturer, electrical requirements, safety function, environmental conditions, installation, and maintenance requirements.

- **Qualification programme** – Defines the standards-compliant programme required to demonstrate that the equipment can perform the safety function identified in the specification.

  The basic performance criterion is that the qualification test programme demonstrates the capability of the equipment to meet the Class 1 performance requirements defined in the EQDP, while subjected to the environmental conditions specified in the EQDP. Where three or more specimens are tested, failure of one of three may be considered a random failure, subject to an investigation concluding that the observed failure is not indicative of a common-mode occurrence.

  For equipment for which ageing is addressed by evaluation of appropriate mechanism(s) through a review of available material and component information, the basic acceptance criterion is that the evaluation of test data demonstrates that the effect of ageing is minor and does not affect the capability of the aged equipment to perform specified functions.

  Qualification by test – Describes any test programme identified in the qualification programme, including number and type of test and test conditions. IEEE Standard 323-1974 (Reference 5.6) recommendations for testing follow a specific sequence: burn-in test, performance extremes test, ageing simulation and testing, synergistic effects, and visual inspections/disassembly. Class 1 electrical and

electromechanical equipment for the AP1000 design equipment qualification programme is type tested according to the guidelines and requirements of IEEE Standards 323-1974 and 344-1987 (Reference 5.7). Additionally, qualification based on type tests performed according to IEEE Standards 323-1974 (Reference 5.6) and 344-1987 (Reference. 5.7), but not specifically for the AP1000 design, may be used as a qualification basis.

- **Qualification by analysis** – Describes analyses to be performed including the specification of codes and methods and acceptance criteria.

  The AP1000 design equipment qualification programme uses analysis for seismic qualification of equipment if the primary requirement is the demonstration of structural integrity during a seismic event. For equipment that performs an active or a dynamic function, seismic qualification by analysis may also be used. However, the similarity between a qualified test unit and an as-supplied unit must be demonstrated unless otherwise justified.

  Chapter 17 of this PCSR describes the qualification requirements for Class 1 mechanical equipment where a fluid pressure boundary is involved. For those mechanical components that are not pressure boundaries, analysis is performed in compliance with the applicable industry design standard. Where age-sensitive materials, such as gaskets and packing, are used in the assembly of mechanical equipment, the ageing of these materials is normally evaluated based on an item-by-item review of the ageing characteristics of the material.

- **Qualification programme conclusions and summary** – Presents the conclusions of the EQDP.

5.9 Equipment Reliability

All SSCs are expected to have a reliability that is commensurate with their safety importance. Class 1 systems, in particular, are expected to have a high level of reliability.

The reliability claims for AP1000 SSCs are based on operating experience. The AP1000 design is similar to other PWRs in many of its systems and, even where the design is novel, the components used are also used in other reactors or other industries. Equipment reliability data is therefore available from actual operating experience.

Chapter 10 discusses common cause failures and human reliability data for SSCs.

5.9.1 AP1000 Design Reliability Programmes for Systems with Safety Importance

5.9.1.1 Assessment of Non-Class 1 SSCs with Importance to Safety

In currently operating plants, active systems provide the class 1 accident mitigation capability for the plant. However, for the AP1000 design, passive systems provide the class 1 accident mitigation capability. The AP1000 has active systems that provide backup to the class 1 SSCs for some transients / accident. As a result, they are not classified as Class 1 systems.

The non-Class 1 active systems in the AP1000 design provide defence-in-depth functions and can supplement the capability of the Class 1 passive systems. Chapter 8 shows that for frequent faults, diverse mitigation is provided which in most cases is provided by diverse Class 1 passive features and not the non-class 1 active features. The most often used non-class 1 SSC is the diverse actuation system (DAS) which provides backup actuation of the

class 1 passive SSCs. The AP1000 design uses an industry defined process to evaluate the importance of the non-Class 1 systems and for identifying appropriate regulatory oversight, as necessary, of these active systems.

The assessment of the non-Class 1 SSCs includes the following three parts:

- Identification of the significant non-Class 1 SSCs
- Development of specific reliability/availability missions for the significant non-Class 1 SSCs
- Specification of proposed regulatory treatment for each of the missions developed

The results of the assessment of the non-Class 1 SSCs of the AP1000 design confirmed that portions of several non-Class 1 systems are important to safety and should have additional regulatory oversight (Appendix A of Reference 5.2).

5.9.1.1.1 Protection from Natural Phenomena

Generally, the reliability/availability missions identified for the important non-class 1 SSCs do not include protection from natural phenomena. The one area where such protection is identified is for the post-72 hour SSCs. The installed non-class 1 SSCs that provide post-72 hour passive system support should have a reasonable expectation to survive natural phenomena. The purpose of this requirement is to minimize the need to transport SSCs to the site from an offsite storage location. Since only a few, small SSCs are required, they are easily transported via smaller trucks or helicopters.

The installed post-72 hour SSCs have considerations for surviving seismic, sustained winds, wind gusts, and wind-borne missiles to provide a reasonable assurance that they will be available within 72 hours. Note that since these installed post-72 hour SSCs are not credited as the means of providing this function they are not included in the internal / external hazard assements relative to providing these functions.

5.9.1.1.2 Quality Assurance

QA requirements are applicable to all SSCs identified in the AP1000 design short-term availability controls. The QA requirements are documented in Chapter 3 of this PCSR.

5.9.1.2 Reliability Assurance Programme

The reliability assurance programme (RAP) represents a dual-staged approach to the design and operation of the AP1000 plant in order to provide increased confidence in plant reliability and the corresponding safety of the public. The first stage of the RAP is the design stage, referred to as the design reliability assurance programme (D-RAP). The second stage of the RAP is referred to as the operational reliability assurance programme (O-RAP).

5.9.1.2.1 Design Reliability Assurance Programme

This stage is described in Reference 5.2, Appendix A.

The D-RAP is implemented as an integral part of the AP1000 design process to provide confidence that reliability is designed into the plant and that the important reliability assumptions made as part of the AP1000 design PSA will remain valid.

The D-RAP is implemented in three phases. The first phase, the GDA phase, defines the overall structure of the AP1000 D-RAP, and implements those aspects of the programme that are applicable to the design process. During this phase, risk-significant SSCs are identified for inclusion in the programme using probabilistic, deterministic, and other methods. The second phase, the post-GDA process, develops component maintenance recommendations for the plant's operations and maintenance activities for the identified SSCs. The third phase is the site-specific phase, which introduces any applicable plant site-specific SSCs to the D-RAP process.

The objective of the D-RAP is to design reliability into the plant and to provide maintenance recommendations that support the AP1000 design PSA safety goals. The following goals have been established for the D-RAP:

- Provide reasonable assurance that:
  - The AP1000 plant is designed, procured, constructed, maintained, and operated in a manner consistent with the assumptions and risk insights in the AP1000 design PSA for these risk-significant SSCs.
  - The reliability of risk-significant SSCs to function when called upon does not degrade to an unacceptable level during plant operations.
  - The frequency of transients that challenge the AP1000 design risk-significant SSCs is consistent with the PSA.
- Provide a mechanism for establishing baseline reliability values for risk-significant SSCs identified by the risk determination methods used to implement the maintenance rule (or equivalent process), consistent with PSA reliability and availability design basis assumptions used for the AP1000 design.
- Provide a mechanism for establishing baseline reliability values for SSCs consistent with the defence-in-depth functions to minimise challenges to the Class 1 systems.
- Generate design and operational information to be used by a licensee for ongoing plant reliability assurance activities.

5.9.1.2.2 Operational Reliability Assurance Programme

The reliability of AP1000 design SSCs will be assured by means of the application of operational phase reliability assurance activities (OPRAAs), which are contained in various operating plant programmes. The OPRAAs are composed of site administrative, maintenance, operational, and testing programmes to enhance operational phase reliability throughout the designed plant life.

This stage is described in Reference 5.2, Appendix A.

5.10 Treatment of Passive Systems

Unlike the current generation of light water reactors, the AP1000 design uses passive Class 1 systems that rely exclusively on natural forces such as density differences, gravity, and stored energy to provide Category A safety functions for reactor faults. The passive Class 1 systems include the following:

- PRHR
- CMTs
- Accumulators
- Passive containment cooling system
- automatic depressurisation system (ADS)
- IRWST

These passive systems do not include active equipment such as pumps, fans or diesel generators. One-time alignment of Class 1 valves that normally keep the Class 1 equipment in standby, actuates the passive systems. Most of these alignments use valve operators that fail safe, such as air operators that reposition to the safeguards position on a loss of the dc power or non-Class 1 compressed air. Some of these alignments use dc motor operators with power provided by Class 1 batteries or check valves that operate by the pressure differential across the valve disc.

The operation of the Class 1 passive systems does not require alternating current (ac) electrical power. For the AP1000 design, the active systems are designated as non-Class 1 systems except for limited portions of the systems that provide Class 1 isolation functions, such as containment isolation.

The passive components are Class 1 components subject to quality, qualification, and reliability requirements as detailed for Class 1 systems in this chapter, including assessment for dependent failures and common-cause failure (CCFs). Note that component diversity is provided in the AP1000 Class 1 passive systems based on PSA insights. This diversity is credited in the mitigation of frequent faults (refer to Chapter 8) where CCF need be considered.

The actuation of the PRHR, CMTs, and PCS all have air-operated valves that fail open on loss of dc power or instrument air. These systems also have component redundancy to provide confidence that their safety functions are performed even in the unlikely event of the most limiting single failure occurring coincident with a postulated DBE. In the case of the PCS, there is also component diversity to improve the protection against CCF.

The ADS actuation involves motor-operated valves (MOVs) and squib valves, which require power from the Class 1 essential electrical supply system (IDS) to actuate. The accumulators only have non-return valves kept closed by primary circuit pressure. As soon as the primary circuit pressure drops below the pressure of the nitrogen gas in the accumulator, accumulator pressure forces these valves open and injection is initiated.

Note that some components have support systems that are not needed for their Class 1 operations and in these situations the support systems are Class 2 or Class 3. For example, compressed air is provided to the CMT isolation valves. This air supply is used to maintain the valves in their normal closed position. The Class 1 operation of these valves is to open and for this operation the air supply is not required. As a result, failure of these support

systems does not compromise the availability of the passive systems. Failure leads to a fail-safe response.

5.11 Use of Metric and US Units

The AP1000 design was developed, for the most part, in US units of measurement; however, because the design is intended for an international market, the issue of the use of metric or dual units is important.

The Westinghouse document "AP1000 Standard Plant Metrication" (Reference 5.18) defines the extent to which metrication shall apply and to what level of detail it shall reach into the design, procurement, licensing, construction, testing, information and configuration management, operation, and maintenance of AP1000 units. For this document, metrication is defined as the act of adopting metric units in the design, procurement, and construction of an AP1000 unit. The AP1000 design is "quasimetric" in that it was originally conceived in US units but will be delivered as fully metric as specified by engineering documentation, with specified and regulatory agreed-upon exceptions.

The document also identifies how future design exceptions that arise will be handled and justifies how currently identified exceptions are ALARP. Current exceptions are listed in the appendix to Reference 5.18.

This PCSR is presented in Système Internationale (SI) units. While SI units are always presented, dual units may be shown here for clarity and cross-referencing purposes.

5.12 Smart Devices

This section addresses the identification and justification of smart devices in AP1000 SSCs. Smart technology is present in many types of modern equipment such as sensors, actuators, valves, protection relays and power supplies. A smart device is defined as any component that:

a. Contains pre-developed software or programmed logic (e.g. an Hardware Description Language Programmed Device) and is a candidate for use in an application important to nuclear safety.

b. Has a primary function performed that is well-defined and applicable to only one type of application within a system, such as measuring a temperature or pressure, positioning a valve, or controlling speed of a mechanical device, or performing an alarm function.

c. The primary function performed is conceptually simple and limited in scope (although the manner of accomplishing this internally may be complex).

d. The device is not designed so that it is re-programmable after manufacturing nor can the device functions be altered in a general way so that it performs a conceptually different function: only pre-defined parameters can be configured by users.

A more extensive definition along with examples of smart devices can be found in UKP-GW-GLR-017, "AP1000 Smart Device Justification Plan" (Reference 5.26).

When a smart device is selected for use in the UK AP1000 design a smart device justification shall be performed in accordance with UKP-GW-GLR-017 (Reference 5.26) and UKP-GW-J0Y-004, "United Kingdom AP1000 Smart Device Assessment Process" (Reference 5.27).

The justification will be based on the categorization of the function important to safety being performed by the device. The UK nuclear regulatory regime requires demanding levels of safety demonstration and justification for any SSC's including smart devices that are to be used in performing Category A safety functions. The current tools and methodology available are deemed impractical to enable the successful justification of the use of Smart devices for Category A safety functions and therefore these devices shall not be used in the UK AP1000 design.

Where there is a need for a component or device to perform a Category A safety function the system designers shall select a non-smart device, select a device that has been designed to IEC nuclear standards or undertake work to specifically design a device to the IEC nuclear standards.

Data sheets or procurement requests for UK AP1000 plant components, equipment or package systems shall include definitive statements as to whether or not smart devices can be part of the delivery. Vendors supplying any equipment or package systems for a UK AP1000 plant also need to provide a definitive statement either in the purchase order or in requirements traceability documentation as to whether or not smart technology is present in what they are supplying.

5.13 References

5.1 Not Used.

5.2 Westinghouse Report UKP-GW-GL-044, Rev. 1, "AP1000 UK Safety Categorization and Classification Methodology," April 2010.

5.3 Westinghouse Report APP-GW-N1-005, Rev. 1, "AP1000 Design Criteria and Guidelines for Protection from Seismic Interaction," September 2008.

5.4 Not Used.

5.5 Westinghouse Report UKP-GW-GL-045, Rev. 2, "AP1000 Equivalence/Maturity Study of U.S. Codes and Standards," September 2011.

5.6 IEEE Standard 323-1974, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers, 1974.

5.7 IEEE Standard 344-1987, "IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers, 1987.

5.8 IEEE Standard 627-1980, "IEEE Standard for Design Qualification of Safety System Equipment Used in Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers, 1980.

5.9 Not Used.

5.10 Not Used.

5.11 Not used.

5.12 Not Used.

5.13 Not Used.

5.14 Not Used.

5.15 Not Used.

5.16 Not Used.

5.17 Not Used.

5.18 Westinghouse Report APP-GW-G1-011, Rev. 7, "AP1000 Plant Metrication Strategy and ALARP Assessment for the United Kingdom," November 2016.

5.19 Westinghouse Report UKP-GW-GL-059, Rev. 3, "UK AP1000 Electrical Systems Codes and Standards Analysis," April 2011.

5.20 Westinghouse Report APP-GW-G1-002, Rev. 4, "AP1000 Equipment Qualification Methodology," September 2014.

5.21 ASME OM Code, "Operation and Maintenance of Nuclear Power Plants," 1995 edition with 1996 addenda

5.22 Westinghouse Report UKP-GW-GL-501, Rev. 0, "AP1000 UK Generic Technical Specifications," January 2016.

5.23 Westinghouse Report UKP-GW-GL-502, Rev. 0, "Recommendation for Development of the AP1000 Technical Requirements Manual," February 2016.

5.24 ASME Boiler and Pressure Vessel Code, Section III, 1998 Edition with 2000 Addenda

5.25 Westinghouse Report UKP-GW-GL-500, Rev. 0, "AP1000 UK Limits and Condition Process Description," December 2015.

5.26 Westinghouse Report UKP-GW-GLR-017, Rev. 4, "United Kingdom AP1000 Smart Device Justification Plan," December 2016.

5.27 Westinghouse Report UKP-GW-J0Y-004, Rev. 2, "AP1000 Smart Device Assessment Process," December 2016.

5.28 Westinghouse Report UKP-GW-GL-105, Rev. 1, "AP1000 Plant Review of UK Class 2 Pressure Equipment and Storage Tank Structures, Systems and Components (SSCs)", August 2016.

Table 5-1. Comparison Matrix of Standard AP1000 and UK Categorisation and Classification Methodologies

UK Safety Classification / US Safety Categorisation	1	2	3
A	AP1000 Class A/B/C	AP1000 Class D	–
B	–	AP1000 Class D	AP1000 Class D & E
C	–	–	AP1000 Class E-W

Table 5-2. Codes and Standards for Class 1 SSCs

SSC Type	Applicable Codes and Standards
Pressure vessels	ASME Code, Section III, Division 1
Piping	ASME Code, Section III, Division 1
Valves	ASME Code, Section III, Division 1
Containment vessel	ASME Code, Section III, Division 1
Atmospheric storage tanks	ASME Code, Section III, Division 1 American Concrete Institute (ACI) 349 (PCS-MT-01)
Cranes and hoists	Nuclear Regulatory Commission technical report designation (NUREG)-0554, Supplemented by ASME NOG-1
Circuit breakers, switchgear, relays, substantiation, and fuses	See note 1
C&I systems (hardware)	IEC 60987. See note 2
C&I systems (software)	IEC 60880. See note 2
Electrical separation	IEEE Standard 384
Control rooms and human machine interface	NUREG-0700
Qualification of electrical and C&I SSCs	IEEE Standard 323 (Environmental) IEEE Standard 344 (Seismic) IEC 61000 Series (electromagnetic compatibility (EMC)) See note 2.

Note:

1. Application of codes and standards for electrical equipment is described in Chapter 18 and in Reference 5.19.
2. Application of codes and standards for Control and Instrumentation is described in Chapter 19.

Table 5-3. Codes and Standards for Class 2 SSCs

SSC Type	Applicable Codes and Standards
Pressure vessels	ASME Section VIII, Division 1
Piping	American National Standards Institute (ANSI)/ASME B31.1
Pumps	API 610 Hydraulic Institute Standards
Valves	ANSI/ASME B31.1 ASME B16.34
Atmospheric storage tanks	API-650 AWWA D-100 ANSI/ASME B96.1
Storage tanks rated < 1 bar	API-620
ac Motors and generators	National Electrical Manufacturers Association (NEMA) MG1
Circuit Breakers, Switchgear, Relays, Substantiation and Fuses	See note 1
Cranes and hoists	None Identified
Battery room exhaust fans	ANSI/AMCA 210 or ANSI/AMCA 211 ANSI/AMCA 300
Fire dampers	ANSI/AMCA 500 UL 555S
Unit heaters	UL 1025 NFPA 70
C&I systems (hardware)	IEC 60987. See note 2
C&I systems (software)	IEC 62138. See note 2
Control rooms and human machine interface	NUREG-0700
Qualification of electrical and C&I SSCs	IEEE Standard 323 (EQ) IEEE Standard 344 (Seismic)IEC 61000 Series (EMC) See note 2

Notes:

1. Application of codes and standards for electrical equipment is described in Chapter 18 and Reference 5.19.
2. Application of codes and standards for Control and Instrumentation is described in Chapter 19..

Table 5-4. Codes and Standards for Class 3 SSCs

SSC Type	Applicable Codes and Standards
Pressure vessels	ASME Code, Section VIII, Division 1
Piping	ANSI/ASME B31.1
Pumps	API 610 Hydraulic Institute Standards
Valves	ANSI/ASME B31.1 ASME B16.34
Atmospheric storage tanks	API-650 AWWA D-100 ANSI/ASME B96.1
Storage tanks rated <1 bar	API-620
ac motors and generators	NEMA MG1
Circuit breakers, switchgear, relays, substantiation, and fuses	See note 1
Control rooms and human machine interface	NUREG-0700
Qualification of electrical and C&I SSCs	IEEE Standard 323 (EQ) IEEE Standard 344 (Seismic) IEC 61000 Series (EMC) See note 2

Notes:

1. Application of codes and standards for electrical equipment is described in Chapter 18 and Reference 5.19.
2. Application of codes and standards for Control and Instrumentation is described in Chapter 19.

Table 5-5. Definition of Operational Modes

Modes	Title	Reactivity Condition (K_{eff})	% Rated Thermal Power[1]	Average Reactor Coolant Temperature (°C)
1	Power Operation	≥ 0.99	> 5	N/A
2	Start-up	≥ 0.99	≤ 5	N/A
3	Hot Standby	< 0.99	N/A	> 216
4	Safe Shutdown[2]	< 0.99	N/A	$216 \geq T_{avg} > 93$
5	Cold Shutdown[2]	< 0.99	N/A	≤ 93
6	Refuelling[3]	N/A	N/A	N/A

Notes:

1. Excluding decay heat
2. All reactor vessel head closure bolts fully tensioned
3. One or more reactor vessel head closure bolts less than fully tensioned

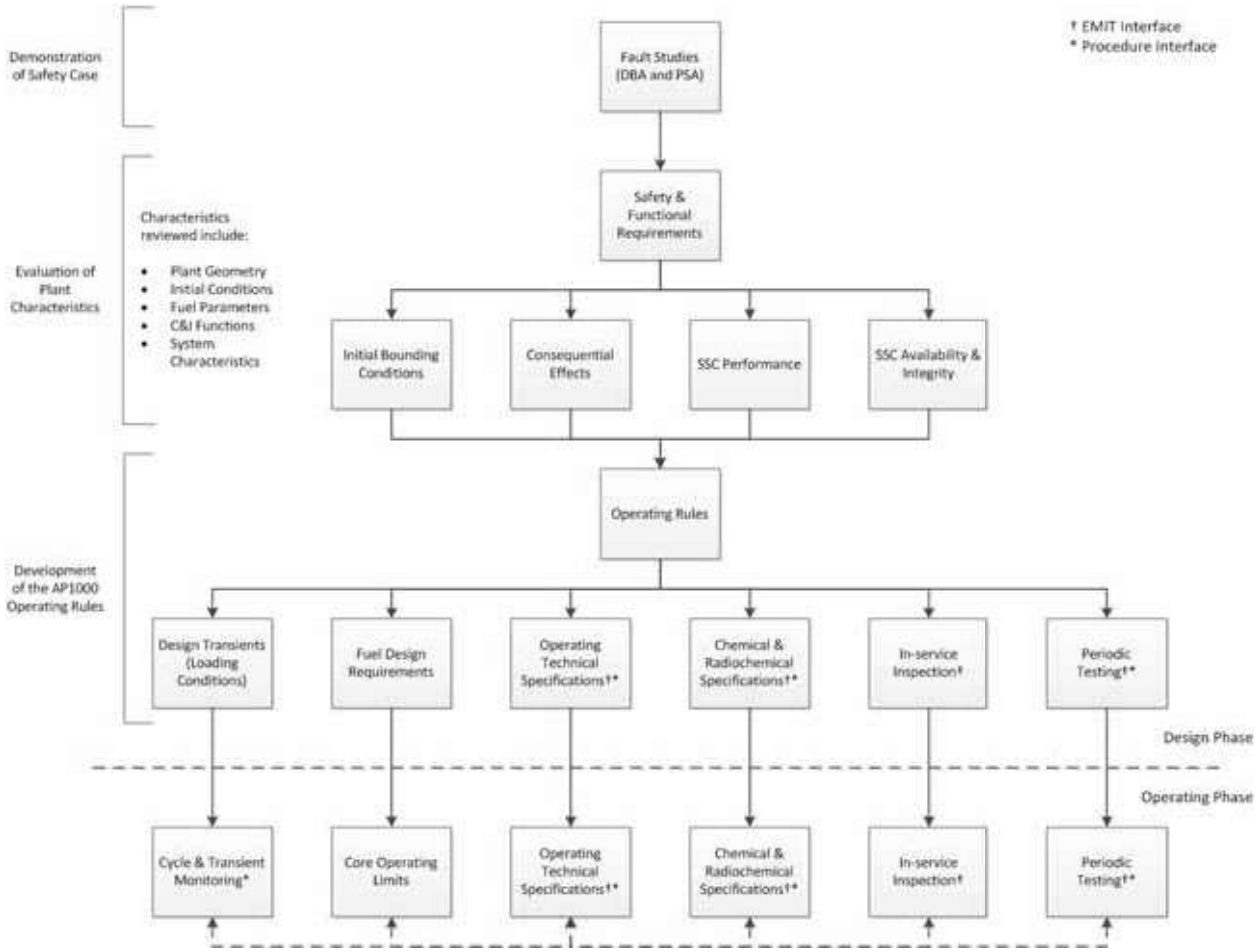


Figure 5-1. Limits and Conditions Methodology Flowchart

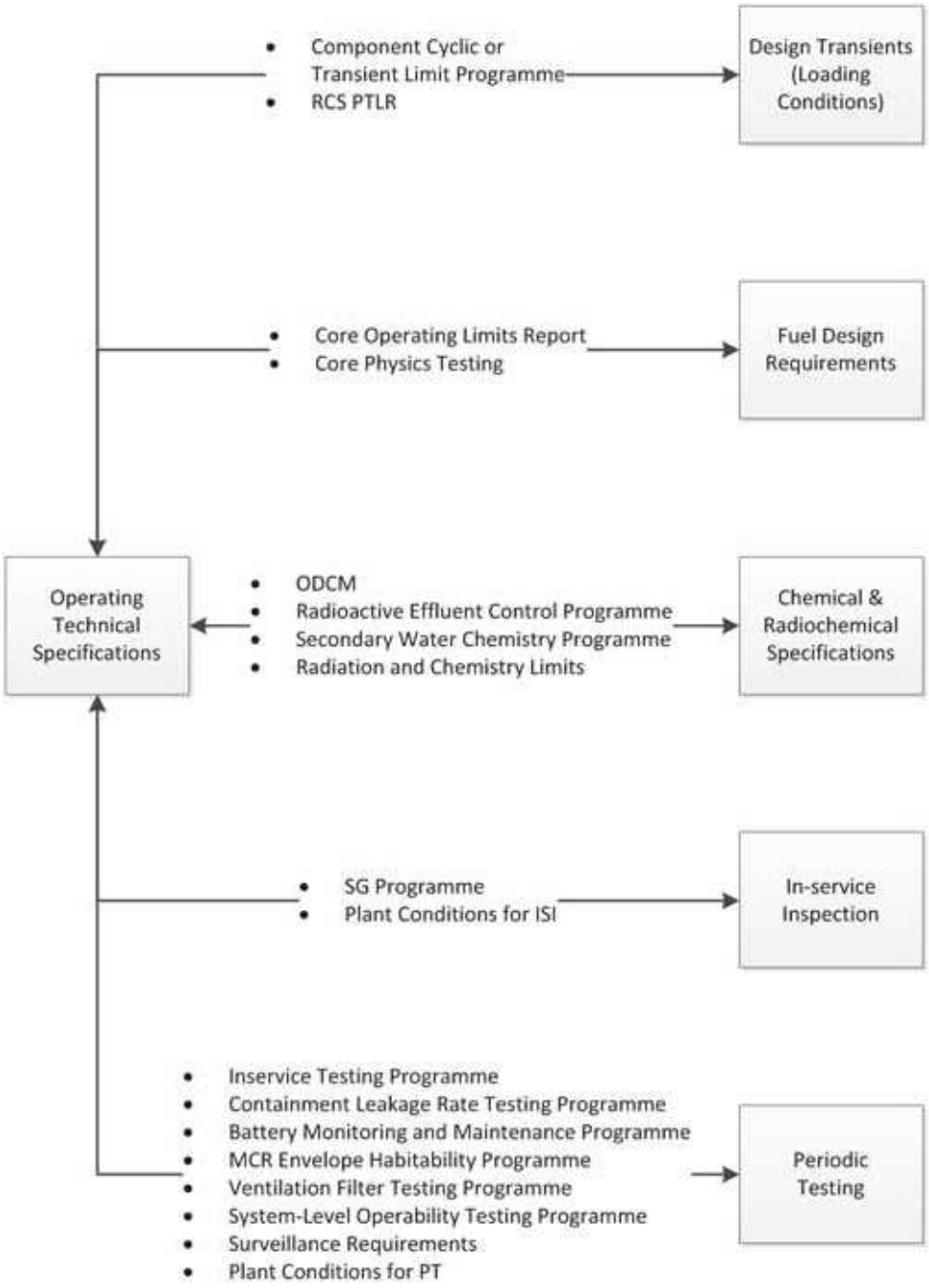


Figure 5-2. OTS Operating Rule Interfaces

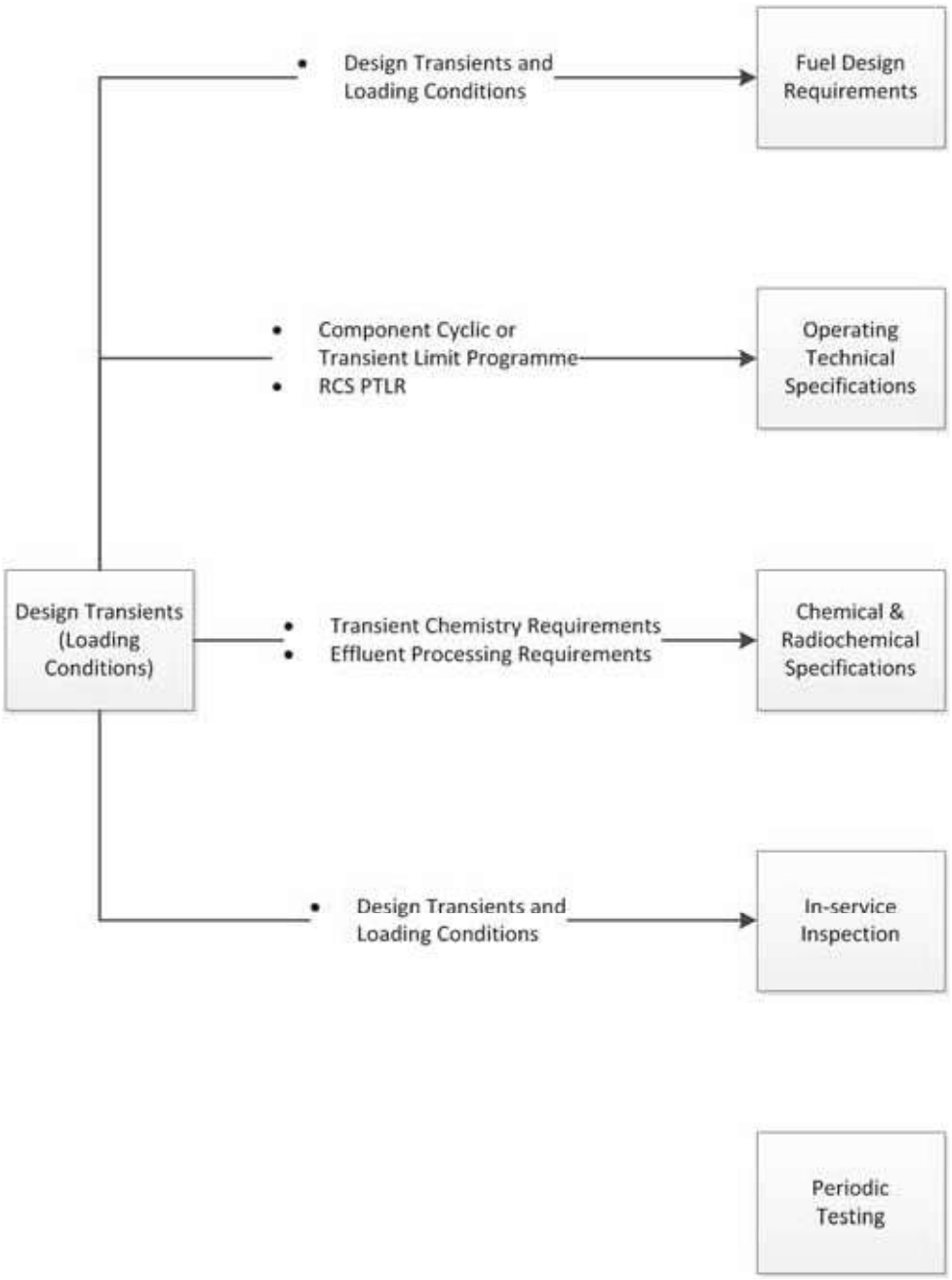


Figure 5-3. Design Transients Operating Rule Interfaces

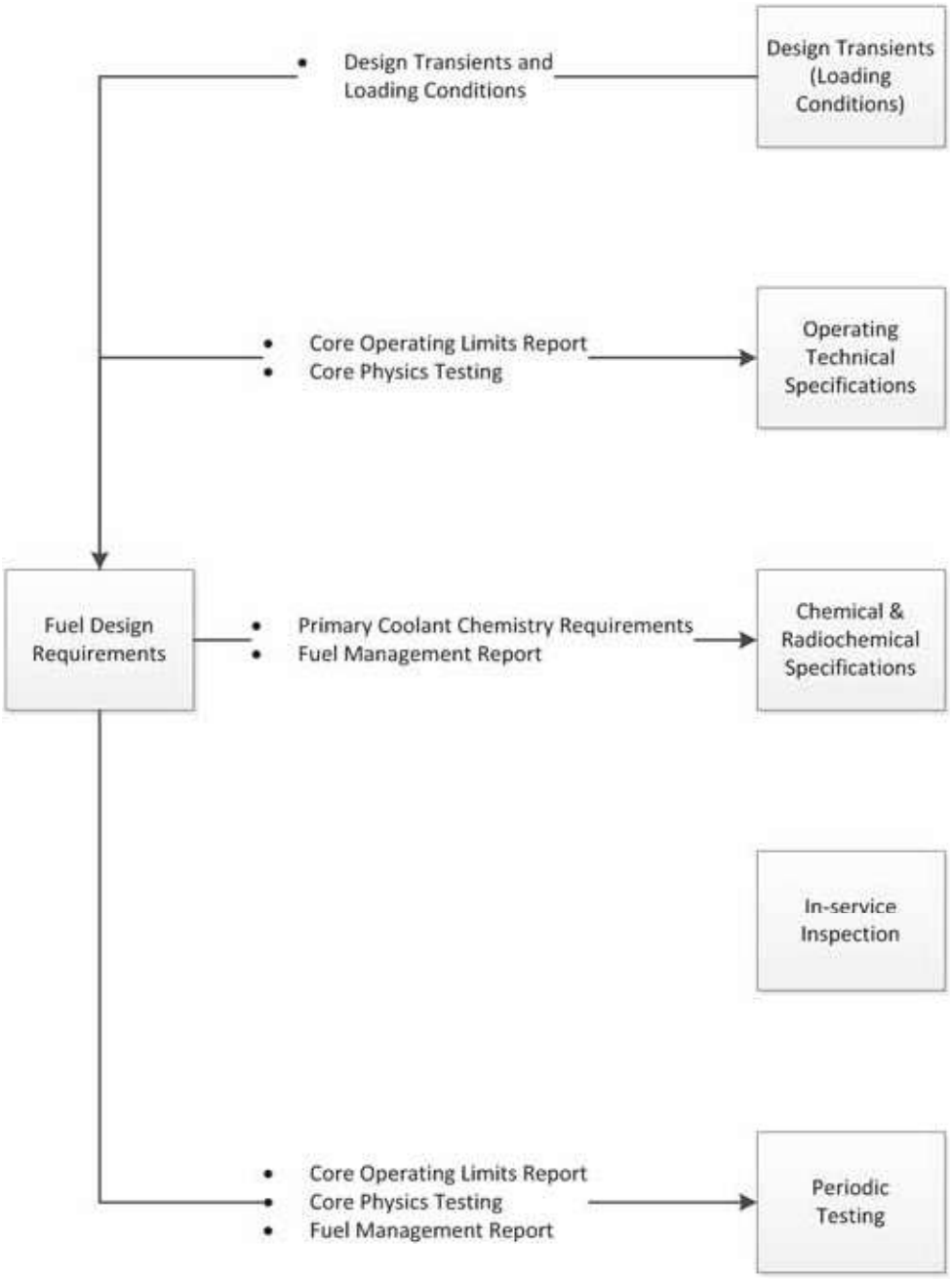


Figure 5-4. Fuel Design Requirements Operating Rule Interfaces

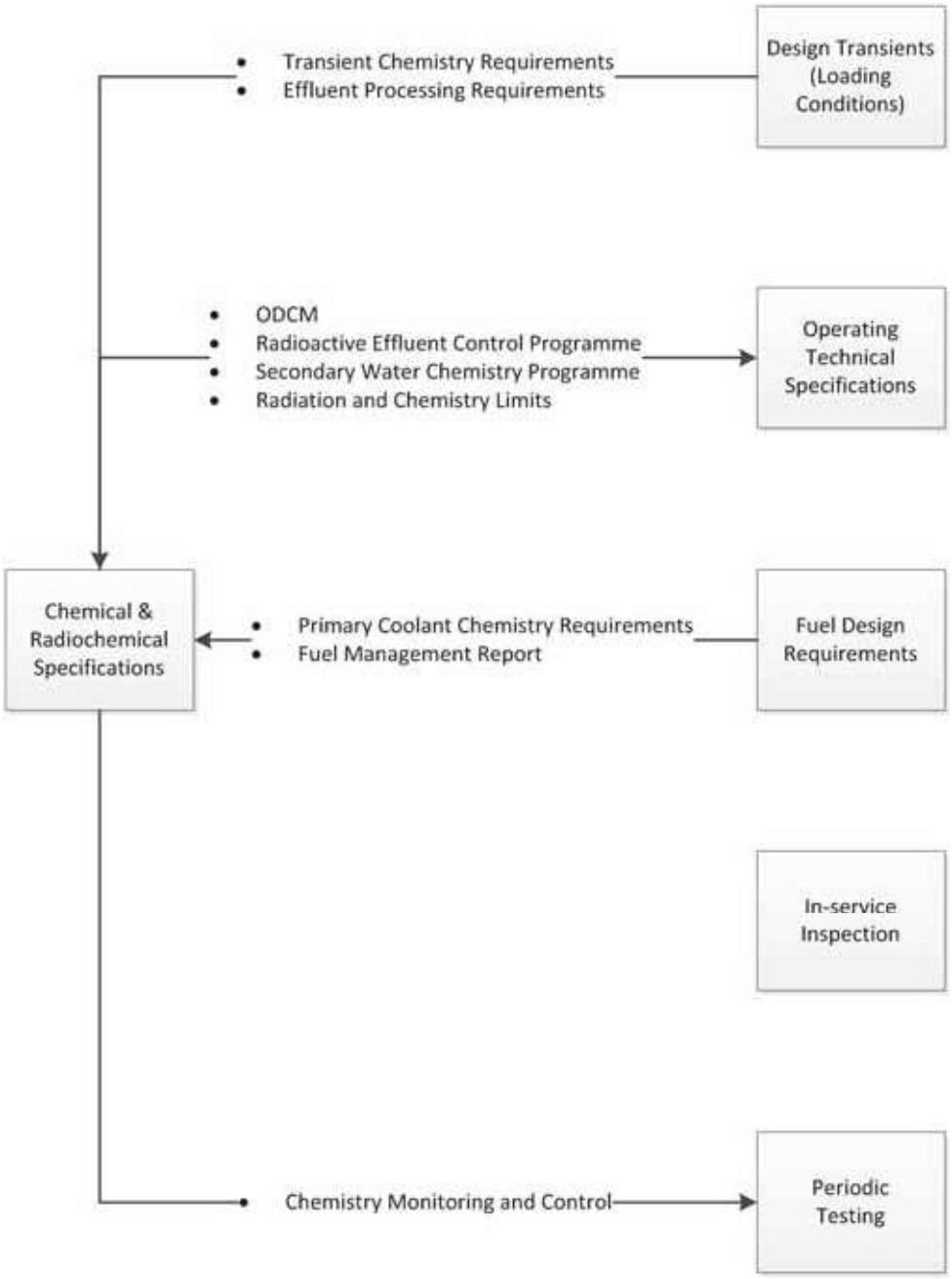


Figure 5-5. Chemical and Radiochemical Operating Rule Interfaces

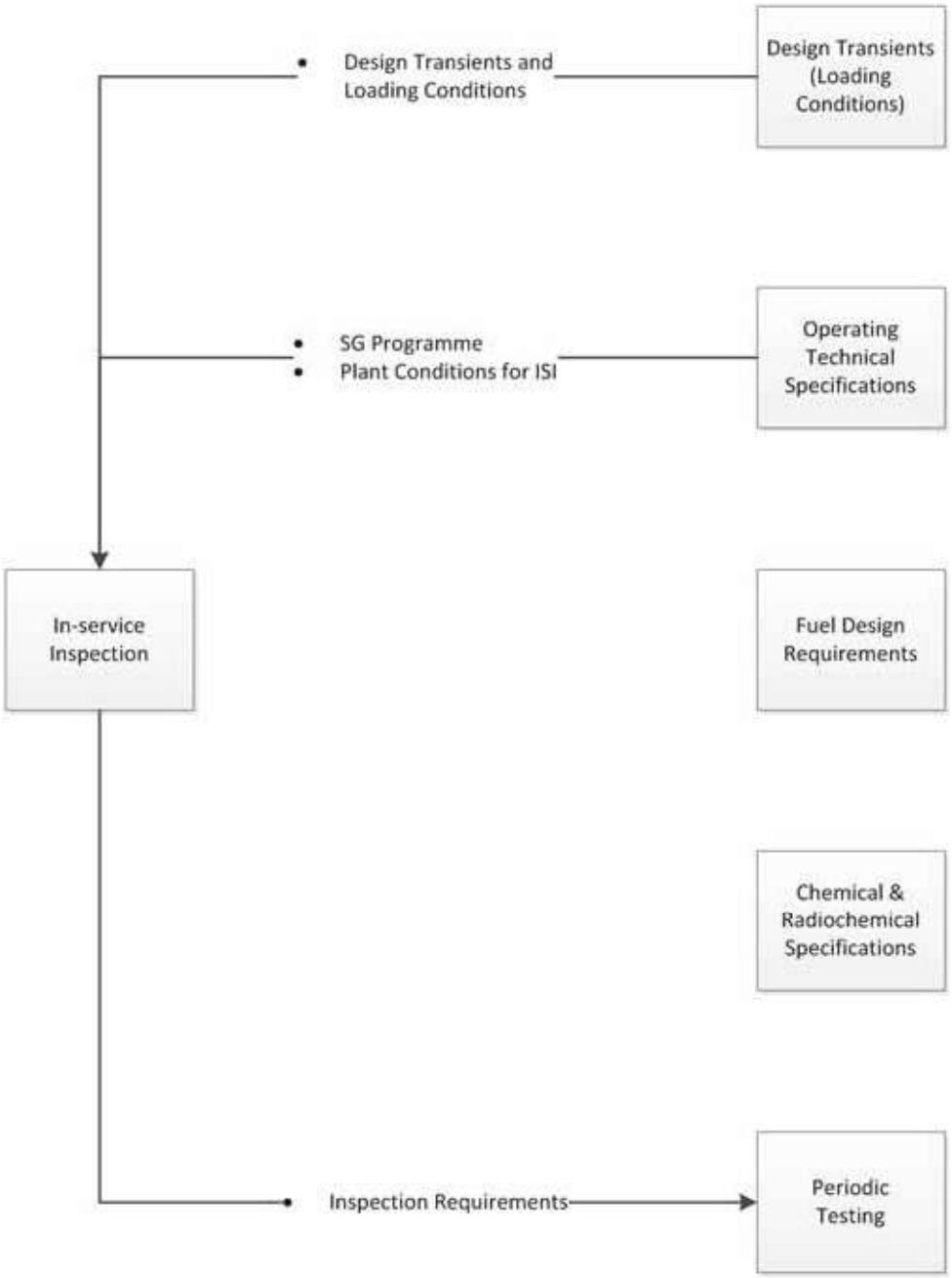


Figure 5-6. In-Service Inspection Operating Rule Interfaces

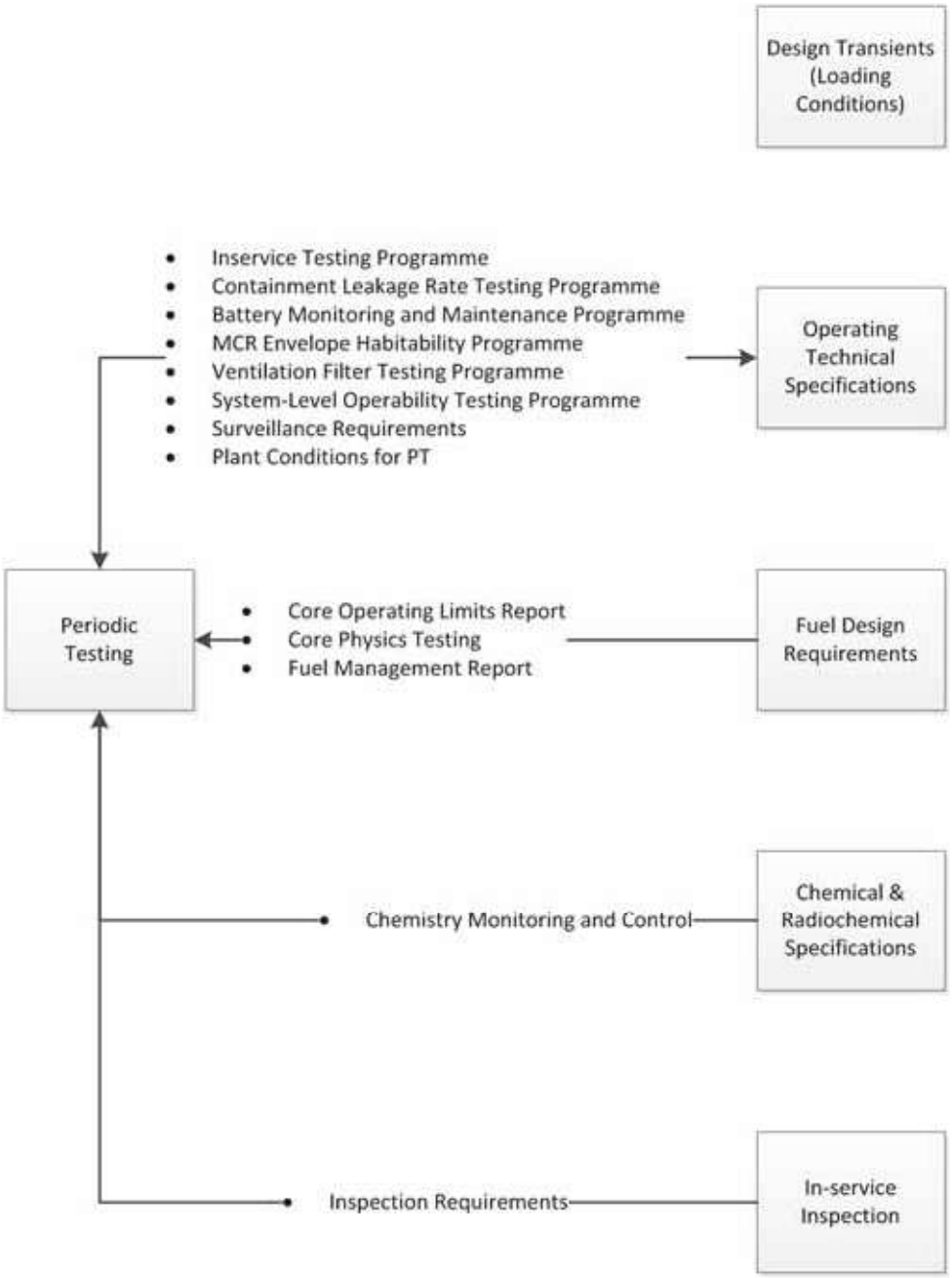


Figure 5-7. Periodic Testing Operating Rule Interfaces

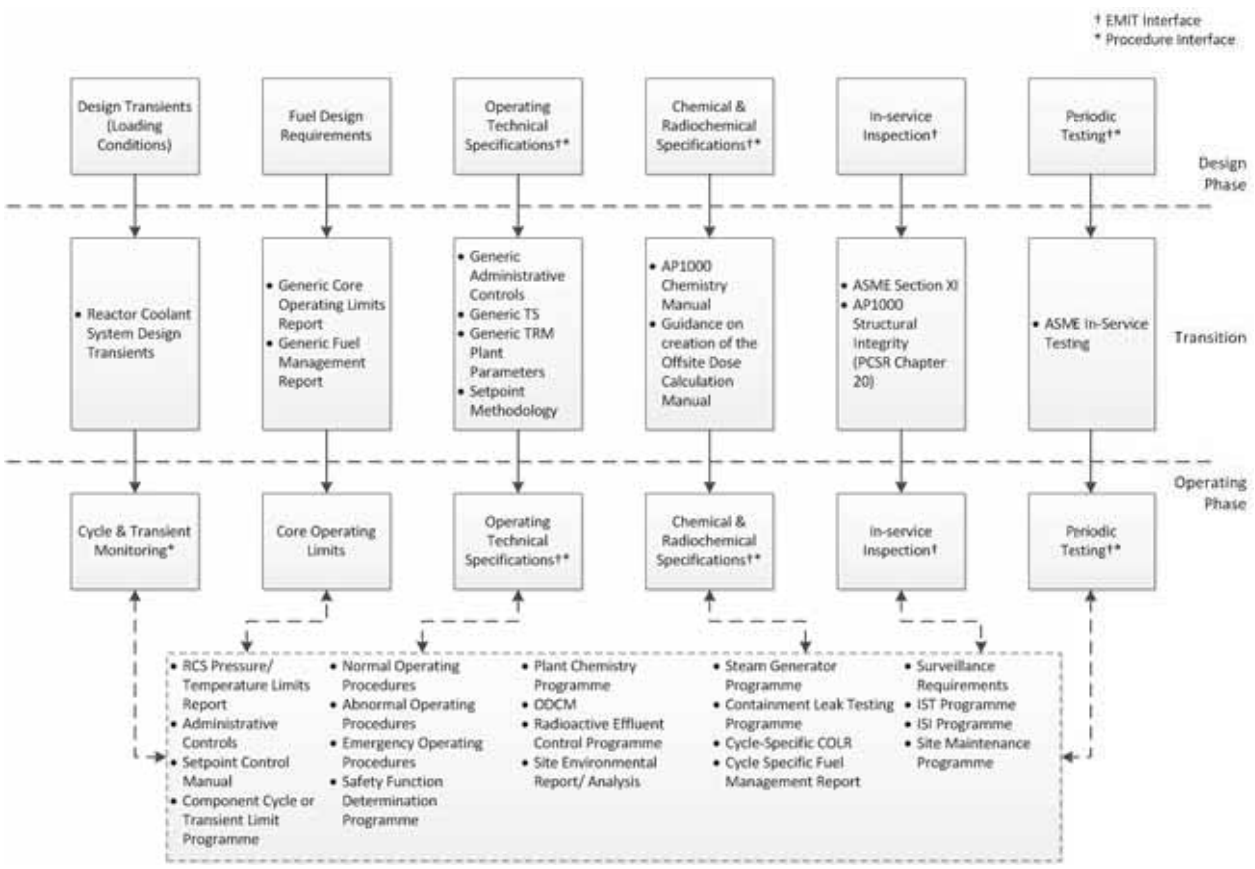


Figure 5-8. Operating rules Transition from Design to Operating Phase

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS, ACRONYMS, AND TRADEMARKS

ac	alternating current
ADS	automatic depressurisation system
ALARP	as low as reasonably practicable
AOV	air-operated valve
ASHRAE	American Society of Heating, Refrigerating, and Air Conditioning Engineers
ASME	American Society of Mechanical Engineers
ASS	auxiliary steam system
ATC	automatic turbine control
ATWT	anticipated transient without trip
BAT	best available technology
BDB	beyond design basis
BDPI	bank demand position indication system
BDS	steam generator blowdown system
CA	containment atmosphere
CAS	compressed and instrument air system
CCF	common cause failure
CCS	component cooling water system
CCTV	closed-circuit television
CDF	core damage frequency
CDS	condensate system
CFS	chemical feed system
C&I	control and instrumentation
C-I	Category I
C-II	Category II
CLP	cask loading pit
CWP	cask washdown pit
CMS	condenser air removal system
CMT	core makeup tank
CNS	containment system
CPS	condensate polishing system
CRDM	control rod drive mechanism
CSA	control support area
CVS	chemical and volume control system
CWP	cask washdown pit
CWS	circulating water system
DAS	diverse actuation system
DBA	design basis accident
DBE	design basis event
dc	direct current
DDS	data display and processing system
D-EHC	digital electrohydraulic
DFBN	debris filter bottom nozzle
DMIMS	digital metal impact monitoring system
DNB	departure from nucleate boiling
DNBR	departure from nucleate boiling ratio
DOP	dispersed oil penetration
DOS	standby diesel and fuel oil system
DRCS	digital rod control system
DRP	design reference point
DRPI	digital rod position indication
DTS	demineralised water treatment system

LIST OF ABBREVIATIONS, ACRONYMS, AND TRADEMARKS (cont.)

DVI	direct vessel injection
DWS	demineralised water transfer and storage system
ECS	main ac power system
EDS	Class 2 dc and Uninterruptible Power Supply System
EFS	communication system
EMIT	examination, maintenance, inspection and testing
ESF	engineered safety feature
FHM	fuel handling machine
FHS	fuel handling and refuelling system
FPS	fire protection system
FTC	fuel transfer canal
FWVMS	feedwater vibration monitoring system
FWS	main and startup feedwater system
GDA	generic design assessment
GDF	geological disposal facility
GRCA	grey rod cluster assembly
GSP	grab sample panel
HC VWS	high cooling capacity subsystem
HEPA	high-efficiency particulate air
HLW	high-level waste
HVAC	heating, ventilation, and air conditioning
HX	heat exchanger
IDS	essential electrical supply system
IFBA	integral fuel burnable absorber
IFM	intermediate flow mixing
IHP	integrated head package
IIS	in-core instrumentation system
ILW	intermediate-level waste
IRWST	in-containment refuelling water storage tank
ISLOCA	interfacing system loss-of-coolant accident
IVR	in-vessel retention
IWS	integrated waste strategy
LC VWS	low cooling capacity subsystem
LLW	low-level waste
LLWR	low-level waste repository
LOCA	loss-of-coolant accident
LRGS	low-resolution gamma spectroscopy
LTOP	low temperature overpressure protection
MCR	main control room
MES	meteorological and environmental monitoring system
MEU	mobile encapsulation plant
MFW	main feedwater
MOV	motor-operated valve
MSIV	main steam isolation valve
MSLB	main steam line break
MSR	moisture separator reheater
MSS	main steam system
MTS	main turbine system
NDA	Nuclear Decommissioning Authority
NNS	non-nuclear seismic
NRC	Nuclear Regulatory Commission

LIST OF ABBREVIATIONS, ACRONYMS, AND TRADEMARKS (cont.)

NSSS	nuclear steam supply system
OCS	operation and control centres system
PCCAWST	passive containment cooling ancillary water storage tank
PCCWST	passive containment cooling water storage tank
PCS	passive containment cooling system
PCSR	Pre-Construction Safety Report
PGS	plant gas system
PIE	postulated initiating event
PLS	plant control system
PMS	protection and safety monitoring system
PORV	steam generator power-operated relief valves
PRHR	passive residual heat removal
PSA	probabilistic safety assessment
PSS	primary sampling system
PWR	pressurised water reactor
PWS	potable water system
PXS	passive core cooling system
QA	quality assurance
QDPS	qualified data processing system
RCCA	rod cluster control assembly
RCDT	reactor coolant drain tank
RCP	reactor coolant pump
RCPVMS	reactor coolant pump vibration monitoring system
RCS	reactor coolant system
RM	refuelling machine
RMS	radiation monitoring system
RNS	normal residual heat removal system
RPI	rod position indicator
RSR	remote shutdown room
RSW	remote shutdown workstation
RTD	resistance temperature detector
RV	reactor vessel
RWM	Radioactive Waste Management
RWS	raw water system
RXS	reactor system
SFW	startup feedwater
SGTR	steam generator tube rupture
SDS	sanitary drainage system
SFP	spent fuel pool
SFS	spent fuel pool cooling system
SG	steam generator
SGS	steam generator system
SJS	seismic monitoring system
SBLOCA	small loss-of-coolant accident
SMS	special monitoring system
SSC	structure, system, or component
SSS	secondary sampling system
SWS	service water system
TCS	turbine building closed cooling water system

LIST OF ABBREVIATIONS, ACRONYMS, AND TRADEMARKS (cont.)

TSP	trisodium phosphate
UK	United Kingdom
UPS	uninterruptible power supplies
US	United States
VAS	radiologically controlled area ventilation system
VBS	nuclear island nonradioactive ventilation system
VCS	containment recirculation cooling system
VCT	volume control tank
VDU	visual display unit
VES	main control room emergency habitability system
VFD	variable frequency drive
VFS	containment air filtration system
VHS	health physics and hot machine shop HVAC system
VIMS	vibration integrity monitoring system
VLS	containment hydrogen control system
VRS	radwaste building HVAC system
VTS	turbine building ventilation system
VUS	containment leak rate test system
VWS	central chilled water system
VXS	annex/auxiliary buildings' nonradioactive HVAC systems
VYS	hot water heating system
VZS	diesel generator building heating and ventilation system
WABA	wet annular burnable absorbers
WGS	gaseous radwaste system
WLS	liquid radwaste system
WRS	radioactive waste drain system
WSS	solid radwaste system
WWS	waste water system
ZIRLO	zirconium alloy
ZOS	onsite standby power system

6 PLANT DESCRIPTION AND OPERATION

6.1 INTRODUCTION

The Westinghouse AP1000 plant is an advanced, passively safe, 1100MWe class, pressurised water reactor (PWR) with an expected service life of 60 years. Its design includes passive safety features not present on the Generation-2 plants in service today or in other Generation-3 designs, and extensive plant simplifications to enhance nuclear safety and facilitate the construction, operation, and decommissioning of the plant. An overview of the plant is shown in Figure 6-1.

The technical characteristics of the AP1000 design are summarized in Table 6-1.

This chapter of the Pre-Construction Safety Report (PCSR) produces an overview of the evolution of the AP1000 design and describes its systems, subsystems, and components and their operation.

Normal Operations

Section 6.2 describes the six defined normal operational modes and the equipment that supports them.

Reactor System

Section 6.3 describes the reactor system (the reactor vessel (RV) and integrated head package (IHP)), reactor internals, fuel assemblies, rod cluster control assemblies (RCCA), control rod drive mechanisms (CRDM), and in-core instrumentation).

Reactor Coolant System and Connected Systems

Section 6.4 describes the reactor coolant system (RCS) the steam generators (SGs), pressuriser, and associated pumps and pipe work. Section 6.4 additionally describes systems which support RCS operation.

Steam and Power Conversion Systems

Section 6.5 describes the secondary side of the reactor systems (main steam and feed systems, turbine and condenser), which use the nuclear heat to generate electricity.

Passive Safety Systems

Section 6.6 describes the passive Class 1 engineered safety features, i.e., those subsystems and components making up the passive core cooling system (PXS); passive containment cooling system (PCS); and other passive structures, systems, and components (SSCs).

Containment and Supporting Systems

Section 6.7 describes the Containment and supporting systems.

Heating, Ventilation, and Air Conditioning Systems

Section 6.8 describes the containment system and the heating, ventilation, and air conditioning (HVAC) in controlled areas that provide the containment function in those areas.

Control and Instrumentation

Section 6.9 describes the control and instrumentation (C&I) systems that control the reactor under normal and accident conditions.

Electrical Systems

Section 6.10 describes the electrical systems that supply the Class 1 and 2 safety systems, and it describes the normal and emergency power supplies.

Fuel Handling, Fuel Storage, and Radwaste Systems

Section 6.12 describes the systems used to transfer nuclear fuel into and out of the reactor; the systems involved in storage of spent fuel, in both the short- and long-term; and the systems involved in handling and storing radioactive wastes.

Auxiliary Systems

Section 6.11 describes the auxiliary systems that support plant operation, Class 2 defence in-depth systems, and other support systems of the plant.

Summary of Systems Providing Category A and B Safety Functions and Defence in Depth

Section 6.6.5 provides a summary of which systems support passive components and class 2 SSCs providing Category A Safety Functions.

Civil Structures

Section 6.13 describes the civil structures that comprise the nuclear island, i.e., containment building, shield building, and auxiliary building; and the main plant buildings outside the nuclear island, i.e., turbine building, annex building, diesel generator building, and radwaste building.

6.1.1 AP1000 Design Reference Point

The design reference point (DRP) is defined as the revision status (configuration), at a specified moment in time, of the safety case documentation and supporting information relevant to the generic design assessment (GDA) application. The AP1000 DRP document (Reference 6.2) defines the United Kingdom (UK) design reference point for the AP1000 design; specifically, it:

- Includes a list of all the documents and their revision status that constitute the design reference point for the Westinghouse AP1000 UK GDA.
- Describes how the design reference point has been set.
- Describes how any changes will be controlled.
- Describes how the design reference point for the conclusion of GDA Step 4 will be updated.

The documents that constitute the design at that point have been used as the basis for this revision of the AP1000 plant PCSR. This facilitates the identification of any safety-

significant changes with regard to the application and issue of any future Nuclear Site Licences for construction and operation of the AP1000 design in the UK.

6.1.2 Overview of Plant Systems and Operation

The reactor core consists of 157 fuel assemblies, each consisting of 264 fuel rods arranged in a square 17×17 grid and supported on the lower core plate, which is itself supported by the core barrel. The fuel rods are clad with a zirconium alloy (ZIRLO®) which provides the first barrier to release of radioactivity. A number of fuel assemblies have moveable absorbers – either RCCAs or grey rod cluster assemblies (GRCAs) located in guide thimble tubes within the fuel assembly. A central thimble is used in some assemblies for in-core instrumentation. The fuel assembly design is similar to those being used in operating PWRs.

The RCS consists of two heat transfer circuits, each with a SG, two reactor coolant pumps (RCPs), a single hot leg, and two cold legs for circulating reactor coolant. In addition, the system includes the pressuriser, interconnecting piping, valves, and instrumentation for operational control and safeguard actuation. All RCS equipment is located in the reactor containment. During operation, the RCPs circulate pressurised water through the RV and then the SGs. The water, which serves as coolant, moderator, and solvent for boric acid (chemical shim control), is heated as it passes through the core. It is transported to the SGs, where the heat is transferred to the steam system. Then the pumps return the water to the RV to repeat the process.

The RCS is shown in Figure 6-2 and described in detail in Section 6.4.

The primary circuit boundary provides the second barrier against the release of radioactivity generated within the fuel. It is designed to provide a high degree of integrity throughout the lifetime of the plant.

With the exception of limited times during plant shutdown, the RCS pressure is controlled by the pressuriser, where water and steam are maintained at saturation within a defined pressure range by the activation of electrical heaters or a water spray. The pressure is increased through the generation of steam formed by the heaters and decreased by the condensation of steam by the water spray. Spring-loaded safety valves are installed at the top of the pressuriser and provide overpressure protection for the RCS. These valves discharge into the containment atmosphere.

The RCS interfaces with a number of fluid auxiliary systems, principally the chemical and volume control system (CVS), the normal residual heat removal system (RNS), the steam generator system (SGS), the primary sampling system (PSS), the liquid radwaste system (WLS), and the component cooling water system (CCS). The RCS also interfaces with the (PXS).

When the reactor is shut down, the SGs provide cooling until system pressure and temperature are reduced to a level that can be accommodated by the RNS. The RNS takes its suction from one of the hot legs, the one that does not have the surge line connection to the pressuriser, and returns its cooled flow into the reactor vessel via both direct vessel injection lines.

When the reactor is to be refuelled, the refuelling cavity is flooded, after which the RV closure head is removed and then placed in its storage stand. The RNS continues to cool the reactor core but now also the refuelling cavity, by virtue of the RV being open to the water in this cavity.

The sections within this chapter of the PCSR provide detailed descriptions of these systems and their operation.

6.2 NORMAL OPERATIONS

Normal operation of the reactor covers all expected modes of operation including startup, power operation, shutdown, standby, and refuelling. Below are the six modes of normal operation defined with reference to nuclear reactivity (K_{eff}), thermal power, average coolant temperature, and vessel closure:

Mode		Reactivity Condition (K_{eff})	% Rated Thermal Power[1]	Average Reactor Coolant Temperature
1	Power Operation	≥ 0.99	> 5	N/A
2	Startup	≥ 0.99	≤ 5	N/A
3	Hot standby	< 0.99	N/A	> 215.6°C (420°F)
4	Safe shutdown[2]	< 0.99	N/A	≤ 215.6°C (420°F) > 93.3°C (200°F)
5	Cold shutdown[2]	< 0.99	N/A	≤ 93.3°C (200°F)
6	Refuelling[3]	N/A	N/A	N/A

Notes:
1. Excluding decay heat
2. All RV head closure bolts fully tensioned
3. One or more RV head closure bolts less than fully tensioned

6.2.1 Power Operation

In this mode, the reactor is producing power and generating electricity through the normal steam and power conversion systems: SGs, turbine, condenser, and main feed systems.

The steam generated in the two SGs is supplied to the high-pressure turbine by the MSS. After expansion through the high-pressure turbine, the steam passes through the two Moisture Separator Reheaters (MSRs) and is then admitted to the three low-pressure turbines. A portion of the steam is extracted from the high and low pressure turbines for seven stages of feedwater heating.

Exhaust steam from the low-pressure turbines is condensed and deaerated in the main condenser. The heat rejected in the main condenser is removed by the circulating water system (CWS). The condensate pumps take suction from the condenser hot well and deliver the condensate through four stages of low-pressure closed feedwater heaters to the fifth stage: an open deaerating heater. Condensate then flows to the suction of the SG feedwater booster pump(s) and then to the main feedwater pump(s). From there it passes through two stages of high-pressure feedwater heating to the two SGs.

Normal operating conditions (at full-power conditions) are defined in the Table below.

Rated thermal power	≈3415 MWt
Nominal power output	1100 MWe Class (actual net power depends on site-specific conditions)

SG outlet steam pressure	≈56 bar (812 psi)
SG outlet steam temperature	≈271°C (520°F)
Moisture carryover limit of the exiting flow	≈0.35%
SG feedwater temperature	≈227°C (440°F)
Flow rate per SG	≈3.40 x 106 kg/hr (7.50 x 106 lbm/hr)

6.2.2 Startup

Startup mode (Mode 2) includes the operations that bring the plant from a hot standby condition (Mode 3) to power operation (Mode 1), and conversely from Mode 1 to Mode 3.

Once the RCS has been heated up to hot standby conditions (Mode 3), the CVS removes boron from the RCS, thereby increasing reactivity until the reactor K_{eff} is ≥ 0.99 and Mode 2 is entered. Further increasing reactivity with boron and control rods raises reactor power. As power increases, feedwater continues to be supplied through the startup feedwater control valves until control of feedwater is automatically transferred from the startup feedwater control valves to the main feedwater control valves. As the main feedwater control valves open and assume responsibility for maintaining the SG water level, the startup feedwater control valves close. When thermal power (excluding decay heat) becomes greater than 5 percent of rated thermal power, Mode 1 is entered.

6.2.3 Hot Standby

Hot standby mode (Mode 3) includes conditions in which the reactor is kept subcritical but otherwise near normal power operation temperature conditions (>215.6°C (420°F)). From this mode, the reactor may be returned to power operation in a short time.

During hot standby conditions, feedwater is supplied to the SGs through the startup feedwater control valves using either one or both startup feedwater pumps drawing from the condensate storage tank, or a booster/main feedwater pump drawing from the deaerator storage tank. The startup feedwater control valves operate to maintain the SG levels, and minimum flow recirculation is automatically used as required to protect the feedwater pumps in use.

The steam generators maintain core decay heat removal as required, by relieving steam via the power operated relief valves or by dumping steam to the condenser via the steam bypass valve(s).

6.2.4 Safe Shutdown

The safe shutdown mode (Mode 4) includes keeping the reactor subcritical and the reactor coolant average temperature less than or equal to 215.6°C (420°F) but greater than 93.3°C (200°F), and providing adequate coolant inventory and core cooling. During normal operations, Mode 4 conditions are entered during plant heatups and cooldowns between Mode 3 (hot standby) and Mode 5 (cold shutdown). During Mode 4 operations the transition is made between decay heat removal by the steam generators and decay heat removal by the RNS.

It is important to note that “safe shutdown mode” (Mode 4) only applies to normal operation and does not apply to the post fault condition of “safe shutdown” discussed in Appendix 9C.

6.2.5 Cold Shutdown

Cold shutdown mode (Mode 5) is the state achieved through plant cooldown when reactor coolant temperature is ≤ 93.3°C (200°F) in preparation for a refuelling or other outage, and is also the starting point for power ascension before plant heat up.

During cold shutdown, decay heat is removed from the core via the RNS and criticality is controlled by maintaining adequate boron concentration of the coolant through the CVS. The RNS provides the motive force for the CVS purification loop during shutdown.

6.2.6 Plant Cooldown (Transition from Mode 1 to 5)

Plant cooldown are the operations that bring the reactor plant between power operation conditions (Mode 1) and cold shutdown conditions (Mode 5).

The initial phase of plant cooldown consists of reactor coolant cooldown and depressurisation. Heat is transferred from the RCS via the SGs to the MSS. Depressurisation is accomplished by spraying reactor coolant into the pressuriser, which cools and condenses the pressuriser steam bubble.

Operation during power descent and shutdown is generally the reverse of operation during startup and power ascent. At low feedwater flows, control of feedwater is automatically transferred from the main feedwater control valves to the startup feedwater control valves. Feedwater is supplied by an operating booster/main feedwater pump drawing from the deaerator storage tank. Feedwater can continue to be supplied by a booster/main feedwater pump during the shutdown process; alternatively, feedwater supply can be transferred to the startup feedwater pumps when flow demand has decreased to within their capacity. Feedwater continues to be supplied until the RNS is placed in service.

When the reactor coolant temperature and pressure have been reduced to approximately 176.7°C (350°F) and 31 bar (450 psi) respectively, the second phase of plant cooldown is initiated with the RNS being placed in service. The RNS continues to cool the RCS to cold shutdown conditions and is employed throughout the shutdown to remove core decay heat and maintain the RCS at low temperature.

Before cooldown and depressurisation of the RCS are initiated, the reactor coolant boron concentration is increased to a concentration necessary to maintain shutdown margin requirements. The operator sets the reactor makeup control to “borate” and selects the volume of boric acid solution necessary to perform the boration. Correct concentration is verified by reactor coolant samples using the PSS. The operator then sets the reactor makeup control for makeup at the shutdown reactor coolant boron concentration.

Contraction of the coolant during cooldown of the RCS results in actuation of the pressuriser level control system to maintain normal pressuriser water level. Makeup continues to be automatic, with the reactor makeup pumps starting and stopping as required. RCS letdown to the WLS is initiated as required to achieve the required boron concentration.

After the cooldown operations to cold shutdown conditions and as dictated by planned outage activities, the RCS water level is reduced. For normal refuelling, when maintenance activities will be performed on the SGs, the RCS is drained to the mid-loop level to allow air to be vented into the SGs from the pressuriser to drain the SG inverted U-tubes. The RCS is then

partially refilled, after placement of nozzle dams in the SG channel heads, in preparation for removal of the reactor vessel head.

6.2.7 Refuelling

6.2.7.1 Refuelling Operations

Refuelling is achieved by removing the IHP from the RV to access the fuel assemblies. The reactor is deemed to be in the refuelling mode (Mode 6) once any of the head bolts has begun to be untensioned.

To start refuelling operations, the IHP is unbolted and removed prior to the refuelling cavity being flooded from the IRWST. The reactor upper internals are then removed and placed on a stand in the refuelling cavity. Fuel may now be removed from the core.

The fuel handling equipment is designed to handle the spent fuel assemblies underwater from the time they leave the RV through storage in the spent fuel pit and until they are placed in a container for shipment from the site. Underwater transfer of spent fuel assemblies provides an effective and transparent radiation shield, as well as a reliable cooling medium for removal of decay heat.

The refuelling cavity (inside containment) and the fuel storage area (outside containment) are connected by the fuel transfer tube, which is fitted with a quick-opening transfer tube closure (blind flange) on the refuelling cavity end and a valve on the fuel storage area end and kept full of water at all times. The closure is in place except during refuelling to provide containment integrity. Fuel is carried through the tube on an underwater transfer car.

Fuel is moved between the RV and the fuel transfer system by the refuelling machine. The fuel transfer system is used to move a fuel assembly and its associated core component between the containment building and the auxiliary building fuel handling area. After a fuel assembly is placed in the fuel basket in the fuel transfer system, the lifting arm pivots the fuel assembly to the horizontal position for passage through the fuel transfer tube. After the transfer car transports the fuel assembly through the transfer tube, the lifting arm at that end of the tube pivots the assembly to a vertical position so that it can be lifted out of the fuel basket and placed in the spent fuel storage rack.

In the fuel handling area, fuel assemblies are moved about by the fuel handling machine. Initially, a short tool is used to handle new fuel assemblies, but the new fuel elevator must be used to lower the assembly to a depth at which the fuel handling machine and associated long-handled tool can place the new fuel assemblies in or remove them from the spent fuel storage racks.

New fuel assemblies received for refuelling are removed one at a time from the shipping container and moved into the new fuel assembly inspection area. After inspection, the accepted new fuel assemblies are stored in the new fuel storage rack. For the initial core load, new fuel assemblies may be stored in the SFP.

New fuel is moved into the core using the reverse procedure of the one for removing spent fuel from the core.

The new and spent fuel storage areas are accessible to operating personnel.

6.2.7.2 Fuel Storage

The spent fuel pool (SFP) provides storage space, heat removal and shielding for the spent fuel. The pool is approximately 12.8-m (42 ft.) deep and contains borated water with a nominal boron concentration of 2700 ppm. The spent fuel is stored in high-density racks that include integral neutron-absorbing material to maintain the specified degree of subcriticality. The design of the racks is such that a fuel assembly cannot be inserted into a location other than one designed to receive an assembly. The spent fuel storage racks include storage locations for 612 fuel assemblies and five defective fuel assemblies. This capacity affords at least 10 years of cooling time before dry casking. The defective fuel cell storage locations are designed to accommodate both new and spent fuel assemblies.

The spent fuel pool cooling system (SFS) is designed to remove decay heat generated by stored fuel assemblies from the water in the SFP. This is done by pumping the heated water from within the fuel pool through a heat exchanger (HX), and then returning the cooled water to the pool. A secondary function of the SFS is clarification and purification of the water in the SFP, the transfer canal, and the refuelling water.

The SFS consist of two independent pump/HX cooling trains. During normal plant power operation, only one of two SFS cooling trains is required to operate to maintain the fuel pool temperature at or below 48.9ºC (120ºF). During refuelling operations when the spent fuel is removed from the reactor vessel, both SFS cooling trains are required to be in operation to maintain the pool temperature at ≤48.9ºC (120ºF). In addition, an RNS cooling train can be aligned to cool the spent fuel pool if additional heat removal is required; for example, when all the fuel is removed from the reactor vessel and stored in the spent fuel pool.

Water transfers from the IRWST to the refuelling cavity are performed by the SFS. This function has traditionally been performed by the RNS. That capability still exists if the need arises. To improve clarity in the refuelling cavity and reduce operational radiation exposure, the SFS is used to flood the refuelling cavity without flooding through the RV.

Both residual heat removal pumps and HXs remain operating during refuelling to remove core decay heat from the fuel that remains in the reactor vessel. As decay heat decreases and as fuel is moved to the SFP, one residual heat removal pump and HX may be taken out of service. However, the RNS valves remain aligned to the RCS should the need arise to start this pump quickly in case the operating residual heat removal pump fails.

New fuel is stored in a high-density rack that includes integral neutron-absorbing material to maintain the required degree of subcriticality. The rack is designed to store 72 fuel assemblies of the maximum design-basis enrichment.

New fuel is initially stored in the new fuel storage racks. The fuel is then moved into the SFP before being loaded into the core by the refuelling machine.

The fuel handling machine is used to handle new fuel assemblies in the rail car bay, new fuel rack, and new fuel elevator. The capacity of the fuel handling machine, while over the new fuel storage rack, is limited to lifting a fuel assembly, control rod assembly, and handling tool. The new fuel storage rack is not accessed by the cask handling crane. This precludes the movement of loads greater than fuel components over stored new fuel assemblies.

During fuel handling operations, the Radiologically Controlled Area Ventilation System (VAS) removes gaseous radioactivity from the atmosphere above the new fuel pit and spent fuel storage pool.

The Technical Specifications (Reference 6.11) detail the requisite PCS make up water flows and requisite volumes (e.g. Fuel Transfer Canal, Cask Loading Pit, Cask Washdown Pit) depending on the Containment and SFP decay heat balance.

6.2.8 Other System Operations during Shutdown

The following aspects of system operation apply to several shutdown modes. A more detailed description of design features to mitigate shutdown risks is provided in Chapter 9 of this PCSR.

- Isolation of the main steam line on a high (large) negative rate of change in steam pressure is provided to address a steam line break that could occur in Mode 3. This signal is operable during Mode 3 when a secondary side break or stuck-open valve could result in the rapid depressurisation of the steam lines. In Modes 4, 5, and 6, this function is not needed for accident detection and mitigation.

- In Modes 2, 3, and 4, when the RCPs are operating, the secondary side of the SG is cooled by steaming to the main steam system (MSS). Once the RNS is aligned and steaming to the MSS is decreased, the primary side of the SGs is cooled by operation of the RNS. However, once the RCPs are tripped, there is no forced circulation through the primary side of the tubes and the secondary side of the SGs remains at elevated temperature. With the ability to cool the secondary side via the steam generator blowdown system, the AP1000 plant design reduces the probability that an RCP would be started with the secondary side of the SG at elevated temperature. This cooling also promotes equipment availability for maintenance at the earliest time in an outage.

- The core makeup tank (CMTs) provide RCS makeup. During shutdown, the CMTs are available in Modes 3, 4, and 5 until the RCS pressure boundary is open and the pressuriser water level is reduced. During power operation, the CMTs are automatically actuated on various signals including a safeguards actuation signal (low RCS pressure, low RCS temperature, low steam line pressure, and high containment pressure) and on low pressuriser water level.

- The in containment refuelling water storage tank (IRWST) provides a means for long-term RCS makeup. During shutdown, the IRWST is available until Mode 6, when the RV upper internals are removed and the refuelling cavity flooded. At that time, the IRWST is not required because the large heat capacity of its water is in the refuelling cavity.

- The passive residual heat removal (PRHR) HX provides decay heat removal following reactor trip during power operation and is required to be available in Mode 2 and in shutdown Modes 3, 4, and 5 until the RCS is open. In these modes, the PRHR HX provides a path for passive decay heat removal. In Mode 3, the accumulators must be isolated to prevent their operation when the RCS pressure is reduced to below their operating pressure.

- In Modes 5 and 6, containment closure capability is required to be available during shutdown operations when there is fuel inside containment. Containment closure is required to maintain the containment barrier capability in the unlikely event of radiation release from the fuel.

6.3 REACTOR SYSTEM

The reactor system (RXS) generates heat by a controlled nuclear fission reaction and transfers the heat generated to the reactor coolant, provides a barrier that prevents the release of fission products to the containment atmosphere, and provides a means via the control rods to insert negative reactivity into the reactor core and to shut it down.

The RXS consists of those major items of equipment constituting the operating nuclear reactor: RV (including the part of the head vent pipe shipped with the head), core, reactor internals, flow skirt, CRDMs, incore instrumentation system (IIS), rod position sensors, and IHP. The components of the RXS are integrated in a manner which will assure safe and economical operation of the system and equipment.

Further design details of the system and its constituent components are delineated in Reference 6.12. The fuel is described in further detail in Chapter 22.

6.3.1 Reactor System Components

The reactor system consists of the following components:

- RV
- IHP
- Reactor upper and lower internals assemblies
- Fuel assemblies (157)
- Rod cluster control assemblies (53) and grey rod cluster assemblies (16)
- Discrete burnable absorber and neutron source assemblies
- Control rod drive mechanisms (69)
- In-core instrumentation (IIS)

Major components of RXS are shown in Figures 6-9, 6-10, and 6-19. The location of the RV and the IHP with respect to the layout of the major RCS components is shown in Figure 6-2.

The AP1000 plant reactor internals consist of two major assemblies: the lower internals and the upper internals. The reactor internals provide alignment and support for the core, control rods, and grey rods in order to provide safe and reliable reactor operation. In addition, the reactor internals help to accomplish the following: direct the main coolant flow to and from the fuel assemblies; absorb control rod dynamic loads, fuel assembly loads, and other loads and transmit these loads to the RV; support instrumentation within the RV; provide protection for the RV against excessive radiation exposure from the core; and position and support RV radiation surveillance specimens.

The AP1000 plant CRDM design is based on a proven Westinghouse design that has been used in many operating nuclear power plants.

The IHP combines several components in one assembly to simplify refuelling the reactor. The IHP includes: a lifting rig, seismic restraints for CRDMs; supports for reactor head vent piping, power cables, cables for in-core instrumentation, cable bridge, quickloc connectors, and cables; and the CRDM cooling shroud assembly.

The reactor core contains a matrix of fuel rods assembled into fuel assemblies using structural elements. RCCAs are normally withdrawn, inserted, or held within the fuel assemblies by the CRDMs. The CRDMs unlatch upon termination of electrical power to them, thereby releasing the RCCAs to fall by gravity into core region. During operation, the RCPs circulate

pressurised water through the RV and the SGs. The water serves as coolant, moderator, and solvent for boric acid (chemical shim control). The water is heated as it passes through the core and then flows to the SGs, where the heat is transferred to the secondary side of the SGs. The SGs produce steam that is transported to the turbine via the main steam system. The cooled water is then returned to the reactor (core) by the pumps to repeat the process.

6.3.1.1 Reactor Vessel

The RV (RCS-MV-01) is cylindrical, with a hemispherical bottom head and a removable, flanged, hemispherical upper head. The vessel contains the core, core support structures, control rods, and other parts directly associated with the core (see Figure 6-9). The vessel interfaces with the reactor internals, the IHP, and reactor coolant loop piping, and is supported on the containment building concrete structure.

The design of the AP1000 plant RV closely matches the existing vessel designs of Westinghouse three-loop plants. New features for the AP1000 plant have been incorporated without departing from the proven features of existing vessel designs.

The vessel has inlet and outlet nozzles positioned in two horizontal planes between the upper head flange and the top of the core. The nozzles are located in this configuration to provide an acceptable crossflow velocity in the vessel outlet region and to facilitate optimum layout of the RCS equipment. The vessel inlet and outlet nozzles are offset, with the inlet nozzles positioned above the outlet nozzles, to allow draining of the RCS cold legs to facilitate maintenance operations while maintaining RNS flow for core decay heat removal into the RV direct vessel injection (DVI) lines through the core to the hot leg.

A large circumferential spring is positioned on the top surface of the core barrel flange. The upper support plate rests on the top surface of the spring. The spring is compressed by installation of the RV closure head and the upper and lower core support assemblies are restrained from any axial movements.

Coolant enters the vessel through the inlet nozzles and flows down the core barrel vessel wall annulus, passes through the flow skirt, turns at the bottom, and flows up through the core to the outlet nozzles.

The RV supports and encloses the reactor core. It provides flow direction with the reactor internals through the core and maintains a volume of coolant around the core. The vessel is cylindrical, with a transition ring, hemispherical bottom head, and removable flanged hemispherical upper head. The vessel is fabricated by welding together the lower head, the transition ring, the lower shell, and the upper shell. The upper shell contains the penetrations for the inlet and outlet nozzles and direct vessel injection nozzles. The closure head is fabricated with a head dome and bolting flange. The upper head has penetrations for the CRDMs, the in-core instrumentation, and head vent; and has support lugs for the IHP.

The RV (including closure head) is approximately 12 m (40 feet) long and has an inner diameter at the core region of approximately 4 m (159 inches). The total weight of the vessel assembly (including closure head, CRDMs, studs, nuts, and washers) is approximately 408.2 tonnes (450 tons).

The RV surfaces that can become wetted during operation and refuelling are clad to a nominal 5.6 mm (0.22 inch) of thickness with a stainless-steel welded overlay that includes the upper shell top flange surface but not the stud holes. The AP1000 plant RV is designed to have a 60-year operational life considering its neutron flux exposure, design pressure and temperature (172.3 bar (2500 psi) and 343.3°C (650°F)), and operational transients.

The major factor affecting vessel life is radiation degradation of the lower shell. As a safety precaution, there are no penetrations below the top of the core.

6.3.1.2 Reactor Vessel Insulation

Stainless steel reflective insulation (RXS-MN-01) is used to insulate the RV outside surface and minimize heat losses through the wall.

In the unlikely event of a design basis accident in which the reactor cavity is flooded with water, water inlet assemblies at the bottom of the RV insulation will self-actuate to permit a water layer to form between the RV and insulation and promote heat transfer from the RV to the surrounding environment. The resultant steam-water mixture will uncap steam vent ducts located near the top of the vessel insulation and return back to the containment flood water.

For post loss of coolant accident (LOCA) long-term core cooling, the plant is designed to automatically depressurize the RCS to equilibrium pressure with the containment atmosphere and to submerge the reactor vessel up to the upper head flange elevation.

6.3.1.2.1 In-Vessel Retention

The insulation around the RV is specially designed for In Vessel Retention (IVR) of molten core debris to mitigate a severe accident (see Figure 6-18). IVR in the lower plenum of the AP1000 plant is an inherent severe accident management strategy of the passive plant. The IVR function is a passive means of providing mitigation of severe core damage accidents. In a postulated severe accident, failure of Class 1 and 2 SSCs providing the core decay heat removal or core reactivity control Category A safety functions would lead to core damage and, eventually, to core melting. The behaviour of the molten core is the subject of severe accident analysis and probabilistic risk assessment. The Reactor Vessel Cavity Reflective Insulation is Category A Class 1 equipment and is Seismic Category II (see Table 15A). This special RV insulation is also discussed in Chapter 10.

IVR of molten core debris through water cooling of the external surface of the RV is a severe accident management feature of the AP1000 design. During postulated severe accidents, the accident management strategy to depressurise the RCS and flood the reactor cavity with IRWST water submerging the RV, is credited with preventing vessel failure in the AP1000 Probabilistic safety Assessment (Chapter 10). The water cools the external surface of the vessel and prevents molten debris in the lower head from failing the vessel wall and relocating into the containment.

Retaining the debris in the RV protects containment integrity by eliminating the occurrence of ex-vessel severe accident phenomena, such as ex-vessel steam explosion and core-concrete interaction, which have large uncertainties with respect to containment integrity.

The AP1000 design provides for IVR with the following features that promote external cooling of the RV:

- The reliable multistage RCS depressurisation system results in low stresses on the vessel wall after the pressure is reduced.
- The vessel lower head has no vessel penetrations to provide a failure mode for the vessel other than creep failure of the wall itself.
- The floodable reactor cavity can submerge the vessel above the coolant loop elevation with water intentionally drained from the IRWST.

- The RV insulation provides an engineered pathway for water-cooling the vessel and for venting steam from the reactor cavity.

The phenomena associated with melting the core and relocating the molten debris to the lower plenum play an important role in the composition and configuration of the debris pool following an unprotected severe accident (Reference 6.4). In turn, the characteristics of the debris pool significantly impact the heat loading to the lower head wall and the challenge to lower head integrity (Reference 6.4). Therefore, understanding the melting and relocation scenarios plays an important role in the assessment of IVR of molten core debris in the lower plenum.

The important conclusions from the analysis of the lower plenum debris pool formation are as follows:

- The lower plenum debris bed is cooled with water during the entire relocation process prior to contact with the support plate. Transient debris configurations are not predicted to threaten vessel integrity.

- The lower plenum oxide debris subsumes the lower core support plate before dryout in the lower plenum occurs. If the relocated debris is assumed to be instantaneously quenched in the lower plenum water, the oxide debris contacts the lower support plate before the debris can return to a superheated condition. Therefore, the lower core support plate, core shroud, and a sizeable fraction of the core barrel are subsumed in the debris bed. The inclusion of these components in the debris bed provides sufficient metal to ensure adequate heat transfer surface to the vessel wall such that the focusing effect of a thin metal layer is mitigated.

- The lower plenum debris bed is predicted to form a metal layer over oxide pool configuration.

- The potential for debris interaction creating a bottom metal pool of uranium dissolved in zirconium is expected to be small.

- The earliest time to achieve the fully molten circulating debris bed in the lower plenum is several hours after event initiation.

With the cavity adequately flooded, significant margin to failure for IVR via external RV cooling is achieved provided that the following conditions are met:

- The RCS is depressurised.

- The vessel is submerged adequately to promote natural circulation of water through the annular space between the vessel insulation and the vessel lower head and sidewalls.

- RV reflective insulation remains structurally sound under the pressure loads produced by the boiling external to the RV, allows water inlet at the bottom and venting of steam at the top, and provides the proper baffling to increase the critical heat flux on the external surface of the vessel lower head.

- The RV external surface conditions do not preclude the wetting phenomena identified as the cooling mechanism in system testing.

RCS depressurisation is achieved using the automatic depressurisation system (ADS) in the event of intact RCS faults or small and medium LOCAs, or by the LOCA itself.

Reactor cavity flooding is accomplished through either operator action or the progression of the accident. The operator manually floods the cavity by opening a motor-operated valve and a squib valve in the recirculation lines between the IRWST and the containment recirculation sump. The water floods the containment by flowing out of the recirculation screens, filling the floodable region of the containment.

To achieve the high critical heat flux for the AP1000 plant lower head, the water level in containment must be sufficient for two-phase natural circulation flow. The vents from the AP1000 plant RV insulation exit to the vessel nozzle gallery.

With respect to IVR severe accident management, the goal of the RV insulation is to ensure that there will always be an adequate water layer next to the RV to promote heat transfer from it. The insulation will define an optimised flow path next to the lower head to enhance the critical heat flux. The cooling of the vessel in a severe accident is accomplished by providing the following:

- A means of allowing water-free access to the region between the RV and insulation.
- A frame that maintains the structural integrity of the insulation surrounding the lower head, which provides the annular space for the water flow next to the vessel.
- A means to vent steam generated by the water cooling the vessel wall from the insulation surrounding the RV.
- A support frame to prevent the insulation panels above the vessel lower head from breaking free and blocking water from cooling the RV exterior surface.

6.3.1.3 Integrated Head Package

The IHP (Figure 6-10) combines several components in one assembly to simplify refuelling the reactor. The IHP includes a lifting rig, seismic restraints for CRDMs, support for the reactor head vent piping, cable bridge, quickloc connectors, power cables, cables for in-core instrumentation, cable supports, and the CRDM cooling shroud assembly.

The IHP provides the ability to rapidly disconnect cables, including the CRDM power cables, digital rod position indication cables, and in-core instrument cables from the connector/penetration components on the upper head. The IHP also provides the ability to rapidly disconnect the reactor head vent system.

The IHP provides the ability to disconnect these components so that the RV upper head can be lifted and removed. In addition, the IHP provides support for the vessel head stud tensioner/detensioner during refuelling.

The purpose of the IHP is to reduce the outage time and personnel radiation exposure by combining operations associated with movement of the RV head during the refuelling outage.

In addition, the integrated head concept reduces the laydown space required in the containment. With the IHP, disconnections from and connections to the interfacing components are not made at the individual component. This applies to the CRDMs, rod position indicators (RPI), and other components within the cooling shroud assembly. The IHP consists of the following components:

- Shroud assembly
- Lifting system
- Mechanism seismic support structure
- Cable support structure
- Cables
- In-core instrumentation (IIS)

These principal elements of the IHP are described in the following paragraphs.

Shroud Assembly

The shroud assembly is a carbon steel structure that includes a shielding shroud and an air baffle. During normal operation, it directs the flow of cooling air to the CRDM coil stacks. The Rod Position Indicators are also cooled by this airflow. The duct work and air baffle are integral to, and supported by, the shroud assembly. The air-cooling fans are attached to the IHP. The shroud also provides shielding at the vessel flange region.

CRDM Cooling Fan System

The cooling of the CRDM coil stacks and digital rod position indication (DRPI) system is provided by four vane axial fans mounted 90° apart on the IHP shroud. Each fan is connected to the IHP shroud by flexible expansion joint connectors. Containment air is drawn in through multiple cut-outs located on the lower portion of the shroud and directed by baffles up through the CRDM rod travel housings. The air is then pulled through four inlet ducts located near the top of the IHP shroud positioned 90° apart, pulled through fans, and exhausted back into containment. Any two of the fans can operate to provide CRDM cooling, and two backup fans are available.

Reactor Vessel Head Lifting Rig

This apparatus supports the RV head and IHP as a single unit when it is lifted by the polar crane. The lift legs transfer the head load during a head lift from the head attachment lugs to the lift rig. The lifting system consists of lift legs, sling block, clevises, sling rods, and a lifting linkage assembly required for interfacing with the polar crane hook.

Mechanism Seismic Support Structure

This structure provides seismic restraint for the CRDMs. It is located near the top of the CRDM rod travel housings. The digital rod position indication connector plate attached to the rod travel housing interfaces with spacer plates, where required, to form a system of bumpers that interface with the mechanism seismic support structure. This support interfaces with the shroud assembly to transfer seismic loads from the mechanisms to the Reactor Vessel head.

Cable Support Structure

The cable support structure is located at an elevation above the top of the rod travel housings. It provides permanent support and routing for the CRDM power cables and RPI cables, which remain with the IHP and are normally not disturbed. These cables terminate at the connector plates, which constitute the interface with the mating cables.

Cable Bridge

The cable bridge provides support for the cables between the connector plate on the containment operating deck and the IHP. The cable bridge is attached to the IHP by a pivot-type connection, which allows upward movement of the bridge. For a refueling or other operation requiring movement of the IHP, the cables on the bridge are disconnected at the connector panel on the operating deck. Then, the bridge is swung up and away from the containment operating deck and secured to the IHP.

6.3.1.4 In-Core Instrumentation System

The IIS consists of thermocouples to measure fuel assembly coolant outlet temperature, and in-core flux thimbles containing fixed detectors to measure the neutron flux distribution within the reactor core. The in-core thimble tubes have enhanced resistance to fluid-induced vibration and wear. The thimble is stiffer than the design in previous operating plants; the gap between the thimble tube and the tubes used to guide and protect the thimble inside the RV is smaller to minimise vibration. The design of the thimble tube assembly also precludes a non-isolatable leak of reactor coolant. The thermocouples and neutron detectors are routed through the IHP. They are inserted into the core through the RV head and upper internals assembly.

The CRDMs (described in more detail later) are contained within the IHP located on top of the RV head. This assembly provides the support required for seismic restraint in conjunction with the attachment of the CRDMs to the RV head. An outer shroud (an integral portion of the head lifting system) and the seismic support plate isolate the CRDMs from the effects of ruptured high-energy lines outside the shroud, and from missiles. The shroud is also used to direct air from the cooling fans past the CRDMs. The cooling system maintains the temperature of the coils in the CRDMs below their design operating temperature.

The lines for the RV vent system are located among the CRDMs and are supported by the IHP. These lines are pressurised to RCS pressure and are considered high-energy.

6.3.1.5 Reactor Internals

The interfaces between the RV and the lower internals core barrel are such that the main coolant flow enters through the inlet nozzle and is directed down through the annulus between the RV and core barrel and through the flow skirt, and flows up through the core. The annulus is designed so that the core remains in a configuration that can be cooled for all design conditions.

Lower Internals (RXS-MI-02)

The lower core support assembly consists of the core barrel, lower core support plate, secondary core support, vortex suppression plate, core shroud, neutron panels, radial supports, and related attachment hardware. The major material for the lower internals is 300 series austenitic stainless steel. The lower core support assembly is supported at its upper flange from a ledge in the RV flange. Its lower end is restrained in its transverse movement by a support system attached to the vessel wall. The support system consists of keys attached to the lower end of the core barrel subassembly. These keys engage clevis inserts in the RV. This system restricts the lower end of the core barrel from rotational and/or translational movement, but allows for radial thermal growth and axial displacement.

The flow skirt is a perforated cylindrical ring that is an attachment to the RV bottom head. Since this structure is located within the pressure boundary, it will be described here. The

flow skirt is welded to support lugs on the inside surface of the RV bottom head. A vertical clearance is provided between the top of the flow skirt and the bottom surface of the lower core support plate to prevent contact during operation. The flow skirt provides a more uniform core inlet flow distribution.

The core shroud is located inside the core barrel and above the lower core support. This shroud forms the radial periphery of the core. The core shroud is between the lower core barrel and core, surrounding the core and forming the core cavity. The core shroud consists of formed vertical plates with fully welded vertical seams to prevent lateral flow from the fuel assemblies.

The core shroud serves to provide a transition from the round core barrel to the square fuel assemblies. Through the dimensional control of the cavity (the gap between the fuel assemblies and the shroud) and the shroud cooling flow hole inlet size, the core shroud limits the reactor coolant flow around the core periphery and maintains the required flow through the core.

During assembly, as the internals are lowered into the vessel, keys engage keyways in the axial direction. Correct positioning of the internals is provided by the installation equipment (lifting rig) guide studs and bushings. In this design, the internals have a support at the furthest extremity, and the core barrel is modelled as a beam, which is supported at the top and bottom.

Upper Internals (RXS-MI-01)

The support grid assembly establishes the spacing between the upper support and the upper core plate. The support columns are fastened at the top and bottom to these plates. The support columns transmit the mechanical loadings between the two plates; some serve the supplementary function of supporting the tubes that house the fixed in-core instrumentation.

The instrument columns housing the in-core instrumentation provide a protective path for the detectors during installation, reactor operation, and removal at refuelling outages.

The guide tube assemblies sheath and guide the control rod drive shafts and control rods. The guide tubes are fastened to the upper support and are restrained by pins in the upper core plate for proper orientation and support.

The upper core support assembly is positioned in its proper orientation, with respect to the lower core support assembly, by flat-sided pins in the core barrel. Four equally spaced flat-sided pins are located at an elevation in the core barrel where the upper core plate is positioned. Four mating sets of inserts are located in the upper core plate at the same positions. As the upper support assembly is lowered into the lower support assembly, the inserts engage the flat-sided pins in the axial direction. Lateral displacement of the plate and the upper support assembly is restricted by this design.

Fuel assembly locating pins protrude from the bottom of the upper core plate and engage the fuel assemblies as the upper assembly is lowered into place. This system of locating pins and guidance arrangement provides proper alignment of the lower core support assembly, the upper core support assembly, the fuel assemblies, and the control rods.

6.3.1.6 Fuel Assemblies and Core Components

Within the reactor core there are 157 fuel assemblies. Each fuel assembly contains 264 fuel rods, 24 guide thimble tubes, and an instrumentation thimble tube arranged to form a 17 x 17

fuel assembly (see Figure 6-11). Further design details of the fuel assemblies and its constituent components are delineated in Reference 6.12. The fuel assembly is also described in Chapter 22.

The instrumentation thimble is located in the center position and provides a channel for insertion of seven incore neutron flux detectors and one core exit thermocouple. The performance of the core is monitored by fixed neutron detectors outside the core, removable fixed neutron detectors within the core, and thermocouples at the outlet of selected fuel assemblies. The fuel assembly structure is designed to completely enclose the fuel rods and to provide a clearance between the fuel rod ends and the top and bottom nozzles of the fuel assembly structures. All fuel assemblies in the core are identical in construction.

Each fuel assembly is installed vertically in the reactor vessel and stands upright on the lower core plate, which is fitted with alignment pins to locate and orient the assembly (See Figure 6-9). Once the fuel assemblies are properly positioned in the core, the upper core plate is installed by lowering it in place over the fuel assemblies. Alignment pins, built into the upper core plate, engage and fix the upper ends of the fuel assemblies. The upper core plate then bears downward against the fuel assembly top nozzle with the holddown springs to keep the fuel assemblies in place.

The bottom nozzle serves as a bottom structural element of the fuel assembly and directs the coolant flow distribution to the assembly (see Figure 6-11). Coolant flow through the fuel assembly is directed from the plenum in the bottom nozzle upward through the penetrations in the plate to the channels between the fuel rods. The top nozzle assembly functions as the upper structural element of the fuel assembly in addition to providing a partial protective housing for the core components.

The previously mentioned 24 guide thimbles are structural members which provide channels for the RCCAs, GRCAs, wet annular burnable absorbers (WABAs), and source assemblies. The guide thimbles are fastened to the grids and end nozzles to create an integrated structure. The grid assemblies support the fuel rods and maintain the lateral spacing between the rods. Depending on the position of the assembly in the core, the guide thimbles are used for RCCAs, GRCAs, neutron source assemblies, WABA rods, or thimble plugs.

The fuel grids consist of an egg-crate arrangement of interlocked straps that maintain lateral spacing between the rods. The grid straps have spring fingers and dimples that grip and support the fuel rods. In addition, there are four intermediate flow mixing (IFM) grids that have coolant mixing vanes to provide improved departure from nucleate boiling (DNB) performance. The IFM grid straps contain support dimples and coolant mixing vanes only. The top and bottom grids and protective grid do not contain mixing vanes. The AP1000 plant fuel assembly design also includes a protective grid for enhanced debris resistance.

The bottom nozzle is a box-like structure that serves as the lower structural element of the fuel assembly and directs the coolant flow distribution to the assembly. The size of flow passages through the bottom nozzle limits the size of debris that can enter the fuel assembly.

The AP1000 plant fuel assembly design is similar in design to fuel assemblies used in legacy Westinghouse power plants. These two legacy fuel assembly designs are the 17×17 Robust and 17×17 XL Robust. The 17×17 Robust fuel assemblies have an active fuel length of 3.66 m (12 feet) and three IFM grids in the top mixing vane grid spans. The 17×17 XL Robust fuel assemblies have an active fuel length of 4.27 m (14 feet) with no IFM grids. The AP1000 plant fuel assemblies are the same as the 17×17 XL Robust fuel assemblies except that they have four IFM grids in the top mixing vane grid spans.

Core components include RCCAs, GRCAs, burnable absorbers rods (which include WABAs and integral fuel burnable absorbers (IFBAs)), thimble plugs, and source rods. A brief description of each component is provided in the following sections.

6.3.1.6.1 Fuel Rods

The fuel rods consist of uranium dioxide ceramic pellets contained in cold-worked and stress-relieved ZIRLO™ tubing, which is plugged and seal-welded at the ends to encapsulate the fuel. The rod is pressurized with an inert gas (helium) to prevent collapse under the RCS pressure. The fuel pellets are right circular cylinders consisting of slightly-enriched uranium.

The reactor contains a matrix of fuel rods assembled into mechanically identical fuel assemblies along with control and structural elements. The fuel assemblies contain various fuel enrichments, are configured into the core arrangement and are located and supported by the reactor internals.

Fuel rods are pressurised internally with helium during fabrication to reduce clad creep-down during operation and thereby prevent clad flattening. The fuel rods in the AP1000 plant fuel assemblies contain additional gas space above the fuel pellets, compared with the 17×17 Robust, 17×17 XL Robust, and other previous fuel assembly designs, to allow for increased fission gas production due to high fuel burnups.

6.3.1.6.2 Rod Cluster Control Assemblies

Each RCCAs consist of 24 absorber rodlets fastened at the top end to a common hub, or spider assembly. Each absorber rod consists of an alloy of silver-indium-cadmium (Ag-In-Cd), which is clad in stainless steel. The RCCAs are used to control relatively rapid changes in reactivity and to control the axial power distribution.

The absorber Ag-In-Cd alloy, which is essentially “black” to thermal neutrons and has sufficient additional resonance absorption to significantly increase worth. As such, these rods are sometimes referred to as “black” rods. The absorber material is in the form of solid bars sealed in cold-worked stainless-steel tubes.

The RCCAs are divided into two categories: control and shutdown. The control groups compensate for reactivity changes due to variations in operating conditions of the reactor, that is, power and temperature variations. Two nuclear design criteria have been used to select the control group. First, the total reactivity worth must be adequate to meet the nuclear requirements of the reactor. Second, in view of the fact that these rods may be partially inserted at power operation; the total power peaking factor should be low enough to confirm that the power capability is met. The control and shutdown groups provide adequate shutdown margin.

The control rods have bottom plugs with bullet-like tips to reduce the hydraulic drag during reactor trip and to guide smoothly into the dashpot section of the fuel assembly guide thimbles.

The spider assembly is in the form of a central hub with radial vanes containing cylindrical fingers from which the absorber rods are suspended. Internal groove-like profiles to facilitate handling tool and drive rod assembly connection are machined into the upper end of the hub. Coil springs inside the spider body absorb the impact energy at the end of a trip insertion. The radial vanes may either be joined to the hub by welding or brazing. The fingers are joined to the vanes by brazing, or the vanes and fingers may be integral with the spider body. A bolt,

which holds the springs and retainer, is threaded into the hub within the skirt and is welded to prevent loosening while in service.

The overall length of the RCCA is such that, when the assembly is withdrawn through its full travel, the tips of the absorber rods remain engaged in the guide thimbles so that alignment between rods and thimbles is always maintained. Because the rods are long and slender, they are relatively free to conform to any small misalignments with the guide thimble.

Each RCCA is moved independently in and out of the reactor core by CRDMs. The CRDMs operate in response to the actuation and control of the signals provided by the PLS and PMS.

6.3.1.6.3 Grey Rod Control Assemblies

Externally, the mechanical design of the GRCA is identical to the RCCA. In addition, the CRDM and the interface with the fuel assemblies and guide thimbles are identical to those of the RCCA.

The GRCAs consist of 24 rodlets fastened at the top end to a common hub or spider assembly. Geometrically, the GRCA is the same as an RCCA except that the absorber rods consist of tungsten contained within a nickel-chromium-iron Alloy 718 sleeve. Stainless steel spacers are provided at the bottom of the rodlet between the bottom of the sleeve and the bottom end plug of the stainless steel cladding. The GRCAs are used in base load operation and load follow manoeuvring. The assemblies provide a mechanical shim reactivity mechanism to minimise the need for changes to the concentration of soluble boron.

Soluble boron in the moderator/coolant serves as a neutron absorber. The concentration of boron is varied to control reactivity changes that occur relatively slowly, including the effects of fuel burnup. Burnable absorbers are also used in the initial cycle to limit the amount of soluble boron required and thereby maintain the desired negative reactivity coefficients.

Each GRCA is moved independently in and out of the reactor core by CRDMs. The CRDMs operate in response to the actuation and control of the signals provided by the plant control system (PLS) and protection and safety monitoring system (PMS).

6.3.1.6.4 Burnable Absorbers

Burnable absorbers are normally used to compensate for some of the installed excess reactivity and to ensure that a negative moderator temperature coefficient is maintained. When needed for nuclear considerations, BA assemblies are inserted into selected thimbles within fuel assemblies.

The WABAs are discrete burnable absorber rods which use aluminum oxide-boron carbide (Al_2O_3-B_4C) as an absorber material. They are attached to a holddown assembly which consists of a flat perforated base plate and a spring pack assembly. The number of absorber rods per assembly varies depending on its position in the core. The length of the absorber can also vary. The WABA rods consist of pellets of alumina-boron carbide material contained within zirconium alloy tubes. These zirconium alloy tubes, which form the outer clad for the BA rod, are plugged, pressurised with helium, and seal-welded at each end to encapsulate the stack of absorber material.

The WABA is an alternative discrete BA. The BA material is boron carbide contained in an alumina matrix.

IFBAs use a thin coating of boride on the surface of the fuel pellets, thus the absorber is said to be integral to the fuel rather than discrete. The number of fuel rods containing IFBA within a given fuel assembly can vary, as can the number of the fuel pellets in a fuel rod coated with absorber.

Discrete BA rods are designed so that the absorber temperature does not exceed 649°C (1200°F) during normal operation or an overpower transient.

6.3.1.7 Neutron Source Assemblies

The neutron sources are normally required for the initial cycle only. The neutron source rods provide a minimum base neutron level to maintain a detectable signal even under reactor shutdown conditions. The primary source contains a radioactive material which spontaneously emits neutrons during initial core loading, reactor start up, and initial operation of first core. Secondary source rods contain a stable material which is activated by neutron bombardment during reactor operation.

The purpose of a neutron source assembly is to provide a base neutron level to give confidence that the detectors are operational and responding to core multiplication neutrons. For the first core, a neutron source is placed in the reactor to provide a positive neutron count of at least two counts per second on the source range detectors attributable to core neutrons. The detectors, called source range detectors, are used primarily during subcritical modes of core operation.

Both primary and secondary neutron source rods are used. The primary source rod, containing a radioactive material, spontaneously emits neutrons during initial core loading, reactor startup, and initial operation of the first core. After the primary source rod decays beyond the desired neutron flux level, neutrons are then supplied by the secondary source rod. The secondary source rod contains a stable material, which is activated during reactor operation. The activation results in the subsequent release of neutrons.

Four source fuel assemblies are typically installed in the initial load of the reactor core: two primary source fuel assemblies and two secondary source fuel assemblies. Each primary source assembly contains one primary source rod and a number of BA rods. Each secondary source assembly contains a symmetrical grouping of secondary source rodlets.

Neutron source assemblies are employed at opposite sides of the core. The source assemblies are inserted into the rod cluster control guide thimbles in fuel assemblies at selected locations.

The primary and secondary source rods both use the same cladding material as the absorber rods. The secondary source rods contain antimony-beryllium pellets stacked to a height of approximately 2235 mm (88 inches). The primary source rods contain capsules of californium (or plutonium-beryllium as a possible alternative) source material and alumina spacers to position the source material within the cladding.

The neutron source rods are designed to withstand the following:

- The external pressure equal to RCS operating pressure with appropriate allowance for overpressure transients.
- An internal pressure equal to the pressure generated by released gases over the source rod life.

6.3.1.8 Control Rod Drive Mechanisms

CRDMs are located within the CRDM pressure housings, which penetrate through the head of the RV, and include electrically powered magnets located outside the pressure housing. They are coupled to drive rods of the RCCAs that have neutron absorber material over the active length of the control rods and the GRCAs. Externally, the GRCAs are geometrically identical to the RCCAs.

The primary function of the CRDM is to insert or withdraw, at a designated speed, 53 RCCAs and 16 GRCAs to/from the core to compensate for reactivity changes due to variation in power and temperature.

CRDMs independently move each of the RCCAs and GRCAs into and out of the reactor core.. Each cluster is in a bank used for reactivity control, axial power distribution control, or shutdown control. The control assemblies of each bank of several RCCAs or GRCAs move at the same time.

The design of the CRDMs also permits holding the RCCAs and the GRCAs at any step elevation within the range of rod travel during normal operation. The RCCAs and GRCAs have the same mechanical coupling with the CRDM.

The CRDM is a magnetically operated jack (magjack). A magjack is an arrangement of three electromagnets energised in a controlled sequence by a power cycle to insert or withdraw RCCAs and GRCAs in the reactor core in discrete steps. The CRDM is designed to release the drive rod and RCCA or GRCA during any part of the power cycle sequencing if electrical power to the magnetic coils is interrupted. When released from the CRDM, the drive rod and RCCA or GRCA fall by gravity into a fully inserted position.

The CRDM withdraws and inserts a RCCA or GRCA as shaped electrical pulses are received by the operating coils. An on or off sequence is repeated by silicon-controlled rectifiers in the power programmer and causes the control rod to be withdrawn or inserted. The drive rod and RCCA or GRCA are withdrawn by magnetic forces, or inserted by gravity.

During plant operation, the stationary gripper coil and movable gripper coil of the drive mechanism hold the RCCA in a static position until a stepping sequence is initiated, at which time the stationary gripper coil, movable gripper coil, and lift coil are energised sequentially.

The control rod position is measured by 48 discrete coils mounted on the position indicator assembly surrounding the rod travel housing. Each coil magnetically senses the entry and presence of the top of the ferromagnetic drive rod assembly as it moves through the coil centreline.

The design and construction of the CRDM include provisions to establish that gross failure of the housing sufficient to allow ejection of a control rod from the core is not credible. (Control rod ejection is discussed further in Section 9.4.)

During most of the plant operating time, the CRDMs hold the RCCAs withdrawn from the core in a static position. During most plant operation, the GRCAs are held by the CRDMs withdrawn or inserted in the core in a static position as directed by flux shape considerations. In the holding mode, two coils – stationary gripper coil A and movable gripper coil B – are energised on each mechanism. The drive rod assembly and attached RCCAs or GRCAs hang suspended from the three latches of the stationary gripper. In addition, the three latches of the movable gripper are engaged to hold the drive rod assembly in place in the event of a failure that would cause the release of the stationary gripper.

When the driveline is positioned in the last few steps, the RCCAs and GRCAs are out of the last portion of the core, although not fully withdrawn from the fuel assemblies. The rod clusters cannot be physically withdrawn from the guide tubes by the CRDMs since no additional grooves are machined in the drive rod past the last position.

If power to the stationary and movable gripper coils is cut off, the combined weights of the drive rod assembly and the RCCA or GRCA (plus the stationary gripper and movable gripper return springs) move the latches out of the drive rod assembly groove. The trip occurs as follows:

- The magnetic field, holding the stationary gripper plunger against the stationary gripper pole, collapses; the stationary gripper plunger is forced down by the stationary gripper return spring and the weight acting upon the latches.

- The magnetic field, holding the moveable gripper plunger against the movable gripper pole, collapses; the movable gripper plunger is forced down by the moveable gripper return spring and the weight acting upon the latches.

The control rod falls by gravity into the core. After the driveline is released by the mechanism, it falls freely until the control rods enter the dashpot section of the fuel assembly, where the coolant in the guide tubes slows the rate of descent until the rods are fully inserted. Figures 17A-1 through Figure 17A-7 provide further detail of the CRDM.

6.3.1.9 Control and Instrumentation

This section describes the control and instrumentation for the RV/core.

Rod Position Indicators

The only instrumentation required for the CRDM and supporting systems to operate safely is the RPI. Both the digital rod position indication (DRPI) system and the digital rod control system (DRCS) are functions of the plant control system (PLS).

The DRPI system measures the position of each control rod assembly using rod position detector assemblies. A detector assembly consists of discrete coils mounted concentrically with the rod drive pressure housing. The coils are located axially along the pressure housing and magnetically sense the entry and presence of the rod drive shaft through its centreline. The signals from the detectors are processed by the data cabinets and transmitted to the distributed controllers. The distributed controllers further process the rod position information and transmit this information to the real-time data network.

Rod Position Indication Systems

The axial position of shutdown rods and control rods is indicated by two separate and independent systems: the bank demand position indication (Bank Demand Position Indication (BDPI), also commonly called group step counters) and DRPI.

Bank Demand Position Indication System

The BDPI system counts the pulses generated in the rod control system and provides a digital readout of the demanded bank position. There is one step counter for each group of rods. Individual rods in a group all receive the same signal to move and should, therefore, all be at the same position indicated by the group step counter for that group. The BDPI system is considered highly precise (±1 step). If a rod or the group does not move one step for each

demand pulse, the step counter will still count the pulse and incorrectly reflect the position of the rod or group.

The demanded and measured rod position signals are displayed in the main control room (MCR). An alarm is generated whenever an individual rod position signal deviates from the other rods in the bank by a preset limit. The alarm is set with appropriate allowance for instrument error and within sufficiently narrow limits to prevent core design hot channel factors from being exceeded.

Digital Rod Position Indication

The DRPI system measures the position of each control rod assembly using a detector consisting of discrete coils mounted concentrically with the rod drive pressure housing. The coils are located axially along the pressure housing and magnetically sense the entry and presence of the rod drive shaft through its centreline.

The DRPI system provides an indication of actual control rod position with a lower precision than the step counters. This system is based on inductive analogue signals from a series of coils spaced along a hollow tube. To increase the reliability of the system, the inductive coils are connected alternately to data system A or B. Thus, if one data system fails, the DRPI will work on half-accuracy. The DRPI system is capable of monitoring rod position within at least ±5 steps on full accuracy.

Controls

The reactor power control system, as a function of the PLS, coordinates the responses of the various reactivity control mechanisms. The system enables daily load follow operation with a minimum of manual operator control. Load regulation and frequency control are compatible with the reactor power control system operation. The reactor power control system also performs axial nuclear power distribution control.

The rod control system (as a function of the PLS), in conjunction with the reactor power control system, maintains nuclear power and reactor coolant temperature without challenges to the protection systems during normal operating transients.

6.4 REACTOR COOLANT SYSTEM AND CONNECTED SYSTEMS

The RCS removes heat from the reactor core and transfers it to the secondary side of the SGs for power generation. The RCS contains two vertical U-tube SGs (RCS-MB-01 and RCS-MB-02), four sealless RCPs (RCS-MP-01A/B and RCS-MP-02A/B), and one pressuriser (RCS-MV-02) (See Figure 6-2).

The RCS consists of two heat transfer circuits In addition, the system includes a pressuriser, ADS, interconnecting piping, valves, and instrumentation necessary for operational control and safeguards actuation.

A description of the reactor coolant loop supports is provided in section 16.13 and 20E.

Figure 6-2 shows the main components of the RCS. The RCS pressure boundary provides a barrier against the release of radioactivity generated within the reactor and is designed to provide a high degree of integrity throughout the operation of the plant.

Spring-loaded safety valves are installed above, and connected to, the pressuriser to provide overpressure protection for the RCS. These valves discharge into the containment atmosphere.

Three stages of RCS automatic depressurisation valves are also connected to the pressuriser. These valves discharge steam and water through spargers to the IRWST of the PXS. The steam and water discharged to the spargers is condensed and cooled by being mixed with the water in the tank. The Stage 4 automatic depressurisation valves are connected by two redundant paths to each reactor coolant loop hot leg and discharge directly to the containment atmosphere.

The RCS is also served by a number of auxiliary systems, including the CVS, the PXS, the RNS, SGS, the PSS, the WLS, and the CCS.

6.4.1 Reactor Coolant System

The following SSCs are addressed in this section of the document:

- Primary Coolant Loop
- Reactor coolant piping and valves
- Pressuriser
- RCPs
- SGs

Further design details of this system and its constituent components are delineated in Chapter 17 and Reference 6.26.

6.4.1.1 Primary Coolant Loop

The RCS is shown schematically in Figure 6-2. The RCS consists of two heat transfer circuits, each with a steam generator, two RCPs, a single hot leg and two cold legs, for circulating reactor coolant between the reactor and the steam generators. In addition, the system includes a pressurizer, interconnecting piping, and valves and instrumentation necessary for operational control and safeguards actuation. All system equipment is located in the reactor containment.

During operation, the RCPs circulate pressurized water through the reactor vessel and the steam generators. The pressurized water, which serves as coolant, moderator, and solvent for boric acid (used for chemical shim control), is heated as it passes through the core. It next flows to the steam generators where the heat is transferred to the SGS, and then is returned to the reactor by the reactor coolant pumps to repeat the process. The steam generators have a vertical shell and u-tube configuration with integral moisture separating equipment. The reactor coolant pumps are enhanced-inertia, high-reliability, low-maintenance, sealless-motor pumps and are integrated into the steam generator channel heads in an inverted position.

The pressurizer integrates the following subsystems: spray, heaters, safety valves, and the automatic depressurization valves (ADS). Using electrical heaters and/or a water spray, the Pressurizer controls RCS pressure by maintaining a single major water-steam interface in equilibrium under saturated conditions. The pressurizer is a vertical cylindrical vessel, with hemispherical top and bottom heads; it communicates with the RCS primary coolant loops through a surge line connected to one RCS hot leg. Electrical heaters are installed through the bottom head of the vessel and are removable for maintenance or replacement. Steam is formed by the heaters or condensed by the spray (circulated from the cold legs by the driving

head of the RCPs) to control pressure variations caused by expansion and contraction of the reactor coolant. The pressurizer pressure, temperature, and level instrumentation is provided as required by the PMS and the PLS. To allow continuous monitoring of pressurizer/hot leg reactor coolant loop level during reduced inventory operation (i.e., mid-loop), the bottom tap of the pressurizer cold-calibrated wide range level channel is connected to the bottom of the hot leg that communicates with the pressurizer. Surge line temperature is monitored to detect thermal stratification and pressurizer insurges from the RCS hot leg.

6.4.1.2 Primary Coolant Piping and Valves

RCS piping is configured with two identical main coolant loops, each of which uses a single 787-mm (31-inch) inside-diameter hot leg pipe to transport reactor coolant to a steam generator. The two RCP suction nozzles of each loop are welded directly to the outlet nozzles on the bottom of the steam generator channel head. Two 558.8-mm (22-inch) inside-diameter cold leg pipes in each loop (one per pump) transport reactor coolant back to the RV (RCS-MV-01) to complete the circuit.

Supplemental design practices have been applied to pipe systems in the AP1000 plant, including the primary loop, where an improvement in reliability has an appreciable beneficial impact on plant safety, radiation exposure, and plant examination, maintenance, inspection and testing (EMIT) activities obligations. See Chapter 20 for more detail.

RCS piping is fabricated from stainless steel. The piping is forged seamless without longitudinal or electroslag welds. The RCS piping does not contain any cast fittings. Changes in direction are accomplished in most cases using bent pipe instead of elbows to minimise the number of welds, fittings, and short-radius turns.

The RCS piping includes those sections of reactor coolant hot leg and cold leg piping interconnecting the RV, SGs, and RCPs. The RCS pressure boundary also includes piping connected to the reactor coolant loop piping and primary components.

The RCS pressure boundary includes the second of two isolation or shutoff valves and the piping between those valves.

The connected piping in the RCS includes the following:

- CVS purification return line from the system isolation valve up to the nozzle on the steam generator channel head.
- CVS purification line from the branch connection on the pressuriser spray line to the system isolation valve.
- Pressuriser spray lines from the reactor coolant cold legs up to the spray nozzle on the pressuriser vessel.
- RNS pump suction lines from one reactor coolant hot leg up to the designated isolation valves.
- RNS pump discharge lines from the designated check valves to the connections to the core makeup tank return lines to the RV direct injection nozzles.
- Accumulator lines from the designated check valves to the RV direct injection nozzles.

- PXS lines from the cold legs to the CMTs and back to the RV direct injection nozzles.
- Drain, sample, and instrument lines to the designated isolation valves.
- Pressuriser surge line from one reactor coolant loop hot leg to the pressuriser vessel surge nozzle.
- Pressuriser spray scoops, reactor coolant temperature element installation boss, and the temperature element well itself.
- All branch connection nozzles attached to reactor coolant loops.
- Pressure-relief lines in the pressuriser safety and relief valve module from the nozzles on top of the pressuriser vessel up to and including the pressuriser safety valves and ADS lines from the pressuriser relief lines to the Stage 1, 2, and 3 ADS valves.
- ADS lines from the connections to the hot legs up to the Stage 4 ADS valves.
- Auxiliary spray line from the isolation valve up to the main pressuriser spray line.
- PXS lines from one hot leg to the PRHR HX, and back to the nozzle on the steam generator channel head.
- Vent line from the RV head to the vent isolation valves.
- IRWST injection/containment recirculation lines from the designated valves to the RV direct injection nozzles.
- Level and pressure instrumentation lines.

The RCS piping accommodates the system pressures and temperatures attained under all expected modes of plant operation or anticipated system interactions. Note that level and instrumentation lines connected to the RCS water space include a 9.5-mm (3/8-inch) diameter flow limiting orifice. If one of these lines breaks, the chemical volume control makeup pumps can provide makeup flow while maintaining pressuriser water level. Also, level and instrumentation lines connected to the RCS steam space include a 6.35-mm (1/4-inch) diameter flow limiting orifice. If one of these lines breaks, the pressuriser heaters can produce sufficient steam to maintain pressuriser pressure.

6.4.1.3 Pressuriser

The AP1000 plant pressuriser (RCS-MV-02) is a principal component of the RCS pressure control system. It is a vertical, cylindrical vessel with hemispherical top and bottom heads, where liquid and vapour are maintained in equilibrium at saturated conditions.

One spray nozzle and two nozzles for connecting the safety and depressurisation valve inlet headers are located in the top head. Electrical heaters are installed through the bottom head. The heaters are removable for replacement. The bottom head contains the nozzle for attaching the surge line. This line connects the pressuriser to a hot leg, and provides for the flow of reactor coolant into and out of the pressuriser during RCS thermal expansions and contractions.

The pressuriser provides a point in the RCS where liquid and vapour are maintained in equilibrium under saturated conditions for pressure control of the RCS during steady-state operations and transients. The pressuriser provides a controlled volume from which level can be measured.

The pressuriser contains the water inventory used to maintain RCS volume in the event of a small break LOCA (SBLOCA) for a reasonable period without replenishment. (The SBLOCA fault description can be found in Chapter 9.) The pressuriser surge line connects the pressuriser to one reactor coolant hot leg. This allows continuous coolant volume and pressure adjustments between the RCS and the pressuriser.

The pressuriser is designed to meet following requirements:

- The combined saturated water volume and steam expansion volume is sufficient to provide the desired pressure response to system volume changes.
- The water volume is sufficient to prevent a reactor trip during a step-load increase of 10 percent of full power, with automatic reactor control.
- The water volume is sufficient to prevent uncovering of the heaters following reactor trip and turbine trip, with normal operation of control systems and no failures of nuclear steam supply systems.
- The steam volume is large enough to accommodate the surge resulting from a step-load reduction from 100 percent power to house loads without reactor trip, assuming normal operation of control systems.
- The steam volume is large enough to prevent water relief through the safety relief valves following a complete loss of load with the high water level initiating a reactor trip, without steam dump.
- A low pressuriser pressure-engineered safety features actuation signal will not be activated because of a reactor trip and turbine trip, assuming normal operation of control and makeup systems and no failures of the nuclear steam supply systems.

The pressuriser is sized to have sufficient volume to accomplish the preceding requirements without power-operated relief valves. The AP1000 plant pressuriser has approximately 40 percent more volume than the pressurisers for previous plants with similar power levels. This increased volume provides plant-operating flexibility and minimises challenges to the safety relief valves.

The pressuriser and surge line provide the connection from the RCS coolant loop to the safety relief valves and the ADS valves. The safety relief valves provide overpressure protection for the RCS. The ADS is provided to reduce RCS pressure in stages to allow stored water in the IRWST to flow into the RCS to provide cooling.

The pressuriser surge nozzle and the surge line between the pressuriser and one hot leg are sized to maintain the pressure drop between the RCS and the safety relief valves within allowable limits during a design discharge flow from the safety relief valves or the valves of the ADS. Requirements for the surge line and piping connecting the pressuriser to safety and automatic depressurisation valves is discussed in Chapter 17.3.

The pressuriser provides a location for high-point venting of non-condensable gases from the RCS. The gas accumulations in the pressuriser can be removed by remote manual operation of the Stage 1 ADS valves following an accident. Degassing the pressuriser using the automatic depressurisation valves will not be required on a routine basis for normal- and moderate-frequency events.

6.4.1.4 Pressuriser Safety Relief Subsystem

Overpressure protection during power operation is provided for the RCS by the pressuriser safety relief valves (V005A/B), which are spring-loaded and self-actuated with backpressure compensation. Their set pressure and combined capacity is based on not exceeding the RCS maximum pressure limit during the Level B service condition loss of load transient. This protection is afforded for the following events to envelop those credible events that could lead to overpressure of the RCS if adequate overpressure protection were not provided:

- Loss of electrical load and/or turbine trip
- Uncontrolled rod withdrawal at power
- Loss of reactor coolant flow
- Loss of normal feedwater
- Loss of offsite power to the station auxiliaries

The downstream piping directs the valve discharge away from the pressurizer, ADS valves, and safety-related equipment and into the containment atmosphere (where it is collected in either the IRWST or the containment sump). The downstream piping consists of a short length of piping fitted with a rupture disc to provide an enclosed volume (discharge chamber) in which valve leakage may cool and condense.

6.4.1.5 RCS Automatic Depressurization Subsystem

The ADS valves (RCS-PL-V001A/B, RCS-PL-V002A/B, RCS-PL-V003A/B, RCS-PL-V004A/B) act in conjunction with the PXS to mitigate design basis accidents. Their function is to reduce the RCS pressure in a controlled fashion, to allow the required safety injection flow rates from the CMTs, accumulators, and IRWST. Automatic depressurization is required primarily to mitigate small-break LOCAs.

The automatic depressurization valve subsystem consists of four different valve stages that open sequentially to reduce RCS pressure sufficiently so that long term core cooling can be provided from the PXS.

Stages 1, 2, and 3 are arranged into two identical groups. Each group has a common inlet header connected to the top of the pressurizer and a common discharge line connected to one of the spargers in the IRWST.

For Stages 1, 2, and 3, each valve stage consists of two lines, each line containing two valves in series that are both normally closed. Each stage line is arranged with an isolation valve in series with, and upstream of, a control valve. When the ADS is actuated, the isolation valve opens first, then the control valve subsequently opens to initiate and control the flow to the

IRWST. The upstream ADS isolation valves for Stages 1 through 3 are gate valves. The downstream ADS control valves are globe valves.

Stage 4 is arranged into two identical groups. Each group has a common inlet header connected to one of the hot legs. Each Stage 4 group discharges separately into a steam generator compartment at an elevation above post-accident flood up level.

6.4.1.6 Reactor Vessel Head Vent Subsystem

The reactor vessel head vent portion of the RCS provides redundant, remotely operated head vent paths to be used to prevent pressurizer overfill during certain design basis events.

Each flow path contains two normally closed, fail-closed, solenoid-operated valves (RCS-PL-V150A/B/C/D). Each valve is powered by a separate essential electrical supply system (IDS) power train. The two flow paths reconnect, and the common header traverses the refueling cavity and discharges to the IRWST through the common discharge header of one train of automatic depressurization valves.

A normally isolated, manually operated, branch line from the common discharge header is located above the reactor vessel and discharges to the containment sump so that vessel venting and filling operations during plant startup can be monitored and performed by the plant personnel at a location remote from the reactor vessel.

6.4.1.7 Reactor Coolant Pumps

The AP1000 plant RCPs (RCS-MP-01A/B and RCS-MP-02A/B) are high-inertia, high-reliability, low-maintenance, sealless pumps that circulate the reactor coolant through the RV, loop piping, and SGs. The pumps are integrated into the steam generator channel head in the inverted position. A RCP is directly connected to each of two outlet nozzles on the steam generator channel head.

Sealless pumps have an extensive operational history in both conventional and nuclear plants with a record of very good reliability and significantly reduced maintenance as compared to shaft-seal pumps. In addition, they require no support after the pumps are tripped during fault sequences.

The integration of the pump suction into the bottom of the steam generator channel head eliminates the crossover leg of coolant loop piping; reduces the loop pressure drop; simplifies the foundation and support system for the steam generator, pumps, and piping; and reduces the potential for uncovering of the core by eliminating the need to clear the loop seal during a cold leg side SBLOCA.

The AP1000 plant design uses four pumps. Two pumps are coupled with each steam generator and have shafts that rotate in the same direction.

Each AP1000 plant RCP is a vertical, single-stage centrifugal pump designed to pump at high pressures and temperatures. Because of its sealless design, it is more tolerant of off-design conditions that could adversely affect shaft seal designs. The main impeller attaches to the rotor shaft of the driving motor, which is an electric induction motor. The motor is contained within a casing that provides the pressure boundary and primary coolant circulates between the stator and rotor, obviating the need for a seal around the motor shaft. In addition, the motor bearings are lubricated by primary coolant. Thus, the motor is an integral part of the

pump. The basic pump design has been proven by many years of service in other applications.

The pump motor size is minimised through the use of a variable frequency drive to provide speed control to reduce motor power requirements during pump startup from cold conditions.

In the UK design of AP1000 plant, a variable frequency drive (VFD) is run continuously to provide a 60-Hz power supply to the pump motor. The VFD is also used to reduce the pump speed during heatup and cooldown when the reactor trip breakers are open.

A sealless pump contains the motor and all rotating components inside a pressure vessel. The RCP driving motor is a vertical, water-cooled, squirrel-cage induction motor. The pressure vessel consists of the pump casing, stator closure, stator main flange, stator shell, stator lower flange, and stator cap, which are designed for full RCS pressure. The AP1000 plant utilizes a sealless RCP design. Sealless refers to the absence of a dynamic seal where the pump shaft penetrates the pump casing. Because the shaft for the impeller and rotor is contained within the pressure boundary, seals are not required to restrict leakage from the pump into containment.

The motor and other pump internals are cooled by primary RCS coolant circulating through the motor cavity. Primary coolant used to cool the motor enters the lower end of the rotor and passes axially through the motor cavity to remove heat from the rotor and stator and circulates to an external HX. An auxiliary impeller provides the motive force for circulating the coolant. Heat from the primary coolant is transferred to component coolant water in the external HX.

The RCP also includes a cooling jacket cooled by CCS that removes heat from the upper flywheel and bearing assembly.

Flywheel assemblies provide rotating inertia that increases the coastdown time for the pump. Each flywheel assembly is of bimetallic design consisting of a heavy-metal alloy and stainless steel. Surrounding the flywheel assemblies are the heavy walls of the stator closure, casing, thermal barrier, or stator lower flange.

The materials in contact with the reactor coolant and cooling water (with the exception of the bearing material) are austenitic stainless steel, nickel-chromium-iron alloy, or equivalent corrosion-resistant material.

The RCP is equipped with a vibration monitoring system that continuously monitors pump structure (frame) vibrations. Five vibration monitors provide pump vibration information. The readout equipment includes warning alarms and high-vibration level alarms, as well as output for analytical instruments.

Four resistance temperature detectors (RTDs) monitor the motor cooling circuit water temperature. These detectors indicate anomalous bearing or motor operation. They also provide inputs to automatic reactor and RCP trips in the event of a prolonged loss of component cooling water.

A speed sensor monitors rotor speed. In addition, voltage and current sensors provide information on motor load and electrical input.

An important advantage of sealless pump designs with water-lubricated bearings is that they eliminate the following problem areas:

- No RCP seals (no “seal LOCA” and no seal maintenance)
- No seal injection, seal return, or seal leakoff systems
- No lube oil reservoirs, lube oil cooling, oil lift, oil spillage collection systems, and associated fire protection systems
- Simplified RCP operations
- No need to establish and maintain flows, pressures, and levels to support seal operation
- No need to run the oil lift pump to pressurise the lubrication system before starting the RCP

6.4.1.8 AP1000 Plant Steam Generator

The AP1000 plant SG (RCS-MB-01 and RCS-MB-02) is a vertical shell and U-tube evaporator with integral moisture separating equipment. The basic design and features of the steam generator have been proven in tests and in previous SGs, including replacement SG designs. Design enhancements include nickel-chromium-iron-alloy-690 thermally treated tubes on a triangular pitch, improved anti-vibration bars, single-tier separators, enhanced maintenance features, and a primary-side channel head design that allows for easy access and maintenance by robotic tooling. The AP1000 plant SG employs tube supports utilising a broached hole support plate design. All tubes in the SG are accessible for sleeving, if necessary.

The basic function of the AP1000 plant SG is to transfer heat from the single-phase reactor coolant water through the U-shaped HX tubes to the boiling, two-phase water/steam mixture in the secondary side of the SG. The SG separates dry, saturated steam from the boiling mixture, and delivers the steam to an outlet nozzle, from which it is delivered to the turbine. Water from the feedwater system replenishes the SG water inventory by entering the SG through a feedwater inlet nozzle and feedring.

In addition to its steady-state performance function, the SG secondary side provides a water inventory that is continuously available as a heat sink to reduce the severity of primary-side high-temperature transients or decreased heat removal transients.

On the primary side of the SG, the reactor coolant flow enters the inlet portion of the SG primary chamber or channel head via the hot leg nozzle. The lower portion of the primary chamber is an ellipsoid and merges into a cylindrical portion, which mates to the tube sheet. This arrangement provides enhanced access to all tubes, including those at the periphery of the bundle, with robotics equipment. This feature enhances the ability to inspect, replace, and repair portions of the AP1000 plant unit compared to the more spherical primary chambers of earlier designs. The head is divided into inlet and outlet chambers by a vertical divider plate extending from the apex of the channel head to the tube sheet.

The reactor coolant flow enters the inverted U-tubes, transferring heat to the secondary side fluid during its traverse, and returns to the cold leg side of the primary chamber. The flow exits the SG via two cold leg nozzles to which the RCPs are directly attached.

Steam is generated on the shell or secondary side of the SGs (which is part of SGS), flows upward, and exits through the outlet nozzle at the top of the vessel. Feedwater enters the SG at an elevation above the top of the U-tubes through a feedwater nozzle. The feedwater enters a feedring via a welded thermal sleeve connection and exits through nozzles attached to the top of the feedring. The nozzles are fabricated of nickel-chromium-iron alloy that is very resistant to erosion and corrosion with the expected secondary water chemistry and flow rate through the nozzles. The nozzles are essentially holes in the top of the feedring. They are debris-filtering in that any loose parts larger than the hole diameter are retained in the feedring. After exiting the nozzles, the feedwater flow mixes with saturated water removed by the moisture separators. The flow then enters the downcomer annulus that is between the tube wrapper and the SG shell.

The SG channel head, tube sheet, and tubes are a portion of the reactor coolant pressure boundary. The tubes transfer heat to the steam system while retaining radioactive contaminants in the primary system. The SG removes heat from the RCS during power operation and anticipated transients, and under natural circulation conditions.

The SG heat transfer function and associated secondary water and steam systems are not required to provide safe shutdown of the plant. The secondary side systems are addressed in Section 6.5.

6.4.2 Chemical and Volume Control System

The design of the Chemical and Volume Control System consists of various heat exchangers as well as demineralizers, filters, pumps, tanks, and associated valves, piping, and instrumentation. The system functions as a whole to fulfill the requirements of controlling Reactor Coolant System chemistry, purity, and inventory for normal plant operations. Further design details of this system and its constituent components are delineated in Chapter 17 and Reference 6.18. The description of this system within this section is consistent with the System Specification Document (Reference 6.18).

The Class 1 safety functions provided by the CVS are limited to containment isolation of CVS lines penetrating containment; termination of inadvertent RCS boron dilution; isolation of makeup on a SG or pressuriser high-level signal; and preservation of the RCS pressure boundary, including isolation of normal CVS letdown from the RCS.

The CVS is made up of two subsystems: a purification subsystem located inside containment, which consists of regenerative and letdown HXs, mixed bed demineralisers, and filters; and a makeup subsystem, located largely outside containment and consisting of makeup pumps, miniflow HXs, chemical dosing tanks, the boric acid tank, and a letdown path to the WLS. Containment isolation valves are provided on both sides of the containment penetrations. Under normal operation, the CVS purification subsystem is connected to RCS cold leg 1B, and returns to the SG 1 outlet chamber.

6.4.2.1 Chemical Control and Chemical Shim

The CVS incorporates the following functions to support the water chemistry and chemical shim requirements of the RCS:

- Provisions to add and remove chemicals for RCS pH control at startup, during normal operation, and in support of shutdown operations

- A means of adding and removing a soluble chemical neutron absorber (boron) at concentrations and rates compatible with normal plant operation and plant shutdown.

- Provisions for adding any other chemicals to the RCS through a Chemical Mixing Tank, such as hydrogen peroxide during shutdown operations.

- A means for scavenging oxygen during startups through the addition of hydrazine via the Chemical Mixing Tank and for controlling the formation of free oxygen due to radiolysis in the core during normal operation through the addition of hydrogen.

- A means for purification, which may include the need to control RCS chemistry parameters such as chlorides, fluorides, and sulfates.

- Provisions for adding a liquid zinc acetate solution into the RCS during plant operation.

6.4.2.2 Reactor Coolant Inventory Control and Makeup

Changes in the reactor coolant volume will be accommodated by the Pressurizer Level Control Program for normal power changes, including transition from hot standby to full power operation and returning to hot standby. In addition, the pressurizer has sufficient volume, within the deadband of the level control program, to accommodate minor RCS leakage for some period of time. The CVS provides inventory control to accommodate minor leakage from the RCS, expansion during heatup from cold shutdown, and contraction during cooldown. This inventory control is provided by connections with the letdown and makeup subsystems.

6.4.2.3 Filling and Pressure-Testing the RCS

RCS filling is accomplished by using the CVS Makeup Pumps (CVS-MP-01A/B) to provide fluid at the proper boron concentration (refueling concentration). The CVS Makeup Pumps take suction from both the Boric Acid Storage Tank and the Demineralized Water Transfer and Storage System (DWS) through a three-way blend valve (CVS-PL-V115), which ensures the proper boron concentration.

The CVS Makeup Pumps produce sufficient head to pressure test the RCS after maintenance and refueling outages. However, a temporary hydrostatic test pump will be required for initial hydrotesting which will require higher operating pressures than can be achieved with the Makeup Pumps.

6.4.2.4 Borated Makeup to Auxiliary Equipment

The CVS Makeup Pumps will also be used to provide makeup at the proper boron concentration to the PXS Accumulators (PXS-MT-01A/B), Core Makeup Tanks (PXS-MT-02A/B), In-Containment Refueling Water Storage Tank (PXS-MT-03), and the SFP.

6.4.2.5 Pressurizer Auxiliary Spray

The CVS Makeup Pumps provide auxiliary spray to the pressurizer through a connection on the pressurizer main spray header. The Makeup Pumps take suction from the BAST (CVS-MT-01) and the DWS to provide borated water at a selected boron concentration. The pumps use the normal makeup path to the RCS through the shell side of the RHX and continue through the auxiliary spray isolation valve (CVS-PL-V084) to the RCS and the connection on the main spray header.

6.4.3 Normal Residual Heat Removal System

The RNS can provide closed loop heat removal from the core and the RCS during shutdown operations or mitigation of an accident.

The RNS includes two mechanical trains of decay heat removal equipment. Each train includes one RNS pump (RNS-MP-01A/B) and one RNS heat exchanger (RNS-ME-01A/B) located in the Auxiliary Building. Additional design details of this system and its constituent components are delineated in Reference 6.19 and Chapter 17. The description of this system within this section is consistent with the System Specification Document (Reference 6.19).

The Class 1 safety functions provided by the RNS are containment isolation of RNS lines penetrating containment, preventing the release of radioactive material through the boundary of RCS, and removing decay heat from the reactor during normal operation and accident conditions.

6.4.3.1 Normal Cooldown

The first phase of RCS cooldown normally consists of transferring heat from the RCS through the steam generators and the MSS to the main condensers. The RNS removes decay heat from the core and reduces the temperature of the RCS during the second phase of plant cooldown.

6.4.3.2 Refueling Heat Removal

Following cooldown, the RNS continues to remove heat from the core and the RCS during refueling operations. Once refueling of the reactor is complete, and as decay heat decreases, one subsystem of RNS equipment may be taken out of service. This occurs approximately 11 days after reactor shutdown.

6.4.3.3 Refueling Draindown

During some cooldown operations, the RCS water level is drained to a “mid-loop” level to permit steam generator draining and maintenance activities. The RCS drain path is from the CVS branch through a DVI inlet line after the RNS discharge header splits inside containment. For normal refueling operations, the RCS is drained to a level that allows air to be vented into the steam generator from the pressurizer.

6.4.3.4 Shutdown Purification

The RNS provides CVS purification flow during shutdown and refueling operations when the RCPs are not operating or are operating at reduced speeds, and whenever the CVS return line to the steam generator is unavailable for normal RCP purification flow while the RNS is aligned with the RCS.

6.4.3.5 IRWST Cooling

The RNS provides cooling for the IRWST during operation of the PRHR heat exchanger. The system is manually aligned and initiated by the operator within one to two hours of initiation of the PRHR heat exchanger, if possible. The RNS cooling limits the IRWST water temperature to less than boiling during extended operation of the PRHR heat exchangers. In the event of a single failure in the RNS, boiling of the IRWST may occur during extended operation of the PRHR.

During power operation, the RNS provides cooling for the IRWST if required and limits the IRWST to 48.9°C (120°F).

6.4.3.6 Shutdown or Post-Accident Heat Removal

Following an accident which actuates all stages of ADS, including IRWST injection, the RNS can be aligned to provide decay heat removal in order to bring the plant to cold shutdown conditions. The flow path through the RNS for this operation is the same as that used during a normal refueling shutdown.

The RNS can also be used for decay heat removal during non-LOCA scenarios after the PXS has cooled the RCS to a temperature at which the RNS can be aligned. The PRHR would provide initial cooling to bring the RCS to a temperature and pressure which the RNS could be aligned. Normal RNS cut-in temperature is 176.7°C (350°F), but for a limited number of occurrences the RNS can be aligned at 204.4°C (400°F). For this situation, it would also be assumed that the RNS was also used to cool the IRWST during PRHR operation to prevent IRWST steaming.

6.4.3.7 Low-Pressure RCS Injection

6.4.3.7.1 Injection from the Cask Loading Pit

The RNS is capable of providing low-pressure makeup from the SFS Cask Loading Pit to the RCS. The system must be manually initiated by the operator following receipt of an ADS signal. If the RNS is available, it will provide RCS makeup once the pressure in the RCS falls below the shutoff head of the RNS pumps.

Following an ADS signal in the event of a small break LOCA or a non-LOCA event, the RNS is designed to provide sufficient makeup flow so that the water level in the CMTs does not drain below the ADS Stage 4 valve actuation setpoint. In this way, successful operation of the RNS will prevent the ADS Stage 4 valves (located off the RCS hot legs) from opening, and thereby prevent substantial flooding of the containment and the need for cleanup.

6.4.3.7.2 Injection from the IRWST

The RNS is capable of providing low-pressure makeup from the IRWST to the RCS. The system must be manually initiated by the operator following receipt of an ADS signal. If the RNS is available, it can provide RCS makeup once the pressure in the RCS falls below the shutoff head of the RNS pumps.

Following an ADS signal in the event of a SBLOCA or a non-LOCA event, the RNS is designed to provide sufficient makeup flow so that the water level in the CMTs does not drain below the ADS Stage 4 valve actuation setpoint. In this way, successful operation of the RNS will prevent the ADS Stage 4 valves (located off the RCS hot legs) from opening, and thereby prevent substantial flooding of the containment and the need for clean up.

6.4.3.8 Forced Core Cooling by Containment Recirculation

After an event that results in containment flooding, the RNS can be aligned to take suction from the containment sump to provide additional core cooling. This alignment is possible after the PXS containment recirculation squib valves (PXS-PL-V118B and PXS-PL-V120B) have actuated.

If the RNS was previously used to inject water from the CLP or IRWST into the RCS to prevent the CMTs from draining, RNS containment recirculation through RNS can also be used to continually hold up the CMT level, thereby preventing actuation of ADS Stage 4.

If the RNS was not used to prevent draining of the CMTs below the ADS Stage 4 valve actuation setpoint, ADS Stage 4 will actuate and containment recirculation will still be possible. In this scenario, the RNS will take suction from the containment sump and inject through the DVI lines into a depressurized reactor vessel to provide additional core cooling.

6.4.3.9 Long-Term Post-Accident Makeup Capability from Outside Containment

After an accident which has included ADS Stage 4, long-term makeup may be required from outside containment. The flow path for this long-term supply of water is through the discharge containment penetration test connection valves (RNS-V012A/B), by administratively controlled water addition.

6.4.3.10 Low-Temperature Overpressure Protection (LTOP)

The RNS LTOP function is required to be available during shutdown, refueling, and heatup operations when the RCS cold leg temperature is ≤ 135°C (275°F).

6.4.3.11 Spent Fuel Pool Cooling

RNS can supplement or replace normal SFS cooling of the SFP during plant operation modes when the RNS is not needed for reactor core cooling.

6.4.3.12 RCS Vacuum-Refill Subcooling

The RNS provides cooling of RCS during vacuum refill operations.

6.4.3.13 Cask Loading Pit Circulation

The RNS pump suction can be aligned with the cask loading pit (CLP), by aligning valve RNS-PL-V055A/B in the MCR, and the discharge aligned to the SFP, by opening normally locked closed valve RNS-PL-V053A/B, to provide circulation of the CLP. The gate between the SFP and CLP must also be opened. This flow path allows the CLP water inventory to be recirculated to prevent stagnation and stratification and provide the required water chemistry.

6.4.4 Primary Sampling System

The primary sampling system (PSS) collects representative samples of fluids from the process streams of the reactor coolant system and associated auxiliary systems and from the containment atmosphere for analysis by the plant operating staff. This sampling process can be performed during normal plant operations or post-accident operations. Most components and equipment are common to both modes of operation. This arrangement permits the operator to gain the necessary operational experience with the PSS during normal operations, which is directly applicable to post-accident operations.

The PSS is composed of two main subsystems:

- Liquid Sampling
- Containment Atmosphere Sampling

Additional design detail of this system and its constituent components are delineated in Reference 6.36 and Chapter 21.

The Class 1 safety functions provided by the PSS are containment isolation of PSS lines penetrating containment and preventing the release of radioactive material through the boundary of RCS.

6.4.4.1 Liquid Sampling

The liquid samples have three flow paths: (1) grab sampling of the auxiliary systems and RCS pressurizer process streams (2) continuous sampling of the RCS hot legs (3) grab sampling of PXS. The paths maintain separation such that the continuous and grab sampling paths can be used simultaneously.

6.4.4.1.1 Liquid Grab Sampling

The liquid sampling portion of the PSS is used to collect and transport liquid samples from the reactor coolant system and associated auxiliary systems to a common location in a sample room located in the Auxiliary Building. Additionally there is another liquid sampling path of the PSS is used to collect and transport liquid samples from the PXS sample sources to the aforementioned sample room located in the Auxiliary Building. A radiological chemical laboratory facility is located immediately above the sampling room. Instrumentation and controls are provided to ensure safe and reliable operation of the system.

6.4.4.1.2 Continuous Liquid Sampling

The continuous liquid sampling path of the PSS is used to collect and transport liquid samples from the reactor coolant system hot leg sample sources to a common location in a sample room located in the Auxiliary Building.

The continuous flow of RCS hot leg fluid through the PSS makes it possible to (1) collect grab samples of the auxiliary systems' process streams while maintaining continuous flow of the RCS hot legs, (2) collect a representative zinc sample, (3) collect a representative corrosion product sample, and (4) collect a continuous sample of dissolved hydrogen while keeping the daily PSS effluent below the WLS design limit.

6.4.4.2 Containment Atmosphere Sampling

The containment atmosphere (CA) sampling portion of the PSS is employed to collect gaseous samples from the containment atmosphere. CA sampling is conducted in the same sampling room in the Auxiliary Building as liquid sampling. The CA sampling components, valves, and piping share the same grab sampling panel (GSP) as the liquid sampling accessories, and CA sampling control is from the same local control stations.

Similar to the liquid sampling subsystem, the valves used in the CA sampling portion of the GSP are manually operated from outside the enclosure via valve-stem extensions that penetrate the front of the GSP. To supply the motive force for CA sample collection, the CA sampling subsystem uses an ejector which employs pressurized nitrogen gas as its motive force.

Containment atmosphere samples are drawn from the inlet of each set of containment recirculation fans inside containment. Air flow inside of containment is circulated to the containment recirculation fans.

The capability to collect a containment atmosphere sample for radionuclide analysis is provided by the PSS. The PSS only collects a containment atmosphere sample; the analysis must be performed in the radiochemistry laboratory.

Containment atmosphere hydrogen monitoring is performed by the hydrogen analysers provided by the containment hydrogen control system (VLS). However, the PSS is designed to collect a representative containment sample for subsequent analysis and can therefore provide backup capability to the hydrogen control system.

6.4.4.3 Boron Concentration Monitoring System

The boron monitor will pull a sample from the RCS sample lines in order to provide semi-continuous samples.

6.4.4.4 Corrosion Product Sample Filter Package

The corrosion filter package utilizes lines which branch off of the PSS continuous sample line in order to provide .

6.5 STEAM AND POWER CONVERSION SYSTEMS

6.5.1 Summary Description

The steam and power conversion system is designed to remove heat energy from the RCS via the two SGs and to convert it to electrical power in the turbine generator. The main condenser and deaerator removes air from the condensate and transfers unusable heat in the cycle to the circulating water system (CWS). The regenerative turbine cycle heats the feedwater, and the main feedwater system (FWS) returns it to the SGs (see Chapter 17.4).

The steam generated in the two SGs is supplied to the high-pressure turbine by the main steam system. After expansion through the high-pressure turbine, the steam passes through the two moisture separator reheaters (MSRs) and is then admitted to the three low-pressure turbines. A portion of the steam is extracted from the high- and low-pressure turbines for seven stages of feedwater heating.

Exhaust steam from the low-pressure turbines is condensed and deaerated in the main condenser. The heat rejected in the main condenser is removed by the CWS. The condensate pumps take suction from the condenser hot well and deliver the condensate through four stages of low-pressure, closed, feedwater heaters to the fifth stage, the open deaerating heater. Condensate then flows to the suction of the SG feedwater booster pump and is discharged to the suction of the main feedwater pump. The SG feedwater pumps discharge the feedwater through two stages of high-pressure feedwater heating to the two SGs. Further design details of this system and its constituent components are delineated in Chapter 17, Reference 6.27, and Reference 6.28.

The turbine generator has an output of approximately 1200 MW for the Westinghouse nuclear steam supply system (NSSS) thermal output of 3415 MWt.

The following SSCs are addressed in this section:

- Main feedwater and condensate systems
- Main steam system
- Steam generator system

- Main turbine generator
- Turbine bypass feature of the MSS
- MSRs
- Condenser air removal system
- Gland seal system
- Main condenser
- Steam generator blowdown system
- Startup portion of the main feedwater system
- Circulating water system
- Auxiliary steam supply system
- Turbine island chemical feed system
- Condensate polishing system

6.5.2 Main Feedwater and Condensate Systems

The main feedwater and condensate systems provide feedwater at the required temperature, pressure, and flow rate to the SGS. The systems are located within the turbine building and are discussed further in Section 17.4). Additional design details of this system and its constituent components are delineated in Reference 6.31 and Reference 6.50.

The SGS contains the piping and valves in the auxiliary building that deliver the feedwater to the SGs.

The main portion of the feedwater flow originates from condensate pumped from the main condenser hot well by the condensate pumps. The main feed water system contains three 50% capacity main feedwater pump trains. The main condenser hot well receives makeup from the condensate storage tank, as required. The condensate passes through the condensate polishing system and/or the condensate polishing bypass, and is delivered to the deaerator tank.

During plant startup, three recirculation paths facilitate system cleanup and adjustment of water quality prior to initiating feed to the SGs. These cleanup loops are designed for approximately 33 percent of design condensate flow and include a hot well recirculation loop, a deaerator recirculation loop, and a long-cycle recirculation loop from downstream of the No. 7 feedwater heaters. Steam is provided to the deaerating feedwater heater from the auxiliary steam supply system (ASS) to preheat the feedwater to over 93.3°C (200°F) during the initial cleanup and startup recirculation operations. This preheating action, along with chemical addition, minimises the formation of iron oxides in the condensate system.

The feedwater and condensate systems supply the SGs with heated feedwater in a closed steam cycle using regenerative feedwater heating. The system comprises the CDS, the heater drain system, the main feedwater system, and portions of the SGS. The condensate system (CDS) collects condensed steam from the condenser and pumps condensate forward to the deaerator. The feedwater system takes suction from the deaerator and pumps feedwater forward to the SGS using high-pressure main feedwater pumps.

This system consists of the pipes, valves, pumps, feed heaters, and deaerator supplying feedwater from the main condenser to the two SGs via the SGS. It is required to do this during startup and operation at power, to remove the heat intentionally produced by the reactor core; and in the initial phase of shutdown operation before the RNS can be connected to the RCS, to remove the fission product decay heat from the reactor core.

The feed and condensate systems are located within the turbine building, and the SGS is located within the auxiliary building and containment.

The main feedwater and condensate systems perform the following major functions:

- Supplies main feedwater to the SGS during operation at power
- Supplies startup feedwater to the SGS during startup and during the initial phase of shutdown and RCS cooldown operation before the RNS is connectable.
- Pressurises the feedwater above the current SG pressure, and automatically controls the flow of the water into each SG to the rate required to remove the heat generated by the reactor core under the prevailing conditions, without the SG becoming overfilled.
- During operation at power, heats the feedwater to the optimum temperature for maximising the thermodynamic cycle efficiency.
- In conjunction with the condenser air removal system and the turbine island vents and drains system, removes from the feedwater those dissolved gases originating from air leaking into the sub-atmospheric parts of the CDS and from gases dissolved in the condensate in the condenser hot well.
- The heater drain system extracts some of the moisture from the steam as it expands through the turbine cylinders by draining condensate from the feedwater heaters and removing moisture from the high-pressure exhaust steam in the MSRs, thereby improving thermodynamic cycle efficiency and minimising turbine blade erosion.

Condensate is pumped out of the main condenser hot well, which is at sub-atmospheric pressure, by the condensate pumps. The water passes through the low-pressure feedwater heaters, which heat it using steam extracted from the low-pressure turbines. The last-stage low-pressure heater is incorporated into the deaerator tank, which also removes dissolved air and non-condensable gases from the feedwater and, by virtue of its substantial volume, acts as a reservoir of feedwater equivalent to 3.5 minutes supply at full-delivery flow.

The feedwater pumps (FWS-MS-01A/B/C) pressurise the water up to the high pressure required to deliver flow to the SGs. The main feedwater pumps are each preceded by a booster pump to pressurise the inlet of the main feed pump and thereby prevent cavitation. The booster pumps draw their suction from the deaerator tank. The high-pressure feed flowing out of the main feed pumps passes through the high-pressure feed heaters, which heat it up further using steam extracted from the high-pressure turbine.

Main feedwater is supplied to the SGS and then to each of the two SGs through its own main feedwater line. Each of the two lines is anchored at the interface between the auxiliary building and the turbine building, and has sufficient flexibility to provide for relative movement of the line and its associated SG resulting from thermal expansion. Each main feedwater line contains a control valve, a check valve, and an isolation valve. These valves are installed in the line before it enters the containment. The main feedwater lines are a closed system inside the reactor containment and are therefore not fitted with more valves.

The principal purpose of each main feed control valve is to maintain the level of water in its associated SG at a programmed level; its secondary purpose is to provide the capability for backup isolation. These pneumatically actuated valves are normally under automatic control but can be switched to manual.

An isolation valve (SGS-PL-V057A/B) is installed downstream of each feedwater control valve (SGS-PL-250A/B). The main functions of the isolation valve are to stop hot pressurised

feedwater from leaking into the containment (in the event of a main feedwater line break inside the containment) and to isolate the SGs in the event of a ruptured SG tube. Closure of the isolation valve uses compressed nitrogen as its energy source.

Each main feedwater line also includes a check valve (SGS-PL-V058A/B). During normal and abnormal conditions, this check valve prevents reverse flow from the SG should the feedwater pumps be tripped. In addition, the valves stop the uncontrolled blowdown from the SGs in the event of a feedwater line break outside the containment, and they stop more than one SG from blowing down in the event of feedwater line break inside the containment.

In a similar manner, the startup feedwater is supplied to the SGS and then to each of the two SGs through its own startup feedwater line and startup feedwater nozzle on each SG. The startup feedwater is provided by either of two startup feedwater pumps that take suction from the condensate storage tank. Also, the main feed system can be connected to the startup feedwater portion of the system at the feed pump outlet header. The connection has an isolation valve (SGS-PL-V067A/B) and a check valve (SGS-PL-V265A/B), allowing the main feed pumps to supply the SGs through the startup feedwater control valves.

6.5.3 Startup Portion of the Main Feedwater System

The startup portion of the main and startup feedwater system (FWS) supplies feedwater to the SGs during plant startup, hot standby, and shutdown conditions; and during transients in the event of main feedwater system unavailability. The startup feedwater flow path includes components from the FWS and the SGS. The startup flow path to the SG has an isolation valve (SGS-PL-V067A/B) and a check valve (SGS-PL-V265A/B). Further details of this subsystem and its components are given in subsection 17.4. Further design details of this system and its constituent components are delineated in Reference 6.31.

There are no Class 1 safety functions provided by the FWS. The startup feed water pumps (FWS-MP-03A/B) provide decay heat removal from the reactor during normal operation and accident conditions which is a Class 2 safety function. This decay heat removal function can prevent unnecessary actuation of the passive decay heat removal system. These events include loss of main feedwater and loss of normal alternating current (ac) power.

Startup feedwater is defined to be feedwater that passes through the startup feedwater control valves, and can be supplied from either of two sources:

1. A booster/main feedwater pump drawing from the deaerator storage tank and delivering through cross-connect piping to the startup feedwater header.

2. One or both startup feedwater pumps drawing from the condensate storage tank and delivering to the startup feedwater header.

The startup feedwater pumps are much smaller and do not require booster pumps. They draw their suction from the condensate storage tank; they supply directly to the SGs, with no feed heating at all. A cavitating venturi is installed at the discharge of each startup feedwater pump to prevent runout of the startup feedwater pump. The venturi flow elements provide a passive means of limiting the maximum achievable flow. The startup feedwater pumps start automatically on conditions that exist after a reactor trip. The pumps are automatically loaded on the standby diesel generators if offsite power is lost.

There are two startup feedwater lines, with the same disposition of valves as the two main feedwater lines. Each line supplies its own SG through an injection nozzle at the same elevation as the main feedwater nozzle but rotated circumferentially away from it. During

startup, feed is supplied through the startup feedwater control valves (SGS-PL-V255A/B) until the capacity limit of the startup pumps is approached, at which point the main feedwater pumps are placed into service and feedwater control is automatically transferred from the startup feedwater control valves to the main feedwater control valves; the startup feed isolation valves are then closed.

6.5.4 Main Steam Supply System

The main steam supply system as described in this section includes components of the steam generator system (SGS), main steam system (MSS), and main turbine system (MTS). The system is described in Section 17.4. Further design details of this system and its constituent components are delineated in Reference 6.27, 6.28, and 6.29.

The MSS supplies steam from the SGs to the high-pressure turbine over a range of flows and pressures covering the entire operating range from system warmup to maximum calculated turbine conditions. The steam generator system includes the pipes and valves that take the steam from each SG to the main steam isolation valves at the boundary of the auxiliary building and turbine building. The MSS consists of the pipes and valves that then take the steam downstream of the main steam isolation valves to the stop valves of the high-pressure turbine. It diverts a proportion of the steam to the MSR and a small amount of steam to seal the low-pressure turbine glands. A turbine bypass connection allows the steam to be dumped directly into the main condenser without passing through the turbine.

The SGS and MSS are required during operation at power to remove the heat produced by the reactor core, and also in the initial phase of shutdown operation before the RNS can be connected, to remove the fission product heat from the reactor core. The heat sinks are provided either by venting steam to atmosphere or by the turbine bypass system dumping steam to the condenser.

The system provides steam to the MSRs and the gland seal system for the main turbine. The system can dissipate heat generated by the NSSS when the turbine generator is not available by using steam dump valves to the condenser or by using the SG power-operated atmospheric relief valves or spring-loaded main steam safety valves, which discharge to the atmosphere, when the condenser is unavailable.

The main steam lines deliver a steam flow from the secondary side of the two SGs.

A portion of the main steam flow is directed to the reheaters and steam seals, with the turbine receiving the remaining steam flow. Each main steam line from the SGs is anchored at the auxiliary building wall and has sufficient flexibility to accommodate thermal expansion. The layout of the steam piping, with its proper sloping of lines and use of condensate drain pots, provides for collection and drainage of condensate to avoid water entrainment.

Turbine bypass valves are provided between the main steam isolation valves and turbine generator stop valves, as discussed in the paragraphs about the turbine bypass system in the later subsections.

Main steam piping is designed to consider the effects of erosion and corrosion. Piping containing dry, single-phase steam is constructed of carbon steel. Piping exposed to wet, two-phase steam is constructed of erosion- and corrosion-resistant low-alloy steel or carbon steel with a stainless-steel inner liner. Velocities in the main steam piping to the high-pressure turbine are limited to reduce the potential for pipe erosion. Low point drains are provided for collecting and draining moisture and to help reduce the potential for water carryover to the high- and low-pressure turbines.

Upstream of the main steam isolation valves, there are connections for the power-operated atmospheric relief valves, main steam safety valves, low point drains, high point vents, and nitrogen blanketing. Branch piping downstream of the main steam line isolation valves includes connections for the two-stage reheaters, gland seal system, turbine bypass system, auxiliary steam system, and low point drains.

Each main steam line goes from its SG and passes through the containment boundary. Each line contains a MSIV that is located outside of containment to isolate the steam lines. Upstream of the MSIV in each of the two steam lines are the six steam safety valves; each one vents to atmosphere through a discharge pipe and vent stack. Downstream of the safety valves is the power-operated atmospheric relief valve, which vents to atmosphere through a vent pipe and silencer. The operation of the power-operated atmospheric relief valves is automatically controlled by steam line pressure during plant operations; the valves automatically modulate open and exhaust to atmosphere whenever the steam line pressure exceeds a predetermined setpoint. As steam line pressure decreases, the relief valves modulate closed. Each main steam line is anchored at the point where it passes through the wall between the auxiliary building and the turbine building; the section of it from the SG to the anchor has sufficient flexibility to accommodate thermal expansion. Beyond this wall the two main steam lines are cross-connected into a common header, which itself subsequently branches into four lines to the turbine stop valves; the connections to the two MSRs, the gland sealing system, and the turbine bypass also branch from this common header.

6.5.4.1 Main Steam Safety Valves

Main steam safety valves with sufficient rated capacity are provided to prevent the steam pressure from exceeding 110 percent of the MSS design pressure following:

- A turbine trip without a reactor trip and with main feedwater flow maintained
- A turbine trip with a delayed reactor trip and the loss of main feedwater flow

At the same time, the individual safety valves are limited to the maximum allowable steam relief valve capacity (Section 17.4) to limit the potential uncontrolled blowdown flow and the ensuing reactor transient should a single safety valve inadvertently fail or stick in the open position.

Six safety valves (SGS-PL-V030A/B, V031A/B, V032A/B, V033A/B, V034A/B, and V035A/B) are provided per main steam line for the plant. The main steam supply system safety valves are located in the portion of the main steam piping upstream of the main steam isolation valves and outside the containment in the auxiliary building.

6.5.4.2 Power-Operated Atmospheric Relief Valves

A power-operated atmospheric relief valve (PORV) (SGS-PL-V233A/B) is installed on the outlet piping from each SG to provide controlled removal of reactor decay heat during normal reactor cooldown when the main steam isolation valves (SGS-PL-V040A/B) are closed or the turbine bypass system is not available. The maximum capacity of the relief valve at design pressure is limited to reduce the magnitude of a reactor transient if one valve would inadvertently open and remain open.

Each power-operated atmospheric relief valve is located outside the containment in the auxiliary building upstream of the main steam isolation valves, in the portion of the main steam line associated with each SG. This location permits valve operation following transient conditions, including those that could result in closure of the main steam isolation valves.

The operation of the power-operated atmospheric relief valves is automatically controlled by steam line pressure during plant operations. The power-operated atmospheric relief valves automatically modulate open and exhaust to atmosphere whenever the steam line pressure exceeds a predetermined setpoint. As steam line pressure decreases, the relief valves modulate closed, reseating at a pressure at least 0.7 bar (10 psi) below the opening pressure. The setpoint is selected between no-load steam pressure and the set pressure of the lowest set safety valves.

The SG power-operated atmospheric relief valves provide a means for plant cooldown by discharging steam to the atmosphere when the turbine bypass system is not available. Under such circumstances, the relief valves (in conjunction with the startup feedwater system) allow the plant to be cooled down at a controlled cooldown rate from the pressure setpoint of the lowest set of safety valves down to the point where the RNS can remove the reactor heat.

For their use during plant cooldown, the power-operated atmospheric relief valves are automatically controlled by steam line pressure, with remote manual adjustment of the pressure setpoint from the MCR or the remote shutdown room (RSR) (which contains the remote shutdown workstation (RSW)). To effect a plant cooldown, the operator manually adjusts the pressure setpoint downward in a stepwise fashion. The maximum cooldown rate achievable is limited by the flow-passing capability of the relief valves, the number of SGs (and hence the number of relief valves) in service, the available startup feedwater pumping capacity, and the desire to either maintain or recover SG water levels during the cooldown.

The PORVs also help to avoid actuation of the safety valves during certain transients and, following safety valve actuation, assist the safety valves to positively reseat by automatically reducing and regulating steam pressure to a value below the valve reseating pressure. The operation of each power-operated atmospheric relief valve is controlled in response to measurements of steam line pressure provided by four separate pressure taps on the associated steam line.

The valve operator is an air-operated modulating type, providing throttling capability over a range of steam pressures.

The atmospheric relief valves are controlled by control systems for the modulating steam relief function. The capability for remote manual valve operation is provided in the MCR and at the RSW. A solenoid is provided to vent the air from the valve operator to terminate a steam line depressurisation transient.

An isolation valve with remote controls is upstream of each power-operated relief valve, providing isolation of a leaking or stuck-open valve. The upstream location allows for maintenance on the power-operated relief valve operator at power. The motor-operated isolation valve closes automatically on low steam line pressure to terminate steam line depressurisation transients.

6.5.4.3 Main Steam Isolation Valves

The function of main steam isolation (SGS-PL-V040A/B) is to limit the following:

- Blowdown to one SG in the event of a steam line break
- The cooling effect upon the reactor coolant to within the specified fuel design limits
- Containment pressure to a value less than design pressure
- Isolate ruptured SG for SGTR.

Main steam isolation consists of one quick-acting gate valve in each main steam line and one associated globe main steam isolation bypass valve with associated actuators and instrumentation. These valves are located outside the containment, downstream of the SG safety valves and the atmospheric relief valve, in the auxiliary building. The isolation valves provide positive shutoff with minimum leakage during postulated line severance conditions either upstream or downstream of the valves.

The main steam isolation valves (MSIVs) close fully upon receipt of a manual or automatic signal and remain fully closed.

Position indication and remote manual operation of the isolation valves are provided in the main control room and remote shutdown workstation.

6.5.4.4 Steam Generator Isolation Valves

In addition to the main steam isolation valves discussed above, there are additional SGS isolation valves that are automatically actuated in order to completely isolate a SG under faulted or ruptured conditions.

Four valves (SGS-PL-V074A/B and SGS-PL-V075A/B) are associated with the steam generator blowdown system (BDS). Two series isolation valves are on each SG blowdown line as it exits the containment. These fail-closed, isolation valves receive an automatic closure signal from PMS on the following three signals:

- Low narrow-range SG level
- PRHR HX actuation
- Containment isolation signal

The drain line for each main steam line outside containment and upstream of the MSIVs contains two series, fail-closed, isolation valves that are automatically closed on receipt of a steam line isolation signal.

Each MSIV steam bypass line contains a fail-closed isolation valve that is automatically closed on receipt of a steam line isolation signal.

6.5.5 Main Turbine Generator

The main turbine receives steam from the SGs, extracts useful energy from the steam by expanding it, and then exhausts it into the main condenser. The turbine generator consists of a single double-flow, high-pressure turbine cylinder and three double-flow, low-pressure turbine cylinders. It is described fully in Section 17.4. Two MSRs are between the high- and low-pressure cylinders. Some steam is bled off at various points during the expansion of the steam as it passes through the turbine, which is used principally for heating the feedwater and reheating the steam; these processes enhance the cycle thermodynamic efficiency. A number of auxiliary systems are associated with the main turbine: the bearing lubrication oil system, a digital electrohydraulic control system, a turbine gland steam sealing system, overspeed protective devices, and barring (turning) gear. Further design details of this system and its constituent components are delineated in Chapter 17 and Reference 6.29.

The main generator is on the same shaft as the turbine. Its minimum rating is approximately 1375 MVA at 0.90 power factor. Its stator is cooled by deionised water, its rotor by hydrogen

gas. The magnetisation current for the rotor comes from the rectified output of an excitation transformer, which itself is fed from the main generator; the magnetisation current is controlled through a voltage regulator. A number of auxiliary systems are associated with the main generator: the same bearing lubrication oil system as the main turbine, the stator cooling water system, the hydrogen and seal oil systems, and a carbon dioxide system for the purging of hydrogen and air during lay-up or plant outages.

The flow of main steam entering the high-pressure turbine is controlled by four control valves. The turbine control valves are adjusted automatically by electrohydraulic servo actuators. These actuators control the turbine speed when it is starting up, and for load control after the turbine generator unit is synchronised to the grid. In series with each control valve is a stop valve; its function is to shut off and isolate the steam flow to the turbine when required. The control and stop valves all close completely on a turbine trip.

Six intercept valves control steam flow to the low-pressure turbine cylinders. The intercept valves are located in the hot reheat lines at the inlet to the low-pressure turbine cylinders. There is a reheat stop valve in series with each intercept valve. The reheat stop and intercept valves all close completely on a turbine trip.

The turbine generator is supported by a spring-mounted system to isolate the dynamic behaviour of the turbine-generator equipment from the foundation structure. The support system includes a reinforced concrete deck on which the turbine generator is mounted.

6.5.6 Turbine Bypass Function

The turbine bypass pipe work and valves provide the capability to dissipate heat directly to the condenser during plant startup and during the cooldown of the RCS to the point where the RNS can be placed in service. The turbine bypass system is described in Section 17.4. The system reduces the challenges to the main steam PORVs, the main steam safety valves, the SG level control, and the pressuriser safety valves following a reactor trip, rapid load reductions during normal operation, and turbine trips without a reactor trip.

The plant is designed to accommodate a ramp load change of 5 percent per minute between 25 percent and 100 percent of full load without reactor trip or steam dump actuation. Instead, it is accommodated by the reactor power control, the pressuriser level control, the pressuriser pressure control and the SG level control systems.

For medium load rejections (greater than 10 percent but less than 50 percent, or a turbine trip from 50 percent power or less), the turbine bypass system operates in conjunction with the same control systems used for the small power reductions.

For large load rejections (greater than 50 percent power), the turbine bypass system operates in conjunction not only with the previously mentioned control systems but also with the rapid power reduction system, which is designed to rapidly reduce the reactor power to a value that can be handled by the turbine bypass system. Upon the detection of a large and rapid turbine power reduction, a pre-selected number of control rods are dropped into the reactor core, causing the reactor power to reduce to approximately 50 percent.

6.5.7 Moisture Separator Reheaters

After expanding through the high-pressure turbine, the exhaust steam is wet and at saturation temperature. It is routed through two external MSR vessels, where it is dried and superheated. The external moisture separators reduce the moisture content of the high-pressure exhaust steam. It uses multiple-vane chevron banks for moisture removal. The moisture that has been

removed drains to a moisture-separator drain tank, from where it is pumped to the deaerator, which is at similar pressure to the steam entering the low-pressure turbine.

The dried steam is then reheated in a two-stage reheater to superheated conditions: the first stage reheat uses the steam bled from partway down the high-pressure turbine, while the second-stage reheat uses a portion of the much hotter main steam supply from the SGs. Each stage of the reheater is a shell-and-tube HX, the pressure on the tube side being much higher than on the shell side. Condensed steam in the reheater (tube side) is drained to the reheater drain tank, from which it flows into the shell side of the No. 7 feedwater heater and then cascades to the No. 6 feedwater heater.

The dried and superheated steam from the reheater flows to the inlets of the three low-pressure turbines through six reheat steam lines, each with a separate stop and intercept valve.

The MSRs are required to take the wet steam emerging from the high-pressure turbine exhaust, dry it, and then superheat it. This enables the low-pressure turbine cylinders to achieve a much higher thermodynamic efficiency in their expansion of the steam, at the same time experiencing much lower rates of blade erosion from the water droplets than would otherwise be present. The heat remaining in the bled steam after its passage through the reheater is used for feed heating, further enhancing the overall thermodynamic efficiency.

6.5.8 Condenser Air Removal System

The condenser air removal system (CMS) removes non-condensable gases (mainly nitrogen, oxygen, and ammonia) from the main condenser during plant startup, cooldown, and normal operation. Without this, the condenser tubes would become blanketed by these gases and thereby lose their effectiveness in condensing the steam. The air removal system consists of four liquid ring vacuum pumps: one vacuum pump is provided for each of the three condenser shells, and one pump is provided as a standby. The non-condensable gases together with some steam are drawn from the condenser shells to the suction of the vacuum pumps, which exhaust to atmosphere through the turbine island vents drains and relief system. The standby pump package is provided since failure of the condenser air removal system for one of the main condenser shells would result in a gradually increasing backpressure in that particular condenser shell. Eventually, this would result in a turbine trip on high condenser pressure. Further design details of this system and its constituent components are delineated in Reference 6.51.

The mixture of non-condensable gases and steam is not normally radioactive; however, it is possible for the mixture to become contaminated in the event of primary-to-secondary system leakage. Therefore, the exhaust gases are monitored for radioactivity and alarmed in the MCR.

6.5.9 Gland Seal System

The annular space between the turbine shaft and the turbine casing is sealed by glands, which minimise the leakage from those turbine cylinders that are above atmospheric pressure, or the leakage into those turbine cylinders that are below atmospheric pressure. For the former, the sealing steam is the actual leakage steam through the gland; for the latter, the sealing steam is supplied from the main steam system or, during startup of the turbine, from the auxiliary steam system. At the outside ends of the glands, the leaking steam is collected in piping held just below atmospheric pressure, and then routed to the gland seal condenser. Unavoidably, there is air leakage as well into the collection pipe work because of the small gap between it

and the rotating turbine shaft. Further design details of this system and its constituent components are delineated in Reference 6.52.

The gland seal condenser is a shell-and-tube type HX where the steam-air mixture from the turbine seals is discharged into the shell side; condensate from the main condenser flows through the tube side as the cooling medium. The gland seal condenser internal pressure is maintained at a slight vacuum by motor-operated blowers. Condensate from the steam-air mixture drains to the main condenser, and the non-condensable gas (mostly air) is exhausted to the atmosphere through the turbine island vents drains and relief system through a common discharge line shared by the vapour extractor blowers.

The main condenser can be utilized for cooling down the SGs and the RCS during several design-basis initiating events. Failure of the gland seal system during such fault transients would rapidly result in the main condenser becoming unavailable. A reliable gland seal system is thus desirable but not essential.

The mixture of non-condensable gases discharged from the gland seal condenser blower is not normally radioactive, but it is possible for the mixture to become contaminated in the event of primary-to-secondary system leakage. The turbine island vent discharge radiation monitor measures the concentration of radioactive gases in the gland seal steam condenser steam as in the non-condensable gases that are discharged by the condenser vacuum pumps. This measurement provides early indication of leakage between the primary and secondary sides of the SGs.

6.5.10 Main Condenser

The main condenser is part of the AP1000 plant CDS. The main condenser provides the heat sink for the steam cycle, receiving and condensing exhaust steam from the main turbine or the turbine bypass system, accepting high-energy cycle drains, and providing partial deaeration of condensate. The main condenser is a three-shell, single-pass, multi-pressure, spring-supported unit that is hard-connected at the turbine exhaust flange. Each shell is located beneath its respective low-pressure turbine.

The cooling water passes through the tube side of each condenser shell.

The condenser is equipped with titanium tubes and has titanium-clad tube sheets. The titanium material exhibits high corrosion and erosion-resisting properties and good mechanical properties. The condenser tubes are mechanically expanded and seal-welded to the tube sheet cladding to minimise leakage at the joints.

The condenser water boxes are structurally designed as pressure vessels and constructed from reinforced steel plate. Rubber lining is applied to the water box interior surface to provide resistance to corrosion.

The main condenser is designed to receive and condense the full-load steam flow exhausted from the main turbine. It also receives discharges from auxiliary systems such as the feedwater heater vents and drains and the gland sealing steam spillover and drains. To protect the condenser shells and turbine exhaust hoods from overpressurisation, steam relief blowout diaphragms are provided in the low-pressure turbine exhaust hoods. Excessive temperature conditions are mitigated by sprays in the low-pressure turbine exhaust hoods. Two low-pressure feedwater heaters are located in the neck area of each condenser shell, adjacent to where their steam is bled from the low-pressure turbine.

The hot wells of the condenser shells are interconnected to facilitate removal of condensate by the condensate pumps. Condensate flows between the condenser shells via interconnecting piping and baffling. A single common connection is provided at the last condenser shell for the condensate pumps. Condensate flows to each condensate pump and is pumped into the feed and condensate system.

The condenser shell hot wells have a condenser storage capacity of 3 minutes of feed flow at normal full power flow rate.

The hot well level controller provides automatic makeup or extraction of condensate to maintain a normal level in the condenser hot wells. On low level, the makeup control valves open and admit condensate by vacuum-draw to the hot well from the condensate storage tank. On high-water level, the condensate reject control valves open to divert water from the condensate extraction pump discharge to the condensate storage tank. The condensate extraction or rejection stops automatically when the hot well level falls within the normal operating range.

Condensate extraction from the hot well to the storage tank can be manually overridden upon indication of high hot well conductivity to prevent transfer of contaminants into the condensate storage tank in the event of a condenser tube or tube/tube sheet joint failure.

Air in-leakage and non-condensable gases contained in the turbine exhaust steam naturally accumulate in the condenser and must be removed. This is achieved by the CMS.

A condenser tube cleaning system mechanically cleans the circulating water side of the tubes. This cleaning, along with chemical treatment of the circulating water, reduces fouling and helps to maintain the thermal performance of the condenser. Further design details of this component are delineated in Reference 6.50.

6.5.11 Steam Generator Blowdown System

The principal purpose of the BDS is to remove impurities from the feedwater within the SG, which would otherwise rise in concentration as pure water and other volatiles boil off. This is particularly necessary during the anticipated operational occurrences of in-leakage of circulating water into the main condenser and SG tube leakage, which would add contaminants. The BDS continuously extracts a small proportion of the water from each SG. The maximum purification blowdown rate is approximately 0.61 percent of the maximum steaming rate or approximately six-thousandths of the feed flow rate. This blowdown flow is cooled and depressurised before being chemically processed to remove the impurities. It completes the process by being returned into the condenser before being returned to the SGs. Further design details of this system and its constituent components are delineated in Chapter 17 and Reference 6.30

The BDS also includes a recirculation-drain pump for use during operating modes when the SG pressure is low. This pump enables the BDS to fulfil the following additional functions:

- Cooling down the SG for inspection and maintenance purposes.
- Establishing and maintaining SG wet lay-up conditions during plant outages.
- Draining the secondary side of the SGs for maintenance.

The system consists of two blowdown trains, one for each SG. The blowdown water is extracted just above the tube sheet of a SG. The blowdown flow is cooled using a regenerative HX, which uses the heat to warm the condensate. Flow control valves adjust the blowdown flow rate from each SG and depressurise it. It then enters an electro deionisation demineralising unit ion-exchange purification unit, which removes impurities. Downstream of the purification unit, both trains combine into a common header, which contains a relief valve for providing overpressure protection for the low-pressure portion of the system.

It is necessary to protect the low-pressure portion of the blowdown system from the high pressure and temperature to which it could be exposed if the pressure is not reduced or the blowdown flow is not cooled. Each of the two blowdown lines has two BDS isolation valves in series (upstream there are two AOV fail closed SGS isolation valves), which are located in the auxiliary building. These BDS valves fail closed on loss of air or power. The SG blowdown lines are a closed system inside the reactor containment, and so they do not require any further valves in the line inside the containment. This is because any radioactivity within the containment atmosphere has no way of passing into a closed system. The BDS isolation valves close automatically on high blowdown system temperature or pressure, on low SG water levels, on actuation of the PRHR HX, on receipt of a containment isolation signal, or on detection of high blowdown system radiation level. The isolation of the BDS contributes to the continued availability of the SGs as a heat sink during various fault transients by not further reducing their water inventory.

The radiation monitors associated with the BDS provide a means of recognising when the secondary side becomes radioactively contaminated, an indication of a SG tube leakage or rupture. The blowdown flow and the ion exchange waste stream flow are both continuously monitored for radioactivity. If such radioactivity is detected, the blowdown flow is automatically re-aligned to the WLS in order to process the blowdown and ion-exchange waste effluent. If radioactivity exceeds a preset level, the blowdown flow control valves and the isolation valves automatically close.

6.5.12 Circulating Water System

The CWS is a site-specific system and consists of three electric-powered water pumps and the associated piping, valves, and instrumentation. The main purpose of the CWS is to supply cooling water to the main condensers to condense steam; as such, it is the principal heat sink during normal operation and during those fault conditions. Its secondary purpose is to supply cooling water to the turbine building closed cooling water system HXs and to the condenser vacuum pump seal water HXs.

The underground portions of the CWS piping are constructed of concrete pressure piping or steel (possibly with an internal coating or lining of a corrosion-resistant compound). Motor-operated butterfly valves provided in each of the circulating water lines at their inlet to and exit from the condenser shell allow isolation of portions of the condenser.

6.5.13 Auxiliary Steam Supply System

ASS provides the steam required for plant use during startup, shutdown, and normal operation. Steam is supplied from either the auxiliary boiler or the MSS. The auxiliary boiler is located in the turbine building. The system consists of steam generation equipment and distribution headers. Further design details of this system and its constituent components are delineated in Reference 6.32.

Condensate from the condensate storage tank is chemically treated and pumped to the auxiliary boiler deaerator where oxygen and non-condensables are removed using auxiliary steam. The auxiliary boiler feedwater pumps deliver condensate from the auxiliary boiler deaerator to the auxiliary boiler. A feedwater control valve, located in the feedwater piping, regulates water level in the auxiliary boiler. Feedwater flow is proportional to the auxiliary boiler steaming rate. Steam generated by the auxiliary boiler is supplied to the plant auxiliary steam distribution piping.

Boiler water quality is maintained by controlling boiler blowdown flow to an atmospheric blowdown tank and by feeding oxygen-scavenging and pH control chemicals to the boiler makeup water system. Water level in the auxiliary boiler deaerator is maintained by an automatic control valve in the condensate supply and deaerator overflow piping. The auxiliary steam boiler is an electric package boiler. It supplies the steam required during a cold start of the MSS and the turbine generator; in addition, it provides the steam for hot water heating. Main steam supplements the auxiliary steam header during startup, and it supplies the auxiliary steam during normal operation at power. The auxiliary boiler provides the steam during a plant shutdown.

The ASS provides the following services:

- Steam to the plant hot water heating system HXs for use by the heating system ventilation coils.
- Steam to the deaerator prior to returning to operation at power and after a turbine trip, to heat, pressurise, and deaerate the feedwater.
- Steam to warm the MSS and turbine SSCs during plant startup.
- Sealing steam to the glands of the main turbine prior to returning to operation at power when main steam is unavailable.
- Steam to the MSRs and to the feedwater heaters when main steam is unavailable.

6.5.14 Turbine Island Chemical Feed System

The turbine island chemical feed system (CFS) injects the required chemicals into the condensate system, the feedwater system, the ASS, the service water system (SWS), the BDS, and the DWS. It is entirely located in the turbine building. Further design details of this system and its constituent components are delineated in Reference 6.32.

6.5.15 Condensate Polishing System

The condensate polishing system (CPS) is used to remove corrosion products and ionic impurities from the condensate system during plant startup, hot standby, power operation with abnormal secondary cycle chemistry, safety shutdown, and cold shutdown operations. Further design details of this system and its constituent components are delineated in Reference 6.33.

6.5.16 Secondary Sampling System

The secondary sampling system (SSS) delivers representative samples of fluids from secondary systems to sample analyser packages. Continuous or semi-continuous online secondary chemistry monitoring detects impurity ingress and provides early diagnosis of

system chemistry excursions in the plant. Secondary sampling monitors send control signals to the CFS that automatically inject corrosion control chemicals into the condensate and feedwater systems. Additional design detail of this system and its constituent components are delineated in Reference 6.37.

6.6 PASSIVE SAFETY SYSTEMS

The AP1000 plant uses passive Class 1 safety systems and features for protecting against accidents.

The distinguishing safety enhancement of the AP1000 plant design over existing PWR technology is the adoption of passive protective safety measures, which operate during fault sequences in the event that normal duty systems have failed. These systems are regarded as passive because they rely on natural physical processes for their operation with no reliance on active components such as pumps, fans, or diesel generators; and they are designed to function without Class 1 support systems such as ac power and component cooling water.

These systems include the following:

- Passive core cooling system (PXS)
- Plant structures inside containment to promote flood-up and natural circulation cooling
- Passive containment cooling system (PCS)
- Main control room (MCR) emergency habitability system (VES)
- Passive structural heat sinks to maintain acceptable temperatures for plant personnel and required equipment
- The spent fuel pool structures and their contained water inventory

These systems and features are described briefly below.

6.6.1 Passive Core Cooling System

The PXS is designed to perform the following major Class 1safety functions:

- Emergency RCS Makeup and Boration
- Safety Injection
- Emergency Core Decay Heat Removal
- Post Accident Containment pH Control
- Nitrogen Supply Line Containment Isolation

These safety-related functions are provided by Class 1 equipment with redundancy to deal with single failures, environmental qualification, and protection from external hazards. These

functions are available during all normal modes of RCS operation including hot / cold shutdowns and refuelling. Further design details of this system and its constituent components are delineated in Reference 6.13 and Chapter 17.

The Technical Specifications (Reference 6.11) detail the requisite PXS water flows, requisite volumes, etc.

The PXS consists of a PRHR HX (PXS-ME-01), two Accumulators (PXS-MT-01A/B), two CMTs (PXS-MT-02A/B), an IRWST (PXS-MT-03), two RCS depressurization spargers (PXS-MW-01A/B), four pH adjustment baskets (MY-Y03A/B, MY-Y04A/B), Containment and IRWST screens (PXS-MY-Y02A/B, Y03A/B, Y04A/B) and associated valves, piping, and instrumentation. Two simplified sketches are included as Figures 6-3 and 6-4. These figures include the four ADS stages (RCS components) since they functionally support the PXS.

The primary function of the PXS is to bring the plant to safe shutdown conditions using only Class 1 equipment by providing the means for boration, coolant injection, and core cooling. The PXS function is performed with no reliance on ac electrical power or active cooling water support systems.

The PXS is designed to perform its Category A safety functions based on the following considerations:

- It has component redundancy to provide confidence that its Category A functions are performed even in the unlikely event of the most limiting single failure occurring coincidentally with postulated DBEs.

- Components are designed and fabricated according to industry standard quality groups commensurate with SSC Class 1.

- It is tested and inspected at appropriate intervals, as defined by standards and Technical Specifications (Tech Specs) appropriate to SSC Class 1.

- It performs its intended Category A functions following events such as fire, internal floods, internal missiles, or pipe breaks.

- It is protected from the effects of external events such as earthquakes, tornadoes, and floods.

The design is sufficiently redundant and diverse to achieve the reliabilities required to support the plant core melt frequency and significant-release frequency targets.

6.6.1.1 PXS Functions

6.6.1.1.1 Emergency RCS Makeup and Boration Function

The PXS provides RCS makeup during transients or accidents in which the normal RCS makeup supply from the chemical and volume control system (CVS) is unavailable or is insufficient. This makeup allows for transfer of heat from the core. This makeup is sufficient to accommodate significant RCS leakage and RCS cooldown without ADS actuation.

The PXS also adds negative reactivity during transients or accidents in which the normal RCS boron makeup supply from the CVS is unavailable or is insufficient. This negative

reactivity provides or recovers core shutdown margin for events which result in cooldown of the RCS, such as steam line break accidents or safe shutdown cooldowns.

During an Anticipated Transient Without Trip (ATWT), the PXS removes sufficient heat to adequately cool the core and inject sufficient boron to shut down the core.

6.6.1.1.2 Safety Injection Function

The PXS provides safety injection to the RCS to ensure adequate core cooling for the complete range of LOCAs up to and including the double-ended rupture of the largest RCS piping. In addition to mitigating the immediate effects of the LOCA, the safety injection function must provide core cooling to support long-term safe shutdown.

The ADS, which is part of the RCS, supports the PXS in performing the safety injection function by depressurizing the RCS to allow lower pressure injection supplies to inject.

6.6.1.1.3 Emergency Core Decay Heat Removal Function

The PXS provides emergency core cooling during transients, accidents, or whenever the normal heat removal paths are unavailable. The emergency core cooling prevents overheating of the core and supports the capability for the plant to meet the safety analysis acceptance criteria, including criteria for primary and secondary system pressure, departure from nucleate boiling ratio (DNBR), and pressurizer volume. During a steam generator tube rupture (SGTR) accident, the emergency core cooling removes sufficient heat to support automatic termination of the loss of reactor coolant.

6.6.1.1.4 Nitrogen Supply Line Containment Isolation

The PXS provides for containment isolation of the nitrogen supply line for the accumulators, outside of containment. It achieves this function during an event by the use of a fail-closed, air-operated valve (PXS-PL-V043) located outside of containment as well as a check valve (PXS-PL-V043) inside of containment. This will prevent additional mass and energy from entering containment during an event.

6.6.1.1.5 In Vessel Retention

The PXS provides the capability to flood the containment so that following a severe accident, the outside of the reactor vessel is flooded. This capability supports cooling of the damaged core inside the vessel.

6.6.1.1.6 RCS Cooldown Function

The PXS is able to cool the RCS to a temperature at which the Normal Residual Heat Removal System (RNS) can be put into operation if cooling with the steam generators is not possible.

6.6.1.1.7 Refueling Cavity Flooding Function

The PXS stores sufficient water to flood the refuelling cavity during normal plant refuelling operations.

6.6.1.2 PXS Subsystems

6.6.1.2.1 RCS Injection Subsystem

The RCS injection subsystem consists of CMTs (PXS-MT-02A/B), Accumulators (PXS-MT-01A/B), an IRWST (PXS-MT-03), and associated valves, piping, and instrumentation.

The safety injection from these three injection sources, as well as the containment recirculation flow paths, has a common discharge through the two DVI lines and into the reactor vessel DVI nozzles. A deflector is located in the reactor vessel downcomer at the end of each DVI nozzle to direct the PXS injection flow downward into the reactor vessel downcomer plenum in order to minimize core bypass flow and to help guide flow toward the bottom of the reactor vessel. The DVI nozzles have a venturi shape, which reduces the loss of reactor coolant in case of a break of the DVI line, and minimizes the pressure loss during PXS injection.

The CMTs provide RCS makeup and boration for LOCAs and non-LOCAs when the normal makeup system is unavailable or insufficient. There are two CMTs located inside the containment at an elevation slightly above the reactor coolant loops. During normal operation, the core makeup tanks are completely full of cold borated water. The boron concentration of this water is somewhat higher than that of the water in the Accumulators and the IRWST. The boration capability of these tanks provides adequate core shutdown margin following a steam line break and for safe shutdown events.

The CMTs are connected to the RCS through a discharge injection line and a cold leg inlet pressure balance line. The discharge line is isolated by two normally closed, parallel air-operated isolation valves that open on a loss of air pressure or electrical power.

6.6.1.2.2 Emergency Core Decay Heat Removal Subsystem

The emergency core decay heat removal subsystem consists of one PRHR HX (PXS-ME-01) and associated valves, piping, and instrumentation.

The heat exchanger is located in the IRWST, which provides the heat sink for the heat exchanger. The heat exchanger consists of a bank of C-tubes, connected at the top (inlet) and bottom (outlet) to a tubesheet and channel head mounted on the IRWST wall. The number of tubes installed provides for tube plugging margin. The PRHR HX is connected to the RCS through an inlet line from one RCS hot leg. This line contains a normally open motor operated valve (MOV). The outlet line connects to the associated steam generator cold leg plenum (reactor coolant pump suction). The outlet line contains parallel normally closed air-operated valves that open on loss of air pressure or electrical power. These valves are opened on receipt of a safeguards actuation signal.

The alignment of the PRHR HX (with a normally open inlet motor-operated valve and normally closed parallel outlet air-operated valves) maintains the heat exchanger full of reactor coolant at RCS pressure and prevents water hammer upon initiation of PRHR HX operation. The inlet line is well insulated and routed continuously upward from the top of the hot leg to a high point above the HX inlet. This arrangement ensures that the water in the line will remain hot, which will provide for natural circulation of the PRHR HX water. The water in the HX is stagnant and will be in thermal equilibrium with the water in the IRWST. This arrangement maintains a thermal driving head during normal plant standby conditions which provides for the initial PRHR HX startup operation.

The heat exchanger is elevated above the RCS loops to induce natural circulation flow

through the heat exchanger when the reactor coolant pumps are not available. The PRHR heat exchanger piping arrangement also allows actuation of the heat exchanger with reactor coolant pumps operating. When the Loop 1 reactor coolant pumps are operating, they provide forced flow in the same direction as natural circulation flow through the heat exchanger. If the pumps are operating and subsequently trip, then natural circulation provides the driving head for the heat exchanger flow.

6.6.1.2.3 Post Accident Containment pH Control Subsystem

The containment pH control subsystem consists of pH adjustment baskets (MY-Y03A/B, MY-Y04A/B). The pH adjustment baskets are located inside the containment, below the minimum post-accident floodup level.

The pH adjustment baskets provide the capability for chemical addition to the containment recirculation water in severe accident floodup conditions where core damage has occurred and core radioactivity has been released from the RCS into containment. The baskets initiate chemical addition passively when the containment flood-up level reaches the baskets. Effective mixing with the water in the containment is ensured by the use of four baskets and their location in the circulation path of water which cools the damaged core. That circulation path starts under the reactor vessel, comes up past the vessel into the loop compartments, flows into the corridor connecting the loop compartments, and flows down the stairwell to beneath the reactor vessel.

The pH adjustment baskets are filled with granulated trisodium phosphate (TSP). The baskets are located on containment floor.

The baskets are elevated about 0.3 m (1 ft) above the floor to reduce the chance that water spills in the containment will dissolve the TSP. This location minimizes the chance that spray from leaks or breaks of high-energy lines will reach them. The baskets are located along walls with adequate exposed areas enclosed with mesh.

During a LOCA, after ADS has been actuated, the TSP dissolves into the containment water as the flood-up level covers the TSP baskets. This design provides automatic pH adjustment:

- To reduce offsite doses during severe accidents (where the core has suffered damage)

- To prevent stress corrosion cracking of stainless steel during design basis accidents

6.6.1.2.4 Valve Leak Test Subsystem

A valve leak test subsystem which is used at shutdown conditions to leak-test some RCS pressure boundary isolation valves. Four PXS valves (the Accumulator isolation check valves) and eight RNS valves (two check and two stop-check valves on the RNS outlet to the DVI and four MOVs in the RNS inlet from the RCS hot leg) are provided with connections that can be used to determine their seat leakage. All of these valves are located inside the containment.

6.6.1.2.5 Automatic Depressurization Subsystem

The ADS is part of the RCS. Since it functions together with the PXS to provide core cooling in LOCA events, a brief description is provided below. Figures 6-3 and 6-4 shows the ADS.

There are four stages of ADS valves. The first three stages are connected to the pressurizer and discharge to the IRWST through spargers. The fourth stage is connected to the RCS hot legs and discharges into the containment loop compartments. Each Stage 1/2/3 has two lines and each line has two valves in series. The fourth stage has four lines with each line having two valves in series.

The valves used in the first three stages are direct current (dc) motor-operated. All of the valves are normally closed. The fourth stage valves are squib valves (see Chapter 17 for further discussion).

6.6.1.3 Operation During Plant Transients and Accidents

6.6.1.3.1 Operation During Loss of Main Feedwater Flow Events

The most severe core conditions resulting from a loss of main feedwater system flow are associated with a loss of feedwater flow at full power. The heatup transient effects of loss of feedwater flow at reduced power levels are bounded by the loss of flow at full power. This event is similar to events such as station blackout.

The AP1000 design startup feedwater (SFW) that is able to remove the core decay heat generated after the reactor trip that follows a postulated non-LOCA event. This avoids excessive heatup of the primary system and loss of subcooling and prevents water relief from the pressurizer.

Should the main feedwater (MFW) and SFW be unavailable, the PRHR HX is actuated by a Low-2 narrow range SG level and coincident Low-2 SFW flow signal. PRHR HX operation removes decay heat and begins to cool down the RCS when the PRHR HX heat transfer capability matches the core decay heat rate. The PRHR HX actuation could be insufficient to prevent pressurizer overfill, but the reactor vessel head vent valves can be used in this situation to relieve mass from the RCS and prevent pressurizer overfill. Once actuated, the PRHR HX does not require electrical power or operator actions for continued RCS cooling.

When PRHR HX cooling has sufficiently reduced the pressurizer level or RCS temperature, the CMTs are automatically actuated to provide RCS makeup and boration. The CMTs inject borated water directly into the reactor vessel downcomer. When the CMTs are actuated, the reactor coolant pumps are tripped, which results in the PRHR HX operating under natural circulation. The CMT injection maintains RCS inventory and adds negative reactivity. In this scenario, the CMTs operate in a water recirculation mode and the cold legs do not void. The CMTs remain full and ADS is not actuated.

The RCS pressure remains above the pressure of the Accumulators so they do not inject. After stabilizing plant conditions and satisfying PXS termination criteria, the operator terminates PXS operation and initiates normal plant shutdown operations.

6.6.1.3.2 Operation During Feedwater Line Break Events

For this event, the PRHR HX and the CMTs are automatically actuated. The PRHR HX removes core decay heat, and the CMTs inject borated water directly into the reactor vessel downcomer. Since the reactor coolant pumps are automatically tripped on actuation of the CMTs, the PRHR HX operates under natural circulation. In this scenario, the cold legs do not void, so the CMTs operate in the water recirculation mode to maintain RCS inventory and add negative reactivity. The CMTs remain full and ADS is not actuated. Once actuated, the PRHR HX and CMTs do not require electrical power or operator actions for continued RCS

cooling.

The RCS pressure remains above the pressure of the Accumulators, so they do not inject.

6.6.1.3.3 Operation During Steam Line Break Events and Inadvertent Opening of a SG Relief/Safety Valve Event

The main steam lines are also isolated to prevent blowdown of more than one steam generator. The CMTs operate with water recirculation to provide borated water to the reactor vessel downcomer for RCS inventory and reactivity control. The negative reactivity provided by operation of the CMTs is not fast enough to prevent the reactor from briefly returning to criticality during the transient. In the longer term, the cooldown slows down and the CMT boration is able to shut down the core. The departure from nucleate boiling design basis is met, thereby preventing fuel damage. The CMT flow also functions to increase RCS inventory so that visible pressurizer level is restored.

For this event, the CMTs operate in a water recirculation mode and the cold legs remain filled. As a result, the CMTs remain full and ADS is not actuated.

6.6.1.3.4 Operation During LOCA Events

A LOCA is a rupture of the RCS piping or branch piping that results in a decrease in RCS inventory exceeding the flow capability of the normal makeup system.

Following a postulated LOCA, the RCS pressure decreases and initiates a reactor trip and safety injection following safeguards actuation. The safeguards actuation signal trips the RCPs and opens the CMT outlet isolation air operated valves (AOVs). The CMTs provide high pressure injection and can operate via water recirculation or steam-compensated injection at full RCS pressure. For smaller LOCAs, the pressurizer level is sufficient to initially establish CMT water recirculation. For larger break sizes, the pressurizer level decreases more rapidly and steam-compensated injection occurs after the cold legs void.

As the CMTs' water level drops, level sensors in the tank actuate the ADS. The use of CMT level to actuate ADS minimizes the chance of unnecessary ADS actuations and provides reliable/timely ADS actuation when it is required during LOCAs. The ADS depressurization of the RCS is staged to limit the RCS depressurization rate and the maximum vent flow to the depressurization spargers. Limiting the RCS depressurization rate minimizes the potential for the core to uncover during ADS operation. Limiting the ADS flow to the spargers reduces the hydrodynamic loading on the IRWST.

The Accumulators begin to inject when the reactor coolant system depressurizes to about 4.8 MPa gauge (700 psig). The Accumulator injection provides for rapid reflooding of the core during large LOCAs, which prevents excessive core clad temperatures.

When the fourth stage ADS valves are actuated, the IRWST injection squib valves are also actuated. However, because the RCS pressure will be somewhat above the IRWST injection head at this time, the check valves in the IRWST injection line will not open until the RCS pressure has been further reduced by the ADS.

As the IRWST injection flow continues, the IRWST level will slowly drop and the containment water level will increase from the break flow. When the IRWST level drops to a Low-3 level setpoint, the containment recirculation lines are opened and water is drained into the PXS sump.

At this time, recirculation will begin; water in the containment will flow into the reactor to provide continued cooling of the core. Redundant flow paths from the containment to the reactor are provided.

In this long-term cooling mode, the core remains covered and decay heat is removed by steaming to the containment through the break and/or the ADS valves. The steam is condensed on the steel containment shell which is cooled by the PCS.

6.6.1.4 Description of the Passive Core Cooling Components

6.6.1.4.1 Core Makeup Tanks

The two CMTs (PXS-MT-02A/B) are vertical, cylindrical tanks with hemispherical upper and lower heads. They are made of carbon steel, clad on the internal surfaces with stainless steel. They are located inside containment on the 102.12-m (107-foot 2-inch) floor elevation. The CMTs are located above the direct vessel injection line connections to the RV, which are located at an elevation near the bottom of the hot leg.

During normal operation, the CMTs are completely filled with borated water and are maintained at RCS pressure by the cold leg pressure balance line. The temperature of the borated water in the CMTs is about the same as the containment ambient temperature since the tanks are not insulated or heated.

The inlet line from the cold leg is sized for LOCAs where the cold legs become voided and higher CMT injection flows are required. The discharge line from each CMT contains a flow-tuning orifice that provides a mechanism for the field adjustment of the injection line resistance. The orifice is used to establish the required flow rates assumed in the CMT design. The duration of CMT injection will be much longer when the CMTs operate in the water recirculation mode as compared to the steam condensation mode, and thus the time for them to drain down is dependent on the break size. An additional design function of the CMT discharge orifice is it splits flow to the DVI and to the CMT such that ADS 4 actuation is precluded by preventing the CMT level dropping to the ADS 4 actuation set point.

Connections are provided for remotely adjusting the concentration of the borated water in each CMT during normal plant operation.

Makeup water for the CMTs is provided by the CVS. Samples from the CMTs are taken periodically to check boron concentration. Each CMT has an inlet diffuser designed to reduce steam velocities entering the CMT, thereby minimising potential water hammer and reducing the amount of mixing that could occur during initial CMT draindown operation.

The CMTs are located inside the containment but outside the secondary shield wall. This facilitates maintenance and inspection of the CMT and its level and temperature sensors.

6.6.1.4.2 Accumulators

The two accumulators (PXS-MT-01A/B) are spherical tanks made of carbon steel and clad on the internal surfaces with stainless steel. They are located inside the containment on the floor just below the CMTs.

The accumulators are filled with borated water and pressurised with nitrogen gas. The temperature of the borated water in the accumulators is about the same as the containment ambient temperature since the tanks are not insulated or heated. Each accumulator is connected to one of the direct vessel injection lines. During normal operation, the

accumulator is isolated from the RCS by two check valves in series. When the RCS pressure falls below the accumulator pressure, the check valves open and borated water is forced into the RCS by the gas pressure. Mechanical operation of the check valves is the only action required to open the injection path from the accumulators to the core.

The accumulators are designed to deliver a high flow of borated water to the RV in the event of a large LOCA. This large flow rate is used to quickly establish core cooling following the large loss of RCS inventory.

The injection line from each accumulator contains a flow-tuning orifice that provides a mechanism for the field adjustment of the injection line resistance. The orifice is used to establish the required flow rates assumed in the accumulator design. The accumulator provides injection for several minutes after a large LOCA starting when the RCS pressure drops below the static accumulator pressure.

Connections are provided for remotely adjusting the level and boron concentration of the borated water in each accumulator during normal plant operation.

Accumulator water level may be adjusted either by draining or pumping borated water from the CVS to the accumulator. Samples from the accumulators are taken periodically to check the boron concentration.

Accumulator pressure is provided by a supply of nitrogen gas and can be adjusted as required during normal plant operation. However, the accumulators are normally isolated from the nitrogen supply. Gas relief valves on the accumulators protect them from overpressurisation. The system also includes the capability to remotely vent gas from the accumulator, if required.

The accumulators are located inside the containment and outside the secondary shield wall, facilitating maintenance and inspection of the accumulators and its level and temperature sensors.

6.6.1.4.3 In-Containment Refuelling Water Storage Tank

The IRWST (PXS-MT-03) is a large, stainless-steel-lined tank located underneath the operating deck inside the containment. The tank is constructed as an integral part of the containment internal structures, and is isolated from the steel containment vessel. The bottom of the IRWST is above the RCS loop elevation so that the borated refuelling water can drain by gravity into the RCS after it is sufficiently depressurised. The IRWST is connected to the RCS through both direct vessel injection lines and contains borated water at the existing temperature and pressure in containment. The IRWST does not contain material in either the tank or the recirculation path that could plug the outlet screens.

Vents installed in the roof of the IRWST are normally closed to minimise water vapour and radioactive gases leaving the tank during normal operation and to prevent debris from entering the tank from the containment operating deck. The vents open with a slight pressurisation of the IRWST to provide a path to vent steam generated by the PRHR HX, or subsequently released by the spargers, into the containment atmosphere, should the IRWST water become heated to saturated conditions. Other vents also open on small pressure differentials to allow air or steam to enter the IRWST from containment, such as during a LOCA, to prevent damage to the tank.

Overflows are provided from the IRWST to the refuelling cavity to accommodate volume and mass increases during PRHR HX or ADS operation while minimising the flooding of the containment.

The IRWST contains one PRHR HX and two depressurisation spargers. The top of the PRHR HX tubes are located underwater and extend down into the IRWST. The spargers are also submerged in the IRWST with the midarms located approximately 3 m (10 ft) below the normal water level.

The IRWST is sized to provide flooding of the refuelling cavity for normal refuelling and post-LOCA flooding of the containment for RCS long-term cooling mode; and to support the PRHR HX operation. Flow from the IRWST during the injection mode includes conservative allowances for spill flow during a direct vessel injection line break. The IRWST can provide sufficient injection until the containment sump floods up high enough to initiate recirculation flow. The injection duration varies greatly, depending upon the specific event. A direct vessel injection line break drains the IRWST more rapidly and speeds containment flooding.

Connections to the IRWST provide for transfer to and from the RCS/refuelling cavity via the RNS, purification and sampling via the SFS, and remotely adjustment of the boron concentration via the CVS. Also, the RNS can provide cooling of the IRWST. Additionally there are connections to the IRWST for sampling and instrumentation.

6.6.1.4.4 pH Adjustment Baskets

The PXS uses TSP to adjust the pH of the recirculation fluid in the containment sump. Granulated TSP is contained in stainless steel baskets (MY-Y03A/B, MY-Y04A/B) that have a mesh front that readily permits contact with water.

The TSP is provided to raise the pH of the borated water in the containment to at least 7.0 following an accident. Margin is added to the basket volume to account to long term acid formation during 30 days following a LOCA as well as for possible TSP loss and degradation during normal operation. After extended plant operation, the granular TSP may cake into a solid form as it absorbs moisture. Assuming that the TSP has caked, the dissolution time of the TSP is approximately 3 hours. Good mixing with the sump water is expected because of the baskets' construction and their placement in locations conducive to recirculation flow post-accident. The baskets are designed for easy replacement of the TSP.

6.6.1.4.5 Passive Residual Heat Removal Heat Exchanger

The PRHR HX (PXS-ME-01) consists of inlet and outlet channel heads connected together by vertical C-shaped tubes. The tubes are supported inside the IRWST. The top of the tubes is more than 1 m (3.3 ft) below the IRWST water surface.

The HX inlet piping connects to an inlet channel head located near the top of the IRWST. The inlet channel head and tube sheet are attached to the tank wall via an extension flange.

The HX is supported by a frame attached to the IRWST floor and ceiling. The extended flange is designed to accommodate thermal expansion. The HX outlet piping is connected to the outlet channel head, which is vertically below the inlet channel head near the tank bottom. The structural configuration of the outlet channel head is identical to the inlet channel head. Both channel head tube sheets are similar to the SG tube sheets and have manways for inspection and maintenance access.

The PRHR HX is designed to remove sufficient heat so that its operation in conjunction with short term heat removal by the SGs provides adequate RCS cooling and prevents water relief through the pressuriser safety valves during loss of main feedwater or main feed line break events.

The PRHR transfer of heat into the IRWST results in the water evaporating out of the IRWST. This steam is condensed on the inside of containment by the PCS and is collected by a downspout piping system and gutter arrangement. Condensation is collected by downspouts connected at the Polar Crane Girder and Internal Stiffener, and by the Gutter at the operating deck elevation, and drained back into the IRWST.

PRHR performance post a non-LOCA fault is calculated utilising either Realistic Assumptions or Conservative assumptions as delineated below.

Realistic Assumptions - In utilising realistic assumptions, the PRHR can achieve “safe shutdown” within 36 hours for approximately 14 days following such an event, with or without AC power or the RCPs. The PRHR is designed to achieve “safe shutdown” post a non-LOCA fault. It is important to note that “safe shutdown mode” (Mode 4) only applies to normal operation and does not apply to the post fault condition of “safe shutdown” as discussed in this section and Section 9C. To achieve “safe shutdown” the PRHR HX must be able to cool the RCS core average temperature to 215.6°C (420°F) (average of hot leg and cold leg temperatures). This cooldown allows the RCS pressure to be reduced, which reduces the stress in the RCS and connecting pipes to low levels, greatly reducing the chance of a subsequent LOCA.

Conservative Assumptions - In utilising conservative assumptions, the PRHR can maintain the RCS pressure and temperature below ADS set points (see Section 9C) for greater than 72 hours, with or without AC power or the RCPs. This cooldown allows the RCS pressure to be reduced, which reduces the stress in the RCS and connecting pipes to low levels, greatly reducing the chance of a subsequent LOCA.

PRHR HX flow and inlet and outlet line temperatures are monitored by indicators and alarms. The operator can take action as required to meet the Tech Spec requirements or follow emergency operating procedures to control the PRHR HX operation.

6.6.1.4.6 Depressurisation Spargers

Two reactor coolant depressurisation spargers (PXS-MW-01A/B) are provided. Each one is connected to an ADS discharge line connected to a set of ADS Stage 1, 2, and 3 valves and is submerged in the IRWST. Each sparger has four branch arms inclined downward. The connection of the sparger branch arms to the sparger hub are submerged below the normal IRWST level by approximately 3 m (10 ft). The spargers are designed to discharge steam and water into the IRWST in small directed jets, thereby promoting more effective steam condensation and IRWST water mixing and avoiding significant dynamic effects that could result in excessive structural loads on the IRWST and thereby the containment. The condensation of steam is not a safety function since the limiting mass / energy release to the containment result from large LOCAs where little if any flow passes through the IRWST spargers.

The first three stages of ADS valves discharge through the spargers and are designed to pass sufficient depressurisation venting flow with an acceptable pressure drop to support the depressurisation system performance requirements. The installation of the spargers prevents undesirable and/or excessive dynamic loads on the IRWST and other structures.

Each sparger is sized to discharge at a flow rate that supports ADS performance, which in turn allows adequate PXS injection from the IRWST and later on from the containment.

6.6.1.4.7 IRWST and Containment Recirculation Screens

The PXS has two different sets of screens that are used following a LOCA: IRWST screens and containment recirculation screens (PXS-MY-Y02A/B, Y03A/B, Y04A/B). These screens prevent debris from entering the reactor and blocking core cooling flow paths during a LOCA. These screens are seismic I Category A Class 1 equipment per Table 15A. A plan and elevation view is provided in Figures 6-20 and 6-21.

These screens are designed to pass the maximum injection flow with up to one half of their area blocked. The containment recirculation screens are located in the east loop compartment along the wall adjacent to the reactor vessel.

The approach to the screens incorporates large settling areas, deep settling pools, low velocities, and a long delay before recirculation initiation to minimize the amount of particles that reach the screens.

A debris weir high is in place in front of the screens to prevent high density debris from being swept along the floor and into the screen face. Additionally there is plate above the screen to prevent debris intrusion from above. The top of the screens is located well below the normal containment recirculation floodup level. This location makes all of their surface area available to screen particles that may be in the recirculation flow.

Each of the two containment recirculation paths is connected to an associated gravity injection line via two parallel flow paths. One path contains a squib valve backed up by a check valve. The other path contains a squib valve backed up by a normally open MOV. The squib valves provide leak-tight isolation of the IRWST and eliminate the normal back-seating differential pressure from the IRWST water column head across the check valves. They also eliminate spillage of water into the containment and potential boric acid buildup during inservice testing of the MOVs. The path with the MOV can also be opened to dump the IRWST water into the containment, which floods the outside of the reactor vessel, in case of a severe accident and complete failure to cool the core. Dumping the IRWST to the loop

compartment cools the molten core while it is located inside the reactor vessel. The PXS Containment Recirculation Screens are also discussed in Chapter 17.

6.6.1.4.8 Valves

Design features used to minimise leakage of valves in the PXS include the following:

- Hermetically-sealed globe valves are used for manual isolation valves that are 50.8 mm (2 inches) or smaller that are high pressure and contain radioactive fluid, except for some valves in the PXS test header whose stems are not normally pressurized.

- Valves that are normally open, except for check valves, and those that perform control function are provided with back seats to limit stem leakage.

Manual valves are generally used as maintenance isolation valves. When used for this function, they are under administrative control. They are located so that no single valve can isolate redundant PXS equipment or are provided with alarms in the MCR to indicate mispositioning.

The motor operators for gate valves are conservatively sized considering the frictional component of the hydraulic unbalance on the valve disc, the disc face friction, and the packing box friction. For motor-operated valves, the valve disc is guided throughout the full disc travel to prevent chattering and to provide easy gate movement. The seating surfaces are hardfaced to prevent galling and to reduce wear.

Remotely operated valves that do not receive a safeguards actuation signal have a position indicator within the MCR. When one of these valves is not in the ready position for injection during plant operation, this condition is indicated and alarmed in the MCR. These valves have various interlocks, automatic features, and position indication. Some valves have their control power locked out during normal plant operation.

The ADS consists of four different stages of valves. Two sets of ADS Stages 1, 2, and 3 are provided. Each set of ADS has three lines and each line has two valves in series, both normally closed. The Stage 4 has four lines with each line having two valves in series, one normally open and one normally closed. The four stages, therefore, include a total of 20 valves. The four ADS valve stages open sequentially.

The Stage 1, Stage 2, and Stage 3 valves have dc motor operators. The Stage 1, 2, and 3 control valves are normally closed globe valves and the isolation valves are normally closed gate valves. The Stage 4 valves are interlocked so that they cannot open until RCS pressure has been substantially reduced. The Stage 4 control valves are squib valves. There is a normally open motor-operated gate valve in series with each squib valve.

Each set of the ADS first three stages have a common inlet header connected to the top of the pressuriser. The outlet of each set of the first to third stages combine to a common discharge line to one of the spargers in the IRWST. A second, identical group of first- to third-stage valves has its own inlet and outlet lines and sparger.

Both sets of the Stage 4 valves connect directly to the top of each reactor coolant hot leg and vent directly to their associated SG compartment.

The ADS valves are designed to automatically open when actuated, and to remain open for the duration of the postulated event. Valve Stages 1 and 4 actuation sequence starts at discrete CMT levels. Valve Stages 2 and 3 actuate based upon a timed delay after actuation of the

preceding first stage. This opening sequence provides a controlled depressurisation of the RCS. The valve actuation logic is based on two-of-four level detectors in either CMT for ADS Stages 1 and 4.

The Stage 1, 2, and 3 automatic depressurisation control valves are designed to open relatively slowly. During the actuation of each stage, the isolation valve is sequenced open before the control valve, so there is some time delay between stage actuation and control valve actuation.

The operators can manually open the Stage 1 valves to a partially open position to perform a controlled degassing or depressurisation of the RCS.

Low Differential Pressure Opening Check Valves

Several applications in the PXS gravity injection piping use check valves that open with low differential pressures. These check valves are installed in the following locations:

- The IRWST gravity injection line flow paths to the reactor vessel direct vessel injection nozzles.

- The containment recirculation lines that connect to the IRWST injection lines.

The check valves selected for these applications incorporate a simple swing-check design with a stainless-steel body and hardened valve seats. The PXS check valves are Class 1, designed with their operating parts contained within the body and with a low-pressure drop across each valve. The valve internals are exposed to low-temperature reactor coolant or borated refuelling water. See section 17.5 for a more detailed description of the accumulator check valves.

Relief Valves

Relief valves are installed for PXS accumulators to protect the tanks from overpressure.

Squib Valves

Squib valves are used in several PXS lines to provide the following:

- Zero leakage during normal operation
- Reliable opening during an accident
- Reduced maintenance and associated personnel radiation exposure

Squib valves are not expected to be opened during normal operation and anticipated transients and it is not necessary that they reclose once they have opened. More details about the squib valves can be found in Chapter 17.

In the IRWST injection lines, the squib valves are in series with normally closed check valves. Inadvertent opening of these injection squib valves is prevented as a design basis event due to the design of the PMS including its diverse blocking device. More details about the blocking device can be found in Chapter 19. In the containment recirculation lines, the squib valves are in series with normally closed check valves in two lines and with normally open motor-operated valves in the other two lines. Inadvertent opening of these recirculation squib valves will not result in loss of reactor coolant or unisolable draining of the IRWST.

The type of squib valve used in these applications provides zero leakage in both directions. It also will allow flow in both directions after it has opened. A valve open-position sensor is provided for these valves.

Squib valves are also used to isolate the Stage 4 ADS lines. These squib valves are in series with normally open motor-operated gate valves. The type of squib valve used in this application provides zero leakage of reactor coolant from the RCS.

6.6.2 Passive Containment Cooling System

The Passive Containment Cooling System (PCS) is a safety-related system which is capable of transferring heat directly from the containment vessel to the environment so that the containment design pressure and temperature are not exceeded following any postulated design basis event, and so that the pressure is significantly reduced in the longer term. The heat transfer mechanism includes conduction, convection, radiation, and mass transfer (water evaporation). Figures 6-5 and 6-15 shows the basic design of PCS.

The Technical Specifications (Reference 6.11) detail the requisite PCS make up water flows and requisite volumes (e.g. Fuel Transfer Canal, Cask Loading Pit, Cask Washdown Pit) depending on the Containment and SFP decay heat balance.

The PCS performs the following Category A Class 1 functions:

- Containment vessel heat removal:
  - The PCS delivers water by gravity flow from the Passive Containment Cooling Water Storage Tank (PCCWST) to the outside, top of the containment vessel.
  - The PCS water flow wets the outside surface of the containment vessel. The process of wetting the containment facilitates the transfer of heat within the containment through the vessel wall.
  - The inside and outside of the containment vessel above the operating deck are coated with an inorganic zinc coating. The coating promotes wetability, heat conduction, inhibits corrosion.
  - The PCS provides counter-current airflow over the outside of the containment vessel driven by a natural circulation in the airflow path from the air inlets to the air discharge structure. The airflow removes the heat transferred from within containment to outside the Shield Building.
  - The PCS drains the excess water from the outside of the containment vessel through the two upper annulus drains.
  - The PCS provides a flow path to containment for long-term (post-72 hour) cooling water makeup.
- Spent fuel pool inventory makeup

- The PCS provides a flow path for long-term water makeup from the PCCWST to the spent fuel pool.

- Process monitoring

  - The PCS monitors the containment conditions that provide indications of the need to initiate various safeguards functions, including actuation of the PCS or the containment air filtration (VFS) Vacuum Relief System.

  - The PCS monitors the process parameters within the PCS required by the operators to monitor status of the system operations and to perform manual operations if necessary during safe-shutdown and accident operations.

Chapter 10 provides details of the Containment vessel functionality during a Serve Accident.

Further design details of this system and its constituent components are delineated in Reference 6.14 and Chapter 17.

6.6.2.1 PCS Functions

6.6.2.1.1 Containment Vessel Heat Removal

The heat removal function is provided following either a safe-shutdown event or a Design Basis Accident (DBA).

The PCS supports limiting the release of fission products by transferring heat from the containment atmosphere to the environment. This is accomplished by providing a volume of water that covers the containment shell to facilitate the transfer of heat to the counter-current airflow and subsequently to the environment. The removal of heat from within containment keeps the internal containment pressure within its design limits thus supporting maintenance of containment integrity. The safety Category A functions associated with heat removal are required to provide the necessary cooling in order to ensure containment integrity by preventing internal over-pressurization, thus maintain containment integrity.

PCS makes use of the steel containment shell as a heat transfer surface. Cooling air is drawn from the environment via an “always open” airflow path over the containment vessel and is returned to the environment after removing heat from the containment shell. The containment shell is wetted by passive draining of the water storage tank that is incorporated into the Shield Building structure above the containment, and is known as the PCCWST (PCS-MT-01).

Actuation of the PCS initiates water flow by gravity from the PCCWST contained in the Shield Building structure above the containment onto the containment dome outer surface, forming a water film over the structure. The water flow is automatically established by the opening of any one of three parallel, safety-related, isolation valves. Two of these isolation valves are AOV (PCS-PL-V001A/B) and the other is a MOV (PCS-PL-V001C). The AOV’s are normally closed and fail open to enhance system reliability and assure system availability. The third flow path containing the MOV is normally closed and fail-as-is. This flow path was added as a result of PSA insights to aid in mitigating common mode failure if both AOV’s were to fail closed. Opening any or all of the isolation valves will result in acceptable system performance. Upstream of each PCCWST isolation valve is a normally open, safety-related, motor-operated isolation block valve (PCS-PL-V002A/B/C) which is available to isolate

cooling water flow in the event of inadvertent actuation. These MOV's receive a confirmatory opening signal from the PMS in response to a High-2 containment pressure condition.

Valve room heating is provided to keep the room temperature above freezing. The thermal inertia of the room keeps the safety-related flow paths and required instrumentation above freezing for at least 72 hours during all design basis conditions.

As the decay heat from the core decreases with time, the water flow to the containment shell is passively decreased in a way which generally matches decay heat. The change in flowrate is attained from the decrease in storage tank level during gravity draining to containment without the need for active components. The change in flow is accomplished through the use of four standpipes installed within the PCCWST, each terminating at a different level. When the system is actuated, water is delivered via all standpipes at the full flow rate. Prior to uncovering the lowest standpipe, the operator is expected to take action to provide makeup water from the passive containment cooling ancillary water storage tank (PCCAWST) (PCS-MT-05) to the PCCWST using a PCS recirculation pump (PCS-MP01A/B), thereby continuing flow to the containment shell.

The water distribution bucket (PCS-MT-03) and water distribution weir system (PCS-MT-04) are provided to counteract the potentially adverse effects of containment vessel construction and manufacturing tolerances on flow distribution and surface wetting. The cooling water flow from the PCCWST is delivered by redundant parallel discharge lines to a water distribution bucket suspended above the centre of the containment dome.

The cooling water not evaporated from the vessel wall during heat transfer from containment flows down to the floor of the upper containment annulus. There are two sets of drains that remove water from the annulus and prevent accumulation.

Situation where PCS cooling may be employed include:

- During a safe shutdown event, the core decay heat is released to IRWST through the PRHR HX, which is contained within the PXS. The heat is subsequently released to the containment atmosphere as the IRWST attains saturation conditions. If containment pressure is increased to above the PCS setpoint, the PMS will automatically actuate PCS to begin containment cooling.

- During a DBA where large amounts of energy are released immediately from the reactor coolant pressure boundary to containment, for example a Main Steam Line Break (MSLB). These types of DBA scenarios require PCS to facilitate the transfer of heat to the outside environment to ensure containment integrity is maintained.

- During a safe shutdown or DBA scenario where energy is slowly released from within the reactor coolant pressure boundary, for example a small leak across the reactor coolant pressure boundary. PXS provides for reactor coolant makeup using the core makeup tanks and removal of decay heat to the IRWST by the PRHR HX. The IRWST eventually attains saturation conditions and begins steaming to containment. PCS is required to facilitate the transfer of heat to the outside environment to ensure containment integrity is maintained.

During a DBA involving the loss of RCS integrity, the PCS, in conjunction with the PXS, provides a continuous source of makeup to the RCS by condensing steam released to

containment, which is directed back to the IRWST to provide passive injection to the RCS

The initial inventory of PCS cooling water in the PCCWST is sufficient for 72 hours of flow without replenishment or operator action. A Class 1 flow path from a blind-flange connection to either the PCCWST or directly to the distribution bucket allows for use of offsite water supplies and provides a post-72 hour source of containment cooling water.

The PCCAWST provides this onsite supply of cooling water and is delivered to containment by the PCS recirculation pumps and flow path.

6.6.2.1.2 Process Monitoring

PCS sensors provide containment pressure signals for normal plant operations and engineered safeguards system actuation of passive containment cooling or containment vacuum relief. Alternatively the Containment Recirculation Cooling System (VCS) monitors containment temperature, which is used for automatically actuating PCS through the Diverse Actuation System (DAS). DAS is not required for design basis events, but provides a backup for multiple failure accident scenarios.

6.6.2.1.3 Spent Fuel Pool Inventory Makeup

The PCS provides a Class 1 flow path from the PCCWST to gravity drain to the spent fuel pool. In addition, a safety-related flow path from a blind-flange connection to the spent fuel pool is required for use with offsite water sources for spent fuel pool makeup.

During refuelling operations when the containment decay heat is less than or equal to 7 MWt the PCCWST is aligned to the spent fuel pool. In the event spent fuel pool cooling is lost, the PCCWST is gravity drained to the spent fuel pool to provide make up to the water inventory within the pool. The cask washdown pit, cask loading pit, and/or the PCCWST can provide the necessary makeup to the pool over time to assure the spent fuel is not uncovered.

The PCCWST provides makeup flowrate for the remainder of the initial 72 hour period after event initiation in order to prevent uncovering of the stored fuel. Following a design basis accident after a normal refueling, the reactor has returned to full power for sufficient time to build up equilibrium fission products, and assuming the worst case decay heat with 15 years of spent fuel storage, makeup is not required during the initial 72 hour period after accident initiation.

6.6.2.1.4 Other Functions

The PCS also performs the following functions:

- Containment vessel heat removal and spent fuel pool inventory makeup post 72 hours to 7 days.

  - The PCCAWST contains an inventory of cooling water sufficient for containment cooling from hour 72 through day 7. This tank is located outside near the Auxiliary Building. PCS Ancillary Pumps can provide the motive force to pump the water from the PCCAWST.

  - The PCS delivers water from the PCCAWST to containment and spent fuel pool simultaneously post 72 hours to 7 days.

- Fire protection water supply

  - The PCCWST and the PCCAWST includes a dedicated water inventory for the Fire Protection System (FPS) by either gravity draining a dedicated volume from the PCCWST or pumping from the PCCAWST.

6.6.3 Main Control Room Habitability System

The VES provides a protected environment from which operators can control the plant following an uncontrolled release of radioactivity. It is designed to operate following a design basis accident or a loss of all ac power condition or event would render the Nuclear Island Non-Radioactive Ventilation System (VBS) inoperable. If ac power is unavailable for more than 10 minutes or if "high-high" particulate or iodine radioactivity is detected in the MCR supply air duct, or low MCR differential pressure with respect to the surrounding rooms for 10 minutes, the PMS automatically isolates the MCR; operator habitability requirements are then met by the VES. The system operates passively (that is, without relying on ac power or active components) other than the one-time alignment of valves.

The MCR VES provides breathable air to the MCR and maintains the MCR at positive pressure for at least 72 hours after an accident, from a compressed air supply. Passive heat exchange to the structures surrounding the MCR together with automatic non Class 1 MCR electrical load de-energization (load de-energization provided by Class 1 IDS) provides adequate cooling of the space for at least 72 hours after a loss of all ac electrical power. Further design details of this system and its constituent components are delineated in Reference 6.16.

6.6.3.1 Ventilation and Filtration

The VES provides emergency ventilation and filtration to the MCR pressure boundary by using a bank of emergency air storage tanks which are connected to a common manifold feeding two air supply lines that route to the MCR. There are a total of 32 tanks in the VES system. The tanks contain breathable quality compressed air which is piped into the control room if the normal HVAC system is deactivated or disabled. There is one main air supply line and one alternate air supply line that connect to one main delivery line. An educator (VES-PY-N01) is attached to the end of the main air delivery line. The eductor induces a recirculation flow rate by using the energy of the compressed breathable air that is discharging from the emergency air storage tanks. The induced flow rate passes through ducting which is contained completely within the MCR pressure boundary. The ducting contains an air filtration unit (VES-MY-F01, F02, F03) that is located downstream from the discharge of the eductor.

The air filtration unit removes potentially contaminated air that could enter the MCR during ingress and egress of the boundary. The compressed air supply provided to the MCR accomplishes three purposes: 1) it provides a source of uncontaminated breathing air to the occupants in the MCR to dilute the CO_2 concentration produced by respiration of the MCR occupants; 2) it provides a constant air flow rate that is required to maintain pressurization of the MCR pressure boundary; and 3) it provides a motive air source to the eductor to passively induce a filtration and recirculation flow rate throughout the MCR pressure boundary.

In the unlikely event that power to the VBS is unavailable for more than 72 hours, then the MCR doors and air ducts may be opened up to allow for ventilation and cooling using VBS MCR Ancillary Supply Fans outside air to the MCR.

6.6.3.2 Pressurization

The VES maintains the MCR at a positive pressure with respect to the surrounding areas to minimize the ingress of airborne contaminants with a supply of compressed air. Inleakage of unfiltered and potentially contaminated air is controlled by maintaining the MCR pressure boundary at a slight positive pressure of at least 31.13 Pa (1/8-inch Water Gauge). Any leakage into and out of the MCR boundary is controlled through the use of low-leakage construction techniques. Over pressurization protection of the MCR boundary is achieved by using redundant low pressure gravity relief dampers.

Normal system makeup is provided by a connection to the breathable-quality high-pressure air compressor in the compressed and instrument air system (CAS).

6.6.3.3 Cooling

The VES limits the heatup of the Class 1 C&I equipment rooms, and the IDS equipment rooms by using the heat capacity of surrounding structures. The VES also limits the heatup of the MCR by the use of VES operation in conjunction with automatic load shedding and the heat capacity of surrounding structures.

The function of providing passive heat sinks for the MCR, C&I rooms, and IDS equipment rooms is part of the VES. The heat sinks for each room are designed to limit the temperature rise inside each room during the 72-hour period following a loss of VBS operation. The heat sinks consist primarily of the thermal mass of the concrete that makes up the ceilings and walls of these rooms.

To enhance the heat-absorbing capability of the ceilings, attached metallic plates are extended into the room and act as thermal fins to enhance the heat transfer from the room air to the concrete.

When a source of ac power is available or radiological concentrations don't trip VBS, the VBS provides normal and abnormal HVAC service to the MCR, remote shutdown workstation, control support area (CSA), C&I rooms, dc equipment rooms, battery rooms, and the nuclear island nonradioactive ventilation system equipment room.

6.6.4 C&I and Electrical Systems Supporting Passive Systems

C&I and electrical systems support the operation of Passive Systems. Table 10-29 of Chapter 10 provides a system dependency matrix that goes into greater detail for systems and the systems they depend on for operation.

6.6.4.1 Protection and Safety Monitoring System

The PMS provides detection of abnormal conditions and actuation of the appropriate Class 1 systems necessary to achieve and maintain the plant in a safe shutdown condition (Reference 6.5).

In addition, the PMS provides the equipment necessary to monitor the plant's Category A safety functions during and following an accident.

Further details about the PMS can be found in Section 6.9. Further design details of control and instrumentation systems are delineated in Chapter 19.

6.6.4.2 Diverse Actuation System

The DAS is a Class 2 system that provides diverse backup to the PMS for actuating a number of Class 1 passive systems. The DAS also provides manual actuation capability for a number of Class 1 passive systems, implemented by hardwiring the controls located in the MCR directly to the final loads in a way that completely bypasses the normal path through the PMS and the DAS automatic logic. DAS processor cabinets are located in the radiologically-controlled portion of the auxiliary building.

Further details about the DAS can be found in Section 6.9. Further design details of control and instrumentation systems are delineated in Chapter 19.

6.6.4.3 Class 1 Essential Electrical Supply System

The IDS, referred to as the essential electrical supply system in this PCSR, consists of four static battery-backed divisions.

IDS provides power for the Class 1 equipment required for the plant instrumentation, control, monitoring, and other vital functions needed for shutdown of the plant. In addition, IDS provides power to the normal and emergency lighting in the MCR and at the remote shutdown workstation.

Further details about the IDS and electrical systems are delineated in section 6.10 and Chapter 18.

6.6.4.4 Standby Electrical Supply System

The standby electrical supply system (EDS) comprises the battery-backed dc electrical power supply system and uninterruptible power supply system. EDS supports the operation of DAS.

Further details about the EDS can be found in Section 6.11. Further design details of electrical systems are delineated in Chapter 18.

6.6.5 Class 2 Systems, Structures, and Components Providing Category A Safety Functions to Preclude Operation of Passive Safety Systems

Some Class systems if available in an accident can be used to preclude the need to operate passive safety systems.

6.6.5.1 Startup Portion of the Feedwater System

The startup portion of the FWS supplies feedwater to the SG during plant startup, hot standby, and shutdown conditions. In the event of a loss of the main feedwater pumps, the startup feedwater pumps are automatically started. One operating startup feedwater pump delivers sufficient flow to the SGs to remove core decay heat and avoid actuation of the Class 1 PXS, and thus provides defence in depth for these transients. On this basis, portions of the FWS are designated as Class 2. Note that the SFW is not formally credited in Chapter 8 with the mitigation of frequent faults. The function of the startup portion of the FWS to remove core decay heat includes components from the AP1000 plant MSS and/or the SGS.

Further details about the FWS can be found in Section 6.5. Further design details of this system and its constituent components are delineated in Reference 6.31 and Chapter 17.

6.6.5.2 Chemical and Volume Control System

The CVS includes two centrifugal makeup pumps that provide makeup flow to the reactor primary circuit. One makeup pump is capable of maintaining normal RCS inventory following an RCS leak of up to a 9.5-mm (3/8-inch) inside diameter without an actuation of the PXS safety injection systems. The CVS thus provides defence in depth for these small LOCAs and, on this basis, the CVS makeup pumps are designated as Class 2. Note that the CVS is not formally credited in Chapter 8 with the mitigation of frequent faults.

The CVS also provides means of controlling boron concentrations in the primary circuit during normal operation and provides backup boration capability to the PXS in fault conditions.

Further details about the CVS can be found in Section 6.4 and Chapter 17; details about normal operation of the CVS can be found in Chapter 21. Additional design details of this system and its constituent components are delineated in Reference 6.18.

6.6.5.3 Normal Residual Heat Removal System

The RNS removes heat from the core and RCS and provides RCS low-temperature, overpressure protection at reduced RCS pressure and temperature conditions after shutdown.

The RNS cooling trains are designated as Class 2 as they provide part of the defence in depth heat removal capability. In intact circuit fault conditions, decay heat removal is provided initially by the FWS and SGs. Later in the fault when the RCS has been partially depressurized this function is provided by the RNS. When the RNS is aligned to the RCS, the RNS performs a Class 1 pressure boundary function.

Further details about the RNS can be found in Section 6.4 and Chapter 17.

6.6.5.4 Component Water Cooling System

The CCS is a closed-loop cooling system that supports the RNS, SFS, and CVS during normal operations and fault conditions. On this basis, portions of the CCS are designated as Class 2. Note that the CCS is not formally credited in Chapter 8 with the mitigation of frequent faults.

Further details about the CCS can be found in Section 6.11 and Chapter 17. Additional design details of this system and its constituent components are delineated in Reference 6.20.

6.6.5.5 Service Water System

The SWS supplies cooling water to remove heat from the CCS HXs in the turbine building. On this basis, portions of the SWS are designated as Class 2. Note that the SWS is not formally credited in Chapter 8 with the mitigation of frequent faults.

Further details about the SWS can be found in Section 6.11 and Chapter 17. Additional design details of this system and its constituent components are delineated in Reference 6.21.

6.6.5.6 Spent Fuel Cooling System

The SFS functions to remove the decay heat generated by stored spent fuel from the spent fuel pool water. On this basis, portions of the SFS are designated as Class 2 as they provide

part of the defence in depth heat removal capability. Note that the SFS is not formally credited in Chapter 8 with the mitigation of frequent faults.

Further details about the SFS can be found in Section 6.12 and Chapter 17. Additional design details of this system and its constituent components are delineated in Reference 6.17.

6.6.5.7 Nuclear Island Nonradioactive Ventilation System

When operating in supplemental air filtration mode, the VBS functions to maintain MCR habitability. On this basis, portions of the VBS are designated as Class 2 since they provide defence in depth protection for the MCR. If available it precludes the need to actuate VES.

Further details about the VBS can be found in Section 6.8 and Chapter 23.

6.7 CONTAINMENT AND SUPPORTING SYSTEMS

6.7.1 Containment

The containment system is the collection of boundaries that separate the containment atmosphere from the outside environment during design basis initiating events.

The containment building is a freestanding, cylindrical, steel vessel with elliptical upper and lower heads. It is surrounded by a seismically qualified reinforced-concrete steel-concrete sandwich shield building (see Figure 6-5 for simplified drawing of the shield building and containment vessel). The containment vessel (CNS-MV-001) provides a safety-functional interface with the ultimate heat sink, which is the surrounding atmosphere. The cylindrical section of the shield building serves as shielding and a missile barrier and is a key component of the PCS. It structurally supports the roof and is a major structural member for the entire nuclear island. Floor slabs and structural walls of the auxiliary building are structurally connected to the cylindrical section of the shield building.

The containment, shield, and auxiliary buildings are structurally integrated on a common basemat embedded below the plant grade level. The shield building is reinforced concrete and, in conjunction with the internal structures of the containment building, provides shielding for the RCS and the other radioactive systems and components housed in the containment. The shield building roof is a reinforced concrete structure containing an integral, steel-lined PCCWST. Further discussion on the containment, shield, and auxiliary buildings is provided in Chapter 16.

The HVAC systems VCS and VFS which also support containment are described in section 6.8.

6.7.2 Containment Isolation

Containment isolation is provided by containment penetrations, redundant means of isolating flowpaths through the containment shell, and the connections for verifying containment isolation leak tightness. The AP1000 plant containment system (CNS) provides the requirements the containment isolation. The SSCs that provide the isolation (penetrations, pipe, isolation valves) are part of the systems whose lines pass through the containment vessel. This includes such systems as the CAS, CVS, FPS, RNS, etc. (see Chapter 17 for the requirements of valves and components that isolate containment). Further design details of this system and its constituent components are delineated in Reference 6.15.

The CNS allows the normal or emergency operation of the plant while preserving the integrity of the containment boundary, when required. Wherever possible, the containment isolation valves are fail-closed AOVs that automatically shut when their air supply is lost or when their electrical signal is removed.

The AP1000 design has fewer mechanical containment penetrations (including hatches) than current plants. Pipe work crossing the containment boundary needs to be isolated in the event of an accident to limit the escape of fission products that may result from postulated accidents.

The function of the containment isolation valves is to allow the normal or emergency passage of fluids through the containment boundary while preserving the integrity of the containment boundary following an accident.

Each line that crosses the containment boundary is provided with containment means of isolation. The barrier inside containment is usually provided by one isolation valve, and the barrier outside containment consists of pipe work and an isolation valve. Both barriers are qualified to an appropriate level

During normal system operation, most of the piping penetrations are not isolated. The majority of these incorporate fail-closed isolation valves that close automatically with the loss of support systems, such as instrument air. Power-operated (air, motor, or pneumatic) containment isolation valves have position indication in the MCR.

Lines not in use during power operation are normally closed and remain closed under administrative control during reactor operation.

Containment isolation is achieved by closing all the isolation valves on receipt of an actuation signal from the PMS or DAS. Electrical power is provided by IDS where required.

If a change in valve position is required at any time following primary actuation, a secondary actuation signal is generated, which places the valve in an alternate position.

The containment air filtration system (VFS) is used to purge the containment atmosphere of airborne radioactivity during normal plant operation. These valves close automatically on a containment isolation signal. Chapter 17 provides further detail on the containment isolation valves by fluid system. Chapter 19 provides further detail on the PMS and DAS Control and Instrumentation systems.

6.7.3 Containment Hydrogen Control System

Hydrogen is postulated to be released following accident sequences in which the reactor overheats to the extent that the zirconium fuel cladding chemically reacts with the steam that is present. Any breach in the RCS boundary would provide a route for this hydrogen to escape into the containment atmosphere. When mixed with the air in the containment, the hydrogen may ignite and create a dynamic pressure or elevated temperature that could potentially damage containment structures and potentially create a pathway to the environment for any radioactivity released into the containment during the accident. Further design details of this system and its constituent components are delineated in Reference 6.34.

This scenario is prevented by gradually removing any hydrogen introduced into the containment by chemically combining it with the oxygen in the air in a controlled manner using the VLS. The VLS consists of three elements:

- Two passive autocatalytic recombiners (VLS-MY-E01A/B) installed above the operating deck that combine any hydrogen as it arises.

- 66 electrically powered hydrogen igniters (VLS-EH-01 through -66) distributed throughout the containment to ignite any hydrogen at their respective locations before the concentration of hydrogen can build to levels where large pressures may be generated.

- Three hydrogen sensors in the upper dome to monitor the bulk hydrogen concentration and alert the operators to the need for remedial action.

The structures within the containment are arranged to promote mixing by means of natural circulation. For a postulated break low in the containment, buoyant flows develop through the lower compartments because of density differences between the rising plume and the surrounding containment atmosphere, tending to drive mixing through the lower compartments and into the region above the operating deck. There is also a degree of mixing within the region above the operating deck, which occurs as the steam-rich leakage plume rises from the operating deck openings.

The following four general characteristics have been incorporated into the AP1000 design to promote mixing and eliminate dead-end compartments, thereby reducing the likelihood of hydrogen concentration reaching levels at which large pressures may be generated:

- The compartments below the operating deck are large, open volumes with relatively large interconnections, which promote mixing throughout the below deck region.

- All compartments below the operating deck are provided with openings through the top to eliminate the potential for a dead pocket of high hydrogen concentration.

- The operation of the PCS condenses steam and cools the non-condensable gases adjacent to the containment shell, promoting natural circulation flow in the containment.

- In addition, if forced containment air circulation is operated during post-accident recovery, the fan coolers contribute to circulation in containment.

The autocatalytic recombiners are effective for very low hydrogen concentrations (less than 1 percent) at ambient temperature, and they are not impaired by being wet or by the presence of very high steam concentrations. They begin to recombine hydrogen and oxygen almost immediately upon exposure to oxygen and hydrogen when the catalyst is not wetted. If the catalyst material is wet, then a short delay is experienced. The autocatalytic recombiners are effective over a wide range of ambient temperatures, concentrations of reactants (rich and lean oxygen/hydrogen less than 1 percent), and steam inerting (steam concentrations greater than 50 percent).

The autocatalytic recombiners are sized to accommodate the hydrogen production rate anticipated for the limited amounts of damage to the fuel and its cladding hypothetically arising from a LOCA with multiple failures in mitigation features; they have been shown to be effective at minimising the buildup of hydrogen inside the containment following LOCAs.

The hydrogen igniters can burn hydrogen at higher concentrations and prevent the concentrations from exceeding 10 percent by volume even with rapid generation of hydrogen. The hydrogen igniters are designed to accommodate the relatively fast release of hydrogen resulting from severe accident sequences.

The hydrogen ignition subsystem consists of 66 hydrogen igniters strategically distributed throughout the containment based on evaluation of hydrogen transport in the containment and hydrogen combustion characteristics. When an igniter is energised, its surface heats up to ≥926.6°C (1700°F), which is sufficient to ignite hydrogen in its vicinity once the concentration exceeds the lower flammability limit. The primary objective of installing an igniter system is to promote hydrogen-burning at a low concentration and, to the extent possible, to burn it more or less continuously so that the hydrogen concentration does not build up to high levels in the containment. To achieve this goal, the igniters are placed in the major regions of the containment where hydrogen might be released, through which it could flow or where it might accumulate. The igniter coverage, distribution, and power supply has been designed to minimise the potential loss of igniter protection globally for containment and locally for individual compartments.

A spray shield is provided to protect each igniter from falling water drops resulting from the condensation of steam on the containment shell and on nearby equipment and structures. The hydrogen sensors are designed to provide a rapid-response detection of changes in the bulk containment hydrogen concentration. The igniters are electrically powered and manually actuated. To this end, bulk containment hydrogen concentration is monitored and continuously indicated in the MCR. In addition, high hydrogen concentration alarms are provided. The sensors are powered by the EDS uninterruptible power supply system and have sufficient range to monitor concentrations up to 20 percent.

6.7.4 Containment Leak Rate Test System

The reactor containment, containment penetrations, and isolation barriers are designed to permit periodic leak rate testing. Additional design details of this system and its constituent components are delineated in Reference 6.35. The three following types of test are performed:

- Containment integrated leak rate testing (Type A) − The containment is pressurised with clean, dry air and the leak rate from the containment structure is established. Type A testing uses temporary equipment connected through the VFS exhaust penetration (C02).

- Local leak rate testing of containment penetrations with a design that incorporates features such as resilient seals, gaskets, and expansion bellows (Type B) − The leakage limiting boundary is pressurised with air or nitrogen and the pressure decay or the leak flow rate is measured. Type B testing uses permanently installed connections.

- Local leak rate testing of containment isolation valves (Type C) − The piping test volume is pressurised with air or nitrogen and pressure decay or the leak flow rate is measured. Type C testing uses features built into the tested subsystems.

6.8 HEATING, VENTILATION AND AIR CONDITIONING SYSTEMS

Nuclear containment and ventilation systems serve an important nuclear safety function in terms of supporting containment of nuclear material by ensuring that air movements and

discharges are adequately directed and filtered to reduce doses to operators and the public under both normal and accident conditions. Chapter 23 provides further discussion on the following systems.

6.8.1 Containment Recirculation Cooling System

The VCS recirculates and cools air within the containment during power operations and shutdown. This results in an energy savings and a reduction in waste generated in the form of used filters when compared to what would result from the level of a once through HVAC ventilation system. The air recirculated by this system is expected to contain some activity (mostly noble gases and some iodine), although it does not penetrate the containment boundary and thus does not give rise to any discharges to atmosphere. Therefore, Best Available Technology (BAT) for reducing discharges is not applicable to this system.

During shutdown operations in the containment, local, filtered extract systems are available for particular operations where airborne activity may be generated. This reduces the potential for airborne activity to be released into the general containment atmosphere, which the recirculation system could spread to other parts of the containment building.

The extracted air is continuously monitored for airborne activity to give an early warning of the presence of airborne activity to workers in the containment.

There is no path to discharge the VCS to the environment and so high-efficiency particulate air (HEPA) filtration is not provided.

The VCS controls containment air temperature and humidity to provide a suitable environment for equipment operability during normal operation and shutdown.

The VCS is comprised of four 50-percent-capacity fan coil units that connect to a common duct ring header and distribution system. Each fan coil unit contains a fan and associated cooling coil banks. The fan coil units are located on platforms approximately 180 degrees apart to provide a proper return air and mixing pattern through the ring header. The ring header and the fan assemblies are designed to provide uniform air and temperature distribution inside the containment. (One fan coil unit on each side of containment is normally in operation. The systems are not designed to have two fans at one side of containment operating simultaneously.) More details on VCS are provided in Section 23.4 and Reference 23.3.

6.8.2 Containment Air Filtration System

The VFS purges the containment by providing fresh air from outside and exhausting containment air into the plant vent. The air exhausted by the VFS is filtered with high-efficiency filters, charcoal filters, and postfilters. The VFS also exhausts from areas served by the VAS and health physics and hot machine shop HVAC system (VHS). The VFS is supported by diesel backup to improve its reliability.

The VFS comprises two parallel systems that may be operated individually or simultaneously as required by the operating regime with or without associated inlet air handling units. Each one is equipped with high-efficiency particulate air (HEPA) filtration and charcoal filters for removal of particulate and iodine vapour respectively. A high-efficiency filter (80 percent American Society of Heating, Refrigerating, and Air Conditioning Engineers (ASHRAE)) is installed before the HEPA filter to increase operational life and reduce the quantity of low level waste (LLW). A high-efficiency filter has a greater capacity, therefore requiring less frequent changing and potentially reducing the volumes of LLW produced.

A high-efficiency filter is also installed after the charcoal filter to ensure that discharges are as low as reasonably practicable (ALARP). Continuous monitoring of airborne discharges is provided to detect deterioration in the performance of either ventilation train. These provisions represent good industry practice for ensuring that discharges to the atmosphere and doses to members of the public are ALARP. Continuous monitoring of airborne discharges is provided to detect deterioration in the performance of either ventilation train.

The containment air filtration system consists of two 100 percent-capacity supply air handling units, a ducted supply, and an exhaust air system with containment isolation valves and piping, registers, exhaust fans, filtration units, automatic controls, and accessories. The supply air handling units are located in the south air handling equipment room of the annex building. The supply air handling units are connected to a common air intake plenum.

A gaseous radiation monitor is located downstream of the exhaust air filtration units in the common ductwork to provide an alarm if abnormal gaseous releases are detected. The plant vent exhaust flow is monitored for gaseous, particulate, and iodine releases to the environment.

During conditions of abnormal airborne radioactivity in the fuel handling area and auxiliary and/or annex buildings, the filtration units provide filtered exhaust to minimise unfiltered offsite releases.

The exhaust air containment penetrations also serve as a connection for the containment integrated leak rate test system to pressurise and depressurise the containment during integrated leak rate testing. Otherwise, the containment air filtration exhaust subsystem is not involved with the containment integrated leak rate test and is isolated from the containment during this time.

More details on VFS and its components are provided in Chapter 23 and Reference 23.5.

6.8.3 Radiologically Controlled Area Ventilation System

The VAS serves the radiologically controlled areas of the auxiliary and annex buildings. The VAS consists of two separate subsystems, the fuel handling area ventilation subsystem and the auxiliary/annex building ventilation subsystem. Both subsystems are once–through-type ventilation systems. More details on VAS and its components are provided in Chapter 23 and Reference 23.30.

During normal operations, the supply air handling units and both the exhaust fans on each of the ventilation subsystems operate continuously to ventilate the areas served on a once through basis. The supply airflow rate is modulated to maintain the areas served at a slightly negative pressure differential with respect to the outside environment.

If abnormal airborne radioactivity is detected in the duct, VFS provides filtered exhaust to mitigate unfiltered releases to the environment by maintaining the isolated zone at a slightly negative pressure differential.

The VAS serves the fuel handling area of the auxiliary building and the radiologically controlled portions of the auxiliary and annex buildings except for the VHS areas.

The VAS consists of the auxiliary/annex building ventilation subsystem and the fuel handling area ventilation subsystems.

6.8.3.1 Fuel Handling Area Ventilation Subsystem

The fuel handling area ventilation subsystem supply and exhaust ductwork is arranged to exhaust the SFP area separately from the auxiliary building. It provides directional airflow from the rail car bay/filter storage area into the spent resin equipment rooms. The exhaust fans discharge normally unfiltered exhaust air into the plant vent system for monitoring of offsite airborne gaseous and other radiological releases.

All spent fuel handling operations are performed under borated water to provide radiation protection; activity levels in the SFP are controlled by Tech Specs. In normal operation the effluent from the fuel handling area passes through HEPA filtration. Routine releases and accidental release for the fuel handling area are both low, however, if the radiation monitors detect a high level of radiation, the fuel handling extract is diverted to the VFS, which contains HEPA and charcoal filters. It can also be diverted manually if particular operations being performed could result in a release of activity.

HEPA filtration is also provided for the spent fuel pool relief panel. In the unlikely case of spent fuel pool boiling, the HEPA filters ducted to the relief panel will remove particulates from the discharged air-steam mixture. This is discussed further in Appendix 23A.

The fuel handling area ventilation subsystem serves the fuel handling area, rail car bay/filter storage area, resin transfer pump/valve room, spent resin tank room, waste disposal container area, solid waste management system (WSS) valve/piping area, and elevator machine room. The fuel handling area ventilation subsystem consists of two 50-percent-capacity supply air handling units, a ducted supply and exhaust air system, isolation dampers, diffusers, registers, exhaust fans, automatic controls, and accessories. Hot water heating coils supplied with water from the hot water heating system (VYS) and cooling coils supplied with water from the central chilled water system (VWS) are used to maintain ambient room temperatures within the normal range. The ventilation airflow capacity is designed to maintain environmental conditions that support worker efficiency during fuel handling operations. The supply air handling units are located in the air handling equipment room of the annex building. They are connected to the air intake plenum number two, located on the annex building. The units discharge into a ducted supply distribution system routed to the fuel handling and rail car bay/filter storage areas of the auxiliary building.

The supply and exhaust ducts are provided with isolation dampers that close upon detection of high airborne radioactivity in the exhaust air or high pressure differential with respect to the outside atmosphere.

The supply and exhaust ductwork is arranged to exhaust the SFP plume and to provide directional airflow from the rail car bay/filter storage area into the spent resin equipment rooms.

6.8.3.2 Auxiliary/Annex Building Ventilation Subsystem

The auxiliary/annex building ventilation subsystem serves radiologically controlled equipment, piping and valve rooms, and adjacent access and staging areas.

The radiologically controlled part of the auxiliary and annex building air ductwork is routed to minimise the spread of airborne contamination by directing the supply airflow from the low-radiation access areas into the radioactive equipment and piping rooms with a greater potential for airborne radioactivity. In addition, the exhaust air ductwork is connected to the radwaste effluent holdup tanks to prevent the potential buildup of gaseous radioactivity or

hydrogen gas within these tanks. The exhaust fans discharge the exhaust air into the plant vent system for monitoring of offsite airborne radiological releases.

The supply and exhaust ducts are configured so that two building zones may be independently isolated. The annex building staging and storage area, containment air filtration exhaust rooms, containment access corridor and adjacent auxiliary building staging, equipment areas, middle annulus, middle annulus access room, and security rooms are aligned to one zone. The other zone includes the remaining rooms and corridors, including but not limited to the radiation chemistry laboratory, primary sample room, SFP cooling water pump and HX rooms, normal residual heat removal pump and HX rooms, CVS makeup pump room, lower annulus, various radwaste equipment rooms, pipe chases, and access corridors. A radiation monitor is located in the exhaust air duct from each zone.

The auxiliary/annex building ventilation subsystem consists of two 50-percent-capacity supply air handling units, with a ducted supply and exhaust air system, isolation dampers, diffusers and registers, exhaust fans, automatic controls, and accessories. The supply air handling units are located in the air handling equipment room of the annex building. They are connected to the air intake plenum located in the extreme south end of the annex building. The units discharge into a ducted supply distribution system routed through the radiologically controlled areas of the auxiliary and annex buildings. The supply and exhaust ducts have isolation dampers that close to isolate the auxiliary and annex buildings from the outside environment when high airborne radioactivity is detected in the exhaust air duct.

The two 50-percent-capacity exhaust air fans, sized to allow the system to maintain a negative pressure, are located in the upper VAS equipment room of the auxiliary building. The exhaust air ductwork is connected to the radioactive waste drain system (WRS) sump to maintain the sump atmosphere at a negative air pressure; this prevents the exfiltration of potentially contaminated air into the surrounding area. The sump vent line is constructed of pipe work, routed upward from the sump to the interface with the HVAC system. The exhaust air ductwork is connected to the radwaste effluent holdup tanks to prevent the potential buildup of airborne radioactivity or hydrogen gas within these tanks. The vent line is constructed of pipe and is routed upward from the tank to the interface with the HVAC system. The exhaust fans discharge the exhaust air into the plant vent system for monitoring of offsite airborne radiological releases.

Unit coolers are located in the RNS and CVS pump rooms because they have significant cooling loads on an intermittent basis when large equipment is operating. Each unit cooler is sized to accommodate 100 percent of its corresponding pump cooling load. The unit coolers are provided with chilled water from redundant trains of the VWS low-capacity subsystem.

The RNS pump room unit coolers have two cooling coils per unit cooler so that chilled water supplied by either train A or train B alone can support concurrent operation of both RNS pumps. The two CVS makeup pump room unit coolers are connected to redundant trains of the chilled water system. However, operating either the train A or train B unit cooler alone maintains the common makeup pump room temperature conditions and supports operation of either makeup pump. Condensation from these cooling coils drains to the WRS.

Heating coils are located in the supply air ducts serving plant areas that require supplemental heating during periods of cold outside air temperature conditions. The heating coils are supplied with hot water from the VYS. The radiation chemistry laboratory and security room supply air ducts are provided with local electric coils and humidifiers to maintain the environmental conditions within the areas suitable for personnel comfort.

6.8.3.3 Security Room Ventilation Subsystem

The security room subsystem consists of two (2) 50% local fan coil cooling units which provide cooling via the recirculation of air. These components are provided to maintain the environmental conditions within the areas suitable for personnel comfort and special electronic equipment. Each fan coil unit includes a low efficiency-filter, chilled water cooling coil, fan and associated instrumentation and controls. The VWS is connected to the fan coil unit cooling coils.

6.8.4 Nuclear Island Nonradioactive Ventilation System

The nuclear island nonradioactive ventilation system (VBS) serves the MCR, CSA, essential power electrical spaces, the PCS valve room, RSR, and HVAC equipment rooms. The VBS is designed to perform its design functions during normal plant operations, shutdown and during and following a DBA, if VBS is operable and the supporting systems are available. See Chapter 23 and Reference 23.33 for more details pertaining to VBS.

VBS provides the following Class 1 functions;

- Provide isolation of the MCR envelope from the surrounding areas and outside environment during and following a design basis accident.
- Provide radiological monitoring of MCR supply air airborne process streams and initiation signals to the PMS for actuation of the VES.

VBS provides the following Class 2 and 3 functions;

- Provide protection of MCR and/or CSA areas from infiltration of smoke from an external source.
- Provide smoke removal capability for the MCR envelope, CSA area and Class 1E electrical equipment rooms from an internal source.
- Exhaust room air from the Class 1E battery rooms and limit the concentration of hydrogen gas to prevent a potential explosive mixture.
- Provide protection from tornado depressurization and provide security barriers.

These areas do not have sources of radioactive contamination present during normal operation or fault conditions. During a fault condition, activity could be present in the radioactive drain system that passes through (but does not serve) this area. Since the drain system has no valves or connections and operates at low pressure, the chance of leakage into this area is negligible as there would need to be a pre-existing leak coincident with a fault. Because it is not reasonably foreseeable that activity will be present in the areas served by the VBS, the exhaust systems from the VBS do not have any provisions for HEPA filtration.

The system consists of the following independent subsystems:

- MCR/control support area HVAC subsystem
- Essential power electrical room HVAC subsystem
- PCS valve room heating and ventilation subsystem

6.8.4.1 Main Control Room/Control Support Area HVAC Subsystem

MCR/control support area HVAC subsystem serves the MCR and control support area with two 100-percent-capacity supply air handling units, return/exhaust air fans, supplemental air filtration units, associated dampers, control and instrumentation, and common ductwork. The supply air handling units and return/exhaust air fans are connected to common ductwork that distributes air to the MCR and CSA areas. The MCR envelope consists of the MCR, shift manager's office, operation work area, toilet, and operations break room area. The CSA area consists of the main control support area, operations area, conference rooms, computer rooms, shift turnover room, kitchen/rest area, and restrooms. The MCR and control support area toilets have separate exhaust fans.

Outside supply air is provided to the plant areas served by the MCR/control support area HVAC subsystem through an outside air intake duct protected by an intake enclosure located on the roof of the auxiliary building. The supply, return, and toilet exhaust are the only HVAC penetrations in the MCR envelope.

Redundant radiation monitor sample line connections are located upstream of the VBS supply air isolation valves. These monitors initiate operation of the supplemental air filtration units on high gaseous radioactivity concentrations and isolate the MCR from the VBS on high-high particulate or iodine radioactivity concentrations.

The MCR/control support area HVAC subsystem is designed so that smoke, hot gases and fire suppressant will not migrate from one fire area to another and so affect safe shutdown capabilities, including operator actions. Fire or combination fire-and-smoke dampers are provided to isolate each fire area from adjacent fire areas during and following a fire. These combination fire-and-smoke dampers close in response to smoke detector signals or to the heat from a fire.

6.8.4.2 Class 1 (Essential Supply) Electrical Room HVAC Subsystem

The essential supply electrical room HVAC subsystem serves the essential supply electrical rooms, C&I rooms, electrical penetration rooms, battery rooms, spare Class 1 battery room, remote shutdown room, and reactor coolant pump trip switchgear rooms. The A and C electrical divisions, spare battery room, and reactor coolant pump trip switchgear rooms are served by one ventilation subsystem; the B and D electrical divisions and remote shutdown room are served by a second ventilation subsystem. Each subsystem consists of two 100-percent-capacity supply air handling units, return/exhaust air fans, associated dampers, C&I, and common ductwork. The supply air handling units and return/exhaust air fans are connected to a common ductwork that distributes air to the essential supply electrical rooms. The outside supply air intake enclosure for the A and C subsystem is common to the MCR/control support area intake located on the roof of the auxiliary building. The outside supply air intake for the B and D subsystem is located separately from the MCR/control support area air intake enclosure on the auxiliary building roof.

The exhaust ducts from the battery rooms are connected to the turbine building vent to remove hydrogen gas generated by the batteries.

The supply air handling unit cooling coils are provided with chilled water from the air-cooled chillers in the central chilled water system (VWS). The two air handling units for each set of electrical divisions are provided with chilled water from redundant air-cooled chillers.

Each subsystem for the Class 1 battery rooms is provided with two 100-percent-capacity exhaust fans.

The subsystem is designed so that smoke, hot gases, and fire suppressant do not migrate from one fire area to another so that they could adversely affect safe shutdown capabilities, including operator actions. Separate ventilation subsystems are provided to serve the electrical division A and C equipment rooms and the electrical division B and D equipment rooms. The use of separate HVAC distribution subsystems for the redundant trains of electrical equipment prevents smoke and hot gases from migrating from one distribution division to the other through the ventilation system ducts.

These combination fire-and-smoke dampers close in response to smoke detector signals or to the heat from a fire. During a fire, the pressure difference across the doors in the stairwells is maintained by dedicated stairwell pressurisation fans.

6.8.4.3 Passive Containment Cooling System Valve Room Heating and Ventilation Subsystem

The PCS valve room heating and ventilation subsystem serves the thermally insulated PCS valve room. The subsystem consists of one 100-percent-capacity ventilating fan, two 100-percent-capacity electric unit heaters, associated dampers, controls, and instrumentation. The PCS valve room heating and ventilation subsystem equipment is located in the PCS valve room in the containment dome area.

The exhaust fan draws outside air through an intake louver damper and exhausts it directly to the environment.

6.8.5 Annex/Auxiliary Buildings Nonradioactive Heating, Ventilation, and Air Conditioning Systems

The annex/auxiliary buildings' nonradioactive HVAC systems (VXS) serve the office areas, switchgear rooms, locker rooms, battery rooms, computer rooms, toilets, non-class 1 electrical equipment room (location of PLS cabinets), and other similar spaces. These areas do not typically have sources of radioactive contamination present during normal operation. A drain line from the BDS to the WLS passes through the areas served by the VXS. The drain line can be contaminated by the BDS system if there are fuel leaks and SG leakage, combined with a radiation monitor failure or an isolation valve failure. Since the drain system has no valves or connections within the area served by the VXS and it is gravity-drained, the chance of leakage into the VXS area is negligible because there would need to be a pre-existing leak coincident with a fault. Because the presence of activity in the areas served by the VXS is not reasonably foreseeable, the exhaust systems from the VXS have no provisions for HEPA filtration. See Chapter 23 and Reference 23.40 for more details pertaining to VXS.

The VXS serves the nonradioactive personnel and equipment areas, electrical equipment rooms, clean corridors, the ancillary diesel generator room and demineralised water deoxygenating room in the annex building, and the MSIV compartments, reactor trip switchgear rooms, and piping and electrical penetration areas in the auxiliary building.

The VXS consist of the following independent subsystems:

- General area HVAC subsystem
- Switchgear room HVAC subsystem
- Equipment room HVAC subsystem
- MSIV compartment HVAC subsystem
- Mechanical equipment areas HVAC subsystem
- Valve/piping penetration room HVAC
- Annex building offices

6.8.5.1 General Area HVAC Subsystem

The general area HVAC subsystem serves personnel areas in the annex building outside the security area. These areas include the men's and women's change rooms, the briefing room, operational support centre, offices, corridors, men's and women's toilet facilities, conference rooms, and office areas. The general area HVAC subsystem consists of two 50-percent-capacity supply air handling units and humidifiers, a ducted supply and return air system, diffusers and registers, exhaust fan, automatic controls, and accessories. The air handling units are located on the low roof of the annex building. The units discharge into ducted supply distribution systems that are routed through the building to provide air into the various rooms and areas served via registers. Electric heating coils are provided in the branch supply duct to the men's and women's change rooms and rest rooms for tempering the supply air. A humidifier is provided in the system to provide a minimum-space relative humidity of 35 percent.

6.8.5.2 Switchgear Room HVAC Subsystem

The switchgear room HVAC subsystem serves electrical switchgear rooms one and two in the annex building. The switchgear room HVAC system consists of two 100-percent-capacity air handling units, a ducted supply and return air system, and automatic controls and accessories.

The air handling units are located in the air handling equipment room in the annex building. They are connected to a common intake plenum adjacent to their air handling equipment room. This plenum also supplies air for the equipment room HVAC subsystem. The air handling units discharge into a common duct distribution system routed through the building to the rooms served. Air is returned to the air handling units from the rooms served by a return duct system.

The switchgear room HVAC subsystem is designed so that smoke can be removed after a fire by placing the system in a once-through smoke exhaust ventilation mode.

6.8.5.3 Equipment Room HVAC Subsystem

The equipment room HVAC subsystem serves electrical and mechanical equipment rooms in the annex and auxiliary buildings. These rooms include the standby power battery charger rooms one and two, the standby power battery rooms one and two, the reactor trip switchgear rooms one and two, and the standby power penetration room. This subsystem also serves the rooms and areas in the annex building, which include two rest rooms, access areas, and corridors. The equipment room HVAC system consists of two 100-percent-capacity air handling units, two battery room exhaust fans, a toilet exhaust fan, a ducted supply and return air system, and automatic controls and accessories.

The air handling units are located in the air handling equipment room in the annex building. They are connected to a common intake plenum adjacent to their air handling equipment room. This plenum also supplies air for the switchgear room HVAC subsystem. The air handling units discharge into a common duct distribution system routed through the buildings to the various areas served. Air is returned to the air handling units from the rooms served (except the battery rooms and rest rooms) by a return duct system. Electric reheat coils are provided in the ductwork to areas requiring close temperature control such as the security rooms and restrooms. Hot water unit heaters are provided in the north air handling equipment room to keep the area above 10°C (50°F).

A humidifier is provided in the branch duct to the security areas to provide a minimum space relative humidity of 35 percent.

Each standby power battery room is provided with an individual exhaust system to prevent the buildup of hydrogen gas in the room. Each exhaust system consists of an exhaust fan, an exhaust air duct, and a gravity backdraft damper located in the fan discharge. Air supplied to the battery rooms by the air handling units is exhausted to atmosphere. Air from the rest rooms is exhausted to atmosphere by a separate exhaust fan.

The portion of the equipment room HVAC subsystem servicing the auxiliary building is designed so that smoke, hot gases, and fire suppressant will not migrate from one fire area to another to the extent that they could adversely affect safe shutdown capabilities, including operator actions. Fire or combination fire-and-smoke dampers are provided to isolate each fire area from adjacent fire areas during and following a fire.

These combination fire-and-smoke dampers close in response to smoke detector signals or in response to the heat from a fire.

6.8.5.4 MSIV Compartment HVAC Subsystem

The MSIV compartment HVAC subsystem serves the two MSIV compartments in the auxiliary building that contain the main steam and feedwater lines routed between the MSIV containment and the turbine building. Each compartment is provided with separate heating and cooling equipment.

The MSIV compartment HVAC subsystem consists of two 100-percent-capacity supply air handling units per compartment with only low-efficiency filters, ducted supply air distribution directly to the space served, automatic controls, and accessories for each MSIV compartment.

The supply air handling units are located directly within the space served. One unit in each compartment normally operates to maintain the temperature of that compartment. The air handling units can be connected to the standby power system, for investment protection, in the event of loss of the plant ac electrical system.

6.8.5.5 Mechanical Equipment Areas HVAC Subsystem

The mechanical equipment areas HVAC subsystem serves the ancillary diesel generator room, demineralised water deoxygenating room, boric acid batching room, upper south air handling equipment room, and lower south air handling equipment room in the annex building.

The mechanical equipment areas HVAC subsystem consists of two 50-percent-capacity air handling units with supply fans and return/exhaust fans, a ducted supply and return air system, automatic controls, and accessories.

The air handling units are located in the air handling unit equipment room of the annex building. They are supplied from the air intake plenum number two located at the extreme end of the annex building. This plenum also supplies air for the VAS, the VHS, and the VFS.

Air from the air handling units is supplied to the ancillary diesel generator room to maintain normal design temperatures. Air supplied to the room is exhausted directly outdoors by means of a separate exhaust fan.

When the ancillary diesel generators operate, ventilation and cooling for the room are provided by manually operated dampers and opening doors to allow radiator discharge air to be exhausted directly outdoors.

6.8.5.6 Valve/Piping Penetration Room HVAC Subsystem

The valve/piping penetration room HVAC subsystem serves the valve/piping penetration room of the auxiliary building. The valve/piping penetration room HVAC subsystem consists of two 100-percent-capacity air handling units, a return air duct system, automatic controls, and accessories.

The air handling units are located directly within the space served.

6.8.6 Health Physics and Hot Machine Shop HVAC System

The VHS supply air system consists of two 100-percent-capacity air handling units, consisting of a low-efficiency filter bank and a high-efficiency filter bank, heating and cooling coils, and a supply fan with automatic inlet valves. The exhaust air system consists of two 100-percent-capacity exhaust fans sized to allow the system to maintain negative pressure. See Chapter 23 and Reference 23.45 for more details pertaining to VHS.

During normal operations, one supply air handling unit and one exhaust fan operate continuously to control air pressures in the health physics and hot machine shop areas of the annex building. The other standby supply and exhaust fans are started if the primary fans fail.

The supply airflow is automatically modulated to maintain a negative pressure in the areas served with respect to the outdoors and to surrounding areas that do not have their exhausts monitored for radioactivity. Differential pressure controllers with sensors in the general health physics area and sensors mounted outdoors modulate the automatic inlet vanes of the supply fan to maintain negative pressure. In addition, a separate differential pressure controller with a sensor in the hot machine shop modulates a damper in the supply air duct to the hot machine shop to maintain a negative pressure in the shop with respect to the outdoors and surrounding areas that do not have their exhausts monitored.

The hot machine shop provides a location within the controlled area for repair and refurbishment of equipment items from within the controlled area, i.e., they may not actually be contaminated or activated but it is easier to have a dedicated workshop rather than to undertake clearance monitoring, which may not be possible. Operations in the hot machine shop are conventional hands-on work, i.e., there is no provision for remote handling. The routine arising of airborne contamination from machining operations is not expected because equipment that can be repaired will be decontaminated beforehand. Equipment that is too active to handle manually and cannot be decontaminated will be packaged and disposed of as radioactive waste.

Airborne contamination from the remaining space extract from the hot machine shop and other areas served by this system is not expected to be significant during either normal or fault conditions.

The facility has a dedicated decontamination facility with HEPA filtration and a glove box that also has HEPA filtration. The HEPA filters on the decontamination chamber and glove box are typically ported so that a dispersed oil penetration (DOP) test can be performed.

Individual machine tools have local exhaust ventilation arrangements and HEPA filtration will be provided. The capability to perform DOP testing on the installed filters is a feature that would be included in the design as part of the local extract ventilation systems.

Filtered provision for specific areas of the hot machine shop are as follows:

- Glove boxes are red areas, and so HEPA filtration is provided.
- Individual machine tools are amber areas with significant potential for low level of activity release, so HEPA filtration is provided.
- Airborne contamination from the remaining space of the hot machine shop and other areas served by this system is not expected to be significant during either normal or fault conditions. Therefore, the remaining space is a green area with low risk, so no constant HEPA filtration is provided but the extract will be directed to the VFS if necessary. See Chapter 23 for more details pertaining to VHS.

6.8.7 Radwaste Building HVAC System

The radwaste building HVAC system (VRS) supplies and exhausts air from the radwaste building. The discharges from this ventilation system are continuously monitored for airborne activity by the VRS exhaust radiation monitor. In addition, the plant vent combined discharge is monitored and alarmed. See Chapter 23 and Reference 23.31 for more details pertaining to VRS.

The radwaste building has three potential sources of radioactive contamination, which are the following:

- Tanks for low-level liquid effluent for monitoring and sentencing − The monitor tanks contain water that has the potential for radiological contamination. The water in the monitoring tanks is not expected to contain significant contamination and will typically be below environmental discharge limits.
- An area for loading packaged solid LLW into containers for dispatch to the low level waste repository (LLWR) − Packaged solid radwaste is stored in the radwaste building. This material is bagged or loaded into storage containers at the point where it is generated or processed, so the chance of a significant release is low. All LLW will have been pre-packaged. Currently primary circuit resins are classified as intermediate-level waste (ILW). Condensate polishing resins might be LLW in the event of SG tube failures and are encapsulated at the spent resin tank. Other LLW is not encapsulated. LLW processing equipment is currently expected to be permanently installed. ILW processing equipment is mobile. If ILW and LLW are subjected to further treatment such as low- or high-force compaction in the radwaste building, then the equipment used will be self-contained with integral ventilation and HEPA filtration. The equipment may be permanently located at each site or may be transportable to undertake campaigns at more than one site. The standard radwaste equipment located in the radwaste building is portable.
- Portable or permanently installed equipment for packaging ILW and/or compacting LLW and ILW − The design has provisions for portable radwaste processing equipment. This equipment will connect to the railcar bay auxiliary building HVAC systems. Therefore, the risk of contamination from equipment and processing equipment is small. In addition, all potential sources are filtered at the component level.

The VRS general extract may contain significant airborne activity during either normal operation or fault conditions if the portable or permanently installed radwaste equipment is not properly operated.

The VRS serves the radwaste building, which includes the clean electrical/mechanical equipment room and the potentially contaminated HVAC equipment room, the packaged waste storage room, the waste accumulation room, and the mobile systems facility.

The VRS is a once-through ventilation system that consists of two integrated subsystems: the radwaste building supply air system and the radwaste building exhaust air system. These systems operate in conjunction with each other to maintain temperatures in the areas served while controlling airflow paths and building negative pressure.

The supply air system consists of two 50-percent-capacity air handling units with a ducted air distribution system, automatic controls, and accessories.

The air handling units are located in an electrical/mechanical equipment room on the side of the building. Each unit draws 100 percent outdoor air through individual louvered outdoor air intakes. The two units discharge into a common duct distribution system routed through the building. Branch connections from the main duct supply air through registers into the various areas served.

The exhaust air system consists of two 50-percent-capacity exhaust centrifugal fans sized to allow the system to maintain a negative pressure, high efficiency filtration, HEPA filtration, an exhaust air duct collection system, and automatic controls and accessories. The airflow rates are balanced to maintain a constant exhaust design airflow through the fans. The exhaust fans are located in an equipment room in the corner of the radwaste building.

The exhaust fans discharge to a common duct routed to the plant vent. A radiation monitor records activity in the discharge duct and activates an alarm in the MCR when excess activity in the effluent discharge is detected.

The exhaust air collection duct inside the radwaste building exhausts air from areas and rooms where low levels of airborne contamination may be present. Exhaust connection points are provided to allow the direct exhaust of equipment located on the mobile systems. Where there is potential for significant airborne release, mobile systems include HEPA filtration. Backdraft dampers are provided at each mobile system connection to prevent blowback through the equipment in the event of exhaust system trip. See Chapter 23 for more details pertaining to VRS.

6.8.8 Diesel Generator Building Heating and Ventilation System

The (diesel generator building heating and ventilation system) VZS supplies air to and exhausts from the diesel generator building. The diesel generator building is a physically separate building. See Chapter 23 and Reference 23.42 for more details pertaining to VZS.

The VZS serves the standby diesel generator rooms, electrical equipment service modules, stairwell, security room, diesel fuel oil day tank vaults in the diesel generator building, and the two diesel oil transfer modules located in the yard near the fuel oil storage tanks. Local area heating and ventilation equipment is used to condition the air to the stairwell and security room.

The VZS consists of the following subsystems:

- Normal heating and ventilation subsystem
- Standby exhaust ventilation subsystem
- Fuel oil day tank vault exhaust subsystem
- Diesel oil transfer module enclosures' ventilation and heating subsystem

No credible source or fault would result in a radioactive release from the diesel generator building. There is no reason to provide HEPA filtration on the VZS exhaust systems since there is no normal or fault condition in which a HEPA filter would reduce radioactive releases.

6.8.8.1 Normal Heating and Ventilation Subsystem

The normal heating and ventilation subsystem serves the diesel generator building. Each diesel generator train is provided with independent ventilation and heating equipment for the building areas serving that diesel generator train.

Each normal heating and ventilation subsystem for a diesel generator train consists of one 100-percent-capacity engine room air handling unit, which ventilates the diesel generator room; one 100-percent-capacity service module air handling unit, which ventilates the electrical equipment service module; an exhaust system for the fuel oil storage vault; and electric unit heaters in the diesel generator area. Air intake louvers for these units are located as high in the diesel generator building wall as possible.

Electric unit heaters are provided in the diesel generator room to maintain the space at a minimum temperature of 10°C (50°F) when the diesel generators are off.

Electric unit heaters are provided in the diesel generator stairwell to maintain the space at a minimum temperature.

6.8.8.2 Standby Exhaust Ventilation Subsystem

The standby exhaust ventilation subsystem for each diesel generator room consists of two 50-percent-capacity roof-mounted exhaust fans and motor-operated air intake dampers mounted in the exterior walls of the room.

6.8.8.3 Fuel Oil Day Tank Vault Exhaust Subsystem

Each fuel oil day tank vault is continuously ventilated by a centrifugal exhaust fan. The exhaust fans are mounted on the roof of the vault and ducted to draw air from near the vault floor and from above the oil containment dike to remove any oil fumes generated in the space. Air is drawn into the vault from the diesel generator room through an opening protected with a fire damper.

6.8.8.4 Diesel Oil Transfer Module Enclosures' Ventilation and Heating Subsystem

Each diesel oil transfer module enclosure is ventilated by a roof-mounted exhaust fan. Outside air is drawn into the enclosure through manually operated louvered air intakes. The louvers are closed for winter operation when heating is required. An electric unit heater is provided in each enclosure to maintain the space at a minimum temperature of 10°C (50°F). See Chapter 23 for more details pertaining to VZS.

6.8.9 Turbine Island Building Ventilation System

The turbine building ventilation system (VTS) serves all areas of the turbine building which includes the turbine hall, switchgear rooms, rectifier room, security rooms. See Chapter 23 and Reference 23.41 for more details pertaining to VTS. The general area of the turbine building is ventilated using roof ventilators.

The rooms served by VTS do not have a credible source of radioactive contamination. This part of the AP1000 plant does not have a likely source of radioactive contamination. These areas do not have HEPA filtration because it does not offer a significant protection benefit.

The first bay area of the turbine building contains the RCP variable speed drives, CCS equipment (a nonradioactive system), and the BDS. The BDS may be contaminated in the very unlikely event of concurrent fuel defects, SG leak, radiation monitor or BDS isolation failure, and a BDS leak. The VTS supply and exhaust to the BDS equipment area can be isolated to prevent radioactivity from being spread into the general turbine building areas.

The VTS operates during startup, shutdown, and normal plant operations. The system maintains acceptable air temperatures in the turbine building for equipment operation and for personnel working in the building.

The VTS consists of the following subsystems:

- General area heating and ventilation subsystem
- Local area heating and ventilation subsystem
- Electrical equipment, 1st bay equipment, and personnel work area HVAC subsystem

6.8.9.1 General Area Heating Subsystem

Most of the turbine building is supplied by the general area heating and ventilation subsystem. Air is exhausted from the turbine building to the atmosphere by roof exhaust ventilators. The roof exhaust ventilators pull in outside air through wall louvers. Wall louvers are located at the turbine generator operating deck to provide additional air during plant outage operations. The general area heating subsystem uses electric heaters to provide local heating throughout the turbine building. During heating operation, the general area ventilation system is not operated.

6.8.9.2 Electrical Equipment, 1st Bay Equipment, and Personnel Work Area HVAC Subsystems

This subsystem serves electrical equipment areas (switchgear rooms and the electrical equipment room), the 1st bay equipment (CCS pumps, BDS pumps, and RCP variable-frequency drive power converter areas), personnel work areas, secondary sampling laboratory, and office space. This subsystem is subdivided into three independent HVAC subsystems, one serving the electrical equipment areas, one the 1st bay equipment, and one the personnel work areas.

The electrical equipment HVAC system consists of two 50-percent-capacity air handling units with a supply fan and a return air fan, a ducted supply and return air system, automatic controls, and accessories. The temperature of the rooms is maintained by thermostats that control the chilled water control valves for cooling and the integral face/bypass dampers for heating. Outside air is mixed with recirculated air to maintain a positive pressure.

The 1st bay equipment area HVAC system consists of two 50-percent-capacity air handling units. The temperature of the room is maintained by thermostats that control the chilled water control valves for cooling and the integral face bypass dampers for heating. Outside air is mixed with the recirculation air to maintain a positive pressure.

The personnel work area HVAC system consists of two 50-percent-capacity air handling units, a ducted supply and return air system, automatic controls, and accessories. The temperature of the rooms is maintained by thermostats that control the chilled water control valves for cooling and the integral face/bypass dampers for heating. Electric reheat coils are provided in the ductwork to each room to maintain close temperature control. Outside air is mixed with recirculated air to maintain a positive pressure. See Section 23.13 for more details pertaining to VTS.

6.9 CONTROL AND INSTRUMENTATION

6.9.1 Control and Instrumentation

The C&I systems protect against unsafe reactor operation during steady-state and transient power operations, in addition to normal operational control. Further design details of control and instrumentation systems are delineated in Chapter 19.

The C&I architecture is shown diagrammatically in Figure 6-6. A real-time data network provides communications among the various parts of the C&I system, which include the data display and processing system (DDS), which facilitates the interaction between the plant operators and the other C&I systems; the plant protection and monitoring system (PMS); the plant control system (PLS); the in-core instrumentation system (IIS); the special monitoring system (SMS); and the DAS. Noted below are the:

- **PMS** – Provides C&I to sense fault or accident situations and to initiate the required Class 1 components and systems used to mitigate the fault and bring the plant to safe shutdown conditions.

- **DAS** – Provides a diverse backup to the PMS. This backup is included to support the aggressive risk goals for the AP1000 design by reducing the probability of a severe accident that potentially results from the unlikely coincidence of postulated transients and postulated common mode failure in the protection and control system.

The DAS and the PMS use independent and separated power sources and internal power supplies.

- **PLS –** The plant control system used for normal plant operations and control of the non-Class 1 systems and equipment.

6.9.2 Introduction

The AP1000 plant C&I systems protect against unsafe reactor operation during steady-state and transient power operations. They initiate selected protective functions to maintain the reactor within specified operating limits and respond to mitigate the consequences of DBEs.

This section covers the system descriptions, functional performance requirements, and design bases. The C&I chapter in Section 19 of this PCSR shows that the systems can be designed and built to conform to the applicable criteria, codes, and standards concerned with the safe generation of nuclear power in the UK.

6.9.3 The AP1000 Control and Instrumentation and Architecture

The AP1000 plant C&I systems comprise separate systems that perform duty plant control and monitoring, response to transients, and response to design basis accidents. Figure 6-16 illustrates the C&I architecture for the AP1000 design, which comprises the following systems (discussed in detail in this section):

- plant control system (PLS)
- diverse actuation system (DAS)
- plant protection and monitoring System (PMS)
- special monitoring system (SMS)
- Operation and control centres system (OCS)
- Data display and processing system (DDS)
- incore instrumentation system (IIS)
- main turbine control and diagnostics system (TOS)

Figure 6-16 shows two major sections separated by the real-time data network; the real-time data highway is depicted as a single network.

Figure 6-16 includes the plant protection, control, and monitoring functions. At the lower right-hand side is the PMS. It performs the reactor trip functions, the engineered safety features (ESF) actuation functions, and the qualified data processing system (QDPS) functions. The C&I equipment performing reactor trip and ESF actuation functions, their related sensors, and the reactor trip switchgear are, for the most part, four-way redundant. This redundancy permits the use of bypass logic so that a division or individual channel out of service can be accommodated by the operating portions of the protection system reverting from a two-out-of-four logic to a two-out-of-three logic.

The following control systems are used for duty operations and are not described in detail in this section:

- Meteorological and Environmental Monitoring System (MES)
- radiation monitoring system (RMS)
- Seismic Monitoring System (SJS)

6.9.4 Plant Control System

The PLS provides the functions necessary for normal operation of the plant from cold shutdown through full power. The PLS also contributes to the delivery of Category A and B safety functions (as defined in Chapter 5) in response to transients; parts of the system are therefore classified as Class 2. The PLS controls plant components that are operated from the MCR or remote shutdown workstation.

The PLS uses both discrete- (on/off) and modulating- (analogue) type actuation devices. The real-time data network (Figure 6-16) is a high-speed, redundant communications network that links systems of importance to the operator. Class 1 and 2 safety systems are connected to the network through gateways and qualified isolation devices so that the Category A and B safety functions are not compromised by failures elsewhere. Plant protection, control, and monitoring systems feed real-time data into the network for use by the control room and the DDS.

The upper portion of Figure 6-16 depicts the control rooms and data DDS. The MCR is implemented as a set of compact operator consoles featuring colour graphic displays and soft

control input devices. The graphics are supported by a set of graphics workstations that take their input from the real-time data network. An advanced alarm system, implemented in a similar technology, is also provided.

The DDS (plant computer) is implemented in a distributed architecture. The working elements of the distributed computer system are graphics workstations, although their graphics capability is secondary to their computing performance. The distributed computer system obtains its input from the real-time data network and delivers its output over the network to other users.

The diversity and defence in depth features of the AP1000 plant C&I architecture are described in WCAP-15775 (Reference 6.1) and the systems are substantiated in Chapter 19 of this PCSR.

6.9.5 Protection and Safety Monitoring System

The PMS provides detection of off-nominal conditions and actuation of Class 1 systems necessary to achieve and maintain the plant in a safe shutdown condition. The PMS controls Class 1 components in the plant that are operated from the MCR or remote shutdown workstation. Further design details of this system and its constituent components are delineated in Chapter 19.

The occurrence of a limiting fault, such as a LOCA or a secondary system break, requires a reactor trip plus actuation of one or more of the Class 1 safety systems (designated as ESFs) (Section 19). This combination of events prevents or mitigates damage to the core and RCS components, and provides containment integrity.

In addition, the PMS provides the equipment necessary to monitor the Category A safety functions during and following an accident.

6.9.5.1 Functionality of the Protection and Safety Monitoring System

The PMS consists of the equipment identified in Table 6-2. The PMS has four divisions of reactor trip and ESF actuation, and two divisions of post-accident parameter displays. The functional arrangement of the PMS is shown in Figure 6-17. The PMS is located in the auxiliary building.

The PMS performs the following Category A safety functions:

- Initiates an automatic reactor trip when plant process signals reach specified limits (Table 6-3 lists the PMS reactor trips).
- Initiates automatic actuation of ESFs when plant process signals reach specified limits (Table 6-4 lists the ESF actuations).
- Provides manual initiation of reactor trip and selected ESFs.
- Data communication between Category A and non-Category A safety systems does not inhibit the performance of the Category A safety function.
- Ensures that the automatic safety function and the Class 1 manual controls both have priority over the non-Class 1 soft controls.

The PMS performs the following non-Category A safety functions:

- Provides process signals to the PLS through isolation devices.
- Provides process signals to the DDS through isolation devices.

In conjunction with the operator workstations, the PMS performs the following functions:

- Provides the important displays, visual alerts, and fixed position controls. Instrumentation used for displaying information related to achieving Category A safety functions (information that must not be lost) is defined as Class 1. Instruments of lesser importance in determining the state of the plant do not require the same level of operational assurance and are designated as Class 2 or 3.

- Provides for the transfer of control capability from the MCR to the remote shutdown workstation (RSW) using multiple transfer switches. Each individual transfer switch is associated with only a single Class 1 safety group or with non-Class 1 control capability.

- Displays of the open/closed status of the reactor trip breakers can be retrieved in the MCR.

The PMS automatically removes blocks of reactor trip and ESF actuation when the plant approaches conditions for which the associated function is designed to provide protection. These blocks are identified in Section 19 (Table 19-1 and Table 19-4).

The PMS two-out-of-four initiation logic reverts to a two-out-of-three coincidence logic if one of the four channels is bypassed. All bypassed channels are alarmed in the MCR. The PMS does not allow simultaneous bypass of two redundant channels.

6.9.5.2 Safeguards Actuation Signal

An S-signal is used in the initiation logic of many of the ESFs described above. The variables that are monitored and used to generate an S-signal are typically those that indicate a significant plant transient requiring a response by several ESFs.

The S-signal is generated from any of the following initiating conditions:

- Low-3 pressuriser pressure
- Low-2 steam line pressure
- Low-2 cold leg temperature
- High-2 containment pressure
- Manual initiation

6.9.6 Diverse Actuation System

The DAS is a defence in depth system (Class 2 system) that provides an alternative means of initiating reactor trip, actuating selected ESFs and providing plant information to the operator.

6.9.6.1 Automatic Actuation Function

The DAS provides the following diverse automatic actuations in support of Category A safety functions (separate from the PMS):

- If RCS hot leg temperatures exceed the DAS high hot leg temperature setpoint, automatic reactor trip, turbine trip, and PRHR/IRWST signals are generated.

- If steam generators low wide range level is below the DAS low steam generator level setpoint, automatic reactor trip, turbine trip, and PRHR/IRWST and CMT/RCP signals are generated.

- If pressurizer level inputs fall below the DAS low pressurizer level setpoint, automatic reactor trip, turbine trip, and CMT/RCP signals are generated.

- If containment temperature inputs exceed the DAS high containment temperature setpoint, automatic containment isolation/PCS actuation signal is generated.

6.9.6.2 Manual Actuation Function

The manual actuation function of the DAS is implemented by hardwiring the controls located in the MCR directly to the final loads in a way that completely bypasses the normal path through the control room multiplexers, the PMS cabinets, and the DAS automatic logic.

The DAS provides the following diverse manual actuations in support of Category A safety functions (separate from the PMS):

- Reactor and turbine trip
- Passive containment cooling actuation
- CMT actuation and RCP trip
- Open Stage 1 ADS valves
- Open Stage 2 ADS valves
- Open Stage 3 ADS valves
- Open Stage 4 ADS valves
- Opening PRHR discharge isolation valves and close the IRWST gutter isolation valves
- Selected containment penetration isolation
- Containment hydrogen igniter actuation
- Initiating IRWST injection
- Initiating containment recirculation
- Initiating IRWST drain to containment

In addition to the above functions, a redundant method of actuating the following functions is provided at the DAS processor cabinets 1 and 2 (aka Remote DAS Control Panel) located in the radiological portion of the auxiliary building:

- Reactor and turbine trip
- PRHR & IRWST actuation
- CMT actuation & RCP Trip
- Containment Isolation & PCS Actuation
- ADS Stage 4 actuation
- Initiate IRWST Injection
- Initiate containment recirculation
- Initiate containment recirculation and IRWST drain

6.9.6.3 Actuation Logic Function

DAS automatic actuation functions are accomplished by channel-based subsystems. Plant parameter values from dedicated DAS sensors are compared against predetermined setpoints. If the plant parameter value exceeds the setpoint, a bistable is set in the associated channel. These signals are then voted in either a two-out-of-three or one-out-of-two twice taken basis. When two or more channels are unavailable, the automatic function is unavailable. If the voter is true, an actuation command signal is generated, which operates an interposing/interface relay with an output contact rating that is compatible with the voltage and current capacity of the final actuation devices. The manual actuation mode operates in parallel to independently actuate the final devices.

Actuation signals are output to the loads in the form of normally de-energised energise-to-actuate signals. The normally de-energised output state, along with redundant voting logic, reduces the probability of inadvertent actuation.

The DAS is designed so that, once actuated, each mitigation action goes to completion. Any subsequent return to the un-actuated state requires deliberate operator action.

Display Function

The DAS provides MCR displays of plant parameters separately from the PMS as listed in Table 19-7.

6.9.7 Radiation Monitoring System

The RMS provides plant effluent monitoring, process fluid monitoring, airborne monitoring, and continuous indication of the radiation environment in plant areas where such information is needed. The RMS is installed permanently and operates in conjunction with regular and special radiation survey programmes to help meet applicable regulatory requirements.

The RMS is divided functionally into the following two subsystems:

- Process, airborne, and effluent radiological monitoring and sampling
- Area radiation monitoring

The process and effluent radiological monitoring and sampling subsystem provides radiation monitoring for the four functions listed below. Individual monitors may provide functionality in more than one of these functions:

- Fluid process monitors determine concentrations of radioactive material in plant fluid systems.

- Airborne activity monitors provide operators with information on concentrations of radioactivity at various points in the ventilation system, providing information on airborne concentrations in the plant.

- Liquid and gaseous effluent monitors measure radioactive materials discharged to the environs.

- Post-accident monitors watch potential pathways for release of radioactive materials during accident conditions.

The area radiation monitoring subsystem provides plant personnel information on radiation at fixed locations in the plant. Post-accident monitoring functions are also performed by certain area monitors.

The RMS uses distributed radiation monitors, where each radiation monitor consists of one or more radiation detectors and a dedicated radiation processor. Each radiation processor receives averages and stores radiation data, and transmits alarms and data to the plant control system for control (as required), display, and recording. The alarms provided include low (fail), alert, and high. Selected channels have a rate-of-rise alarm. Additional design detail of this system and its constituent components are delineated in Chapter 19.

6.9.8 Special Monitoring System

The SMS consists of the digital metal impact monitoring system (DMIMS), vibration integrity monitoring system (VIMS) and feedwater vibration monitoring system (FWVMS).

The DMIMS detects the presence of metallic debris in the RCS when the debris impacts the internal parts of the RCS. The DMIMS is composed of digital circuit boards, controls, indicators, power supplies, and remotely located sensors and related signal processing devices. A minimum of two sensors are located at each natural collection region, connected to separate instrumentation channels, to maintain the impact monitoring function if a sensor fails in service.

The RCP vibration monitoring system (RCPVMS) (part of VIMS) is a continuous monitoring system that provides outputs for diagnostic tools and information to assist in evaluating the performance of the RCPs.

The FWVMS monitors the vibration of the main and booster feedwater pumps, motor, and gear unit.

The SMS does not perform any Category A, Category B, or defence in depth safety functions. The SMS consists of specialised subsystems that interface with the C&I architecture to provide diagnostic and long-term monitoring functions.

6.9.9 Operation and Control Centres System

The OCS includes the MCR, the technical support centre, the remote shutdown room, emergency operations facility, local control stations, and associated workstations for these centres (see Section 19.5.2.3 for further details). With the exception of the control console structures, the equipment in the control room is part of the other systems (for example, PMS, PLS, and DDS).

The boundaries of the OCS system for the MCR and the remote shutdown workstation are the signal interfaces with the plant components. These interfaces are via the plant protection and safety monitoring system processor and logic circuits, which interface with the reactor trip and ESF plant components; the PLS processor and logic circuits, which interface with the non-Class 1 plant components; and the plant real-time data network, which provides plant parameters, plant component status, and alarms.

6.9.10 Data Display and Processing System

The DDS provides the equipment used for processing non-Category A safety data, i.e., data that results in alarms and displays for both normal and emergency plant operations, generating these displays and alarms, providing analysis of plant data, providing plant data

logging and historical storage and retrieval, and providing operational support for plant personnel.

The DDS also contains the real-time data network, which is a redundant data highway that links the elements of the AP1000 plant C&I architecture (see Figure 6-16).

6.9.11 In-core Instrumentation System

The primary function of the IIS is to provide a three-dimensional flux map of the reactor core. This map is used to calibrate neutron detectors used by the PMS, as well as to optimise core performance. A secondary function of the IIS is to provide the PMS system with the thermocouple signals necessary for the post-accident inadequate core cooling monitor. The in-core instrument assemblies house both fixed in-core flux detectors and core exit thermocouples.

6.9.12 Main Turbine Control and Diagnostics System

The turbine generator is equipped with a digital electrohydraulic (D-EHC) system that combines the capabilities of redundant processors and high-pressure hydraulics to regulate steam flow through the turbine. The control system provides the functions of speed control, load control, overspeed protection, and automatic turbine control (ATC), which may be used for either control or supervisory purposes, at the discretion of the plant operator.

6.10 ELECTRICAL SYSTEMS

6.10.1 Electrical Power Systems

The electrical power systems comprise four main systems that provide power to various components and also include a number of other systems. Further design details of the electrical power systems and their constituent components are delineated in Chapter 18.

6.10.1.1 Essential Electrical Supply System

IDS provides reliable power for the safety-related equipment required for the plant instrumentation, control, monitoring and other vital functions needed for shutdown of the plant. In the event of a total loss of off-site and on-site ac power sources, the dc batteries constitute the sources of electrical power for operation of the required dc and ac instrument. In addition, the IDS provides power to the normal and emergency lighting in the MCR and at the remote shutdown room (RSW) (which contains the RSW).

The IDS comprises the Class 1 battery-backed dc electrical power supply system and uninterruptible power supply system. Although IDS is defined as the “Class 1E dc and uninterruptible power supply system” in design documentation, for the purposes of this PCSR, “the IDS” or “essential electrical supply system” is used for consistency.

The IDS provides power for the Class 1 equipment required for plant instrumentation, control, monitoring, and other vital functions. In addition, the IDS provides power for the emergency lighting in the MCR and at the remote shutdown workstation.

The IDS can provide power for the safe shutdown and monitoring of the plant for at least 72 hours without the support of battery chargers during a loss of all ac power sources coincident with a design basis accident (DBA). The system is designed so that no single failure will result in a condition that prevents the safe shutdown of the plant.

6.10.1.1.1 Class 1 Battery-Backed dc Supply System

The operating voltage range of the batteries is 210 to 280 Vdc. The maximum equalising charge voltage for batteries is 280 Vdc. The nominal system voltage is 250 Vdc.

The Class 1 dc subsystem is divided into four independent trains: A, B, C, and D. Each of these divisions is supplied from dedicated batteries and battery chargers.

Division A and D battery banks, and one of the battery banks in Division B and C, are designated as 24-hour battery banks and, as such, provide power to the loads required for the first 24 hours following a loss of all ac power event or a design basis accident. The second battery bank in Division B and C, designated as the 72-hour battery bank, is used for the loads requiring power for 72 hours following the same event.

6.10.1.1.2 Class 1 Uninterruptible Power Supplies

The Class 1 uninterruptible power supplies (UPS) provides power at 230 Vac to four independent divisions of Class 1 instrument and control power buses. Divisions A and D each consist of one inverter associated with an instrument and control distribution panel and a backup voltage regulating transformer with a distribution panel. The inverter is powered from the respective 24-hour battery bank switchboard. Divisions B and C each consist of two inverters, two instrument and control distribution panels, and a voltage-regulating transformer with a distribution panel. One inverter is powered by the 24-hour battery bank switchboard and the other by the 72-hour battery bank switchboard.

Under normal operation, the Class 1 inverters receive power from the associated battery bank. If an inverter is inoperable or the Class 1 250-Vdc input to the inverter is unavailable, the power is transferred automatically to the backup ac source by a static transfer switch featuring a make-before-break contact arrangement. The software utilised in the static transfer switch is diverse from the software in the inverter in order to protect against common cause failure. The backup power is received from the diesel-generator-backed, Class 2 400-Vac bus through the Class 1 voltage-regulating transformer. In addition, a manual mechanical bypass switch is provided to allow connection of a backup power source when the inverter is removed from service for maintenance.

6.10.1.2 Standby Electrical Supply System

The EDS comprises the battery-backed dc electrical power supply system and uninterruptible power supply system. Although EDS is defined as the “Non-Class 1E dc and uninterruptible power supply system” in design documentation, for the purposes of this PCSR, “EDS” or “standby electrical supply system” is used for consistency.

The EDS provides dc and uninterruptible ac power to the plant dc and ac loads needed to safely operate the plant under normal conditions and for defence in depth.

The EDS has four DC battery systems (EDS1 to EDS4) organized in two subsystems, 1 and 2 (Figure 18-5), with another dc system – EDS5 (see Figure 18-6). A spare EDS battery system is also provided and can be used in place of any of the EDS battery subsystems. See Chaper 18 and, specifically, Section 18.6 for additional details on EDS.

In addition, the EDS provides power to the hydrogen igniters located inside containment, which make up the VLS.

6.10.1.3 Main Alternating Current Power System

The main ac power system (ECS) is the power source used during plant normal operations to power all required operating equipment. The ECS receives power both from offsite and from the plant main generator should offsite power be lost without an associated reactor trip. The Class 2 standby power is included in the standby power system (ZOS). See Chapter 18 for more detail on ECS.

6.10.2 Onsite Standby Diesel Generator

The onsite ZOS is composed of two Class 2 standby diesel generator units and their separated power cabling to selected separated portions of the ECS that provide power to priority defence in depth (Class 2) loads (listed in Table 18.-6). These loads include each diesel generator subsystem's components to maintain reliability and operability of ZOS.

The onsite standby diesel generator function is to provide a backup source of ac electrical power to Category A onsite equipment needed to support decay heat removal, boration, and inventory control, as well as to minimise plant financial risks associated with the loss of the normal ac power sources.

Each generator is directly coupled to the diesel engine. Each diesel generator unit is an independent self-contained system complete with necessary support subsystems that include the following:

- Diesel engine starting subsystem
- Combustion air intake and engine exhaust subsystem
- Engine cooling subsystem
- Engine lubricating oil subsystem
- Engine speed control subsystem
- Generator, exciter, generator protection, monitoring instruments, and controls subsystems

6.10.3 Post-72-Hour Ancillary Diesel Generator Supply

To supply power during the post-72-hour period following a DBA, Class 2 ECS ancillary diesel generators are provided to supply the Class 1 voltage regulating transformers (divisions B and C only). This powers post accident monitoring systems, MCR lighting, MCR and C&I room ventilation, and pump power to refill the PCS water storage tank and the SFP, when all other sources of power are not available. Figure 18-7 shows the connections to post-72-hour loads. Note that if these diesel generators are unavailable, the plant would utilise diesel generator brought in from offsite.

6.11 AUXILIARY SYSTEMS

The plant auxiliary systems consist of non-electrical and non-HVAC defence in depth safety systems, and other water and other support systems.

6.11.1 Water Systems

6.11.1.1 Component Cooling Water System

The CCS is a closed-loop cooling system that transfers heat from various plant components to one or both SWS cooling trains, which are in turn cooled in a natural heat sink such as the ocean or a river (or cooling towers), depending on the plant operating mode. It operates during normal phases of plant operation, including power operation, normal cooldown, and refuelling. It removes heat from various components needed for plant operation and removes core decay heat and sensible heat for normal reactor shutdown and cooldown. Further design details of this system and its constituent components are delineated in Chapter 17 and Reference 6.20. It provides defence in depth by providing cooling for the following:

- RNS HXs and pumps when the RCS pressure and temperature are below 31 bar (450 psi) and 176.7°C (350°F).
- Miniflow HXs of the CVS makeup pumps.
- SFP HXs for heat removal from the SFP.

The system components are arranged into two interconnected mechanical trains. Each train includes one component cooling water pump, one component cooling water HX, and one component cooling water surge tank. During normal plant operation, only one component cooling water pump, HX, and surge tank is expected to be operating, with the other component cooling water pump on standby. Should the operating component cooling water pumps stop operating; the standby pump is automatically started on low component cooling water flow rate. During normal plant cooldown and startup operations, both component cooling water pumps and HXs would be operated to handle the higher heat loads and flow rates.

The component cooling water pump discharge and suction piping for the two pumps is interconnected so that either pump can cool all the required plant components using either component cooling water HX. A bypass line around each HX containing a throttle valve prevents overcooling of the component cooling water during periods when the SWS water temperature is reduced.

During normal plant operation, one CCS mechanical train of equipment is operating. The operating train is aligned to provide component cooling for the loads identified in the list

below. The other train is aligned to automatically start in case the operating component cooling water pump fails.

The CCS transfers heat from the following plant components:

- RCPs and the RCP variable frequency drives in the RCS
- Letdown and miniflow HXs in the CVS
- Reactor coolant drain tank in the WLS
- Residual heat removal pumps and HXs in the RNS (see subsection 6.8.2)
- SFP HXs in the SFS
- Operating water-cooled chiller in the VWS
- Sample HX in the PSS
- Air compressors in the compressed air system
- Condensate pump oil coolers in the CDS

6.11.1.2 Service Water System

The SWS supplies cooling water to remove heat from the CCS HXs in the turbine building. The service water system is arranged into two trains of components and piping. Each train includes one service water pump, one strainer, and one cooling tower cell. Each train provides 100-percent-capacity cooling for normal power operation. Cross-connections between the trains upstream and downstream of the component cooling water system heat exchangers allows either service water pump to supply either heat exchanger, and allows either heat exchanger to discharge to either cooling tower cell.

The service water system operates during normal modes of plant operation, including startup, power operation (full and partial loads), cooldown, shutdown, and refuelling. The service water system is also available during loss of normal ac power conditions.

In the event of loss of normal ac power, the service water pumps and cooling tower fans, along with the associated motor operated valves, are automatically loaded onto their associated diesel bus. This includes isolation of cooling tower blowdown, which minimizes drain down of the system while both pumps are off. Both pumps and both cooling tower cells automatically start after power from the diesel generator is available. Further design details of this system and its constituent components are delineated in Chapter 17 and Reference 6.21.

6.11.1.3 Central Chilled Water System

VWS provides a source of chilled water to the cooling coils of HVAC systems in order to cool the process air. Further design details of this system and its constituent components are delineated in Reference 6.53.

The Central Chilled Water System consists of two subsystems: a high cooling capacity subsystem (HC VWS), and a low cooling capacity subsystem (LC VWS). The HC VWS provides chilled water to non-defence-in-depth HVAC systems used by the Radiologically Controlled Area Ventilation System (VAS), Containment Recirculation Cooling System (VCS), Containment Air Filtration System (VFS), Health Physics and Hot Machine Shop Ventilation System (VHS), Radwaste Building Ventilation System (VRS), Turbine Building Ventilation System (VTS), and the Annex/Aux Building Nonradioactive Ventilation System (VXS). The HC VWS also provides cooling water for the Secondary Sampling System (SSS) sample cooler, the Liquid Radwaste System (WLS) vapor condenser and gaseous radwaste system (WGS) gas cooler.

The LC VWS provides chilled water to defense-in-depth HVAC cooling coils used by the Nuclear Island Nonradioactive Ventilation System (VBS) air handling units and the VAS units coolers located in the Chemical and Volume Control System (CVS) and Normal Residual Heat Removal System (RNS) pump rooms.

The Class 1 function performed by VWS is that it maintains the integrity of the containment pressure boundary after a design basis event by isolating the chilled water supply and return pipe lines that penetrate the containment (Table 15A-1).

6.11.1.3.1 High Capacity Subsystem

The HC VWS consists of two (2) large capacity chilled water pumps, two (2) large capacity centrifugal water-cooled chillers, a chemical feed tank, an expansion tank, and associated valves, piping and instrumentation for normal operation, and two (2) small chilled water pumps and two (2) small air-cooled chillers for peaking load or low load operation. The chiller water-cooled condensers are supplied with cooling water from the CCS. The HC VWS is arranged in two sets of parallel mechanical trains with common supply and return headers, the water-cooled chiller train and the air-cooled chiller train.

6.11.1.3.2 Low Capacity Subsystem

The LC VWS consists of two (2) 100% capacity chilled water trains. Each train consists of a chilled water pump, an air-cooled chiller, an expansion tank, a chemical feed tank, and associated valves, piping, and instrumentation. The system is arranged in two independent trains with separate supply and return headers.

6.11.1.4 Fire Protection System

The FPS provides a defence in depth functions and comprises of automatic fire detection, an alarm system, and firefighting equipment in order to:

- Detect fires early
- Minimise fire spreading
- Extinguish fires quickly

Further design details of this system and its constituent components are delineated in Reference 6.54.

FPS is designed to minimise the damage to SSCs and thus the spread of radiological contamination is minimised. The AP1000 plant FPS achieves the mitigation of damage by the following:

- Detect and locate fires and provide the operator with an indication of the location.
- Provide the capability to extinguish fires in any plant area, protect site personnel, limit fire damage, and enhance safe shutdown capabilities.
- Supply fire suppression water at a flow rate and pressure sufficient to satisfy the demand of any automatic sprinkler system, plus adequate capacity for fire hoses.
- Maintain 100 percent of fire-pump design capacity, assuming failure of the largest fire pump or the loss of offsite power.
- Following a safe shutdown earthquake, provide water to hose stations for manual firefighting in areas outside of containment containing Class 1 SSCs.

- Satisfy the requirements of the PCS as an alternate source of water to wet the containment dome after a loss-of-coolant accident, if the FPS is available.
- Provide an alternate supply of cooling water to the RNS or SFS HX for decay heat removal after a loss of normal CCS function.
- Provide containment spray capability for severe accident management, if deemed necessary.

The system comprises of the following:

- Automatic fire detection and alarm system;
- Manual firefighting equipment, i.e. portable fire extinguishers and hose stations
- Automatic fire suppression systems, i.e. fixed firefighting systems such as sprinklers in specific locations outside containment.

The fixed firefighting system has seismic design requirements applied to portions of the standpipe system located in areas containing equipment required for safe shutdown following a safe shutdown earthquake so that water is available to manual hose stations. The standpipe system serving areas containing equipment required for safe shutdown following a safe shutdown earthquake is designed and supported so that it remains functional. In addition, the valves and associated penetration piping for the FPS that maintain containment isolation are Category A Class 1 (Table 15A-1).

6.11.1.5 Demineralised Water Transfer and Storage System

The DWS receives water from the demineralized water treatment system (DTS) and provides a reservoir of demineralised water to be supplied to the condensate storage tank and to be distributed throughout the plant. Demineralised water is processed in the DTS to remove dissolved oxygen. In addition to supplying water for makeup of systems that require pure water, the demineralised water is used to sluice spent radioactive resins to the WSS from the ion exchange vessels in the CVS, the SFS, and the WLS.

The DWS consists of the demineralised water storage tank, the demineralised water transfer pump, two catalytic oxygen reduction units, piping, valves, instrumentation, and a condensate storage tank. The system has one containment penetration with isolation valves on either side. Additional design detail of this system and its constituent components are delineated in Reference 6.39.

6.11.1.6 Demineralised Water Treatment System

The DTS receives water from the raw water system (RWS), processes this water to remove suspended solids and ionic impurities, and provides demineralised water to the DWS. The system includes filters, reverse osmosis units, electro deionisation units for secondary demineralisation, piping, valves, and instrumentation. Additional design detail of this system and its constituent components are delineated in Reference 6.40.

6.11.1.7 Potable Water System

The potable water system (PWS) is designed to furnish water for sanitary and domestic use and human consumption. Additional design detail of this system and its constituent components are delineated in Reference 6.41.

6.11.1.8 Turbine Building Closed Cooling Water System

The turbine building closed cooling water system (TCS) provides chemically treated demineralised cooling water for the removal of heat from HXs in the turbine building, and rejects the heat to the CWS. Additional design detail of this system and its constituent components are delineated in Reference 6.42.

6.11.1.9 Waste Water System

The waste water system WWS collects nonradioactive waste from floor and equipment drains in the sumps or tanks in the auxiliary, annex, turbine, and diesel generator buildings. Additional design detail of this system and its constituent components are delineated in Reference 6.43.

6.11.1.10 Sanitary Drainage System

The sanitary drainage system (SDS) is designed to collect the site sanitary waste for delivery to the treatment plant or an offsite facility where it is processed. Additional design detail of this system and its constituent components are delineated in Reference 6.47.

6.11.2 Process Auxiliaries

6.11.2.1 Compressed and Instrument Air System

The CAS consists of the following three subsystems:

- The instrument air subsystem supplies compressed air for air-operated valves and dampers.

- The service air subsystem supplies service air at outlets throughout the plant to power air-operated tools and is used as a motive force for air-powered pumps. The service air subsystem is also utilised as a supply source for breathing air. Individually packaged air purification equipment is used to produce breathing-quality air for protection against airborne contamination.

- The high-pressure air subsystem supplies air to the VES and fire-fighting apparatus recharge station. The high-pressure air subsystem also provides a connection for refilling the VES storage tanks from an offsite source. Major components of the CAS are located in the turbine building.

Additional design detail of this system and its constituent components are delineated in Reference 6.45.

6.11.2.2 Plant Gas System

The plant gas system (PGS) provides hydrogen, carbon dioxide, and nitrogen gas to the plant systems, as required. Other gases such as oxygen, methane, acetylene, and argon are supplied in smaller individual containers, and are not supplied by the PGS. Additional design detail of this system and its constituent components are delineated in Reference 6.46.

6.11.2.3 Standby Diesel Fuel Oil System

The standby diesel fuel oil system (DOS) consists of two standby diesel fuel storage tanks, one ancillary diesel oil storage tank, a standby diesel generator fuel oil transfer system, and an ancillary diesel generator fuel oil supply system. It consists of two independent fuel storage, transfer, and recirculation flow paths, that is, one path per diesel generator. Each path consists of a fuel oil storage tank, one fuel transfer pump, diesel fuel oil supply and fuel return piping, a day tank, and the associated specialty valves, fittings, and instrumentation. The supply lines from the transfer pumps to the day tanks include fuel oil heaters, filters, and moisture separators. The system is protected from the effects of low temperatures by the inline electric oil heater in the transfer line.

The fuel oil storage tanks are sized to provide sufficient capacity for 7 days of operation for each standby diesel generator. This provides time for additional fuel to be transported to the site, if required. The design of the tanks allows fuel to be replenished without interrupting diesel generator operation.

The ancillary diesel generator fuel oil supply portion of the DOS consists of a single tank serving both ancillary diesel generators. The tank is located inside the annex building and is served by the annex building heating and ventilation system. The tank is insulated and provided with heaters to maintain the fuel oil above the oil cloud point. Fuel oil lines from the tank to the ancillary diesel generators are insulated.

The ancillary diesel generator fuel oil storage tank is sized to provide 4 days of operation for both the ancillary diesel generators. The ancillary diesel generators are not required for the first 3 days following a loss of electrical power. Therefore, the operator has 7 days to arrange for the delivery of additional fuel. Additional design detail of this system and its constituent components are delineated in Reference 6.48.

6.11.2.4 Communication System

The communication system (EFS) provides effective intraplant communications and effective plant-to-offsite communications during normal, maintenance, transient, fire, and accident conditions, including loss of offsite power. Additional design detail of this system and its constituent components are delineated in Reference 6.44.

6.12 FUEL HANDLING, FUEL STORAGE, AND RADWASTE

6.12.1 Introduction

The fuel handling and storage and radwaste main components are described in this section for completeness; a further assessment and more specific details are contained in Chapter 26.

Fuel Handling and Storage

The fuel handling equipment is designed to handle the spent fuel assemblies underwater from the time they leave the RV until they are placed in a container for shipment to the appropriate waste facility. Underwater transfer of spent fuel assemblies provides an effective and transparent radiation shield, as well as a reliable cooling medium for removal of decay heat. The boric acid concentration in the water is sufficient to preclude criticality.

The associated fuel handling structures may be generally divided into two areas: the refuelling cavity that is flooded only during plant shutdown for refuelling, and the SFP and

transfer canal, which is kept full of water. The fuel handling and refuelling system (FHS) transfers fuel assemblies and core components during refuelling operations and stores new and spent fuel assemblies in the new and spent fuel storage racks, respectively. The refuelling machine (RM) and the fuel transfer system are operated during refuelling mode. The fuel handling machine in the fuel handling area is used during refuelling operation and during plant power operation,

New fuel is stored dry adjacent to the SFP. For refuelling, new fuel assemblies are transferred into the refuelling cavity via the SFP.

The FHS consists of the following subsystems, which are described below:

- New fuel storage
- Spent fuel storage
- Light load handling system (related to refuelling)

6.12.2 New Fuel Storage

New fuel is stored in a high-density rack that includes integral neutron-absorbing material to maintain the required degree of subcriticality. The rack is designed to store fuel of the maximum design basis enrichment. The rack in the new fuel pit consists of an array of cells interconnected to each other at several elevations and to a thick baseplate at the bottom elevation.

The new fuel rack includes storage locations for 72 fuel assemblies. The rack layout and array centre-to-centre spacing is shown in the Figures 6-12 and 6-13. This spacing provides a minimum separation between adjacent fuel assemblies, which is sufficient to maintain a subcritical array even in the event the building is flooded with unborated water or fire extinguishant aerosols, or during any DBE. The rack is designed so that a fuel assembly cannot be inserted into a location other than a one designed to receive an assembly. Surfaces that come into contact with the fuel assemblies are made from annealed austenitic stainless steel.

The new fuel storage facility is located within the seismic Category I (C-I) auxiliary building fuel handling area. The facility is protected by the external walls of the auxiliary building from the effects of natural phenomena such as earthquakes, wind, tornadoes, floods, and external missiles. The facility is designed to maintain its structural integrity following a safe shutdown earthquake and to perform its intended function following a postulated DBE such as fire, internal missiles, or pipe break. The walls surrounding the fuel handling area and new fuel storage pit protect the fuel from missiles generated inside the auxiliary building. The fuel handling area does not contain a credible source of missiles (see Chapter 11 on internal hazards and Chapter 12 on external hazards).

The dry, unlined, approximately 5.2-m (17-foot) deep reinforced concrete pit is designed to provide support for the new fuel storage rack. The rack is freestanding and sits on bearing pads supported by the pit floor. The walls of the new fuel pit are C-I. The new fuel pit is normally covered to prevent foreign objects from entering the new fuel storage rack. Since the only crane that can access the new fuel pit does not have the capacity to lift heavy objects, the new fuel pit cover is not designed to protect the fuel assemblies from the effects of dropped heavy objects. The cover also provides further protection from a fuel assembly misload. The new fuel storage pit is drained by gravity drains that are part of the WRS, draining to the waste holdup tanks that are part of the WLS.

6.12.3 Spent Fuel Storage

Spent fuel is stored in high-density racks that include integral neutron-absorbing material to maintain the required degree of subcriticality. These rack modules are freestanding, neither anchored to the pool floor nor braced to the pool wall. The spent fuel storage racks include storage locations for 612 fuel assemblies and five defective fuel assemblies. The spent fuel racks are are capable of storing fresh fuel up to 5 weight percent U-235, as well as spent fuel.

The spent fuel storage facility is located within the C-I auxiliary building fuel handling area. The walls of the SFP are an integral part of the C-I auxiliary building structure. The facility is protected from the effects of natural phenomena such as earthquakes, wind and tornadoes, floods, and external missiles. The facility is designed to maintain its structural integrity following a safe shutdown earthquake and to perform its intended function following a postulated DBE such as a fire.

The SFP provides storage space for spent fuel. The pool is approximately 13 m (42.5 ft) deep and constructed of concrete-filled structural modules. The portion of the structural modules in contact with the water in the pool is stainless steel. The normal water volume of the pool is about 721 m^3 (190,500 US gallons) of borated water (including racks without fuel at a water level 0.3 m below the operating deck) with a nominal boron concentration of 2700 ppm.

A gated opening connects the SFP and fuel transfer canal. The fuel transfer canal is connected to the in-containment refuelling cavity by a fuel transfer tube. The spent fuel transfer operation is completed underwater, and the waterways are deep enough to maintain a minimum of 2.67 m (8.75 ft) of shielding water above the active fuel height of spent fuel assemblies.

Next to the SFP and accessible by another gated, gasketed opening is a cask loading pit. It is provided for underwater loading of fuel into a shipping cask and cask draining and decontamination prior to cask shipment to the appropriate waste facility.

The fuel handling machine (FHM) traverses the SFP, the fuel transfer canal, the cask loading pit, the new fuel storage pit, and the rail car bay. It is used in the movement of both new and spent fuel assemblies. A new fuel elevator in the SFP lowers the new fuel to an elevation accessible by the FHM and its associated long handling tool.

The cask handling crane is used for operations involving the spent fuel shipping cask. The cask handling crane traverses the auxiliary building and a portion of the fuel handling area. The cask handling crane's path is designed so that the cask cannot pass over the SFP, new fuel pit, or fuel transfer canal. This precludes the cask handling crane from moving loads greater than fuel components over stored fuel.

6.12.4 Spent Fuel Pool Cooling System

The SFS is designed to remove decay heat which is generated by stored fuel assemblies from the water in the spent fuel pool. This is done by pumping the high-temperature water from within the fuel pool through a heat exchanger, and then returning the water to the pool. A secondary function of the SFS is clarification and purification of the water in the spent fuel pool, the transfer canal, and the refuelling water. The SFS is made up of two redundant mechanical trains. Further design details of this system and its constituent components are delineated in Reference 6.17 and Chapter 17.

If the Spent Fuel Pool Cooling System's normal cooling capability is lost, heat is removed from the spent fuel by heating and boiling the water in the SFP. The SFP water and other safety-related sources of makeup water (e.g. PCCWST) are sufficient to remove heat from the spent fuel via passive means for 72 hours following a design basis event including a seismic event. There is sufficient onsite water to support heat removal by boiling of the SFP for a total of 7 days.

A listing of the major functions of the spent fuel pool cooling system and the corresponding modes of operation is provided below:

- Remove heat from the water in the spent fuel pool during operation to maintain the pool water temperature within acceptable limits.
- Provide purification and clarification of the spent fuel pool water during operation.
- Provide purification of the refuelling cavity during refuelling operations.
- Transfer water between the IRWST and the refuelling cavity during refuelling operations.
- Provide purification and cooling of the IRWST during normal operation.
- The SFS is designed to perform its function in a reliable and failure-tolerant manner. This reliability is achieved with the use of rugged and redundant equipment. The SFS consists of two mechanical trains of equipment. Each train includes one spent fuel pool pump, one spent fuel pool heat exchanger, one spent fuel pool demineralizer, and one spent fuel pool filter. The two trains of equipment share common suction and discharge headers. In addition, the SFS includes the piping, valves, and instrumentation necessary for system operation.

6.12.4.1 Containment Isolation

The SFS preserves containment integrity by isolating the SFS piping lines penetrating containment using Containment Isolation valves.

6.12.4.2 Class 1 Piping Connections for Makeup to the SFP

The SFS provides Class 1 piping connections to the PCCWST, and cask washdown pit (CWP) for makeup to the SFP should normal SFS cooling be disabled following a design basis event, including a seismic event. The Cask Loading Pit (CLP) will be connected by opening the gate between the CLP and SFP. A Class 1 piping connection is provided from the CLP to the SFP and can be used if necessary.

6.12.4.3 Class 1 Drain Path from the Refueling Cavity to Containment

Redundant check valves in the drain line from the Refueling Cavity prevent out-of-sequence flooding of the Refueling Cavity during containment floodup in a design basis accident scenario. During a containment floodup event, water entering the Refueling Cavity from either a Loss of Coolant Accident (LOCA) or the In-Containment Refueling Water Storage tank (IRWST) overflow weirs will be directed through the drain path to the steam generator two (SG2) compartment. This insures proper floodup sequence by allowing this water to contribute to the initial containment floodup level, providing the driving head for containment recirculation.

6.12.4.4 Maintain Proper Refueling Cavity Level during Refueling Operations

During refueling operations, the SFS maintains the proper Refueling Cavity water level.

6.12.4.5 Maintain SFS Water Level above the Top of the Fuel Assemblies (without the RCCA)

The SFS is responsible for maintaining the SFP water level above the top of the fuel assemblies (without the RCCA) at all times during operation. During any design basis event (including a seismic event) that would cause loss of water in the pool due to boiling, makeup water is provided from PCS in order to maintain SFP water level above the top of the fuel assemblies (without the RCCA) for 72 hours.

6.12.4.6 Spent Fuel Pool Purification

The SFS purifies the SFP water during all modes of plant operation. The SFS removes radioactive corrosion products, fission products, and other impurities in order to maintain water clarity and low SFP radioactivity levels.

6.12.4.7 Refueling Cavity Purification

The SFS purifies the Refueling Cavity water during refueling operations. The SFS removes radioactive corrosion products, fission products, and other impurities in order to maintain water clarify and low Refueling Cavity water radioactivity levels.

6.12.4.8 Water Transfers

The SFS transfers water between the IRWST and the Refueling Cavity during refueling operations. The SFS can also transfer water between the IRWST, Fuel Transfer Canal (FTC), CLP, and CWP.

6.12.4.9 IRWST Cooling and Purification

The SFS can be aligned to cool the IRWST water during normal plant operation if the RNS is unavailable. The SFS removes radioactive corrosion products and fission ions to maintain low IRWST radioactivity levels during normal plant operation prior to a scheduled refueling. The SFS is designed to maintain the water in the IRWST in a way consistent with requirements to limit the radioactivity of the water in the Refueling Cavity during a refueling.

6.12.4.10 Refueling Cavity Drain

A drain line is located in the Refueling Cavity to facilitate proper draining of the Refueling Cavity to support refueling operations.

6.12.4.11 SFP Water Tritium Concentration Control

The SFS has the ability to maintain the proper concentration of tritium in the SFP. This can be accomplished by removing water from the SFP and replacing it with non-tritiated water.

6.12.4.12 Removal of Decay Heat from Spent Fuel Assemblies

The SFS removes the decay heat from the spent fuel assemblies stored in the SFP by pumping water from the pool, through a cooling heat exchanger, and back to the SFP.

6.12.4.13 Recover from SFP Boiling

If normal SFP cooling is lost, the SFP temperature will increase up to the boiling point in the pool. Once cooling is restored, the SFS can terminate boiling and reduce the SFP temperature to normal.

6.12.4.14 CLP Support of RNS

The CLP provides a defense-in-depth source of water to the RNS, which may be used to respond to an Automatic Depressurization Signal (ADS) signal after a LOCA has occurred. In this event, water from the CLP will be delivered by the RNS to the RCS to help prevent Fourth Stage ADS actuation by holding up the core makeup tanks.

6.12.4.15 SFS Support of CVS

The CVS can take suction from the SFP through the connection in the SFS pump suction to provide a defense-in-depth borated suction source.

6.12.5 Light Load Handling System

The light load handling system consists of the equipment and structures needed for the refuelling operation. This equipment comprises the following:

- Refuelling machine (RM)
- Fuel transfer system
- FHM
- New fuel elevator
- Long-handled tooling

The refuelling cavity and the fuel storage area are connected by the fuel transfer tube, which is fitted with a quick-opening hatch on the refuelling cavity end and a valve on the fuel storage area end. The hatch is in place except during refuelling to provide containment integrity. Fuel is carried through the tube on an underwater transfer car.

Fuel is moved between the RV and the fuel transfer system by the RM. The fuel transfer system is used to move a fuel assembly and its associated core component between the containment building and the auxiliary building fuel handling area. After a fuel assembly is placed in the fuel container, the lifting arm pivots the fuel assembly to the horizontal position for passage through the fuel transfer tube. After the transfer car transports the fuel assembly through the transfer tube, the lifting arm at that end of the tube pivots the assembly to a vertical position so that the assembly can be lifted out of the fuel container.

In the fuel handling area, fuel assemblies are moved about by the FHM. Initially, a short tool is used to handle new fuel assemblies, but the new fuel elevator must be used to lower the assembly to a depth at which the FHM and associated long-handled tool can place the new fuel assemblies into or remove them from the spent fuel storage racks. Additional design detail of this system and its constituent components are delineated in Reference 6.49.

6.12.6 Treatment of Radioactive Waste

The management of radioactive waste, which may be gaseous, liquid, or solid, spans all the stages in the life cycle of the AP1000 plant. Further details of the radioactive waste management arrangements can be found in Chapter 26.

Management of radwaste is being planned with the expectation that the LLW, ILW, and spent fuel waste streams will be capable of being disposed of at Nuclear Decommissioning Authority (NDA) facilities. Waste forms and treatment processes have been selected with this principle in mind and containers compliant with the Radioactive Waste Management (RWM) have been designated (Reference 6.7).

Waste will be categorised for treatment as conventional or radioactive. Radioactive material will be categorised as LLW, ILW, or high-level waste (HLW). Solid waste will be characterised and segregated using equipment discussed in the Environment Report (Reference 6.7, subsection 3.5.7) and the Westinghouse integrated waste strategy (IWS) (Chapter 26 in this PCSR).

6.12.6.1 Disposal of Spent Fuel and Intermediate-Level Waste

Spent Fuel

The spent fuel assemblies are initially stored in the spent fuel cooling pool to allow radioactive decay to occur and decay heat to be removed before they are transferred to dry cask storage (Reference 6.7). See Section 26 for further detail on spent fuel.

Rod Cluster Control Assemblies, Neutron Source Assemblies and Poison Rod Assemblies

The RCCAs, identified as “control rod clusters” in the estimates for operational wastes, include 53 assemblies assumed to be replaced once per 20 years. There are also 16 grey rod assemblies that are redundant and also assumed to be replaced once per 20 years. The control rod clusters and grey rod assemblies are disposed of within the spent fuel assemblies.

There are two primary and two secondary neutron source assemblies. The primary sources are used once during the first cycle then disposed of as waste within a spent fuel assembly. The secondary source assemblies are assumed to be replaced once every 20 years for the purpose of estimating waste. They are also disposed of within a spent fuel assembly.

The poison rod assemblies are used in the first core and only then disposed of as waste. There are 72 poison rod assemblies, to be disposed of within spent fuel assemblies.

6.12.6.2 Disposal of Low-Level Waste and Intermediate-Level Waste

The disposability of LLW raises fewer issues than that of ILW and spent fuel. Westinghouse has sought assurance from LLW Repository Limited (LLWR) that the expected LLW streams will be available.

LLW will be temporarily stored in a buffer or marshalling area within the radwaste building until required for sorting (Reference 6.7). The package waste storage room is used to store LLW for which processing has been deferred and a period of decay will provide handling benefits, e.g., dose reduction (see Chapter 26 of this PCSR).

Solid ILW will be encapsulated on a campaign basis when a sufficient volume of waste is available to complete an encapsulation run (typically coinciding with refuelling outages that occur after 18 months operation) (see Chapter 26 of this PCSR).

6.12.6.3 Treatment of Large Solid Items of Radioactive Waste: Steam Generators and Reactor Pressure Vessel Head

No large solid radioactive waste items are expected to be generated during normal operation of the AP1000 plant. Nevertheless, there may be a need to replace SGs or the RPV head during the lifetime of the plant, which will be managed in accordance with the licensee's management arrangements at the time of disposal.

6.12.7 Gaseous Radwaste System

The WGS is designed to perform the following major functions:

- Collect gaseous wastes that are radioactive or hydrogen-bearing.
- Process and discharge the waste gas, keeping offsite releases of radioactivity within acceptable limits.

The WGS is a once-through ambient-temperature-activated carbon delay system that collects and processes gaseous wastes originating from the RCS that are radioactive to prevent an uncontrolled atmospheric release. The system includes a gas cooler, a moisture separator, an activated carbon-filled guard bed, and two activated carbon-filled delay beds. The system also includes an oxygen analyser and a gas sampler.

The WGS is designed to receive radioactive gases generated during operation. The radioactive gas flowing into the WGS enters as trace contamination in a stream of hydrogen and nitrogen. The incoming gas first passes through a gas cooler. Moisture formed due to gas cooling is removed in the moisture separator. The waste gas then flows through the guard bed, where iodine and chemical (oxidising) contaminants are removed. The guard bed also removes any remaining excessive moisture from the waste gas. The waste gas then flows through the two delay beds, where xenon and krypton are delayed by a dynamic adsorption process. Additional design detail of this system and its constituent components are delineated in Reference 6.25.

Inputs to the WGS are the following:

- **WLS degasifier** − The degasifier extracts both hydrogen and fission gases from the CVS letdown flow or from the reactor coolant drain tank discharge. The liquid from the degasifier is routed to the WLS.
- **Reactor coolant drain tank** − Hydrogen dissolved in the influent to the reactor coolant drain tank enters the WGS via either the reactor coolant drain tank (RCDT) vent or the WLS degasifier discharge as noted above.

6.12.8 Liquid Radwaste System

The WLS is designed to collect, process, store, and dispose of liquid radioactive waste generated as the result of normal operation, including anticipated operational occurrences such as RCS-level reduction for refuelling. Nonradioactive secondary system waste water is not processed by the WLS. However, if significant radioactivity is detected in secondary-side systems, the SG blowdown or a portion of the blowdown may be diverted to the WLS for processing and disposal. Additional design detail of this system and its constituent components are delineated in Reference 6.24.

The WLS includes tanks, pumps, ion exchangers, and filters. The WLS is designed to either process radioactively contaminated liquid waste or to store it for processing by mobile equipment. The liquid waste is divided into four major categories:

- Borated reactor-grade waste water collected from the RCS effluents received through the CVS, the PSS sink drains, and equipment leakoffs and drains.

- Floor drains and other wastes with potentially high suspended solids content, collected from various building floor drains and sumps.

- Detergent wastes collected from the plant hot sinks and showers and some cleanup and decontamination processes. Such waste generally has low concentrations of radioactivity.

- Chemical waste collected from the laboratory and other relatively small volume sources. This could be a mixture of hazardous and radioactive wastes, or other radioactive wastes with high dissolved solids content.

The liquid waste streams are summarised in this section.

The WLS has effluent holdup tanks that contain the liquid waste prior to processing. They primarily receive borated and hydrogen-bearing liquid from two sources: the reactor coolant drain tank and the CVS letdown. The reactor coolant drain tank collects leakage and drainage from various primary systems and components inside the containment. Effluent from the CVS (letdown) is produced mainly as a result of RCS heatup, boron concentration changes, and RCS-level reduction for refuelling. Input collected by the effluent system normally contains hydrogen and dissolved radioactive gases. Therefore, it is routed through the WLS vacuum degasifier before being stored in the effluent holdup tanks. The contents of these tanks may be recirculated and sampled, recycled through the degasifier for further gas stripping, returned to the RCS by way of the CVS makeup pumps, processed through the WLS ion exchangers and directed to the monitor tanks for discharge, or discharged to the mobile treatment facility,.

The WLS in the AP1000 plant first filters the incoming liquid, which then enters four ion exchange resin vessels in series. Any of these vessels can be manually bypassed, and the order of the last two can be interchanged so as to provide complete usage of the ion exchange resin. The top of the first vessel is normally charged with activated carbon to act as a deep-bed filter and to remove oil from floor drain wastes. Moderate amounts of other wastes can also be routed through this vessel. It can be bypassed for processing relatively clean waste streams. This vessel is somewhat larger than the other three, with an extra sluice connection to allow removal of the top bed of activated carbon. This feature is associated with the deep-bed filter function of the vessel; the top layer of activated carbon collects organic material, and the ability to remove it without disturbing the underlying zeolite bed

minimises solid waste production. The second, third, and fourth beds are in identical ion exchange vessels, which are selectively loaded with resin, depending on prevailing plant conditions.

After deionisation, the water passes through an after-filter, where any remaining radioactive particulates and resin fines are removed. The processed water then enters one of the monitor tanks. When a monitor tank is full, the system automatically realigns to route the processed water to another monitor tank.

6.12.9 Solid Waste Management System

The solid waste management system (WSS) is designed to collect and accumulate spent ion exchange resins and deep-bed filtration media, spent filter cartridges, dry active wastes, and mixed wastes generated as a result of normal plant operation, including anticipated operational occurrences. The system is located in the auxiliary building and the radwaste building. Additional design detail of this system and its constituent components are delineated in Reference 6.23.

6.12.10 Radioactive Waste Drain System

The WRS collects radioactive liquid wastes from equipment and floor drainage of the radioactive portions of the auxiliary building, annex building, and radwaste building, and directs these wastes to a centrally located sump located in the auxiliary building. The contents of the sump are pumped to the WLS tanks. Additional design detail of this system and its constituent components are delineated in Reference 6.38.

6.12.11 Waste Storage

In addition to the nuclear island and non-nuclear island buildings, there are facilities for the storage of solid LLW, ILW, and HLW generated during AP1000 plant operation. These facilities are described in the sections below.

The solid waste management facilities allow an operator to manage waste according to the waste management hierarchy. Much of the GDA information in the UK AP1000 Environment Report (Reference 6.7) provides a licensee with the basis to begin developing waste avoidance, minimisation, and reuse/recycle plans and procedures.

6.12.11.1 Low-Level Waste Storage

The LLW store is located within the boundary of the licensed site (Reference 6.7). The radwaste building holds monitoring tanks containing processed effluent awaiting clearance for release to the environment or further processing if necessary.

LLW is bagged, collected manually, and transported to areas of the waste accumulation room. The waste is packaged in suitable licensed containers, transported to the buffer store, and finally sent offsite for final disposal (Reference 6.7). The transportation of the waste will take into consideration safety procedures, which are discussed in more detail in Reference 6.7.

Design Structure

The radwaste building is a non-nuclear seismic building with lockable doors to minimise unauthorised entry and inadvertent exposure. It is categorised as a non-nuclear seismic (NNS) structure and contains no Class 1 equipment but is designed for wind and seismic loads.

The LLW buffer store is a covered area comprising a concrete hard-standing area with a steel-framed canopy (see Chapter 26 of this PCSR).

Transfer, Inspection, Maintenance and Periodic Testing of Waste packages

The Environment Report (Reference 6.7) describes briefly how the waste packages are handled in the LLW store, giving consideration to the radiation protection, environment, and safety aspects. One example of the safety procedures is that LLW will be sorted under controlled conditions through the use of glove boxes.

Instruments monitor and control the process variables associated with LLW processing. This includes radiometric measurements within LLW handling equipment and general area monitoring. This is discussed in Chapter 26 of this PCSR.

Chapter 26 of this PCSR presents the analytical techniques available and related sample requirements for the LLW wastes to ensure that compliance with the site discharge criteria can be demonstrated. The same report refers to the use of the low-resolution gamma spectroscopy (LRGS) assay when the LLW is drummed in the radwaste building. Once drums have completed quality assurance (QA), they are placed in a suitable licensed container within the radwaste building.

Package Type

The waste package used for LLW is one currently accepted by the LLWR. As such, it has been designed to comply with the current requirements for handling, retrieval, transport, storage, and disposal. More information may be found in Chapter 26 and Reference 6.7.

6.12.11.2 Intermediate-Level Waste Storage

ILW is stored within suitable contamination-zoned and shielded areas of the auxiliary building prior to treatment in the mobile encapsulation plant (MEU). The MEU is described in Chapter 26 and other sections of this PCSR where maintenance, control console, shielding, ventilation, safety, seismic qualification, and waste tracking system are discussed. Once the ILW is encapsulated in RWM waste packages, the boxes and drums will be transported to an onsite ILW store where they will be stored until a national ILW repository becomes available. The transportation of the waste will consider safety procedures that are discussed in more detail in Reference 6.7 and Chapter 26.

The first phase of construction will provide an ILW store suitable for 20 years of ILW production. The ILW store will be designed with a reserve-storage capacity for a total inventory of 60 years of operational waste arisings from one AP1000 plant unit. The ILW store has a 100-year design life and could be used to retain ILW after the AP1000 plant is decommissioned and until the national ILW repository becomes available (Reference 6.7 and Chapter 26).

Design Structure

The ILW store is a reinforced concrete structure (Reference 6.7), consisting of a waste package reception area and a shielded vault serviced by a certified nuclear crane. A seismic assessment for the ILW store has been carried out and the results are summarised in Chapter 26. The seismic assessment has determined that the AP1000 plant ILW store does not need to be seismically qualified from a radiological consequence perspective (Chapter 26).

In-store and encapsulation equipment will be modular and components will be regularly or routinely replaced rather than being designed for the full 100-year storage period. All components subject to wear are located in a way that will allow easy access, removal, and replacement with minimum disturbance to adjacent components (Chapter 26).

Control System

The implementation requirements for the standard security systems for the ILW store will be determined during the detailed design associated with the specific site (Chapter 26).

The ILW store will have a dedicated control console. More details on the operating modes (normal and manual modes; and recovery mode, intended to be used following equipment failure) can be found in the Radioactive Waste Arisings, Management and Disposal report (Chapter 26). The primary control positions for controlling process operations will typically be local to the process and will be provided (where possible) with a direct view of the main operations, supported by closed circuit television (CCTV) where appropriate. The CCTV cameras are described in Chapter 26.

The operators in the control room will be suitably shielded from both packages in the vault and the import/export area (Chapter 26).

Environmental Conditions

The Radioactive Waste Arisings, Management and Disposal report (Chapter 26) shows the intention and the importance of controlling the store environment conditions. The operational limits and conditions, such as surface chloride contamination values, are presented in this section, while temperature is covered in Chapter 26.

Transfer, Inspection, Maintenance, and Periodic Testing of Waste Packages

The ILW store is a reinforced concrete structure (Reference 6.7), consisting of a waste package reception area and a shielded vault serviced by a certified nuclear crane. The ILW storage requirements and procedures to ensure safety, radiation protection, transportability, stock control, and ability to retrieve waste packages are discussed in the Environment Report (Reference 6.7). Some of these topics are also covered in the Radioactive Waste Arisings, Management and Disposal report (Chapter 26). The proposed operation tasks for the encapsulation plant, considering all these concepts, are in Chapter 26.

Instruments monitor and control the process variables associated with ILW processing. These include radiometric measurements within the ILW import/export equipment and general area monitoring. This is discussed in Chapter 26, which presents the analytical technique available and related sample requirements for the ILW wastes to ensure that compliance with the site discharge criteria can be demonstrated.

Reference 6.7 discusses how the design and proposed operation of the ILW store will enable retrieval and visual examination of individual packages. This report states that activity level of ILW waste packages will be monitored before they are transferred to the ILW store vault and before they are sent to the repository. It also describes the remedial action strategy for ILW packages when defects or external damage are found (further described in the Waste Arisings, Management and Disposal report (Chapter 26)).

Package Type

ILW packages will comply with the requirements for handling, retrieval, transport, storage, and disposal. The in-store and encapsulation equipment, such as MEU, 4-drum stillages, and the nuclear crane, will be suitable to engage and handle these RWM waste packages (Chapter 26).

6.12.11.3 HLW storage

After spent fuel is removed from the reactor, it will be stored in the fuel storage pool. Details about the fuel storage pool can be found in subsection 6.12.3.

Because spent fuel is not expected to be reprocessed, HI-STORM 100U system has been proposed to be used to dry-store the spent fuel once it has been removed from the storage pool for the operational period of the plant and beyond. In Reference 6.7, subsection 3.5.8.3 and Figure 3.5-17, the dry-storage features of the HI-STORM 100U System and its components is shown in more detail. Once the spent fuel assemblies have reached the acceptable limits for heat generation (typically 100 years), they will be transported from their dry cask storage to the national geological disposal facility (GDF) when it is available.

The NDA has completed a disposability assessment of AP1000 plant spent fuel to satisfy the GDA requirements. This assessment concluded that the characteristics of spent fuel from an AP1000 plant (with 65-MWd/tonne U burnup) are consistent with those from the Sizewell B PWR and that compared with legacy wastes, no new issues arise that challenge the fundamental disposability of the wastes expected to arise from operation of such a reactor. This assessment has also assumed that spent fuel would be overpacked for disposal. The exact long-term disposal canister material and design remains to be confirmed (Reference 6.7).

Uncertainties remain surrounding the treatment of spent fuel, which is discussed in more detail in subsection 26.7.5.3.

Design Structure

The dry spent fuel storage is a seismically qualified below-ground dry-storage facility (Reference 6.7). The Environment Report (Reference 6.7) indicates the design features that are considered to minimise unauthorised intrusion and to provide radiation shielding for the spent fuel cooling pool and dry spent fuel storage.

Transfer, Inspection, Maintenance, and Periodic Testing of Waste Packages

Spent fuel handling and storage are described in the Environment Report (Reference 6.7). The handling equipment, which takes into account radiation protection aspects, ease of maintenance, and minimisation of the probability and consequences of associated incidents and accidents, is an example of how human intervention and maintenance could be minimised.

Package Type

The decision on how to package spent fuel for storage will be made by a future licensee. Available information at this time is discussed in Chapter 26.

6.12.12 Radwaste Management Strategy

The strategy for managing radioactive waste onsite is described in detail in Chapter 26. It includes an IWS based on the expected waste and spent fuel generation and management practices throughout the AP1000 plant life cycle.

Aspects of waste minimisation, continued safe storage, acceptance criteria, and record keeping are presented in detail in Chapter 26.

6.13 CIVIL STRUCTURES

6.13.1 Introduction

The AP1000 plant consists of the following five principal structures. Each building is constructed on an individual basemat:

- Nuclear island
- Turbine building
- Annex building
- Diesel generator building
- Radwaste building

The structures that make up the nuclear island are as follows:

- Containment vessel
- Shield building
- Auxiliary building

These nuclear island buildings are depicted on the site plan. The Class 1 equipment designed to deliver Category A functions is located in the nuclear island.

6.13.2 Site Layout and Civil Structures

A site plan will be defined in the site-specific licensing process by the licencee. A generic proposed plan has been provided for site interface purposes and is shown in this section with a generic description of the plant arrangement. Site-specific features of the overall site layout are those features outside the standard plant arrangement. Specific details of the site plan will be covered in the utility site application.

6.13.2.1 Plant Arrangement

The standard plant arrangement consists of the following five principal building structures:

- Nuclear island which includes the following structures:
  - Containment Vessel
  - Shield Building
  - Auxiliary Building

- Turbine building
- Annex building
- Diesel generator building
- Radwaste building

The turbine, annex, diesel generator, and radwaste buildings contain no equipment that is essential to nuclear safety, therefore their hazard-withstand requirement is less rigorous than that for the nuclear island.

These building structures are laid out so that the turbine building and the other principal buildings are adjacent to the nuclear island to meet their functional requirement. Figure 6-7 provides a functional representation of the principal systems and components located in each of the key AP1000 plant buildings. This figure identifies major systems and components that are contained in these structures.

The circulating water system (CWS) is site-specific and circulates cooling water to the main condenser and back to the heat sink through supply and return pipes that are below ground. Supply to the CWS will depend on the specific site requirements. Cooling for the CWS can be from either seawater cooling or cooling towers. The preferred design for the UK is to use seawater cooling as described in the Environmental Report. However, the supporting secondary systems design reflected in the PCSR assume the use of CWS cooling towers.

The transformer area is located immediately adjacent to the turbine building. The unit auxiliary transformers, the reserve auxiliary transformers, and the main step-up transformers are located in the transformer area. The main switchyard area and the rail and road access to the site are site-specific. Figure 6-8 shows the typical plant layout.

6.13.2.2 Plant Arrangement Considerations

Radioactive equipment and piping in all buildings are arranged and shielded to minimise radiation exposure. The overall plant arrangement utilises building configurations and structural designs to minimise the building volumes and quantities of bulk materials (concrete, structural steel, and rebar) consistent with safety, operational, maintenance, and structural needs.

SSCs essential to maintaining nuclear safety are contained in the nuclear island. Separation between redundant essential Class 1 equipment and systems ensures that the safety functions can be performed. In general, this separation is provided by partitioning areas with concrete walls. The auxiliary building arrangement provides separation for radioactive and nonradioactive equipment and provides separate pathways to these areas for personnel access. Pathways through the plant are designed to accommodate equipment maintenance and removal from within the plant. Adequate space is provided for equipment maintenance, laydown, removal, and inspection. Hatches, monorails, hoists, and removable shield walls are provided to facilitate maintenance.

6.13.2.3 Nuclear Island

The nuclear island structures are designed to withstand the effects of natural phenomena such as earthquakes and extreme weather, and internal events such as fires and flooding, without losing the capability to perform their safety functions.

The nuclear island structures include the containment (the steel containment vessel and the containment internal structures) and the shield and auxiliary buildings. The containment and the shield and auxiliary buildings are structurally integrated on a common base mat.

Containment Building

The containment building comprises the containment vessel and the structures contained within it. The containment building is designed to house the reactor vessel and core, and the following other related major systems and equipment:

- Reactor coolant system
  - Loop piping
  - Two steam generators
  - Four reactor coolant pumps
  - Pressuriser
  - Automatic depressurisation system
- Passive core cooling system
  - IRWST
  - Passive residual heat removal heat exchanger
  - Two core makeup tanks
  - Two accumulators
- Pipes and valves between the RCS and the RNS
- Purification portion of the CVS
- Inside containment isolation valves
- Polar crane

Shield Building

The shield building surrounds the containment building and supports the PCS storage tank and its associated piping and valves and its own dedicated HVAC system. Additionally the shield building provides missile protection for containment and the PCS air flow path.

Auxiliary Building

The auxiliary building consists of two separated portions: the radiological portion and the non-radiological portion.

The radiological portion of the auxiliary building houses SSCs associated with auxiliary functions involved with radioactive material; it has been designed to meet the nuclear safety functions associated with handling these materials and with the contained systems and functions. In addition, this portion contains DAS processor cabinets. The SSCs within this building are as follows:

- RNS pumps and its HXs
- CVS makeup pump
- Containment isolation valves (outside)
- Spent fuel storage pool and its cooling system, the fuel transfer canal, the cask washdown pit, and the cask-loading pit
- New fuel storage pit and the rail car bay/filter storage area

- Liquid radwaste system (except for monitor tanks in the radwaste building, and discharge piping)
- Gaseous radwaste system
- Solid radwaste system (wet process waste handling equipment)
- MCR emergency habitability system air storage cylinders (although these air cylinders are housed in the radiological auxiliary building, they are included in the containment/shield building fire area)
- DAS processor cabinets

The non-radiological portion of the Auxiliary Building houses SSCs associated with the plant MCR, C&I, the passive DC electrical supplies, and auxiliary functions that do not directly involve radioactive material. The SSCs within this building are as follows:

- Feed and steam mains, the steam isolation valves, the feed isolation valves, the steam generator blowdown lines and isolation valves, and the SG power-operated relief valves and steam safety valves
- Four divisions of the IDS batteries and associated equipment; e.g., chargers; and switchgear
- Four divisions of the PMS, four electrical equipment rooms, and four C&I rooms. Divisions A, B, C, and D of the PMS are segregated between these rooms and compartments.
- MCR
- RCP trip switchgear
- Reactor trip switchgear
- Remote shutdown room
- VBS components
- VWS (chillers outside on building roof)

6.13.2.4 Turbine Building

The Turbine Building houses the Main Turbine, Generator, and associated fluid and electrical systems. It provides weather protection for the laydown and maintenance of major turbine/ generator components. The principal systems and equipment are as follows:

- Two CCS pumps and heat exchangers
- BDS piping, valves, and equipment
- Turbine generator and its auxiliaries
- Main Condenser
- MSS piping and valves
- Moisture separator reheaters
- Low-pressure feed heaters, deaerator, and high-pressure feed heaters

- Three condensate pumps
- Three main feedwater pumps
- Two startup feedwater pumps
- Switchgear rooms
- Electrical equipment room
- Lube oil storage tanks
- Motor-driven fire pump
- Air compressors
- Backup batteries and battery-charging equipment
- Condensate chemical dosing equipment
- Various tanks for storing chemicals
- Component cooling water pumps, HXs, and associated piping, valves
- SWS strainers and piping and valves
- Four RCP variable-speed drives
- VTS
- SSS
- VWS chillers
- CWS piping and valves
- TCS pump, HXs, piping and valves

6.13.2.5 Annex Building

The annex building provides the main personnel entrance to the power generation complex. It includes access ways for personnel and equipment to the clean areas of the nuclear island in the auxiliary building and to the radiologically controlled area. The building includes the health physics facilities for the control of entry to and exit from the radiologically controlled area, as well as personnel support facilities such as locker rooms. The building also contains the non-Class 1 ac and dc electrical power systems, other electrical equipment, the control support area and various HVAC systems. In addition, the annex building contains the ancillary diesel generators and their fuel supply.

The annex building also contains the following equipment:

- Demineralised water deoxygenating equipment
- Boric acid batching equipment
- Air intake plenum for the radiologically controlled area ventilation system and the containment air filtration system
- Exhaust air filtration units from the containment air filtration system
- Ancillary diesel generators and day tank
- EDS batteries and switchgear
- Machine shops
- Control support area (CSA)

6.13.2.6 Diesel Generator Building

The diesel generator building houses two, segregated, standby diesel generators and their associated electrical, HVAC, and limited fuel oil supply equipment. The two standby diesel generators supply power to priority defence in depth (Class 2) loads in the event of loss-of-normal power from the offsite and onsite ac power sources. Only one operating ZOS standby diesel generator is needed to fulfil this defence in depth duty (further details on this requirement can be found in Chapter 18).

The standby diesel generators are supplied from individual day tanks that are in turn supplied from two, segregated, above-ground bulk fuel oil storage tanks, one for each diesel generator. Each tank has sufficient fuel to supply its diesel generator for 7 days of operation at the maximum continuous rating. These bulk tanks are remote from the diesel generator and any other AP1000 plant buildings.

6.13.2.7 Radwaste Building

The radwaste building includes facilities for segregated storage of various relatively low-level categories of waste prior to processing, and for storing processed waste in shipping and disposal containers.

The liquid radwaste processing areas are designed to contain any liquid spills, including a raised perimeter and floor drains that lead to the liquid radwaste system waste holdup tanks in the auxiliary building.

The radwaste building consists of the following:

- Various radwaste processing and packaging operations
- A waste accumulation room
- A packaged waste storage room
- Two liquid radwaste system monitor tank rooms
- A truck staging area
- An HVAC equipment room
- An electrical and mechanical equipment room

6.13.3 Containment

6.13.3.1 Building Function

The containment building is the containment vessel and the structures contained within it. The containment building is an integral part of the overall containment system with the functions of containing the release of airborne radioactivity following postulated DBAs and providing shielding for the reactor core and the RCS during normal operations.

The containment vessel is an integral part of the PCS. The containment vessel, shield building structures, and the PCS are designed to remove sufficient energy from the containment to prevent the containment from exceeding its design pressure following postulated DBAs.

The containment building is designed to house the RCS and other related systems and provides a low leakage barrier.

6.13.3.2 Civil/Structural Features

The containment vessel, a C-I structure (see Chapter 16, Table 16.1), is a freestanding cylindrical steel containment vessel with elliptical upper and lower heads. It is surrounded by a C-I shield building.

There are three floor elevations (grade access, maintenance floor, and operating deck) and four lower equipment compartments within the containment building. Removable hatches are provided for access to equipment at other elevations.

The IRWST is located below the operating deck. Its capacity exceeds the quantity of water required to accomplish safety functions or to fill the refuelling cavity during refuelling operations. The refuelling cavity has several floor elevations. The upper and lower reactor internals storage area and the fuel transfer tube are at the lower elevation. See Appendix 20K for more detail on the structural integrity of the containment vessel.

6.13.4 Shield Building

6.13.4.1 Building Function

The shield building is the structure that surrounds the containment vessel. During normal operations, a primary function of the shield building is to provide shielding for the containment vessel and the radioactive systems and components located in the containment building. The shield building, in conjunction with the internal structures of the containment building, provides the required shielding for the RCS and the other radioactive systems and components housed in the containment.

The shield building protects containment from external events. The shield building protects the containment vessel and the RCS from the effects of tornadoes and tornado-produced missiles.

During accident conditions, the shield building provides the required shielding for radioactive airborne materials that may be dispersed in the containment as well as radioactive particles in the water distributed throughout the containment.

The shield building is an integral part of the PCS.

6.13.4.2 Civil/Structural Features

The shield building is a C-I structure (Chapter 16, Table 16.1). It shares a common basemat with the containment building and the auxiliary building.

Figure 20D-1, provides a sectional view of the shield building. The view show the basic configuration of the shield building and the annulus area between the containment vessel and the shield building.

The following items represent the main features of the shield building and the annulus area:

- Shield building cylindrical structure
- Shield building roof structure
- Lower annulus area
- Middle annulus area
- Upper annulus area

- PCS air inlet
- PCS air inlet plenum
- PCS water storage tank
- PCS air exhaust
- PCS air baffle

The cylindrical section of the shield building serves as shielding and a missile barrier and is a key component of the PCS. It structurally supports the roof and is a major structural member for the entire nuclear island.

A watertight seal is provided between the upper and middle annulus areas to provide an environmental barrier. The middle annulus area contains the majority of containment penetrations and radioactive piping. This environmental barrier is provided to protect against the following:

- Since the upper annulus is open to the environment, the barrier protects the middle annulus from precipitation and environmental temperatures.

- In the event of an accident or spurious actuation, water from the PCS water storage tank drains by gravity onto the containment vessel outer surface. The water, which runs down the outside of the containment vessel, is prevented from draining into the middle annulus area by the watertight seal. Drains are provided to direct the PCS runoff water out of the shield building.

- The PCS is designed to perform with the upper annulus permanently open to the environment to permit sufficient airflow through the shield building in the event of an accident. The watertight seal protects the middle annulus area from ambient environmental conditions.

The shield building roof is a reinforced concrete conical shell supporting the PCS water storage tank and air exhaust. Air intakes are located at the top of the cylindrical portion of the shield building. The conical roof supports the PCS water storage tank, which is constructed with a stainless-steel liner attached to reinforced concrete walls. The PCS air exhaust in the centre of the roof discharges containment cooling air directly upwards.

The PCS air baffle is located in the upper annulus area. It is attached to the cylindrical section of the containment vessel. The function of the PCS air baffle is to provide a pathway for natural circulation of cooling air in the event that a DBA results in a large release of energy into the containment. In this event, the outer surface of the containment vessel transfers heat and mass (water vapour) to the air between the baffle and the containment shell. This heated and higher humidity and thus lower-density air flows up through the air baffle to the air exhaust, and cooler and higher-density air is drawn into the shield building through the air inlets at the top cylindrical portion of the shield building.

6.13.5 Auxiliary Building

6.13.5.1 Building Function

The primary function of the auxiliary building is to provide protection and separation for the C-I mechanical and electrical equipment located outside the containment building.

The auxiliary building provides protection for the Class 1 safety equipment against the consequences of either a postulated internal or external event. The auxiliary building also provides shielding for the radioactive equipment and piping housed within the building.

The most significant equipment, systems, and functions contained within the auxiliary building are the following:

- Main Control Room (MCR)
- Class 1 control and instrumentation systems
- Class 1 electrical system
- Fuel handling area
- Mechanical equipment areas
- Containment penetration areas
- Main steam and feedwater isolation valve compartment

6.13.5.2 Civil/Structural Features

The auxiliary building is a C-I, reinforced concrete structure (Chapter 16, Table 16-1). It shares a common basemat with the shield building.

The auxiliary building wraps around approximately 70 percent of the circumference of the shield building. Floor slabs and the structural walls of the auxiliary building are structurally connected to the cylindrical section of the shield building.

6.13.6 Annex Building

6.13.6.1 Building Function

The annex building, shown in Figure 16-2, provides the main personnel entrance to the power generation complex. The building includes the health physics facilities for the control of entry to and exit from the radiological control area as well as personnel support facilities such as locker rooms. The building also contains the standby power supply system, the ECS ancillary diesel generators and their fuel supply, other electrical equipment, the control support area, and various HVAC systems. No Class 1 safety equipment is located in the annex building.

The annex building includes the health physics facilities and provides personnel and equipment accessways to and from the containment building and the rest of the radiological control area via the auxiliary building. Large, direct accessways are provided to the upper and lower equipment hatches of the containment building for personnel access during outages and for the entry and exit of large equipment. The building includes a hot machine shop for servicing radiological control area equipment. The hot machine shop has decontamination facilities including a portable decontamination system that may be used for decontamination operations throughout the nuclear island. The portion of the annex building which is Category II (C-II) is delineated in Figure 6-7.

6.13.6.2 Civil/Structural Features

The seismic designation of the annex building is shown in Chapter 16, Table 16.1. Certain areas of the building, such as the hot machine shop and the control support area, are provided with shielding for protection against low-level radiation from internal or external sources under accident conditions. This is accomplished by either reinforced concrete walls or reinforced masonry walls. The control support area (CSA) is designed so that it may be used as a technical support centre (TSC) if desired.

The annex building is a combination reinforced concrete and steel-framed structure with insulated metal siding. Floor and roof slabs are reinforced concrete supported by metal decking. Floors are designed to act as diaphragms to transmit horizontal loads to sidewall bracing and to concrete shear walls. The building foundation is a reinforced concrete mat.

6.13.7 Diesel Generator Building

6.13.7.1 Building Function

The diesel generator building. shown in Figure 16-2, houses two identical slide-along diesel generators separated by a 3-hour firewall. These generators provide backup power for plant operation in the event of a disruption of normal power sources. No Class 1 equipment is located in the diesel generator building.

6.13.7.2 Civil/Structural Features

The diesel generator building houses the two diesel generators and their associated HVAC equipment, none of which are required for the safe plant shutdown. The seismic designation of the diesel generator building is shown in Chapter 16, Table 16-1. The building is designed in accordance with the Codes specified in Chapter 16.

The building is a single-story, steel-framed structure with insulated metal siding. The roof is composed of a metal deck supporting a concrete slab; it serves as a horizontal diaphragm to transmit lateral loads to sidewall bracing and thereby to the foundation.

The foundation consists of a reinforced concrete mat. The diesel generators are skid-mounted and rest on vibration isolators supported directly from the mat.

6.13.8 Radwaste Building

6.13.8.1 Building Function

The radwaste building includes facilities for segregated storage of various categories of waste prior to processing, for processing by mobile systems and storing processed waste in shipping and disposal containers. No Class 1 equipment is located in the radwaste building.

Dedicated floor areas and trailer parking space for mobile processing systems are provided for the following:

- Contaminated laundry shipping for offsite processing
- Dry-waste processing and packaging
- Hazardous/mixed waste shipping for offsite processing
- Chemical waste treatment
- Empty waste container receiving and storage
- Storage and loading packaged wastes for shipment

The radwaste building also provides temporary storage of other categories of plant wastes. Three liquid waste monitor tanks are located within the radwaste building. These tanks contain processed effluents that are ready for further treatment and/or disposal.

6.13.8.2 Civil/Structural Features

The radwaste building is shown in Figure 16-2. The seismic designation of the radwaste building is shown in Chapter 16, Table 16.1. The liquid radwaste processing areas are designed to contain any liquid spills. These provisions include a raised perimeter and floor drains that lead to the WLS waste holdup tanks. The foundation for the entire building is a reinforced concrete mat on grade.

6.13.9 Turbine Building

6.13.9.1 Building Function

The turbine building houses the main turbine, generator, and associated fluid and electrical systems. It provides weather protection and space for the laydown and maintenance of major turbine, generator, and other components. The turbine building also houses the CCS pumps and HXs, the startup portion of the FWS, and the condensate tank water purification system. There is no Class 1 safety equipment located in the turbine building.

6.13.9.2 Civil/Structure Features

The turbine building (Figures 16-2) consists of two sections: the first bay and the main area, which houses the turbine. The first bay is immediately adjacent to the auxiliary building and consists of reinforced concrete walls and steel framing with reinforced concrete and steel-grated floors. The main area is a steel-framed building with reinforced concrete and steel-grated floors. The first bay and the main area are seismically separated. The turbine building ground floor (structural mat) is a reinforced concrete slab shared by the first bay and main area structure. The seismic designation of the turbine building and first bay is shown in Chapter 16, Table 16-1.

6.14 REFERENCES

6.1 Westinghouse Document WCAP-15775, Rev. 6, “AP1000 I&C Defence-in-Depth and Diversity Report,” December 2014.

6.2 Westinghouse Report UKP-GW-GL-060, Rev. 10, “AP1000 Design Reference Point for UK GDA,” January 2017.

6.3 Not used

6.4 DOE/ID-10541, “Lower Head Integrity Under In-Vessel Steam Explosion Loads,” U.S. Department of Energy, June 1998.

6.5 Westinghouse Document WCAP-16675-P, Rev. 7, and Westinghouse Document WCAP-16675-NP, Rev. 7, “AP1000 Protection and Safety Monitoring System Architecture Technical Report,” August 2015.

6.6 Not used

6.7 Westinghouse Report UKP-GW-GL-790, Rev. 6, “UK AP1000 Environment Report,” January 2017.

6.8 Westinghouse Report UKP-GW-GL-054, Rev. 1, “UK AP1000 Integrated Waste Strategy,” March 2011.

6.9 Westinghouse Report UKP-GW-GL-027, Rev. 2, "UK AP1000 Radioactive Waste Arisings, Management and Disposal," March 2011.

6.10 Westinghouse Report UKP-GW-GL-053, Rev. 1, "UK AP1000 Radwaste Preliminary Safety Statement," February 2010.

6.11 Westinghouse Report UKP-GW-GL-501, Rev. 0, "AP1000® UK Generic Technical Specifications," January 2016.

6.12 Westinghouse Report APP-RXS-M3-001, Rev. 6, "Reactor System (RXS) System Specification Document (SSD)," May 2014.

6.13 Westinghouse Report APP-PXS-M3-001, Rev. 7, "Passive Core Cooling System, System Specification Document," July 2015.

6.14 Westinghouse Report APP-PCS-M3-001, Rev. 8, "Passive Containment Cooling System – System Specification Document," September 2015.

6.15 Westinghouse Report APP-CNS-M3-001, Rev. 4, "Containment System: System Specification Document," August 2015.

6.16 Westinghouse Report APP-VES-M3-001, Rev. 4, "Main Control Room Emergency Habitability System, System Specification Document," November 2014.

6.17 Westinghouse Report APP-SFS-M3-001, Rev. 8, "AP1000® Spent Fuel Pool Cooling System - System Specification Document," March 2016.

6.18 Westinghouse Report APP-CVS-M3-001, Rev. 7, "AP1000® Chemical and Volume Control System (CVS) System Specification Document," October 2015.

6.19 Westinghouse Report APP-RNS-M3-001, Rev. 5, "Normal Residual Heat Removal System – System Specification Document," May 2015.

6.20 Westinghouse Report APP-CCS-M3-001, Rev. 4, "AP1000 Component Cooling Water – System Specification," June 2013.

6.21 Westinghouse Report APP-SWS-M3-001, Rev. 2, "AP1000 Service Water System – System Specification Document," June 2012.

6.22 Not used

6.23 Westinghouse Report APP-WSS-M3-001, Rev. 4, "AP1000® Solid Radwaste System –System Specification," September 2013.

6.24 Westinghouse Report APP-WLS-M3-001, Rev. 7, "AP1000 Plant Liquid Radwaste System – System Specification Document," June 2015.

6.25 Westinghouse Report APP-WGS-M3-001, Rev. 4, "AP1000 Gaseous Radwaste System – System Specification Document," December 2012.

6.26 Westinghouse Report APP-RCS-M3-001, Rev. 8, "Reactor Coolant System, System Specification Document," June 2015.

6.27 Westinghouse Report APP-SGS-M3-001, Rev. 7, "AP1000 Steam Generator System

(SGS) System Specification Document," March 2016.

6.28 Westinghouse Report APP-MSS-M3-001, Rev. 3, "AP1000 Main Steam System Specification Document," June 2012.

6.29 Westinghouse Report APP-MTS-M3-001, Rev. 4, "AP1000 Main Turbine System – System Specification Document," July 2015.

6.30 Westinghouse Report APP-BDS-M3-001, Rev. 8, "Steam Generator Blowdown System – System Specification Document," April 2015.

6.31 Westinghouse Report APP-FWS-M3-001, Rev. 7, "AP1000 Main and Startup Feedwater System – System Specification Document," June 2015.

6.32 Westinghouse Report APP-ASS-M3-001, Rev. 0, "AP1000 Auxiliary Steam Supply System Specification Document," April 2012.

6.32 Westinghouse Report APP-CFS-M3-001, Rev. 1, "Turbine Island Chemical Feed System - System Specification Document," February 2016.

6.33 Westinghouse Report APP-CPS-M3-001, Rev. 0, "Condensate Polishing System (CPS) System Specification Document," May 2011.

6.34 Westinghouse Report APP-VLS-M3-001, Rev. 5, "Containment Hydrogen Control System: System Specification," February 2014.

6.35 Westinghouse Report APP-VUS-M3-001, Rev. 3, "AP1000 Containment Leak Rate Test System - System Specification Document," August 2015.

6.36 Westinghouse Report APP-PSS-M3-001, Rev. 3, "AP1000 Primary Sampling System – System Specification Document," September 2015.

6.37 Westinghouse Report APP-SSS-M3-001, Rev. 2, "Secondary Sampling System (SSS) - System Specification Document," February 2012.

6.38 Westinghouse Report APP-WRS-M3-001, Rev. 6, "AP1000® Radioactive Waste Drain System – System Specification Document," July 2014.

6.39 Westinghouse Report APP-DWS-M3-001, Rev. 1, "Diagram Demineralized Water Transfer and Storage System Specification Document," September 2015.

6.40 Westinghouse Report APP-DTS-M3-001, Rev. 1, "Demineralized Water Treatment System (DTS) System Specification Document," October 2012.

6.41 Westinghouse Report APP-PWS-M3-001, Rev. 1, "AP1000 Potable Water System (PWS) System Specification Document Seismic Category: I," November 2011.

6.42 Westinghouse Report APP-TCS-M3-001, Rev. 0, "Turbine Building Closed Cooling Water System (TCS)," March 2011.

6.43 Westinghouse Report APP-WWS-M3-001, Rev. 3, "Waste Water System - System Specification Document," January 2012.

6.44 Westinghouse Report APP-EFS-E8-001, Rev. 0, "Emergency Preparedness Communication System, System Specification Document," March 2016.

6.45 Westinghouse Report APP-CAS-M3-001, Rev. 2, "AP1000 Compressed and Instrument Air System (CAS) - System Specification Document," October 2015.

6.46 Westinghouse Report APP-PGS-M3-001, Rev. 1, "Plant Gas System (PGS) System Specification Document," January 2012.

6.47 Westinghouse Report APP-SDS-M3-001, Rev. 1, "Sanitary Drainage System (SDS) System Specification Document," December 2011.

6.48 Westinghouse Report APP-DOS-M3-001, Rev. D, "Standby Diesel Fuel Oil System - System Specification Document," May 2008.

6.49 Westinghouse Report APP-FHS-M3-001, Rev. 2, "AP1000 Fuel Handling System - System Specification Document," October 2014.

6.50 Westinghouse Report APP-CDS-M3-001, Rev. 3, "AP1000 Condensate System – System Specification Document," May 2012.

6.51 Westinghouse Report APP-CMS-M3-001, Rev. 1, "Condenser Air Removal System (CMS) System Specification Document," March 2012.

6.52 Westinghouse Report APP-GSS-M3-001, Rev. 3, "AP1000 Gland Seal System - System Specification Document" August 2015.

6.53 Westinghouse Report APP-VWS-M3-001, Rev. C, "Central Chilled Water System - System Specification Document" December 2008.

6.54 Westinghouse Report APP-FPS-M3-001, Rev. 0, "AP1000 Fire Protection System (FPS) – System Specification Document

Table 6-1. AP1000 Plant Parameters

Parameter	Value
Thermal power	3415 MW
Net electrical power	1100 MWe class
Core fuel enrichment	<5%
Coolant	Light water
Number of tubes per SG	10,025
Operating cycle (time between refuelling outages)	18 months
Containment design pressure	4.06 bar (g) (59 psig)
Containment design temperature	149°C (300°F)
Cold leg temperature	281°C (538°F)
Primary circuit design pressure	171 bar (2485 psi)
Primary circuit flow rate (both hot legs)	80,650 m^3/hr @321°C (355,290 gpm@610°F)
Primary circuit operating temperature (hot leg)	321°C (610°F)
Main steam system design pressure	82.7 bar (1200 psi)
Main Feedwater flow per SG	8,233 m^3/hr @ 227 °C (36,248 gpm @ 440°F)

Table 6-2. AP1000 PMS Equipment

PMS Equipment Name
PMS cabinets, division A
PMS cabinets, division B
PMS cabinets, division C
PMS cabinets, division D
Reactor trip switchgear, division A
Reactor trip switchgear, division B
Reactor trip switchgear, division C
Reactor trip switchgear, division D
MCR/RSW transfer panels
MCR Class 1 display, division B
MCR Class 1 display, division C
MCR Class 1 Controls

Table 6-3. PMS Automatic Reactor Trips

PMS Automatic Reactor Trip Signals (See Chapter 19 for a Detailed Summary)	No. of Channels	Division Trip Logic
Source Range High Neutron Flux Reactor Trip	4	2/4
Intermediate Range High Neutron Flux Reactor Trip	4	2/4
Power Range High Neutron Flux (Low Setpoint) Trip	4	2/4
Power Range High Neutron Flux (High Setpoint) Trip	4	2/4
Power Range High Positive Flux Rate Trip	4	2/4
Reactor Coolant Pump High Bearing Water Temperature Trip	16 (4/pump)	2/4 in any single pump
Overtemperature Delta-T Trip	4 (2/loop)	2/4
Overpower Delta-T Trip	4 (2/loop)	2/4
Pressuriser Low Pressure Trip	4	2/4
Pressuriser High Pressure Trip	4	2/4
Pressuriser High Water Level Trip	4	2/4
Low Reactor Coolant Flow Trip	8 (4/hot leg)	2/4 in either hot leg
Low Reactor Coolant Pump Speed Trip	4 (1/pump)	2/4
Low Steam Generator Water Level Trip	4/SG	2/4 in any SG
High Steam Generator Water Level Trip	4/SG	2/4 in any SG
Automatic Safeguards Actuation Trip	4	2/4
Automatic Depressurisation System Actuation Trip	4	2/4
PRHR actuation	4	2/4
Manual Safeguards Actuation Trip	2 controls	1/2 controls
Manual Depressurisation System Actuation Trip	two sets of 2 controls	2/2 of either set
Manual Core Makeup Tank (CMT) Injection Trip	2 controls	1/2 controls
Manual Reactor Trip	2 controls	1/2 controls

Table 6-4. PMS Automatically Actuated ESFs
(See Chapter 19 for Detailed Summary)

Reactor Trip
Safeguards actuation
Containment isolation
ADS Actuation
Main feedwater isolation
RCP trip
CMT actuation
Turbine trip (isolated signal to non-Class 1 safety equipment)
Steam line isolation
Containment Vacuum Relief
SG blowdown isolation
Passive containment cooling actuation
Startup feedwater isolation
PRHR Heat Exchanger actuation
Block of boron dilution
CVS Makeup Isolation
Steam dump block (isolated signal to non-Class 1 safety equipment)
MCR Isolation, Air Supply Initiation, and Electrical Load De-energization
Auxiliary spray and letdown purification line isolation
Containment air filtration system(VFS) isolation
Normal residual heat removal system (RNS) isolation
Refuelling cavity and SFS isolation
IRWST injection
IRWST containment recirculation
CVS letdown isolation
Pressuriser heater Trip (isolated signal to non-Class 1 safety equipment)
Steam Generator Power-Operated Relief Valves (PORV) isolation
Component cooling system containment isolation
Containment vacuum relief

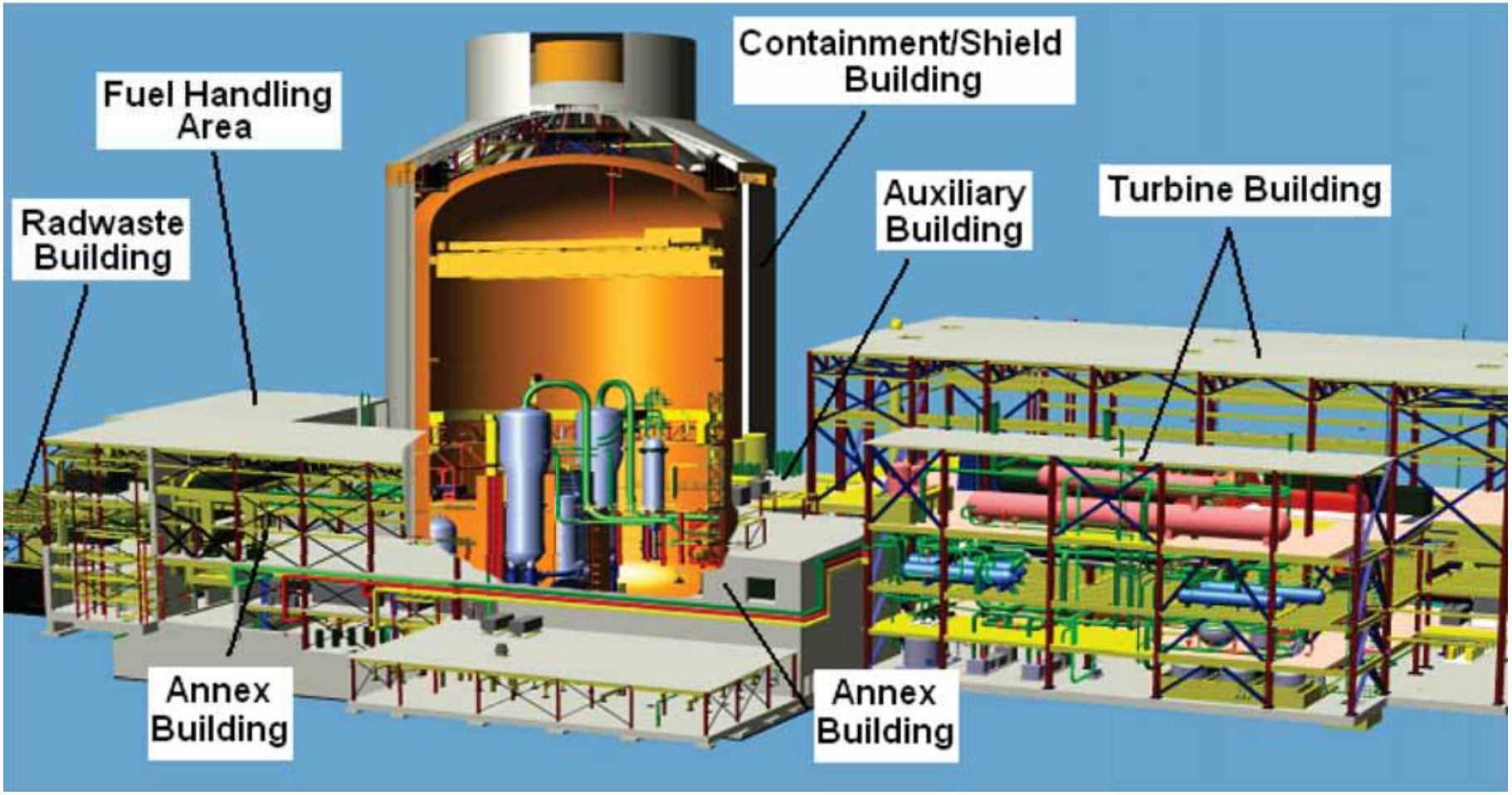


Figure 6-1. Plant Overview

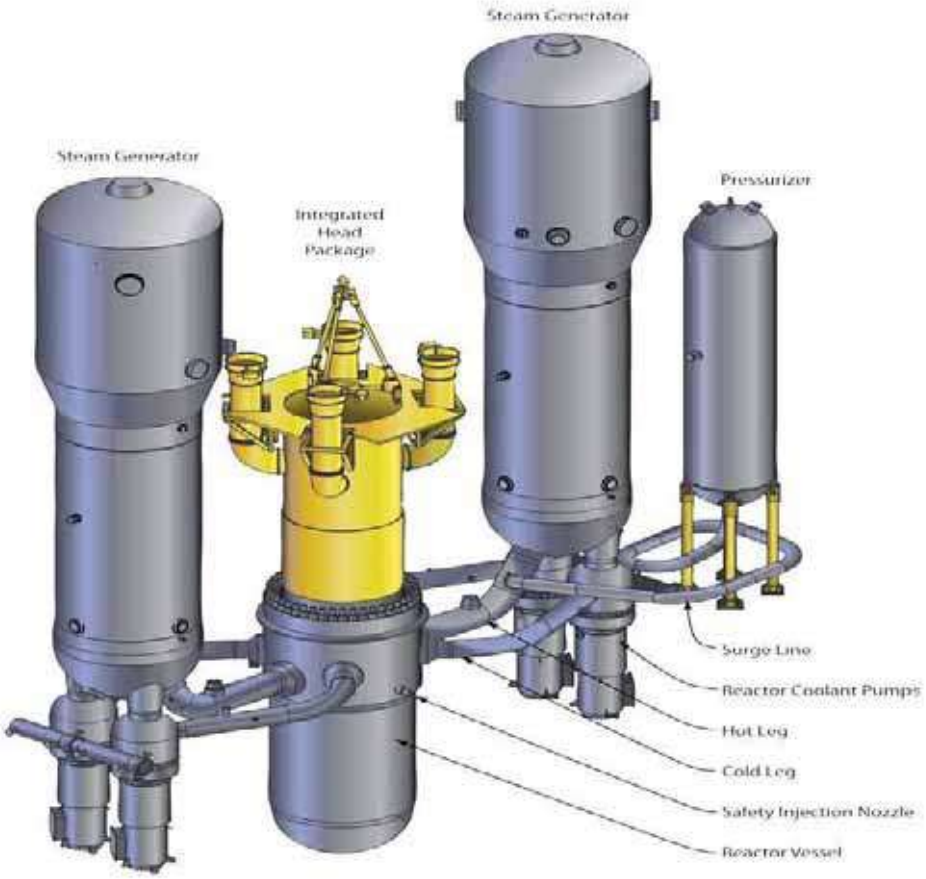


Figure 6-2. Reactor Coolant System

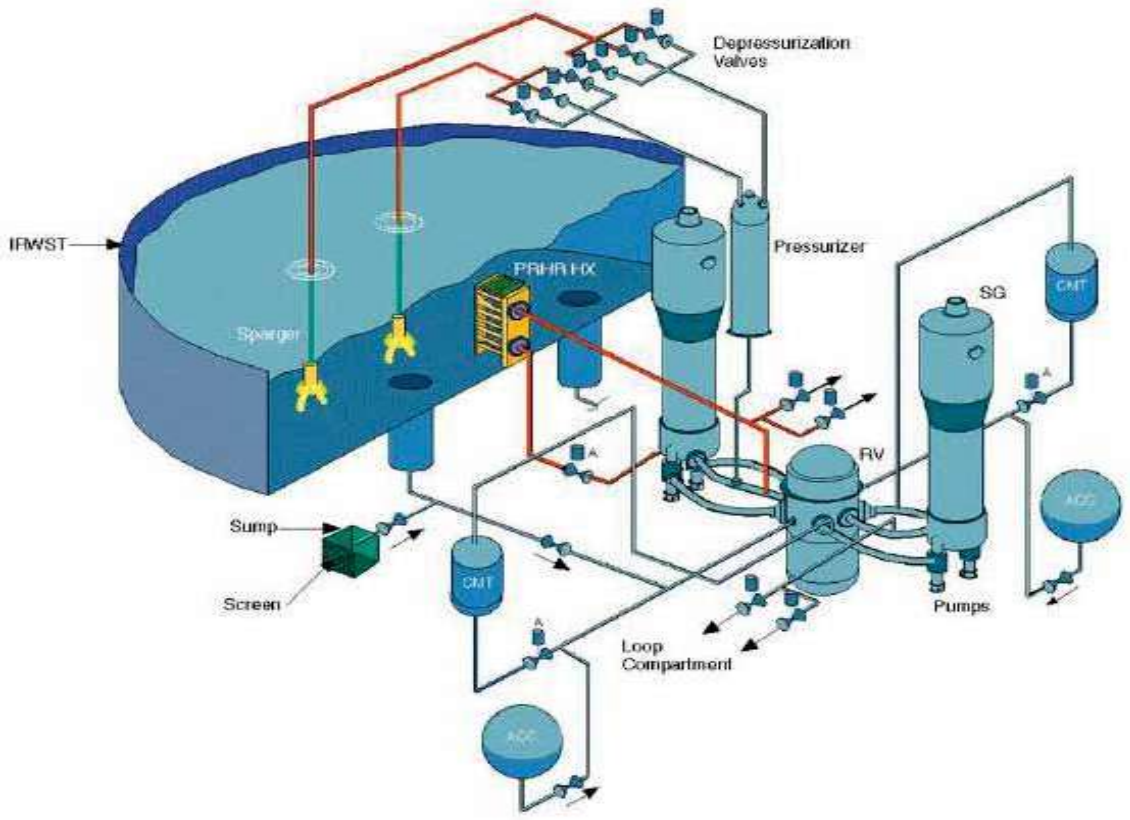


Figure 6-3. Passive Core Cooling System

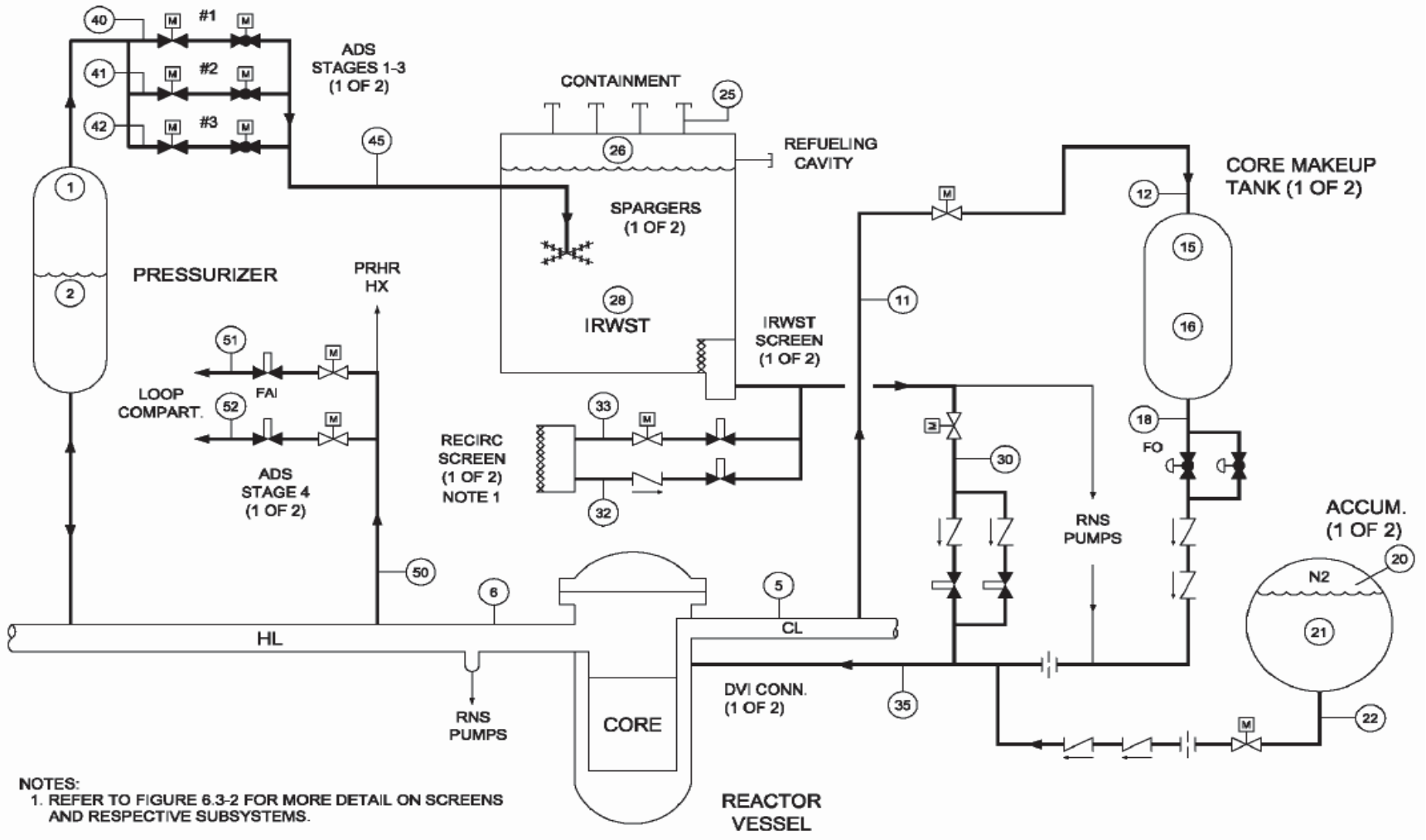


Figure 6-4. Simplified Sketch of Passive Core Cooling System

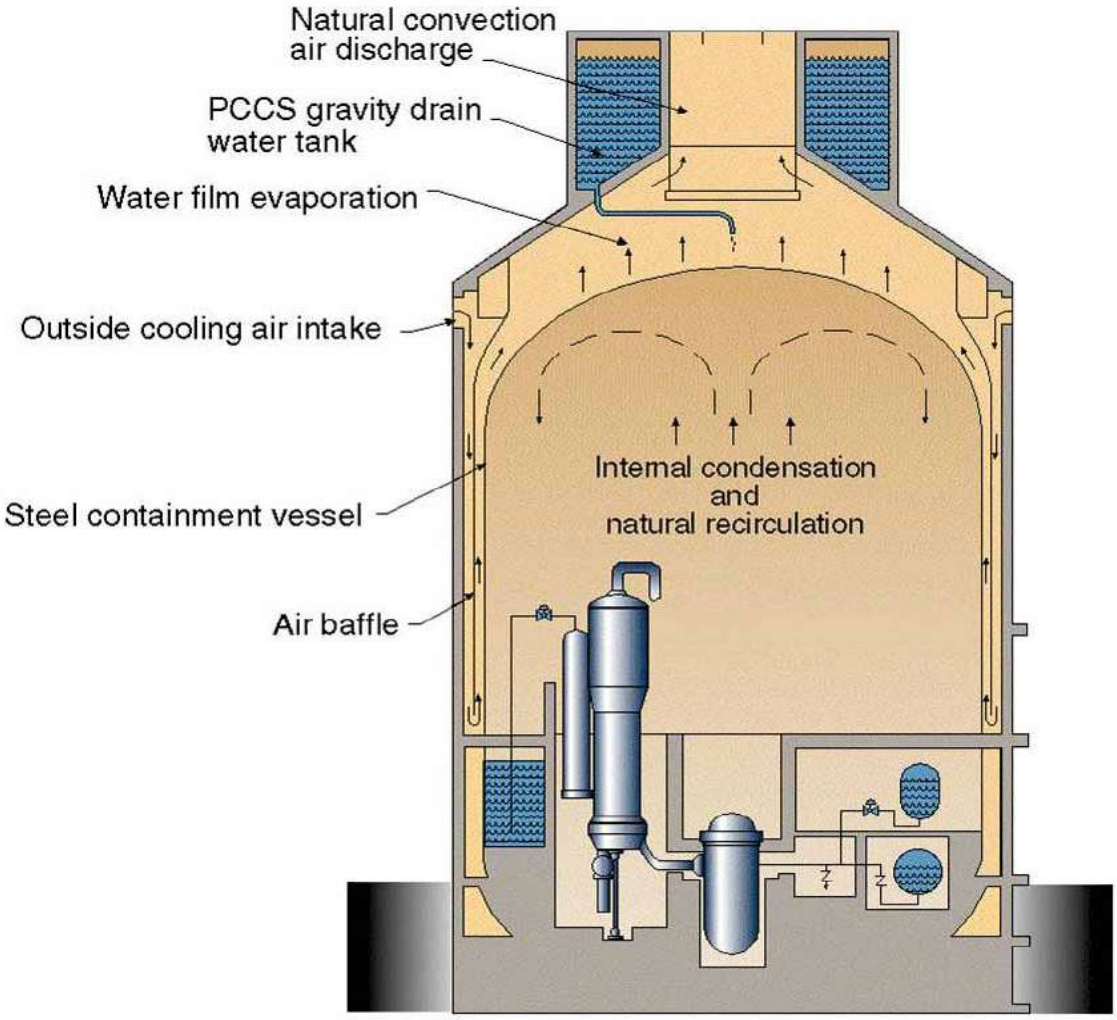


Figure 6-5. Passive Containment Cooling System

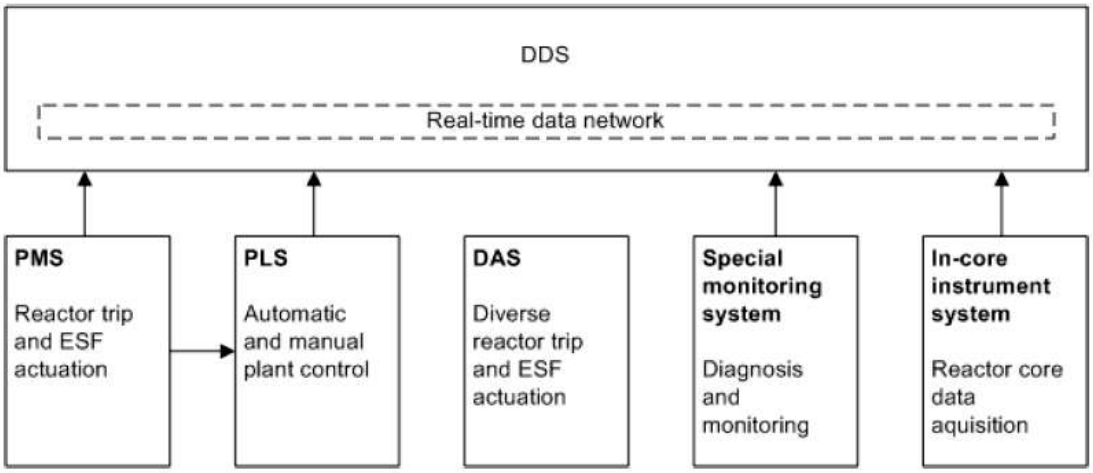


Figure 6-6. Simple C&I Architecture

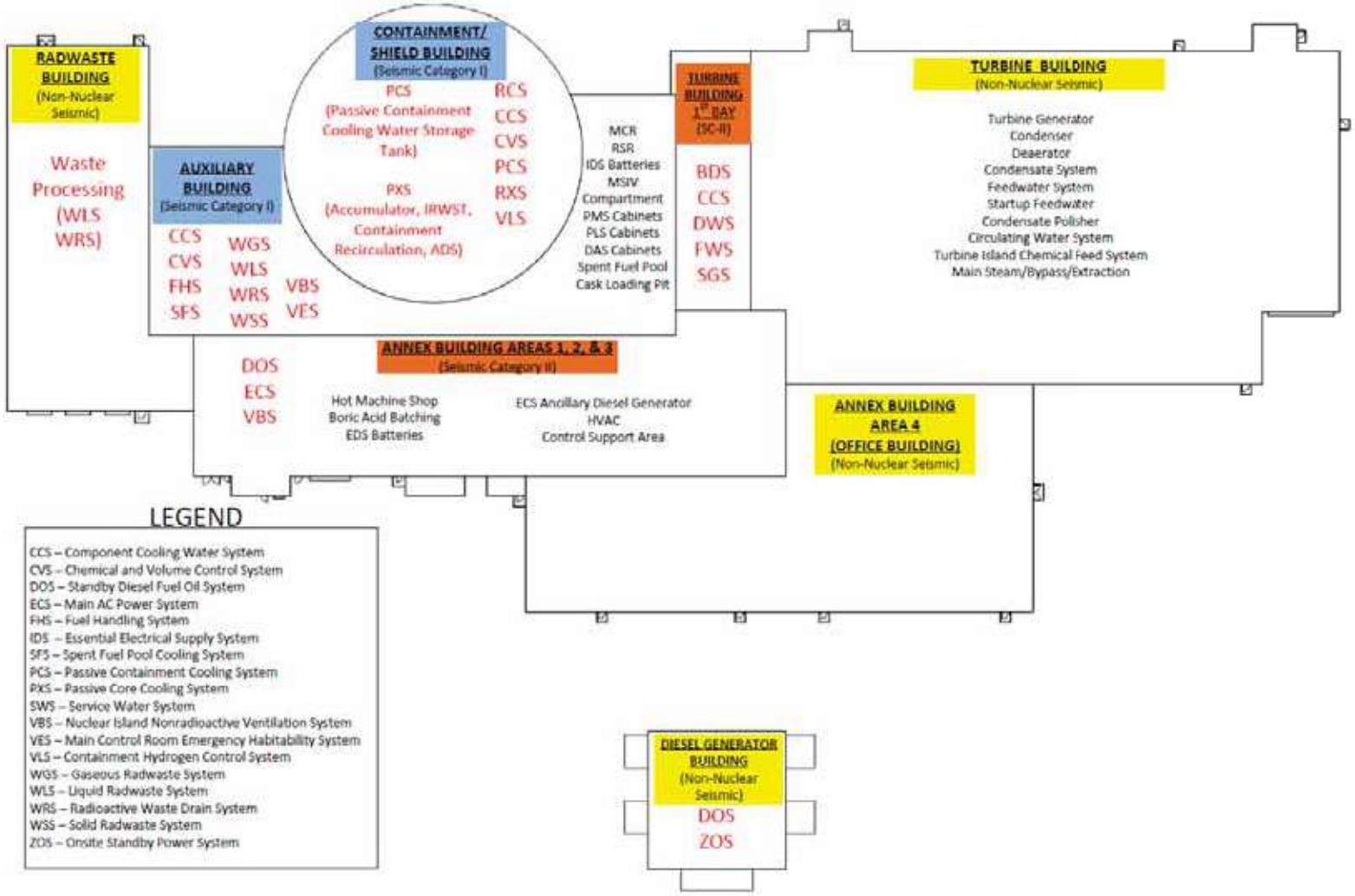


Figure 6-7. Functional Site Allocation of AP1000 Plant Systems, Structures, and Components

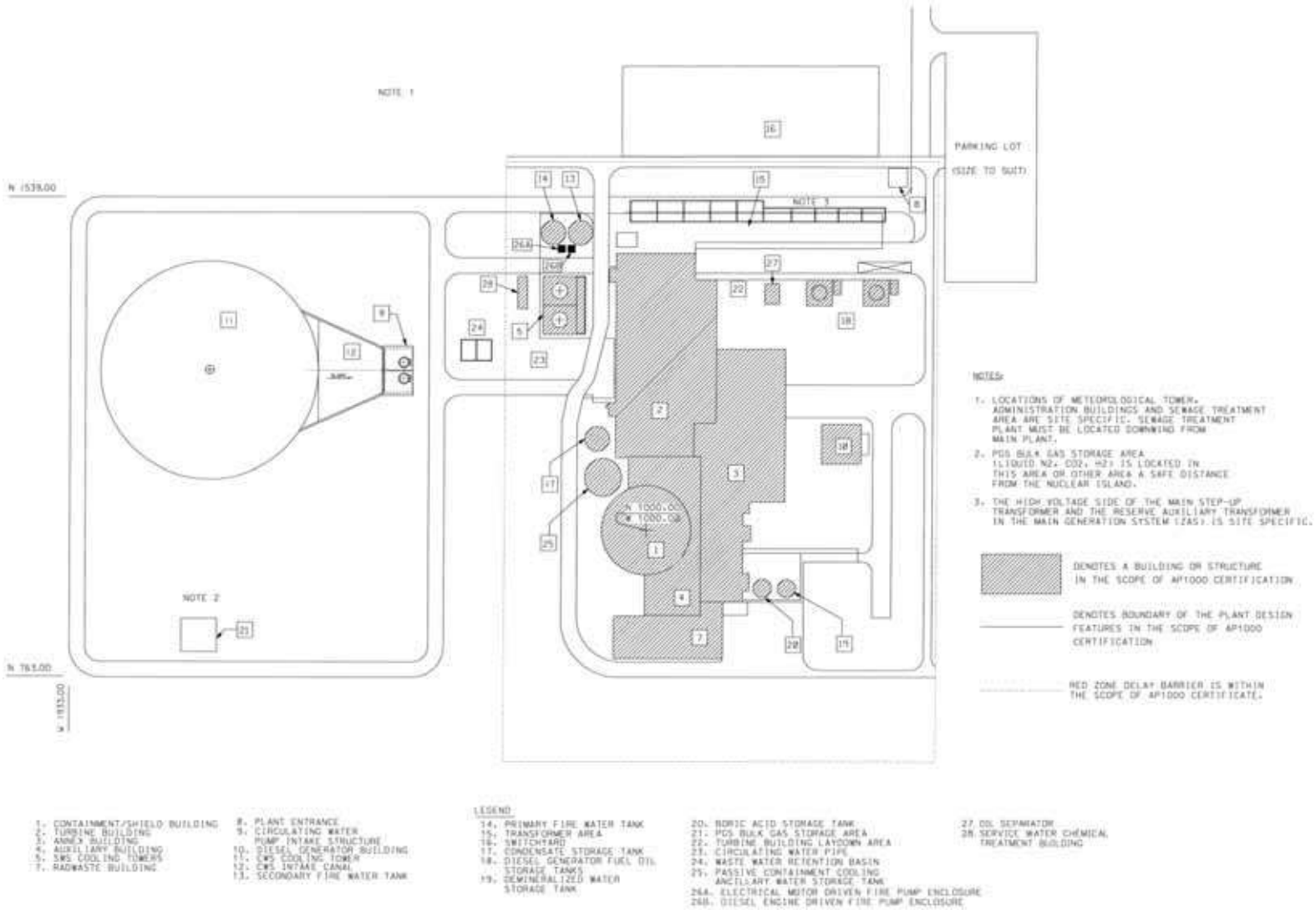


Figure 6-8. Standard Plant Layout

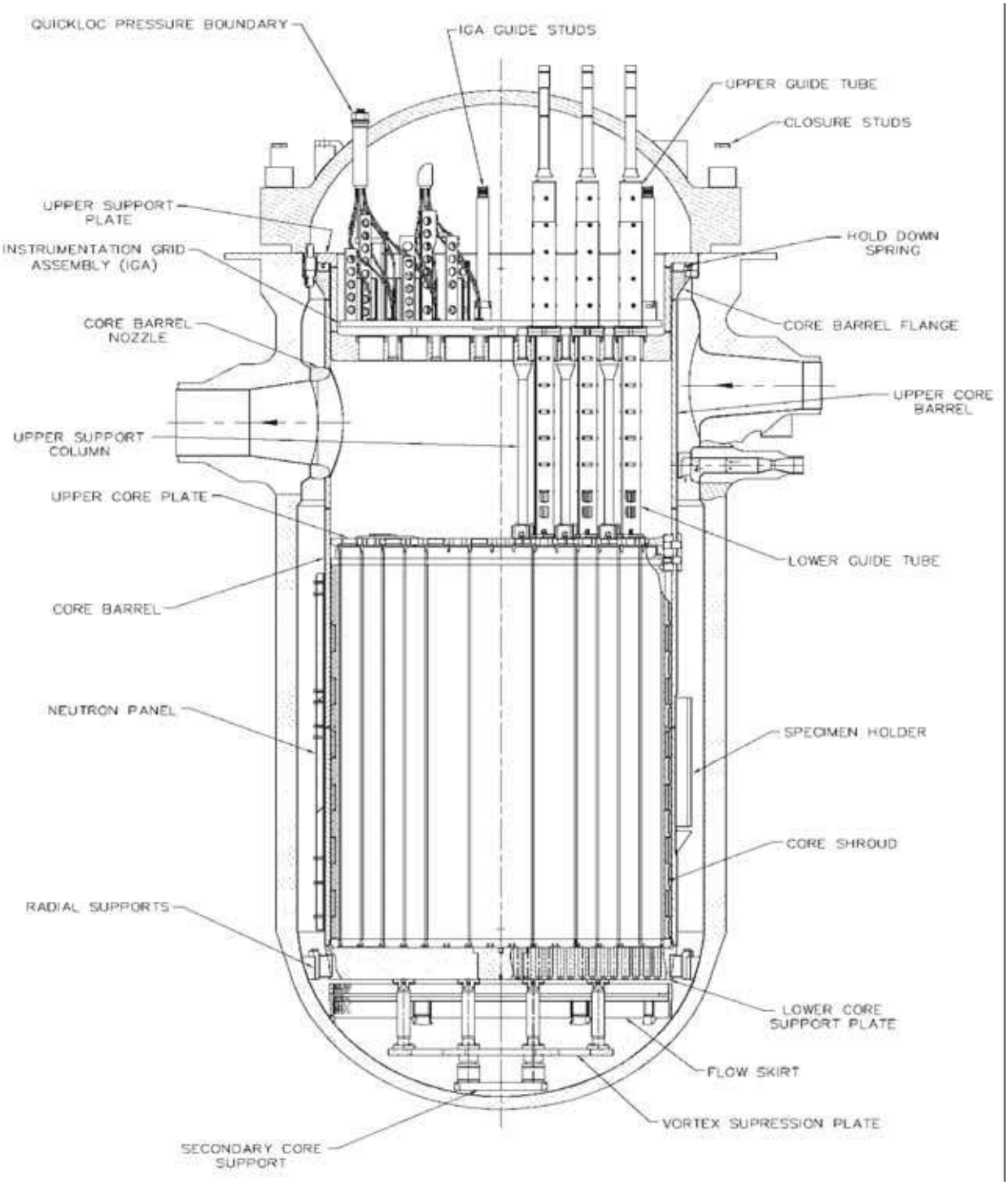


Figure 6-9. Reactor Vessel Arrangement

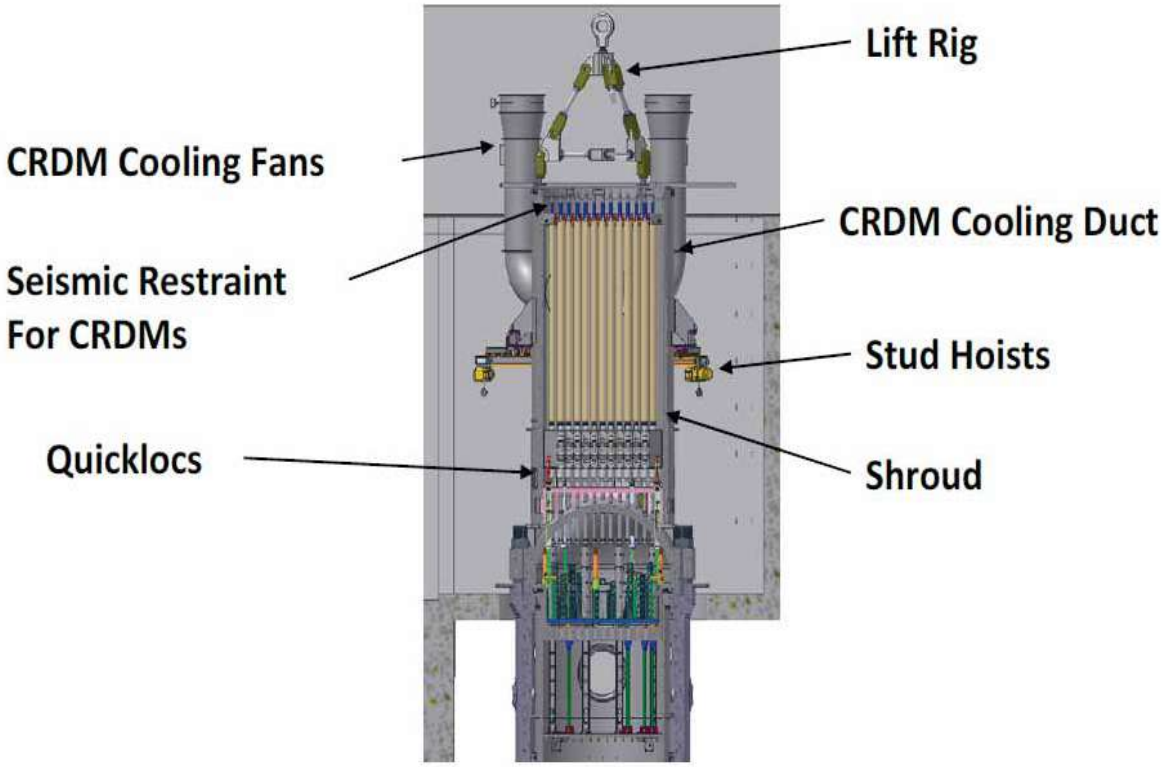


Figure 6-10. Integrated Head Package

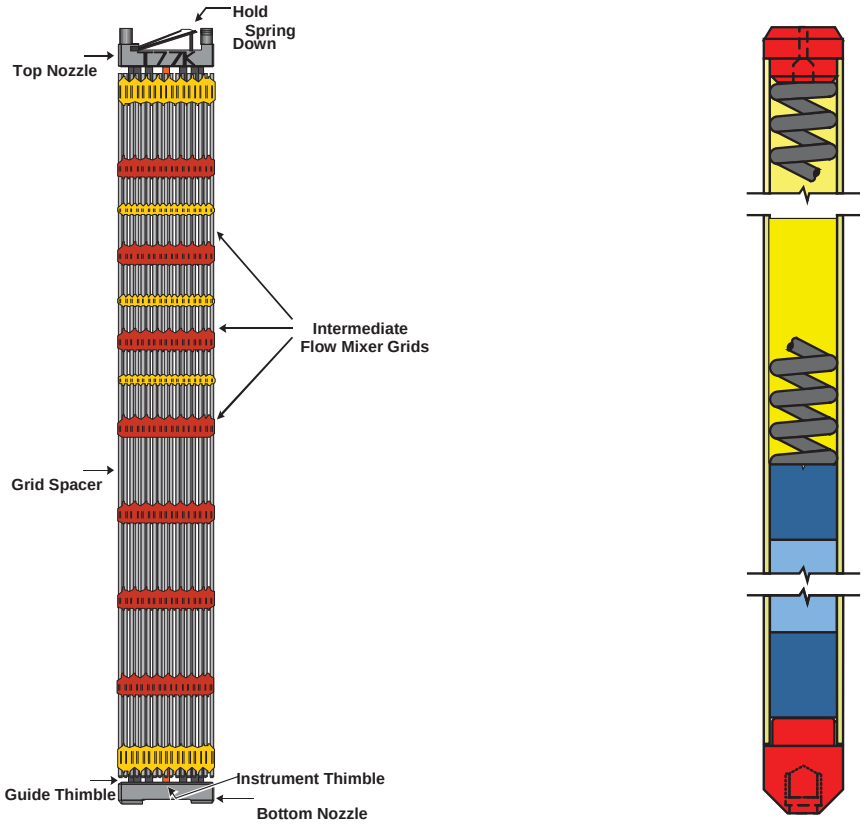


Figure 6-11. Fuel Assembly and Fuel Rod

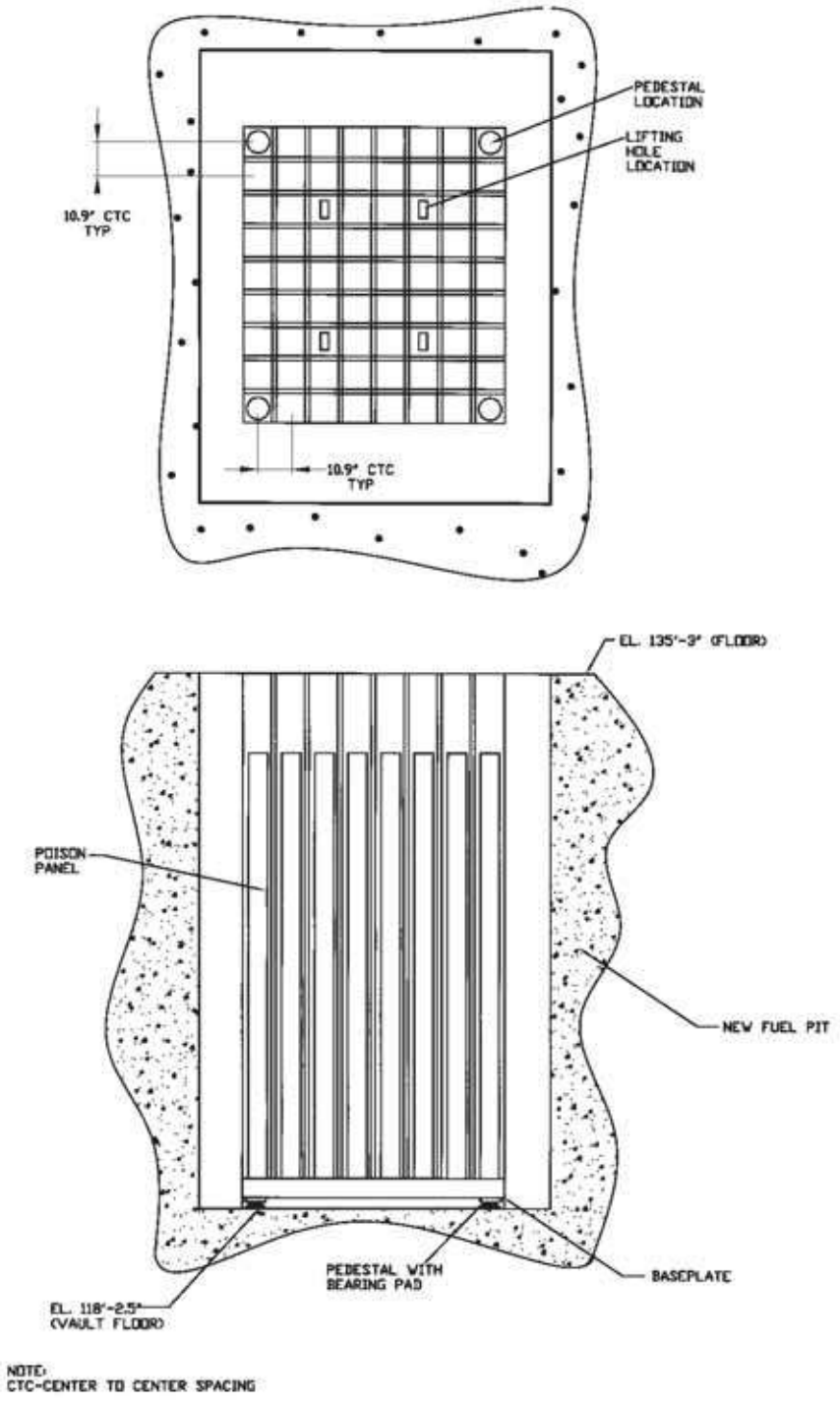


Figure 6-12. New Fuel Storage Rack Layout (72 Storage Locations)

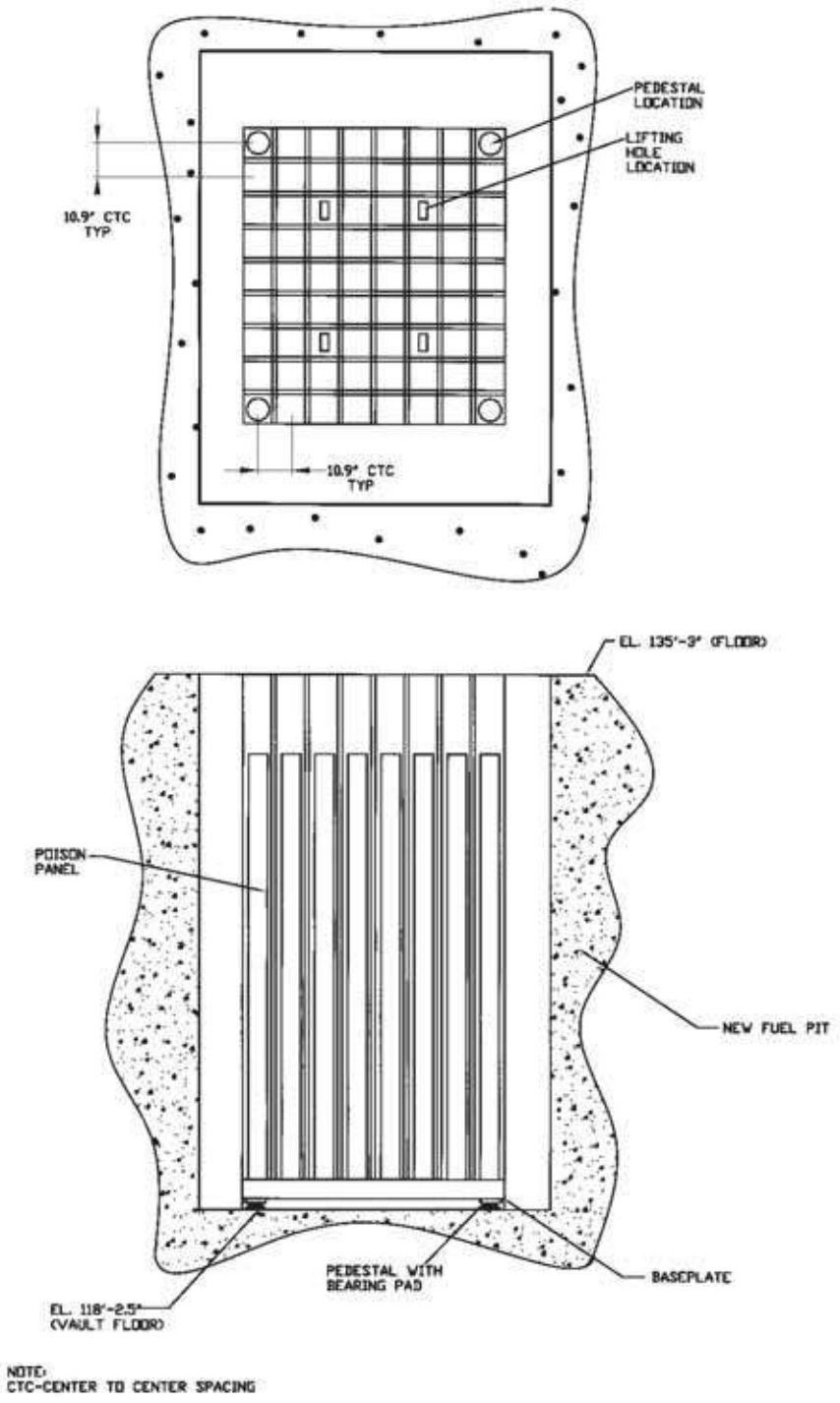


Figure 6-13. New Fuel Storage Rack Cross Section

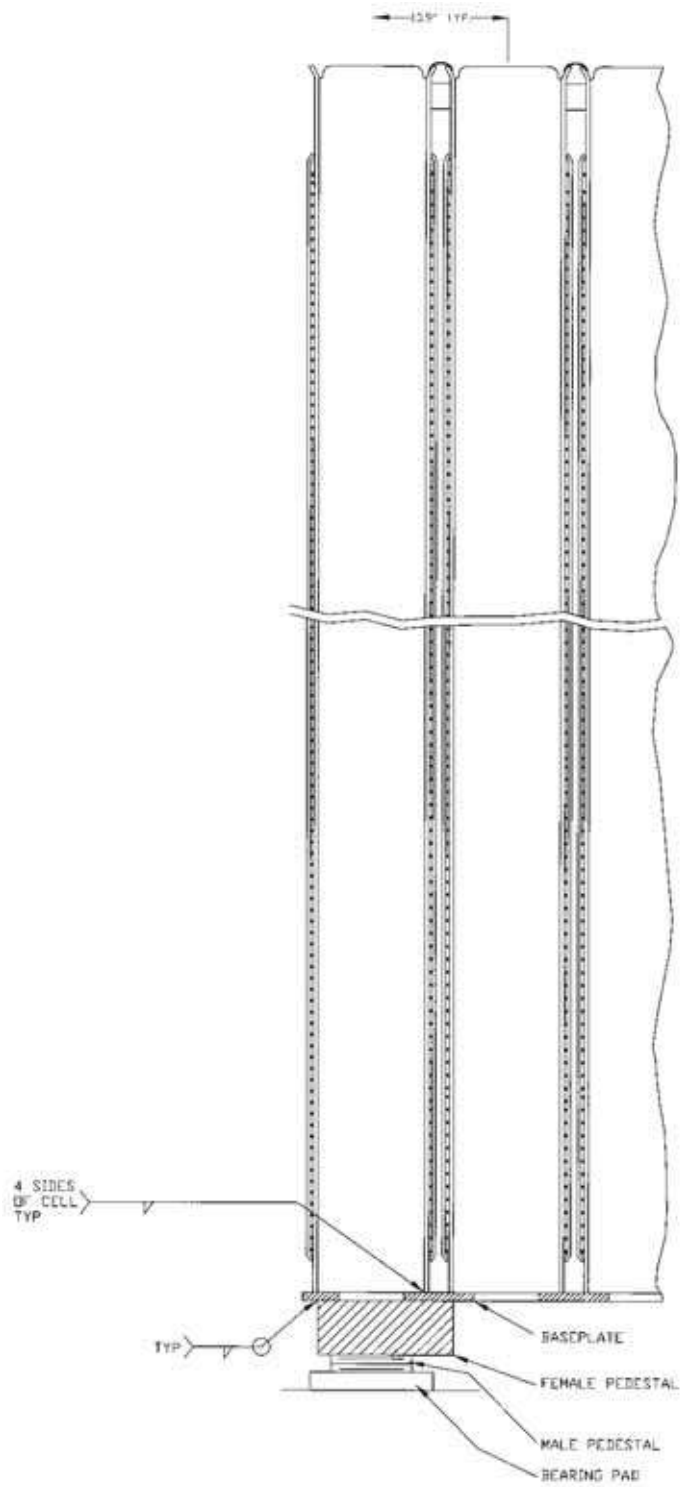


Figure 6-14. New Fuel Storage Rack Cross Section

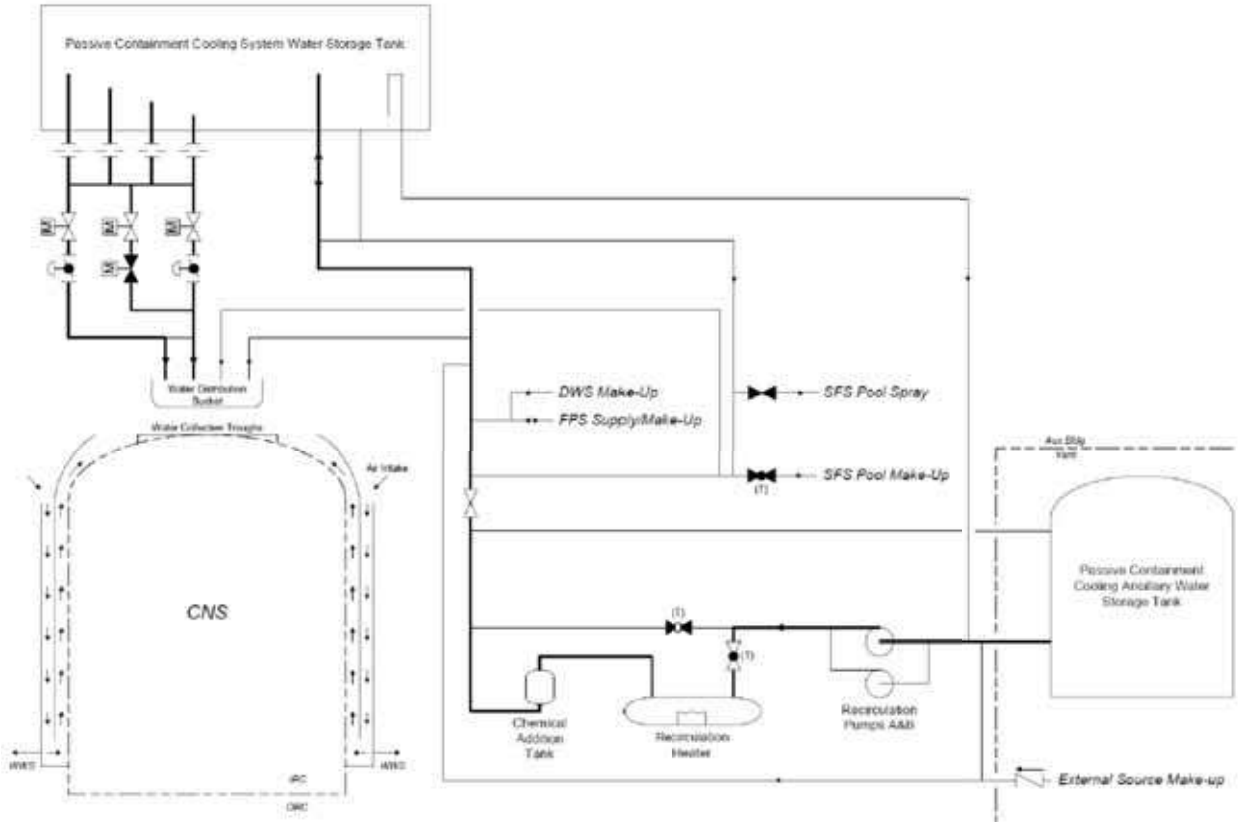


Figure 6-15. Schematic of Passive Containment Cooling System

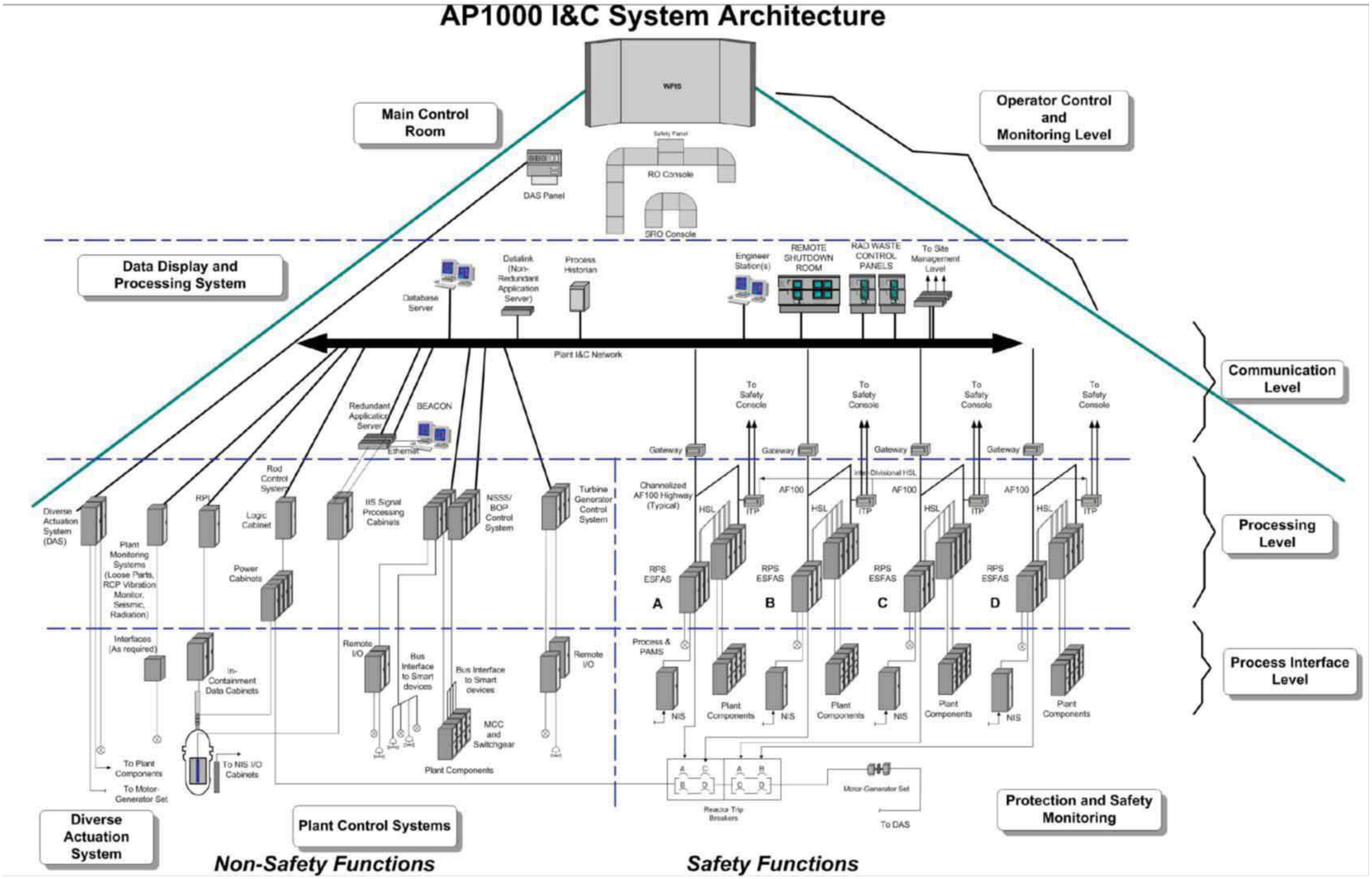


Figure 6-16. AP1000 Design C&I Architecture

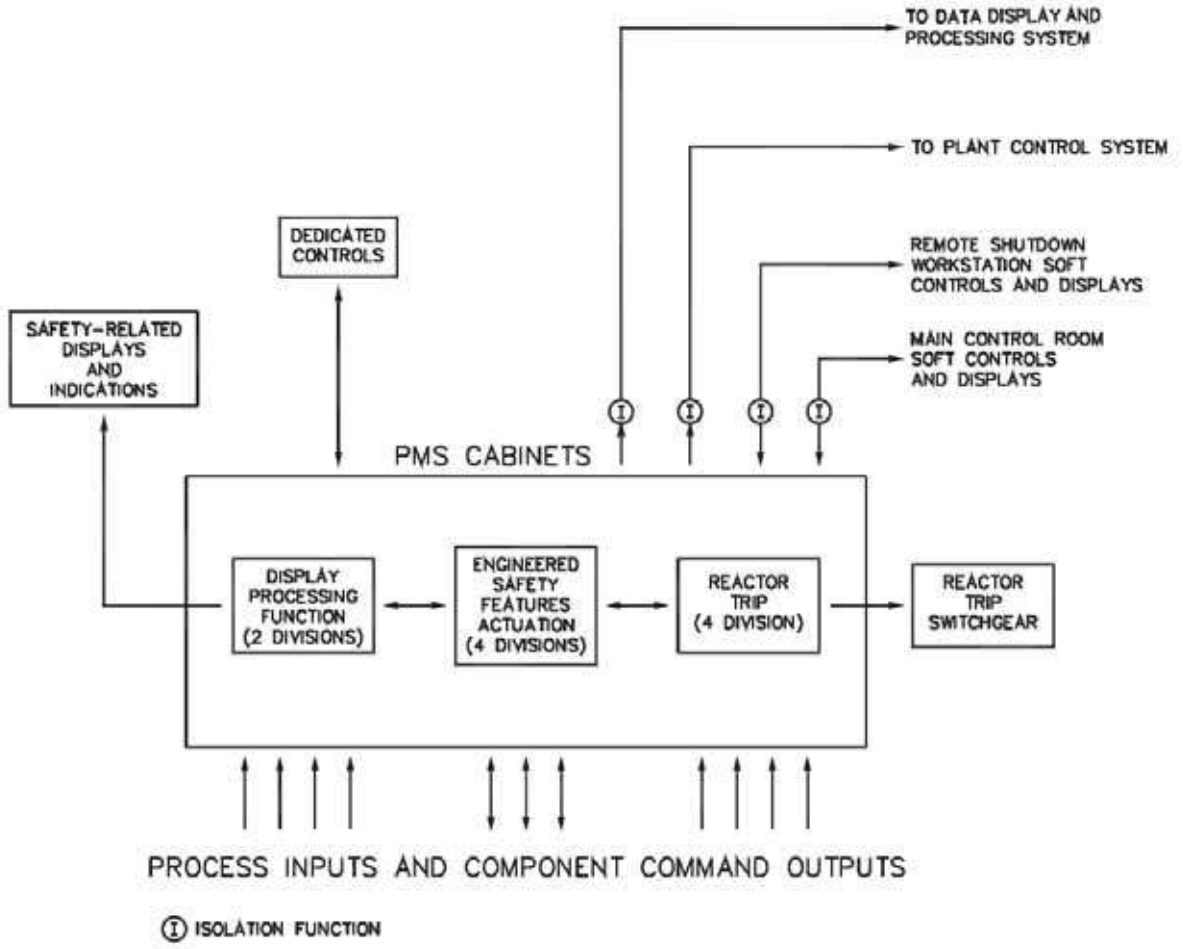


Figure 6-17. Protection and Safety Monitoring System

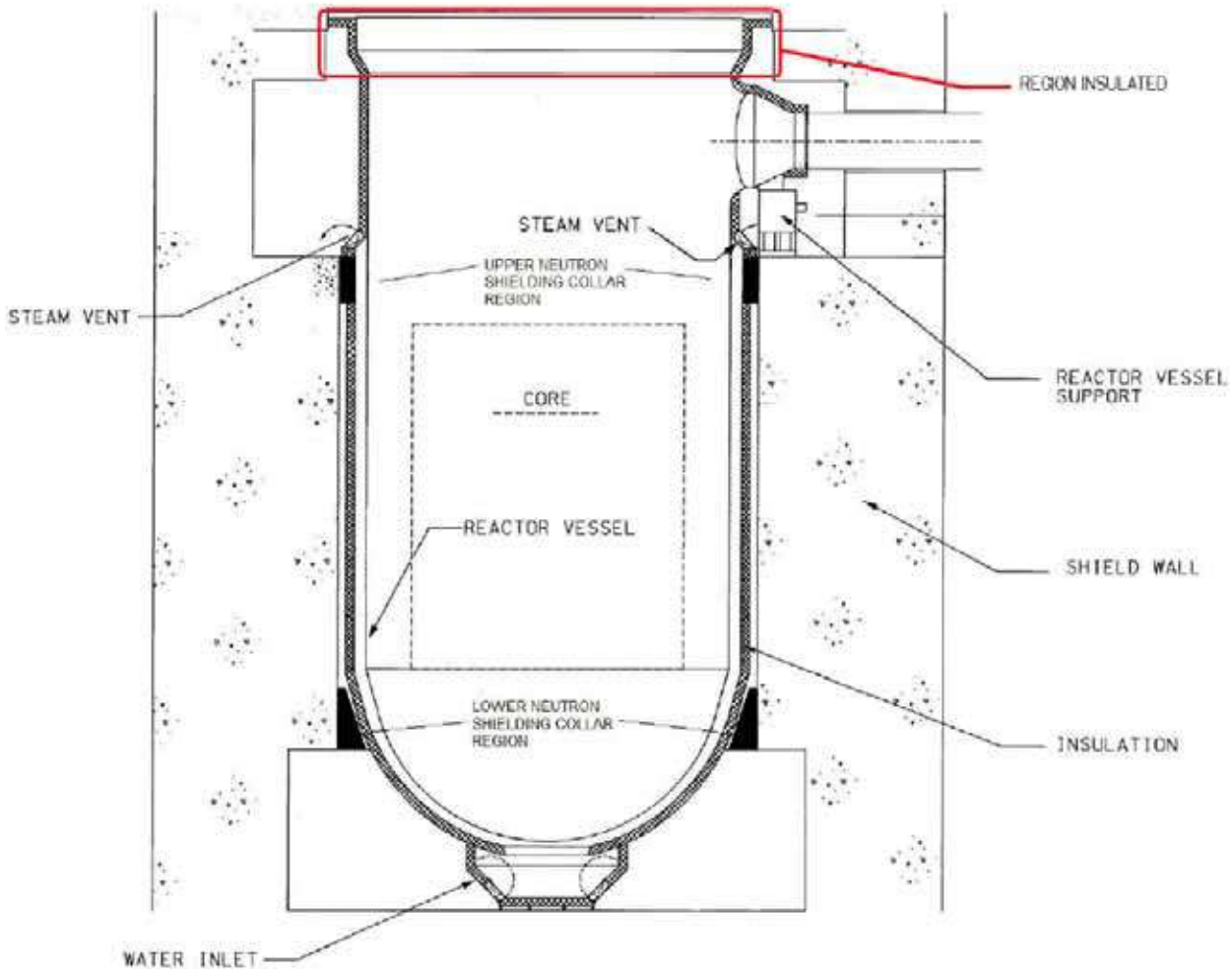


Figure 6-18. Reactor Vessel Cavity Insulation

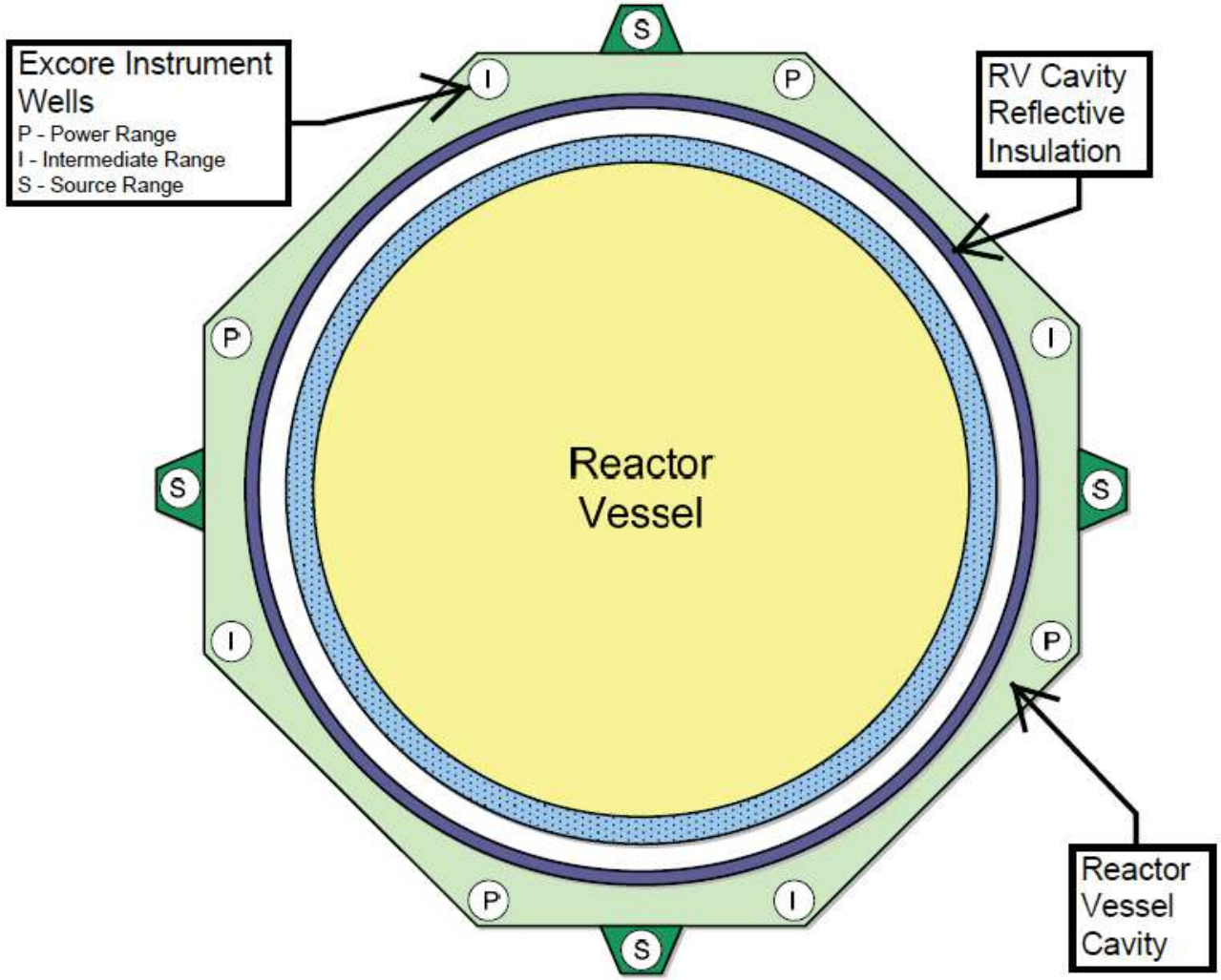


Figure 6-19. Reactor Vessel Cavity Insulation with Excore Instrumentation

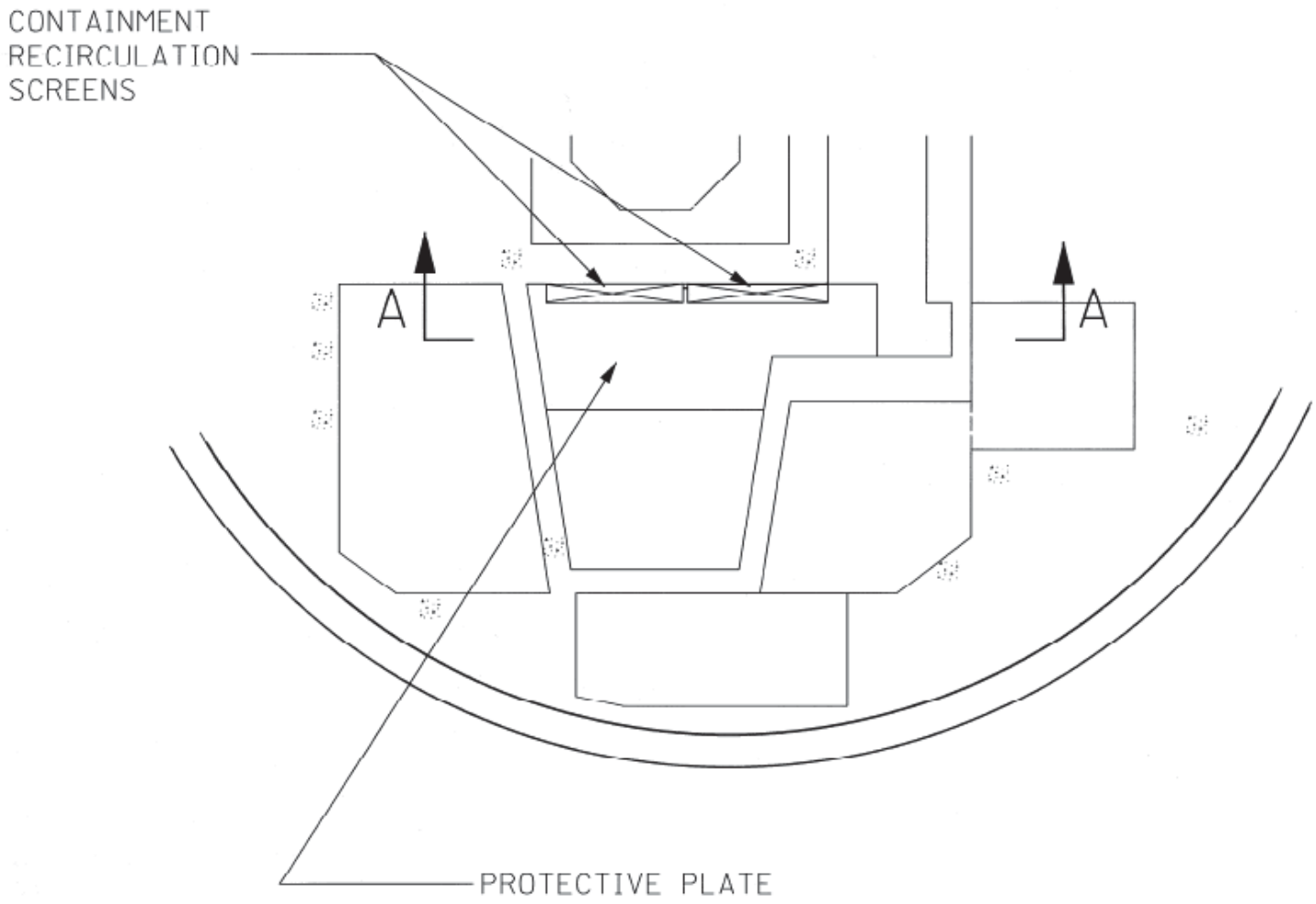


Figure 6-20. Containment Recirculation Screen Location Plan View

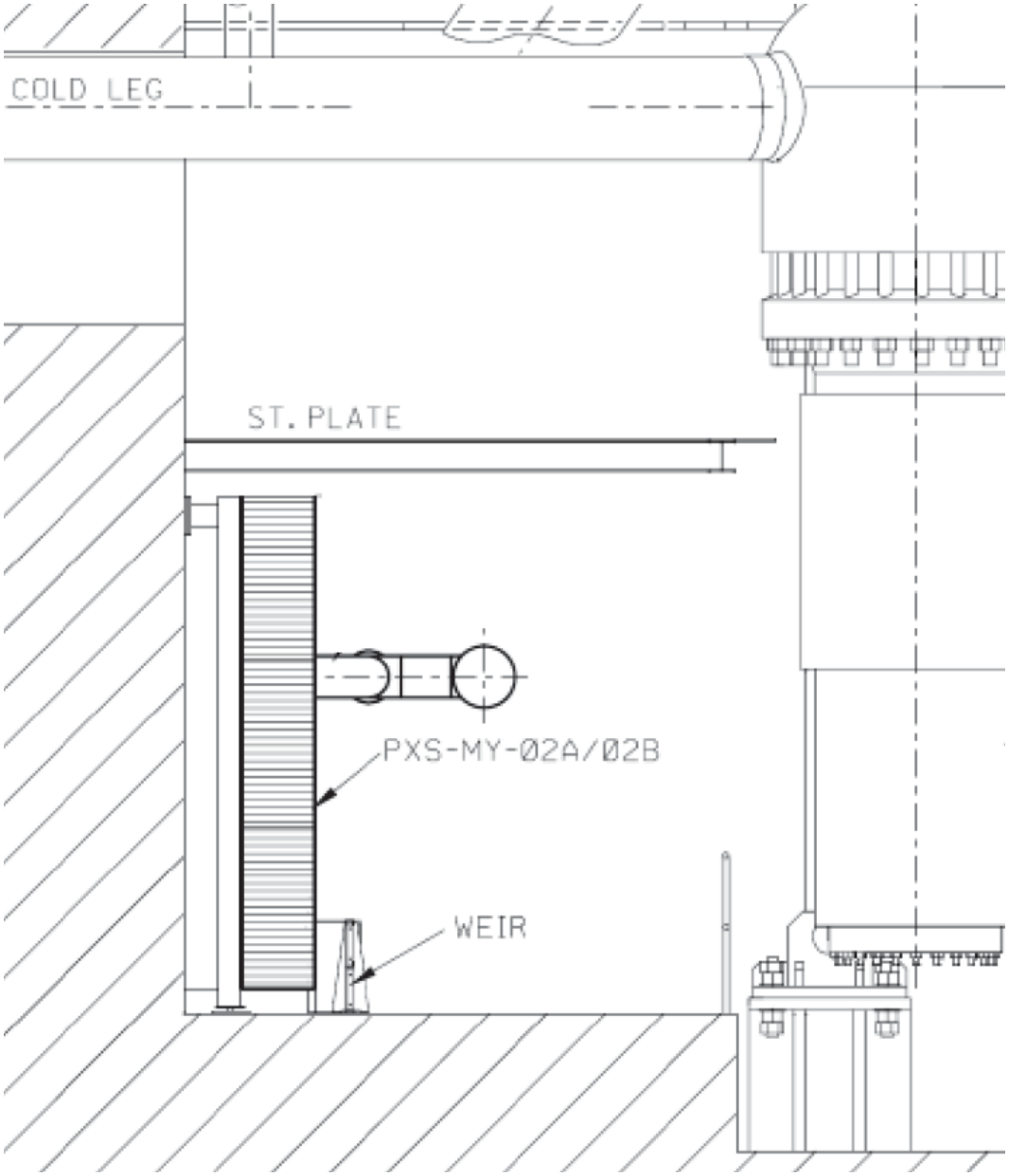


Figure 6-21. Containment Recirculation Screen Location Elevation View

APPENDIX 6A
REVIEW OF MAJOR AP1000 DESIGN DECISIONS

6A.1 INTRODUCTION

Westinghouse has developed the AP1000 design to have an electric power production capability comparable with existing nuclear power stations, but with a level of risk that is more than an order of magnitude lower than the best reactors currently operating. Current nuclear power stations have achieved an acceptable level of risk by evolving ever-increasing complexity with respect to their ESFs but this complexity is subject to the law of diminishing returns. If taken too far in developing a new design, very low levels of risk might be achievable but at a price so high that it would be uneconomical to build the nuclear power station. Westinghouse has taken an alternative approach in designing the AP1000 plant: it has reduced complexity by making the ESFs passive rather than active to the maximum degree feasible, thereby achieving a very high level of safety and a simplified design.

The essence of this review of design decisions is to categorise the plant improvements presented as follows as risk reduction measures that contribute to achieving an overall plant risk that will be ALARP:

- The Westinghouse process has achieved an AP1000 plant design that is in accordance with relevant good nuclear engineering practice through the use of relevant international codes and standards and the use of engineering good practice and operating experience in the design process.

- The designers have followed some key principles – the use of proven technology, the use of passive safety measures for all Category A functions, the pursuit of fault tolerance, and the provision of defence in depth SSCs – that combined, result in very low overall levels of risk throughout the life cycle of the power station.

- The basic design was enhanced by using PSA to identify worthwhile improvements. Thus, each principal design decision contributed to an overall plant risk that is ALARP in its own right.

- No other worthwhile design feature has been overlooked or needs to be incorporated in the design because the resultant further reduction in risk would be achieved at a cost disproportionate to the benefit realised.

6A.2 KEY DESIGN PRINCIPLES

6A.2.1 Proven Technology

In essence, the first engineering key principle is to avoid the hazard by means of good design. The driving design philosophy of the AP1000 plant was to keep it safe by using proven engineering and a simple feasible design arrangement; that is to say, risk can be reduced by using well-established technologies and proven engineering techniques, and the productive path to safety is through the reducing the likelihood of failure modes rather than adding more ESFs.

Design decisions were made in favour of the safer solution, even if it was more expensive. Risks were made ALARP by making the safety systems simple, automatic, driven by natural forces, and diverse from the systems that make power.

Wherever possible, the designers of the AP1000 plant designed out potentially unsafe conditions rather than designing in a complicated recovery strategy. Likewise, the operator response was designed out for the limiting design basis initiating events, thereby eliminating operator reliability from the accident sequence.

6A.2.2 Fault Tolerance

The second engineering key principle requires the design to be fault-tolerant. This involves identifying those faults that might challenge the design and then showing that the design's inherent characteristics are such that most of the fault sequences do not develop to the point where they could challenge a safety function. Section 8.3 describes the fault identification process for the AP1000 design. The AP1000 list of faults is broadly similar to those of current generation PWRs. What is different is that many of the required safety measures are passive, whereas they would be active systems for current-generation plants. This leads to significant improvements in fault tolerance.

6A.2.3 Passive Safety Measures

Chapter 6 provides a list of the safety measures incorporated into the AP1000 design. All the Class 1 safety systems required for design basis initiating events in the reactor are passive in that they only require a valve or circuit breaker to make a one-time change to its state to actuate, and power, if required, coming from a highly reliable battery-backed dc electrical supply.

6A.2.4 Defense in Depth

Typically design basis initiating events can be responded to using active Class 2 components if available. These are identified as defence in depth provisions in addition to the Class 1 passive systems, which satisfy design basis requirements. These systems are described in Chapter 6 and, where supported by further operator action, identified in Chapter 13.

6A.3 REVIEW OF PRINCIPAL DESIGN DECISIONS

6A.3.1 Introduction

This section describes the principal design decisions made for the AP600 and AP1000 plants. Because none of the design decisions described for the AP600 plant were reversed for the AP1000 plant, the entire section ultimately applies to the latter. These decisions occurred over the design life of the AP600 and AP1000 plants, a period of some 15 years, and many occurred concurrently. The selection of these example decisions was such that they are mostly independent of each other. They are included in this report to demonstrate the thorough nature of the AP600 and AP1000 design process; the process reinforced a rigorous, disciplined approach to achieving safety through simplicity and developing a design that improves the risk reduction measures that contribute to achieving a plant judged to be ALARP.

Only a sample of the design decisions made for the AP600 and AP1000 plants are discussed. Many more decisions were made. The following sections address the design decisions made during the evolution of the AP1000 plant, as grouped into the following categories:

- Residual heat removal
- Containment design
- Control room systems
- Primary system design
- Fuel route
- Duty systems

6A.3.2 Residual Heat Removal

6A.3.2.1 Reactor Coolant Post-LOCA Injection, Boration, and Cooling

Following a LOCA, the safety systems must provide borated makeup for the water lost so as to maintain the reactor core reactivity subcritical and immersed in water. Many PWRs today rely on pumped systems and large sources of borated water from outside the containment to provide this makeup and cooling. These types of systems require Class 1 and C-I sources of ac power and water. In the case of the AP1000 design, this is done without reliance on ac power.

Note that a significant simplification of the design has been achieved by the use of the PCS which makes the containment shell the ultimate heat sink heat transfer surface. This avoids the need to have an engineered cooling chain with support systems to transfer heat from the core/containment to the environment. The elements of the design used for core injection, boration, and cooling include:

- The passive core cooling system (PXS)
  - A PRHR HX actuated by opening one of two fail-open AOVs.
  - Two CMT gravity injection flow paths, each actuated by opening one of two fail-open AOVs.
  - Two sets of ADS depressurisation Stages 1, 2, and 3,where each stage is actuated by opening two of two MOVs
  - Four ADS Stage 4 flow paths each actuated by opening one squib valve
  - Two accumulators, which inject when RCS pressure decreases below compressed motive gas
  - Two IRWST injection paths each actuated by opening of one of two squib valves
  - Two passive core cooling long-term recirculation paths each actuated by opening one of two squib valves.
- The passive containment cooling system (PCS)
  - Three PCS flow paths; two paths actuated by opening one of one fail-open AOV and one path actuated by opening one of one MOV.

The only requirement of the above SSCs for dc power, after an accident starts, is to trigger the ESF actuation signals and provide power for one-time realignment of various valves. Heat and fluids then move by natural forces. Of these eight functions, one function requires no valve re-alignment, three functions are accomplished by opening one of two fail-open AOVs (PRHR HX, CMTs, PCS), two functions are accomplished by opening one of four squib valves (IRWST, RECIRC), and one function is accomplished by opening three of four squib valves (ADS Stage 4). Only the six ADS Stages 1, 2, and 3 require opening two of two MOVs in any two of the six flow paths for success

Advantages and Disadvantages

The following detailed advantages result from the chosen design option:

- AOV actuations are fail-open and are actuated on removal or loss of power.
- No reliance on ac power
- No reliance on external sources of water
- No reliance on pumps
- No reliance on HXs cooled by other cooling systems (e.g., CCS, SWS)
- No penetrations through the containment required
- No reliance on operator action during the first 72 hours after the most limiting accidents
- No liquid radioactive effluent
- No risk for accidental loss of coolant outside the containment

The main uncertainty with this design option was that there was little large-scale experience with a total pressure balance and natural-circulation LOCA response systems. However, as part of the AP600 plant development programme, extensive rig testing was performed to validate system functionality and the analysis capability for candidate total pressure balance and natural-circulation LOCA response systems. This testing carries through to the AP1000 design.

One shortcoming of the PCS is that after 72 hours, the PCCWST on top of the containment shield building empties and flow to the top of the containment needs to be supplied using active pumping. The PCS recirculation pumps in the auxiliary building are utilised and they take suction from a hurricane missile-protected, seismic C-II tank: the PCCAWST. Additionally an offsite pump can be brought in to provide flow through the Class 1 External Makeup Flange. The pumps can be powered by normal ac power supply, ancillary diesel generators located in the seismic Class II portion of the annex building, or an offsite portable generator. The PCCAWST has an adequate water supply for an additional 4 days of PCS post-accident cooling of the containment (see subsection 6A.3.3.9 for more details).

6A.3.2.2 Selection of Squib Valves in Preference to Conventional Valve Types

Squib valves are self-contained valves actuated by an explosive charge on receipt of a firing signal. They are widely used on boiling water reactors and in the aerospace industry for one-off emergency operation. Squib valves are used for the following three applications within the safety systems of the AP1000 plant:

- Stage 4 ADS valves
- IRWST injection line isolation valves
- Containment recirculation line isolation valves

Squib valve operation needs to be very reliable. Experience has shown that squib valves are more reliable than other types of valve because of the reliability of their actuating propellants

and the simplicity of their mechanical design. For comparison purposes, the following probabilities for the failure to open on demand of each type are assumed by the AP1000 PSA (Ref. 6A.1) as follows:

- AOVs, 8.76E-3 failures per demand
- Motor-operated valves (MOVs), 1.41E-2 failures per demand
- Squib valves, 5.80E-4 failures per demand

The in-service testing for each squib valve includes both a test of the remote position indication and a test-firing of the igniter and propellant. The squib valve charge assembly is removed and then test-fired outside of the valve in a test rig that can monitor explosive charge performance. Any failures would result in the removal of the charges from the same production lot and replacement with new charges from a different lot. ASME code requires that 20 percent of the charges be tested every 2 years. The plant maintenance schedule defines the performance of these tests during refuelling outages, when the squib valves can be accessed for propellant charge removal.

The nature of a squib valve body design makes it virtually leak–free, that is, the valve is not subject to internal leakage, as with standard valve designs such as globe, butterfly, gate, and nonreturn valves. This is an important safety function because any such leakage would require valve replacement.

Advantages and Disadvantages

Squib valves offer the following advantages over other valve types:

- Greater reliability by at least an order of magnitude. This is because of their simple design and non-reliance on any external power other than for the actuation signal.

- Leak-free design.

- Easily tested and maintained.

The following disadvantages result from choosing squib valves over other valve types:

- The explosive charge and igniter used within a squib valve have limited shelf and service lives. However, the required maintenance and testing can easily be accommodated within the AP1000 plant refuelling outages.

- Functional end-to-end testing is not possible.

6A.3.2.3 Diversity in Squib Valve Design

Squib valves are used for the following three applications within the AP1000 safety systems:

- Stage 4 ADS valves
- IRWST injection line isolation
- Containment recirculation line isolation

Common mode failure within and between the applications of the three systems is minimised by using a different valve design for each of the three applications: one for the Stage 4 ADS squib valves, a second high-pressure valve design for the IRWST injection lines, and a third low-pressure recirculation line squib valves.

Design diversity is achieved through differences in the design details of the key valve actuation components, which requires differences in their physical configurations (and design tolerances) for the following:

- Valve body (inside surface forms shearing piston walls)
- Valve bonnet and retaining hardware (cylinder head that also houses the propellant cartridge)
- Propellant cartridges (volume/arrangement excluding propellant material/igniters)
- Actuation plug (shearing piston)
- Actuation plug piston tensioning (and shearing) bolt
- Shear caps (shearing wall thickness that is pressure-dependent)
- Valve latching mechanism (hold shearing piston in place after actuation)
- Metal foam (compression dampening upon actuation)
- Metal foam retainer plate and retaining hardware
- Various valve body bolts and compression chamber metal O-rings.

In summary, design variations and design tolerances between the various designs provide adequate design diversity to protect against squib valve common failure modes.

Advantages and Disadvantages

Having a diverse valve design for each of the three squib valve applications in the AP1000 design minimises the simultaneous common mode failure of the three applications.

6A.3.2.4 Passive Core Cooling System Pipe Size Increases

The primary function of the PXS is to provide emergency core cooling following postulated design basis initiating events. The PXS is designed to perform the following functions:

- Emergency core decay heat removal
- RCS emergency makeup and boration
- Safety injection
- Containment pH control

The PXS is designed to operate without the use of active equipment such as pumps and ac power sources. Once actuated, the PXS functions depend on natural circulation and processes such as gravity injection and the expansion of compressed gases.

For the AP600 design, the analysis was finished for system performance, pipe size, routing and stresses, and building structural response. The AP1000 design challenge was to increase the capacity of the PXS while changing as little of the AP600 plant physical design as possible. Alternatives included adding Class 1 pumps, increasing the thermal head differences from the core to the heat sinks, rerouting pipe to reduce the pressure drop, or increasing pipe sizes.

Adding Class 1 pumps would have defeated the passive nature of the AP600/1000 concept and was rejected at the outset. Increasing the thermal head differences would have required a redesign of structures inside the containment; this type of redesign affects finished layouts, pipe routings, building structural calculations, building seismic responses, component seismic responses, system flow calculations, accident response calculations, containment free volume, containment flood-up volumes, and more. Rerouting piping for pressure reduction would yield very little because the piping was already routed for minimum resistance while maintaining structural adequacy. The remaining alternative of increasing the size of the pipes was selected because it had the least impact on the finished design.

Scoping calculations were performed to determine the required pipe size. Then the next larger standard pipe size was selected and placed on the same centrelines as those of the AP600 design. This approach created pipe routings that had margin in the pressure drop due to using pipe that was slightly larger than required and that could probably pass structural evaluations because the smaller pipe sizes had already passed. These assumptions proved valid and the PXS design was resized for the AP1000 design with as little extra impact on the fully certified AP600 design as was reasonably practicable.

Advantages and Disadvantages

The following advantages resulted from increasing the pipe sizes within the PXS to accommodate the increased duty required by the AP1000 design:

- Slightly increased margin in the pressure drop ensured achieving the higher natural circulation flow rates required.
- No need for a redesign of any structures inside the containment.
- No need to reroute the PXS pipe work.
- No need to repeat the building structural calculations.
- No need to repeat the building seismic responses and component seismic responses.
- No change in the containment free volume and containment flood-up volumes.

The only disadvantage resulting from increasing the pipe sizes within the PXS to accommodate the increased duty required by the AP1000 design is the minimal extra cost of the larger pipes and valves.

6A.3.2.5 Core Makeup Tanks Size Increase

The CMTs are part of the PXS. They hold cold borated water stored RCS pressure for RCS makeup and boration and for safety injection to the RCS in the event of a LOCA. The amount of water required for the latter duty on an AP1000 plant is more than that required by the AP600 plant, suggesting the need for larger tanks.

Given that design analysis had been completed for the AP600 design with respect to system performance, tank size, stresses, and building structural response, the AP1000 design challenge was to increase the capacity of the CMTs while changing as little of the AP600 physical design as possible.

The CMTs were resized for the AP1000 design by ascertaining the largest tank size that could fit into the rooms assigned to the CMTs and placing them on the same centrelines as in the AP600 design. The PXS performance was then reanalysed.

This showed that the CMT volumes still had margin for small-break LOCAs, while maintaining the in-containment structural, flood-up, and high pressure injection capability.

Advantages and Disadvantages

The following advantages result from resizing the CMT but keeping the other aspects the same:

- No diminution in the flood-up and high pressure injection capability of the resized tanks.
- The ability to carry across the stress analysis and the building structural response analysis because there is no change to the in-containment structural layout.

The only disadvantage resulting from resizing the CMT but keeping the other aspects the same is the reduced but still adequate margin for small-break LOCAs.

6A.3.2.6 Increasing the Capacity of the In-Containment Refuelling Water Storage Tank

It is desirable to increase the post-LOCA containment flood-up level for the AP1000 design to maintain and increase the long-term core cooling safety margins. One of the changes made to the AP1000 design to accomplish this was to increase the water level in the IRWST during normal operation, but without changing any of the structures within the containment, that is, without adding a bigger tank. The option chosen was to fill the tank more fully.

To do this, it is important to be able to measure IRWST level accurately during normal operating conditions. The instrumentation used previously was a wide-range differential pressure-level sensor. This sensor was prone to relatively large errors when the tank was full. Whilst this was adequate for the AP600 design, the AP1000 design needed a better measurement if the tank were to be filled to a higher level.

To maintain the operating margin in the tank, a more accurate narrow-range ultrasonic sensor was added. It is permissible to use this type of sensor for monitoring the water level during normal operation because it does not have to function in the post-accident environment. For the actuation of the ESF signal, lower narrow range IRWST level instruments are installed. In the post-accident environment, the wide-range level sensors are sufficient to monitor the draindown of the IRWST.

In summary, the ultrasonic level sensor is a simple device that is wall-mounted inside the IRWST above the maximum water level. By adding this narrow range instrumentation, much of the error is eliminated, allowing the normal water level in the IRWST to be raised while maintaining the previous operating margin. This allows for a more reliable water volume capacity and thus the ability to increased flood-up level post-LOCA.

Advantages and Disadvantages

The following advantages result from incorporating a more accurate measurement of the IRWST level:

- Increased ability to measure the post-LOCA containment flood-up level, thereby maintaining and increasing the long-term core cooling safety margins.

- Avoiding the cost of making the IRWST larger.
- No change to the in-containment structural layout.
- No reanalysis of the stresses and the building structural response.

The only disadvantage resulting from incorporating a more accurate measurement of the IRWST level is the slight risk of damage to a more sensitive ultrasonic level sensor.

6A.3.2.7 Passive Residual Heat Removal Heat Exchanger

The PRHR HX is part of the PXS. It is located in the IRWST, which provides the heat sink for the HX. The HX is elevated above the RCS loops to induce natural circulation flow through the HX when the RCPs are not available. The PRHR HX piping arrangement also allows actuation of the HX with RCPs operating. When the RCPs are operating, they provide forced flow in the same direction as natural circulation flow through the HX. If the pumps are operating and subsequently trip, then natural circulation continues to provide the driving head for HX flow.

For postulated non-LOCA events, where a loss of capability to remove core decay heat via the SGs occurs, the PRHR HX can automatically remove core decay heat and transfer it to the IRWST water. If or when the IRWST water becomes heated to its saturation temperature, the PRHR HX continues to remove heat from the RCS by boiling the IRWST water. The steam generated in the IRWST is vented into the containment, condensed on the containment vessel, and returned by gravity via the IRWST condensate return gutter.

Thus, the PRHR HX can remove core decay heat and cool the RCS with or without AC power and the RCPs operating for greater than 72 hours days. This PRHR performance is substantiated using either realistic or conservative design basis assumptions.

In utilising conservative design basis assumptions, the PRHR can maintain RCS conditions for greater than 72 hours before degradation of heat removal may occur, which would lead to the eventual actuation of ADS (See Appendix 9C) in order to transition to open loop cooling, assuming no restoration of power.

In utilizing more realistic assumptions, the PRHR has been shown to be able to cool the RCS to 215.6°C (420°F) within 36 hours, and to maintain RCS conditions for greater than 14 days prior to transition to open loop cooling, assuming no restoration of power.

This allows the RCS to be depressurised and the stress in the RCS and connecting pipe to be reduced to low levels. This also allows plant conditions to be established for initiation of RNS operation. During a SG tube rupture event, the PRHR HX removes core decay heat and reduces RCS temperature and pressure, equalising with SG pressure and terminating break flow without overfilling the SG.

Given that design analysis had been completed for the AP600 plant with respect to PRHR HX performance, HX size, stresses, and building structural response, the AP1000 design challenge was to increase the capacity of the CMTs while changing as little of the AP600 physical design as possible.

The principal design change was to add enough extra tubes to the PRHR HX to satisfy the requirements on cooldown time for AP1000 design basis initiating events. There was also a requirement to alter the attachment to the IRWST without changing the in-containment

structural layout. The PRHR HX was placed on the same centrelines as in the AP600 design. The IRWST water volume increase provided by raising the normal water level did not need to be increased for the AP1000 PRHR HX function.

Advantages and Disadvantages

The following advantages result from resizing the PRHR HX but keeping the other aspects the same:

- Adding extra tubes to the PRHR HX results in no diminution in its capability for cooling down the reactor for AP1000 design basis initiating events.

- The stress analysis and the building structural response analysis were carried across because there is no change to the in-containment structural layout.

The only disadvantage resulting from resizing the PRHR HX but keeping the other aspects the same is that it is necessary to alter the HX's attachment to the IRWST.

6A.3.2.8 Increase in the Automatic Depressurisation System Stage 4 Pipe Size

Opening the ADS valves is required for PXS IRWST injection and long-term recirculation to function as required to provide emergency core cooling following postulated accident conditions. Twenty valves are divided into four depressurisation stages. These stages connect to the RCS at three different locations. The ADS Stages 1, 2, and 3 valves are included as part of the pressuriser safety and relief valve module, and are connected to nozzles on top of the pressuriser. The Stage 4 valves connect to the hot leg of each reactor coolant loop. The Stage 1 valves may also be used, as required following an accident, to remove non-condensable gases from the steam space of the pressuriser.

The Stage 1 ADS valves are dc-powered, motor-operated, 10-cm DN (4 inch) valves. The Stage 2 and 3 ADS valves are dc-powered, motor-operated, 20-cm DN (8 inch) valves. The Stage 4 ADS valves are 35-cm DN (14 inch) squib valves arranged in series with normally open, dc-powered, motor-operated valves. The control system for opening the ADS valves has an appropriate level of diverse and redundant features to minimise inadvertent opening of the valves. For each discharge path, a pair of valves is placed in series to minimise the potential for an inadvertent discharge of the ADS valves. The Stage 4 valves are interlocked so that they cannot be opened until RCS pressure has been substantially reduced.

An analysis was carried out to ascertain whether, and by how much, the various ADS pipes and associated valves had to increase in size to accommodate the higher power and reactor coolant volume of the AP1000 design as compared with the AP600 design. PSA conducted for the AP1000 design showed that no additional size increase over the AP600 ADS Stage 1, 2, and 3 pipes valves was required. Calculations indicated the requirement for a larger size for ADS Stage 4 piping and valves; because the required size fell between standard pipe sizes, however, the next larger pipe size, 36 cm, was chosen. The pipe centrelines were kept the same to simplify incorporation of the larger pipe into the layout. This resulted in an ADS Stage 4 capability of slightly more than was required to accommodate the increase in power. The ADS Stage 4 piping size was increased from 25 cm DN (10 inch) to 35 cm DN (14 inch). The only other required ADS change was to revise the CMT level setpoints used for ADS actuation based on the larger AP1000 plant CMT capacity to ensure sufficient RCS pressure decrease in order to ensure timely IRWST gravity draindown initiation.

Advantages and Disadvantages

The following advantages result from using a commercially available standard size for the ADS Stage 4 piping and valves:

- Additional capability for dealing with design basis initiating events
- No change to the in-containment structural layout
- No reanalysis of the stresses and the building structural response

The only disadvantages resulting from using a commercially available standard size for the ADS Stage 4 piping and valves are the slightly more severe consequences from inadvertent operation of the Stage 4 valves.

6A.3.2.9 In-Vessel Retention

Certain beyond design basis accident sequences could lead to a core melt; whilst this is extremely unlikely, it is not incredible. This possibility required some form of mitigation. The AP600 plant designers addressed this challenge by developing the capability for IVR.

The alternative to having IVR capability would be to incorporate some form of "core catcher" outside the RV. A core catcher would have to have features that precluded re-criticality of the mixtures of core structural materials and building structures (known as corium), and to cool it to prevent or slow its reaction with the core catcher materials around the RV. This could have been the design solution for the AP1000 plant reactor.

The AP600 plant achieved IVR capability by taking advantage of the large amounts of water into the lower portions of the containment. The expected level of water in the containment after an accident is above the nozzles of the RV and, hence, above the top of the fuel. It was recognised that a possible design solution for the core melt scenario would be to take credit for this water and use it to cool the corium. The water would flow into the RV insulation structure, and come into contact with the RV where it would then boil and cool the RV. The steam would rise within the insulation structure and be vented into the upper containment, carrying core heat with it. This steam would condense on the inner surface of the containment vessel and then return to the lower portion of the containment, where it could repeat the cycle. This bulk boiling heat transfer from the RV was shown by prototype testing to remove sufficient heat to prevent failure of a depressurised RV. This testing also demonstrated that there was significant margin to the critical boiling heat flux and that steam blanketing of the RV surface would not occur. To realise this solution, the design team had to demonstrate two things: first, prototype testing had to be performed to duplicate bulk boiling heat removal and steam venting, measure the critical heat flux limits, and demonstrate sufficient margin to these limits given the heat fluxes expected during a core melt; second, a mechanical design of the RV insulation had to be developed that allowed water to get next to the RV in a severe accident, while not allowing air to flow next to the RV during normal operation. All of these objectives were achieved. Testing was performed at the University of California, Santa Barbara, to establish the design parameters for cooling the vessel during a core melt. A unique design of the lower portion of the RV insulation was developed that used buoyancy to allow water in, when present, but not to allow air flow into the insulation/vessel annulus during normal plant operation. This design solution for enabling IVR at the AP600 power level was selected and implemented in the design.

Advantages and Disadvantages

The following advantages result from choosing the IVR option:

- The RV remains intact, thereby providing a robust barrier to the release of core material into the containment following a postulated severe accident. This prevents the occurrence of ex-core phenomena such steam explosion or corium concrete interactions that would threaten containment integrity.

- This greatly reduces the calculated frequency of large radioactivity releases to the public.

- Eliminating the RV melt-through failure mechanism obviates the need for a mitigating feature such as a core catcher, thereby avoiding the substantial cost of a core catcher.

6A.3.2.10 Improvements to the Design of the In-Vessel Retention

The additional power capability of the AP1000 design over the AP600 design has increased the severe accident (core melt) demands on the IVR design solution. To maintain the passive response to severe accidents, the design of the AP1000 IVR required some modification. The result of the testing performed for the AP600 design to establish the thermal hydraulic parameters associated with core melt did not provide sufficient margin to the calculated parameters for the AP1000 design.

To achieve the removal of the AP1000's higher decay heat and to maintain significant margin to the critical heat flux, the IVR heat transfer mode could not be by bulk boiling. The design team redesigned the reactor insulation such that the steam generated during the vessel cooling was not vented to the containment atmosphere but was instead re-introduced into the flooded portion of the containment at the RV nozzle level. The purpose of this design change was to create two-phase natural circulation within the RV insulation package; with the containment single phase flood-up water providing water into the bottom inlet of the insulation, and two-phase steam and water exiting the insulation at the nozzle gallery. This two-phase circulation flow path was expected to create significant cooling water velocities along the vessel wall that would significantly increase the critical heat flux and allow greater heat removal rates without failing the RV wall.

To realise this solution, the design team had to demonstrate two things: first, prototype testing had to be performed to duplicate the two-phase natural circulation flow path and establish the cooling fluid flow velocities, measure the critical heat flux limits, and demonstrate sufficient margin to these limits given the heat fluxes expected during a core melt; second, a mechanical design of the RV insulation had to be optimised to maximise the RV heat removal in a severe accident. All of these objectives were achieved. Testing was performed at the University of California, Santa Barbara, to establish the two-phase flow rate capability, determine the heat removal capability, show substantial margin to critical heat flux, and establish the design parameters for the vessel insulation. A unique design of the lower portion of the RV insulation was developed that used buoyancy to allow water in, when present, but not to allow air flow into the insulation/vessel annulus during normal plant operation. This design solution for enabling IVR at the AP1000 plant power level was selected and implemented in the design.

In addition, the RV insulation design was modified to increase the flow areas of the water inlet devices and steam outlet devices, make their operation by natural forces simpler and more reliable, provide additional shielding during normal operations, and make the design easier to fabricate and erect.

This solution was chosen using a process that promoted satisfying design requirements with the least change to the current design, high reliance on proven technology (natural forces), and lowest risk for public or operator radiation exposure.

Advantages and Disadvantages

The following advantages result from improving the design of the IVR:

- Minimum changes from the AP600 design and hence read through of the AP600 design test results.
- Improved reliability of the natural circulation capability.
- Additional shielding provided, thereby reducing operational dose.
- Easier to fabricate and erect, thereby reducing cost.

The only disadvantage resulting from improving the design of the IVR is that it required additional structure and a shaped internal boundary for the RV insulation design, which incurred a development cost.

6A.3.2.11 Alternative Source of Cooling for the Normal Residual Heat Removal System Heat Exchangers

The RNS cools the core when it is shut down at low pressure by reducing the temperature of the RCS during the second phase of plant cooldown, the first (high-pressure) phase of the cooldown being the transfer of heat from the RCS to the MSS through the SGs. The RNS draws reactor coolant from the RCS hot leg and then cools it in two HXs outside the containment before returning it to the RV through the direct vessel injection lines. Its HXs are cooled by the CCS.

An alternative heat sink would be desirable in the unlikely event that component cooling water flow to the RNS HXs should be lost. The FPS provides this additional method for cooling. What the AP1000 design requires is to include a fire hose connection point at the input side of the HXs and a drain at the HX outlet. The cooling water would go through the system once, its supply coming either from one of the two firewater storage tanks or from any external source such as a fire engine.

This simple use of a fire protection connection in a once-through cooling mode provides additional defence in depth capability for cooling the RNS. This solution was chosen using a process that promoted satisfying design requirements with the least change to the current design, high reliance on proven technology, and lowest risk for public or operator radiation exposure.

Advantages and Disadvantages

The advantage of using a fire protection connection in a once-through cooling mode is increased reliability of the RNS.

The only disadvantage is that less firefighting water would be available in the event of a fire simultaneously with the loss of the component cooling water.

6A.3.2.12 High-Pressure Normal Residual Heat Removal System

The core damage frequency from interfacing system LOCA (ISLOCAs) for currently operating PWRs is now known to be substantially greater than the PSA estimates made when they were designed. An ISLOCA is an event in which a break occurs outside the containment in a system connected to the RCS. Early PSAs were typically limited to modelling ISLOCA sequences that included only the catastrophic failures of the check valves that isolate the RCS from the low-pressure systems. Also, the PSAs included little consideration of human errors leading to an ISLOCA and the subsequent effects of the accident-caused harsh environment or flooding on plant equipment and recovery activities. Because of this concern, the AP1000 plant designers have re-evaluated the design pressure of the RNS.

The RNS is a duty system that provides shutdown cooling for the RCS. During normal shutdown operations, the RCS is cooled and depressurised to the RNS's cut-in temperature and pressure.

Once RCS pressure has been reduced, the RNS suction line isolation valves are opened and the RNS pumps are started to provide the shutdown cooling. The RNS takes suction from the RCS hot leg and discharges to the RV through the direct vessel injection lines. The RNS suction lines (one to each RNS pump) contain three normally closed isolation valves in series; with a design pressure equal to RCS design pressure.

The valves are interlocked so that they cannot be opened unless the RCS pressure is reduced to 3 MPa (450 psig), which is within the design pressure of the low-pressure portion of the RNS. The normally closed isolation valves, including the valves that are containment isolation valves, are designed for full RCS pressure.

Overpressurisation would only occur if the three motor-operated isolation valves leaked excessively, or if the valves were inadvertently opened with the RCS pressure above the design pressure of the RNS.

The second potential over pressurisation pathway for the RNS is by way of the discharge lines, which each connect to a direct vessel injection line. Each line contains two normally closed check valves, which, as reactor coolant pressure boundary valves, are designed for the RCS design pressure. The RNS discharge lines penetrate the containment and have two containment isolation valves that are again designed for full RCS pressure.

Overpressurisation would occur only if the three check valves and the motor-operated gate isolation valves leaked excessively. The portions of the RNS from the RCS to the outside containment isolation valves are designed for the design pressure and temperature of the RCS. Traditionally, the portion of the RNS outside containment was designed to 4 MPa (600 psig). In operating plants today, ISLOCAs are discounted, based on the suction valves' interlock with RCS pressure and the power lock-out of these valves at the valve motor control centres. Such a design provides multiple redundant system isolation and a system design pressure that is 27 percent of RCS design pressure and 1 Mpa (145 psig) higher than the operating pressure of the RNS.

Guidance from the Nuclear Regulatory Commission (NRC) has suggested that a design pressure of 40 percent of the normal operating pressure of the RNS and a minimum wall thickness would enhance the survivability of the piping to more than 90 percent when pressurised to full RCS pressure. As a result of this suggestion, the design pressure of the AP1000 RNS outside containment has been increased to 6.1 Mpa (900 psig), to decrease the likelihood of ISLOCAs in the RNS.

Advantages and Disadvantages

The following advantages result from increasing the design pressure of the low-pressure portion of the RNS:

- Significant reduction in the likelihood of an ISLOCA
- Lower risk of public or operator radiation exposure
- Fairly simple to engineer

6A.3.3 Containment Design

6A.3.3.1 Low-Leakage Steel Containment

Containment is the last boundary preventing an uncontrolled release of radioactive fission products or coolant to the environment. It is a design requirement for the containment to retain its contents during any design basis initiating event such as a steam line break or a LOCA, and certain beyond design basis initiating events such as a LOCA. Thus, the containment design must be able to withstand the maximum expected pressure during any design basis accident and following a large-break LOCA.

The containment buildings of currently operating PWRs are typically steel lined, concrete and steel structures that can become relatively porous in time due to small cracks resulting from thermal expansion and contraction and due to periodic pressurisations (leakage tests) during the plant operating life. For this reason these structures are constructed with a thin, steel liner that forms the main barrier to leakage. These containments typically rely on internal sprays and/or water cooled fan coolers to limit containment pressure and reduce pressure following a postulated accident. The sprays are supplied by active pumping systems, and require supporting cooling water, electrical power, and HVAC systems. The same is true of fan cooler type cooling designs. Given the assessed reliability of such arrangements, some regulators require provisions for venting of the containment before it became overpressurised or its concrete weakened by the high temperature to provide defence in depth. These venting systems then require the addition of large filtration equipment or structures to prevent the direct release of radioactivity to the public. The use of containment venting to provide defence in depth for ensuring containment integrity creates specific problems in that, when core steaming is terminated or when containment cooling system function is restored, it is possible that the pressure within the containment is reduced significantly below atmospheric pressure. This results in damage to the thin containment steel liner that forms the leak-tight barrier to the release of radiation such that the design basis leakage may be exceeded. These plants then rely on the containment missile barrier (sometimes referred to as the secondary containment) and large HVAC equipment and filters to remove sufficient radioactivity to minimise releases to the public and operating personnel.

The AP1000 design achieves a containment that can reliably withstand any design basis accident including a large-break LOCA without leaking. It does this by adopting a steel containment structure cooled by water draining by gravity over its outer surface, which evaporates into a naturally flowing current of air. The containment structure is a freestanding steel pressure vessel, designed and built in accordance with the requirements of the ASME Code. This vessel has a high enough design pressure, a large enough free volume, and a large enough heat transfer area to accommodate the worst pressure challenge resulting from any design basis accident or a large-break LOCA without any requirement to vent. Unlike concrete, it is not unduly susceptible to high temperatures. The pressure vessel design requirements extend to its penetrations and attachments.

Advantages and Disadvantages

The following advantages result from using a steel containment structure:

- The gravity-fed arrangement for the distribution of water over the exterior of the steel containment vessel is far more reliable than the traditional pumped containment spray and/or fan coolers and their associated support systems, thereby providing a passive means of removing heat and reducing containment pressure.

- The only real leak paths though the steel containment are through the containment penetrations, which are periodically tested. Leakage though the 44.45-mm (1.75-inch) thick steel or the fully radiographed welds is incredible. This allows the AP1000 plant steel containment to have a greatly reduced design leak rate compared to concrete containments. This alleviates the need to have a double containment with HVAC and filtered exhaust to meet the required onsite and offsite dose limits.

- The steel containment will not exceed its ultimate failure pressure for an extended time following a large-break LOCA, even if no water is applied to the outside surface and there is only air cooling of the containment. This provides the plant operators with a significant time to establish water application to the shell without the need to vent the containment post accident.

The only disadvantage resulting from using a steel containment structure is that it is does not have as high a resistance to external pressure as a concrete and steel reinforce containment.

6A.3.3.2 Containment Height Increase

The increase in electrical power output in moving from the AP600 design to the AP1000 design required increasing the size of some of the principal components within the containment: RV, SGs, and pressuriser. This necessitated some increase in the size of the containment to accommodate them, albeit retaining the same layout as the AP600 design. However, a more important consideration was the internal pressure following a fault sequence.

The increased power of the AP1000 design inherently increases the steam mass and energy released into the containment building as a result of a LOCA or main steam line break. An essential requirement for the containment is to provide sufficient free volume to accommodate the mass and energy release from such an event without challenging the containment design limits. Not only were the mass and energy releases for AP1000 design greater than those for AP600 design, but the limiting event changed from a LOCA to a main steam line break.

The options were to increase the free volume of the containment or to make it stronger, or some combination of the two. Making the containment larger by increasing its diameter was not an attractive option because this would involve extensive redesign. Additionally, increasing the diameter would require a pro-rata increase in steel thickness for a given post-accident pressure, which would contravene the design constraint of containment vessel plate being sufficiently thin that post-welding heat treatment during installation in the field would not be required; this consideration also limits the option of increasing the containment strength whilst keeping its original size (the option of massively strengthening the containment is reviewed in subsection 6A.5.1).

The design decision was to make the containment vessel taller but by as little as possible. Once the diameter is fixed, the strength of the containment vessel is determined by the material type and by maximising the plate thickness to 44.45 mm (1.75-inch) from the AP600 thickness of 39.8 mm (1.66 inches). The selection process was first to investigate alternate plate material to maximise vessel strength. This would minimise height by minimising the volume increase required for the increased mass and energy release.

Once plate material and thickness had been selected, the height was changed by integral increments of commercially available plate width to maximise simplicity of fabrication. As the volume increases for each plate width, the resultant peak accident pressure decreases. The least number of additional plate widths was chosen consistent with the requirement to be within the maximum allowable containment vessel pressures. The design outcome was a slightly increased margin to plate allowable stresses compared with the AP600 design.

In summary, the containment vessel plate material and additional vessel height were chosen in a process that promoted satisfying its design requirements with the lowest risk of a containment breach during an accident sequence, high reliance on proven technology (natural forces), and lowest cost.

Advantages and Disadvantages

The following advantages result from increasing the height of the containment rather than its diameter:

- The existing plant layouts, pipe routings, building structural calculations, building seismic responses, component seismic responses, system flow calculations, accident response calculations, and containment flood-up volumes are largely unaffected, thereby avoiding the substantial costs of redoing them.

- The need for post-welding heat treatment during installation is avoided for the containment vessel plate.

- The containment design basis external pressure limit is not reduced.

Disadvantages resulting from increasing the height of the containment rather than its diameter are as follows:

- A taller shield building is required.
- A taller shield building results in the PCCWST being higher off the ground. A higher PCCWST makes the justification of the seismic withstand of the auxiliary building more challenging.
- The taller containment requires one more heavy lift structural module than the AP600 (this would most likely be true for the increased diameter containment due to the increased plate area vs. height).

Shield Building Air Inlets

The PCS transfers heat directly from the steel containment vessel to cooling air drawn from the external environment, thereby with water evaporation from the shell outer surface, preventing the containment vessel from exceeding its design pressure and temperature following an accident. The PCS has inlets for the cooling air located near the top of the cylindrical section of the shield building.

The air inlets must be structurally robust because they are part of the shield building, which protects the steel containment structure from various external hazards, one of which is the crashing aeroplane. The design of AP600 plant air inlets consists of 15 large discrete openings in the top of the shield building, which penetrate the 914-mm- (3-foot-) thick reinforced concrete shield building. The air inlets are sized to allow containment cooling at a level sufficient to ensure that the peak containment pressure does not surpass the containment design pressure following any design basis initiating event. Air inlets of this type and size are also sufficient to support containment cooling for the AP1000 plant, and were incorporated into its original design.

However, it has since been questioned whether this design is sufficiently robust to withstand the impact of a large commercial aircraft. An additional concern is that the large openings provide a pathway for debris or fuel from a crashing aircraft to reach the steel containment vessel. It has been decided that the shield building must incorporate design features that provide inherent protection against the effects of such aircraft impact, which are regarded as beyond design basis (BDB). Therefore, alternative designs were explored for the AP1000 plant with the goal to maintain the original cooling airflow rate capability but strengthened the shield building at the elevation of the air inlets so as to withstand a BDB impact of a large commercial aircraft.

One solution would have been to greatly increase the thickness of concrete of the shield building at the elevation of the air inlets. However, impact testing has shown that containing high-strength concrete within steel liner plates on both faces significantly increases its impact resistance, so a more modest increase in concrete thickness could provide the required strength. Analysis demonstrated that modifying that portion of the shield building containing the air inlets to a 1.37-m (4.5 feet) thickness of high-strength concrete contained within steel liners on both faces was sufficient for that portion of the shield building to withstand a BDB aircraft impact.

Reducing the size of the air inlets to restrict debris or fuel from entering the building further enhanced the air inlet portion of the shield building. Containment cooling requires a minimum inlet area to provide adequate air cooling for the steel containment vessel. However, each air inlet does not have to be as large as the 15 air inlets of the original design, provided that a significant flow area was maintained. This could be achieved by dividing the flow area into many smaller air inlets. The optimum design was found to be for 236 small inlet ducts to replace the original 15 large openings. The smaller inlets consist of 457-mm (18-inch) diameter circular steel tubes inclined upward from outside face to inside face. The new air inlets present no significant change to the design basis pressure response; for cases when the PCS operates; and does not significantly reduce the time for operator actions to maintain the containment below failure pressure for the BDB, air-only cooling situations assumed by PSA. The redesigned air inlets also provide a significant increase in the shield building's ability to restrict debris and fuel from entering it because of their small size and orientation. This design provides an additional safety benefit by further reducing radiation sky shine.

Advantages and Disadvantages

The following advantages result from strengthening that portion of the shield building containing the air inlets, and replacing the 15 large air inlets with 236 small inlet ducts:

- Strengthening of the upper portion of the shield building provides protection against the impact of a large commercial aircraft.
- Redesign of the air inlets significantly reduces the risk of damage to the steel containment structure from burning fuel and debris from a crashing aircraft.
- Redesign reduces the radiation sky shine.

The disadvantages resulting from strengthening that portion of the shield building containing the air inlets and replacing the 15 large air inlets with 236 small inlet ducts are:

- The BDB air-only PCS cooling capability of the PCS is reduced.

6A.3.3.3 Post-accident Isotope Control

Radioactive isotopes accumulate in the reactor coolant during operation. Some of these isotopes are gaseous or volatile; most are soluble or suspended in reactor coolant water. During a LOCA, these accumulated isotopes are released into the upper containment, thereby creating a radiation source. This source can be strong enough to be a hazard to those outside the containment.

The currently operating PWR plants use a containment spray system to cool the containment atmosphere; however, this spray also washes these soluble and suspended isotopes out of the containment atmosphere and off the containment walls. These containment spray systems include a water source outside the containment, containment penetrations, pumps, valves, nozzles, and other equipment that must be redundant, qualified, controlled, tested, maintained, and repaired.

The AP1000 plant does not need a containment spray system to cool the containment atmosphere because this function is performed by the PCS. The principal means of post-accident isotope control for the AP1000 design relies on natural forces like natural convection, condensation, and conduction to transfer decay heat from the atmosphere of the

containment to the containment walls, which are cooled (there is also a containment spray utilising the FPS (see subsection 6A.3.3.10) as a backup for this function). The resulting steam condenses onto the containment wall and then returns to IRWST or to the containment sump by gravity. Through analysis and testing, it has been shown that the soluble and suspended isotopes move with the water and thus finish up in the water in the IRWST or the lower portions of the containment.

Advantages and Disadvantages

The following advantages result from using the natural convection and condensation of the steam on the containment walls to remove radioactive isotopes from the containment atmosphere:

- The mechanism for isotope removal is entirely passive, with no risk of active failure.
- No risk of containment bypass due to a failed containment spray penetration.
- Reduction in complexity and cost in not having to install a Class 1 safety-grade containment spray system.

The only disadvantage is that it creates a slightly higher general accident dose rate outside the containment, but one still within allowable limits.

6A.3.3.4 Fire Protection Function for the Passive Containment Cooling Water Tank

The regulations for nuclear power plants in the United States (US) require that the fire protection water delivery system for fires affecting Class 1 equipment must be classified as Seismic Category 1. The AP1000 design has the additional requirement that safety functions must be performed without ac power.

Other than the containment building, the AP1000 plant only has one building that houses such Class 1 equipment: the auxiliary building, which is divided at each level by a concrete wall without any doors. On one side are systems with potentially radioactive fluids; on the other, the clean side, are the plant control and protection equipment and control room operators. The lowest level of the auxiliary building is below grade, so there can be no drainage of firewater without ac power. Consequently, there is a restriction of how much water can be put into the nonradiological clean side of the auxiliary building.

The AP1000 design process was directed at creating a FPS that requires no safety claims to be made on fire fighting fluids at all. This was attempted by careful design of the plant layout into fire areas and zones, such that the equipment in a given fire area could be lost to the fire without loss of overall plant safety functions. Within the containment building, additional spatial separation requirements were enforced for redundant equipment to make sure safety functions could be maintained in the event of a fire in the containment. This eliminated the requirement for a pumped FPS for internal fire hazards except for BDB fire events in the clean side of the auxiliary building.

Thus, the only required firewater delivery system is to the clean side of the auxiliary building, and preferably one in which the water to the fire hose stations is delivered by gravity rather than by pumps. The solution adopted by the AP1000 plant designers is to dedicate a specific amount of water within the PCCWST to this particular duty. This tank is seismic Category 1. The firewater delivery system can deliver two hose streams of 17 m^3/hr (75 US gallons per minute) for 2 hours.

A standpipe within the PCCWST limits the amount of PCCWST water that can be drained for fire fighting to less than amount of water that would threaten (flood) the Class 1 safety equipment in the nonradiological portion of the auxiliary building.

Advantages and Disadvantages

The following advantages result from using the PCCWST as the source of fire fighting water to the clean side of the auxiliary building:

- The supply to the firewater delivery system is already seismically qualified because of its primary safety duty, thereby avoiding the substantial cost of a new dedicated, seismic Category 1 tank.
- It does not require safety-related ac power or diesel-powered fire pumps.
- The amount of firefighting water that can be delivered is restricted to less than the amount that could flood Class 1 equipment by the simple expedient of using a standpipe within the PCCWST.

The only disadvantage of using the PCCWST as the source of fire fighting water to the nonradiological side of the auxiliary building is that the PCCWST capacity was slightly increased to include the required firewater volume.

6A.3.3.5 Catalytic Hydrogen Recombiner

A variety of PWR accident sequences can generate free hydrogen gas in the containment atmosphere. Most of these generate very small amounts, but some BDB accidents can generate large amounts. Regardless of the source, accumulations of hydrogen could rise to a potentially explosive level following such accidents.

To provide continuous, hydrogen removal capability that does not rely on ac power, catalytic hydrogen recombiners were chosen for in-containment hydrogen control in addition to the hydrogen igniters placed throughout containment. The passive autocatalytic recombiners are simple and passive in nature, without moving parts and no requirement for electrical power or any other support system. They are self-actuated in the presence of the reactants: hydrogen and oxygen. Passive autocatalytic recombiners are effective over a wide range of ambient temperatures, concentrations of reactants (rich and lean, oxygen/hydrogen less than 1 percent), and steam inerting (steam concentrations greater than 50 percent).

The catalytic hydrogen recombiner capacity is sufficient to reduce the hydrogen released following all design basis events.

A hydrogen ignition system is provided to address the possibility of a BDB event that results in a rapid production of large amounts of hydrogen, such that the rate of production exceeds the capacity of the recombiners. The primary objective of installing the catalytic hydrogen recombiners is to remove hydrogen at low concentrations and, to the extent possible, to remove hydrogen from the containment atmosphere more or less continuously so that the hydrogen concentration does not build up in the containment.

Advantages and Disadvantages

The following advantages result from incorporating catalytic hydrogen recombiners:

- They function at low hydrogen concentrations and operate passively, with no reliance on electrical power.
- They result in the lowest risk for hydrogen detonation, which might possibly result in a release of radioactivity from the containment.
- Proven technology.

Disadvantages resulting from incorporating catalytic hydrogen recombiners are as follows:

- Their capacity is limited to moderate hydrogen production levels and would be inadequate for certain severe accidents that are BDB.

6A.3.3.6 Trisodium Phosphate Baskets

Following a LOCA, it is necessary that the flood-up water inside the containment be treated to make its pH at or above 7.0. This is done to enhance radionuclide retention within the water inside the containment (in particular, prevent the formation of elemental iodine in the containment sump), and to prevent stress corrosion cracking of containment components during long-term containment flood-up. In many operating plants, this pH control is established by the chemistry of the containment recirculation water brought in from tanks outside containment. However, the response of an AP1000 plant to a LOCA without ac power does not involve any water entering or leaving the containment.

The possibilities for pH control inside the containment during a LOCA were investigated and analysed. This included consideration of tanks with buffer solution and baskets with solid TSP placed in containment. TSP is safe, stable, readily soluble in water and easy to inspect. The chosen option was to install baskets containing TSP at a low elevation in the containment, well below the containment flood-up level for continuous recirculation. In the event of a LOCA, the water accumulating in the lower region of the containment would self-buffer by dissolving the TSP. The pH adjustment is capable of maintaining containment pH within a range of 7.0 to 9.5.

Advantages and Disadvantages

The following advantages result from incorporating TSP baskets low in the containment:

- Buffers the containment recirculation water passively with no reliance on operator action or automatic initiation.
- Eliminates the possibility of inadvertent discharge of chemical solutions inside containment.
- Thoroughly tested and practicable

- Lowest initial cost
- Easy to inspect and does not degrade
- Relatively harmless to people

There are no disadvantages identified from incorporating TSP baskets.

6A.3.3.7 Provision for Post-72 Hour Continuation of Class 1 Equipment Functions

It was suggested that 72 hours of operation of Category A functions by Class 1 equipment (i.e., containment cooling, dc electrical power supply, control room habitability, SFP water makeup, and post-accident monitoring) could be insufficient to allow external resources to arrive onsite, based upon the experiences with hurricanes in the US. It was also suggested that potential onsite resources might not be available unless they were qualified. For example, the site firefighting water supply should be assumed to be unavailable for supplying water to continue containment cooling. Hence, there is a requirement that an onsite, qualified capability to continue containment cooling must be available for the period up to 7 days, assuming a total loss of offsite power.

Installing a much larger tank on the top of the shield building, or providing additional batteries to allow continued operation for 7 days would have required a total re-evaluation of the AP1000 design, with major changes in the AP1000 structures and passive safety concept. Given the costs involved, the ensuing time delays, feasibility issues, and limited improvement in actual plant safety; this was not considered to be a practical option.

One option for satisfying this requirement would be to seismically qualify and missile protect the site FPS. Another possibility would be to add a new qualified system for providing water to the PCCWST. After due consideration, the AP1000 plant designers decided that the latter option was their preference. A C-II ancillary water tank (PCCAWST) that is designed for site meteorological conditions and wind-generated missiles was added to provide sufficient water for post-72 hour PCS cooling and SFP water makeup. The existing PCS recirculation pumps equipment anchorage and associated piping inside the auxiliary building were upgraded to seismic class II, and two ancillary diesel generators and their fuel supply were added into the seismic II portion of the Annex building to provide power for the PCS recirculation pumps, MCR ventilation, and for recharging the Class 1 batteries.

Because the FPS and DWS already have piping connections to the PCCWST from the auxiliary building, the designers chose to use it as an additional method for replenishing the water inventory. This can be achieved by supplying it either from the fire protection or demineralised water tanks, or from any external source using a fire pump truck connecting onto the existing fire supply hose connection point on the outside of the auxiliary building. This simple use of using the existing fire protection and DWS connections provides defence in depth capability to replenish the PCCWST.

Advantages and Disadvantages

The following advantages result from adding a new qualified tank, pumps, and diesel generators to continue the required Class 1 SSC operations beyond 72 hours:

- Much lower cost and avoidance of a huge delay in the AP1000 plant programme from making the PCCWST substantially bigger.
- Lower cost than making the entire FPS a qualified system.
- High reliance on simple proven technology, that is, pumps used during normal operations and two small, local diesel generators.
- Ease of connecting a mobile fire-pumping engine to the new qualified PCCAWST water tank to further extend PCS and SFP cooling should the other sources of onsite water remain unavailable after 1 week.

The only disadvantage is that the reliability of the active post-72 hour SSCs is intrinsically lower than the Class 1 SSCs that they support.

6A.3.3.8 Containment Spray from the Fire System

As demonstrated in subsection 6A.3.3.5, the AP1000 design does not rely on containment spray for post-accident isotope control. However, the US NRC requires that the AP1000 design include a manually initiated containment spray for certain BDB initiating events, not only for isotope control but also as an alternate means for flooding the RV (IVR), for debris quenching should vessel failure occur, and to control containment pressure should the PCS fail.

One design solution to this requirement that was considered was to include a dedicated containment spray system with its own pumps, valves, water source, and containment penetrations. An alternative, simpler solution was to feed the containment spray headers and nozzles from an existing system within the containment. The selected system was that portion of the FPS that is within the containment. This provides the containment spray function without the need for the additional equipment of a dedicated spray system.

Advantages and Disadvantages

The following advantages result from providing the water supply to the containment spray headers and nozzles from the existing FPS:

- Substantial reduction in complexity and cost in not having to install an additional spray water supply to the containment spray headers and nozzles.
- The in-containment fire system already achieves the required reliability for a backup system that is only required for BDB fault initiating events.
- There is no increase in the testing and maintenance burden.

The only disadvantage resulting from incorporating the existing FPS in the containment spray system is that there is less water available for fire fighting should there be a fire simultaneous with the BDB sequence where the use of sprays is required.

6A.3.3.9 Minimisation of the Number of Containment Penetrations

The penetrations through the containment are designed to be leak tight and allow pipes and cables to pass through the containment vessel boundary with no loss of the containment atmosphere, which might be pressurised and radioactive after an accident, and escape to the outside environment. Very often, however, they do constitute sites of small leakage pathways. The penetrations and their associated piping up to the first isolation valves are Class 1 and must be periodically inspected and tested. Minimising the number of penetrations reduces the possibility of containment leakage during a fault sequence, and reduces the inspection and maintenance burdens.

The use of passive safety systems and the placement of all PXS components and water supplies inside containment has eliminated many of the containment penetrations that are required for Class 1 systems in evolutionary plant designs. In addition, the AP1000 plant designers have reduced the number of penetrations by using a variety of innovative techniques as follows:

- Service systems within the containment, such as component cooling water or compressed air, are configured inside the containment so as to require only one supply or return penetration for each service.

- Some intermittent services with common fluids share common penetrations. For example, both the chilled water and the hot water heating services to HVAC within the containment share common penetrations, since they will not be used at the same time.

- The fire fighting water and the containment spray supply systems also share a common penetration.

- C&I penetrations are reduced by taking advantage of digital data highway technology. Multiplexing cabinets are located so that C&I signals share a common highway penetration in lieu of multiple individual signal penetrations.

Advantages and Disadvantages

The following advantages result from minimising the number of containment penetrations:

- Reduces the possibility of containment leakage during a fault sequence.
- Reduces the cost of providing penetrations.
- Reduces the inspection and maintenance burden.

There are no significant disadvantages resulting from minimising the number of containment penetrations.

6A.3.4 Control Room Systems

6A.3.4.1 Use of Digital Control and Instrumentation Systems

The digital C&I systems within the AP1000 plant control, protect, and monitor the reactor and plant. They consist of the following systems linked by real-time data highway:

- Protection and Safety Monitoring System (PMS)
- Special Monitoring System (SMS)
- Plant Control System (PLS)

- Incore Instrumentation System (IIS)

The Diverse Actuation System (DAS) does not link to the data highway.

The above systems have been subjected to safety evaluations that show that they can be designed and built to conform to the applicable criteria, codes, and standards concerned with the safe generation of nuclear power.

The real-time data highway is a high-speed, redundant communications network that links systems of importance to the control room and the DDS. Class 1 systems are connected to the network through gateways and qualified isolation devices so that the Category A safety functions are not compromised by failures elsewhere. Plant protection, control, and monitoring systems feed real-time data into the network for use by the control room and the DDS.

Protection and Safety Monitoring System

The PMS detects off-nominal conditions, and then actuates the appropriate Class 1 systems necessary to achieve and maintain the plant in a safe condition. It also controls the Class 1 components in the plant that are operated from the MCR or the remote shutdown workstation. In addition, the PMS provides the equipment necessary to monitor the plant Class 1 functions during and following an accident.

The adequacy of the hardware and software within the PMS has been demonstrated through a verification and validation process so that, in particular, the software development process is consistent with appropriate industry standards.

Special Monitoring System

The SMS does not perform any Category A or defence in depth safety functions. The SMS consists of specialised subsystems that interface with the C&I architecture to provide diagnostic and long-term monitoring functions.

Plant Control System

The PLS provides the functions necessary for normal operation of the plant, from cold shutdown to full power. This system controls the duty systems in the plant, which are operated from the MCR or remote shutdown workstation. The PLS contains the C&I needed to change reactor power, control pressuriser pressure and level, control feedwater flow, turbine control, and perform other plant functions associated with power generation.

Diverse Actuation System

The DAS provides an alternate means of initiating reactor trip and actuating selected ESFs; it also provides plant information to the operator.

In-Core Instrumentation System

The primary function of the IIS is to provide a three-dimensional flux map of the reactor core. This map is used to calibrate neutron detectors used by the PMS, as well as to optimise core performance. A secondary function of the IIS is to provide the PMS with the thermocouple signals necessary for the post-accident inadequate core cooling monitor. The in-core instrument assemblies house both fixed in-core flux detectors and core exit thermocouples.

Advantages and Disadvantages

The following advantages result from adopting digital C&I instead of an analogue system:

- Opportunity to incorporate more advanced control system concepts, thereby allowing better and more refined control.
- Enhanced human-machine interface features to reduce operator burden.
- Online component testing at full power and in less time.
- Improved C&I system availability, achieved through redundancy and advanced diagnostics.
- Significantly reduced costs of initial installation and through-life maintenance.
- Relatively easy to carry out through-life updates of the hardware, as its functionality depends only on the software, which is also relatively easy to update.
- Reduced likelihood of plant trips caused by C&I system problems.
- Use of a data highway eliminates large quantities of C&I system hardware, cabling, cable trays, cable spreading areas, containment penetrations, and other equipment.

The only disadvantage resulting from adopting digital C&I instead of an analogue system is that it is more difficult and expensive to verify the integrity of a programmable electronic system of such complexity.

6A.3.4.2 Use of a Digital Control Room

The control room provides the facilities that the operations personnel need to safely operate the plant, deal with any abnormal conditions, and produce electricity. Over the past few decades there have been many substantial advances in the technology of the operator-machine interfaces in modern control rooms. The success of modern control rooms has been proven in other comparable industries. The AP600 design and the subsequent enhancements in the AP1000 design have taken advantage of this new operator-interface technology, and the resultant MCR represents a move away from the traditional “control board” control room design:

- The number of fixed controls and displays has been minimised to the extent practical.
- The main operator-machine interface is by means of computer-based colour monitors, mice, and keyboards.
- The graphics are supported by a set of graphics workstations, which take their input from the real-time data network.
- An advanced alarm system, implemented in a similar technology, is also provided.

The data display and processing (plant computer) system is implemented in a distributed architecture. The working elements of the distributed computer system are graphics workstations, although their graphics capability is secondary to their computing performance.

The distributed computer system obtains its input from the real-time data network and delivers its output over the network to other users.

Advantages and Disadvantages

The following advantages result from new operator-interface technology in the MCR:

- The advanced control room technology has been proven to improve operator performance, increase productivity, and reduce the likelihood of human errors.
- The visual display units (VDU) -based operator-interface integrates a number of systems into one flexible interface technology. This includes the use of large screen displays that enable plant overview and alarm status information to be visible from any likely operator location in the MCR, thus facilitating crew group plant status awareness and decision-making.
- The number of operations personnel required to be located in the control room may be decreased, thereby reducing electric generation costs.
- Increased ease in modifying the display formats.
- Increased ease in updating the control room hardware.

The only disadvantage resulting from new operator-interface technology in the MCR is that the software driving the displays is difficult and expensive to verify.

6A.3.4.3 Inclusion of a Diverse Actuation System

The DAS provides an alternate means of initiating a reactor trip and actuating specific ESFs in the event of a common mode failure within the PMS; that is, it provides diverse backup to the main protection system. The DAS has three functions: diverse automatic actuation, diverse manual actuation, and diverse indication of the plant information needed by the operator for a manual actuation of critical safety measures.

The DAS is included within the C&I architecture to support the risk goals in the AP1000 plant PSA for analysed events (Chapter 10). The DAS reduces the probability of a severe accident resulting from the unlikely coincidence of a postulated initiating event (PIE) and postulated common-mode failures in the protection and control systems. Common-mode failure between the PMS and the DAS is unlikely because each runs on a different operating system from the other, and there are no sensors shared between the two systems.

The DAS is not claimed as a safety measure by the fault schedule. However, it does provide defence in depth, and as such it possesses either two-out-of-three or a one-out-of two taken twice logic to prevent spurious actuation, and is designed to higher quality standards than normal duty systems.

Advantages and Disadvantages

The following advantages result from the inclusion of the design:

- Diverse initiation of specific safety measures in the event of a common-mode failure within the PMS.

- Diverse indication to the operators in the event of a common-mode failure within the PMS.

Disadvantages resulting from the inclusion of the DAS in the AP1000 design are the following:

- It might cause some spurious reactor trips.
- Initial cost and through-life maintenance cost.

6A.3.4.4 Human Factors Enhanced Control Room

The AP1000 MCR is an evolution of the AP600 design. It takes full advantage of the latest control room operator-interface technology. A detailed human factors engineering programme has supported the development of the AP1000 MCR and its operator-interface design. This programme included task analysis, operating experience reviews, engineering tests, the application of human factors' design guidelines, and verification and validation assessments.

The overall purpose of the MCR is to provide a comfortable environment in which the operators and supervisors can safely, efficiently, and reliably monitor and control plant process during normal, abnormal, and accident conditions. Displays are provided to enable the operators to determine the plant status, and control facilities are provided to allow the operators to execute control actions. Alarms are provided to draw the operators' attention to key indications that may require operator action. It must remain habitable during abnormal or emergency conditions, including earthquakes.

The MCR provides an area that enables the operations personnel to focus their attention on the safe and efficient operation of the plant. It supports good operator performance by supplying the facilities for the operators to interact with other plant personnel, while preventing distractions from nonoperations personnel. It supports the operations personnel in the effective and timely execution of their assigned tasks and responsibilities.

The MCR accommodates an operator console, a supervisor's console, safety consoles, the wall panel information system, large screen displays, and the DAS panel. The operator console provides the displays and controls to start up, manoeuvre, and shut down the plant; it is designed to be staffed by one to six operators. The operator interfaces are the duty system control displays, soft controls, alarm presentation system displays, computerised procedures displays, as well as the VDU monitors, keyboards, and mice. The supervisor's console is a smaller version of the operators' console and is designed to be staffed by one or two personnel. The primary dedicated safety panel and VDU-based safety system workstations are located at the centre of the operator console, with a secondary safety panel located in close proximity to the supervisor's console. The DAS panel is located at a sidewall in the MCR. The MCR also includes communication devices; document laydown areas, printers, and storage space. A meeting table is provided and equipped with a VDU-based workstation to allow access to the duty control system by, for example, a technical advisor or shift manager, without disrupting control room operations. In close proximity to the MCR are

the shift supervisor's office, the operations staff area, an operations work area, restrooms, and kitchen facilities.

Advantages and Disadvantages

Incorporating the improvements from the detailed human factors engineering programme into the design of the AP1000 plant and its operator interfaces results in the following advantages:

- Enhances the performance of the operators during normal, abnormal, and fault conditions, with increased likelihood of success.
- Reduces the possibility of operator distraction, whilst allowing the necessary interaction with other plant personnel.
- Allows access to the duty control system by, for example, a technical advisor or shift manager, without disrupting control room operations.
- Simplifies initial construction of the MCR, resulting in substantial cost savings.
- Simplifies maintenance of the MCR, resulting in cost savings.

The only disadvantage resulting from incorporating the improvements resulting from the detailed human factors engineering programme into the design of the AP1000 plant MCR and its operator interfaces is significant development cost, but this is spread over the entire AP1000 fleet.

6A.3.4.5 Elimination of the Internal Flooding Threat from the Nonradiological Portion of the Auxiliary Building

The AP1000 auxiliary building is designed so that on each floor there is a solid concrete wall separating the spaces that are potentially radioactive and those that are not. The nonradiological side of the auxiliary building (the clean auxiliary building) accommodates the MCR and the rooms housing the plant control and protection hardware and their battery rooms.

Some of these would be under threat from flooding should there be any substantial leak of water within the clean auxiliary building. The potential sources of water in the clean auxiliary building are the potable water for the manned MCR spaces, the fire protection water for the safety-significant equipment within the clean auxiliary building, and the pipes carrying water from the containment building through the clean auxiliary building to the turbine building.

The lowest level within the clean auxiliary building is two floors below ground level, thereby requiring some means of preventing any water that might accumulate from becoming a threat to the safety-significant equipment housed there. This might be achieved either by establishing a large sump or by providing an active means for clearing any accumulating water (without using ac power), or by limiting the amount of potential flooding water to a volume that would not threaten any safety-significant equipment. The latter option was selected.

The potable water day tank is above the MCR area. It is filled as required but is otherwise isolated from external sources; thus any leakage is limited to the day tank volume.

The potable water piping from the tank is sized such that even in the event of a pipe rupture the leak rate would be modest. The pipes are routed within the manned spaces so that any leakage would be detected quickly. The potable water is thus not a flooding hazard to the Class 1 equipment within the clean auxiliary building.

The volume of fire protection water available to the auxiliary building is limited by the design solution discussed in subsection 6A.3.3.6. Even in the event that this fire protection water should flood the lowest level of the clean auxiliary building, the water level would be below that of the Class 1 battery electrical connections, the lowest Class 1 equipment in the clean auxiliary building. The maximum potential volume of water from the fire fighting water supply would thus not be a threat to any of the Class 1 equipment housed there.

The piping carrying water from the containment to the turbine building is routed through two rooms within the clean auxiliary building. Both of these rooms are enclosed in concrete, with the only routes for water to escape from them, including through the doors, being to drains within the turbine building. Thus, any leakage of water from the piping carrying water from the containment to the turbine building would not accumulate within the clean auxiliary building but instead would drain out of it by gravity.

Advantages and Disadvantages

The following advantages result from limiting the maximum potential volume of water that could flood the lowest level of the clean auxiliary building:

- Limiting the volume of the potable water tank costs nothing, and might even be slightly cheaper than a larger tank.

- The volume of fire protection water is restricted to below the amount where flooding could be a problem by the simple expedient of using standpipes within the PCCWST (see subsection 6.A3.3.).

Disadvantages resulting from limiting the maximum potential volume of water that could flood the lowest level of the clean auxiliary building are the following:

- The filling of the potable water tank needs to be manually initiated and performed on a regular basis.

- Reinforcing the two rooms containing the transfer piping from the containment building to the turbine building and installing drain paths to turbine building does incur a cost.

6A.3.5 Primary System Design

6A.3.5.1 Selection of the Reactor Coolant Pump Type

The type of RCP adopted for many currently operating plants is a shaft seal pump, A weakness of the shaft seal-type RCP is the potential for seal degradation and coolant leakage from the seal unless high-pressure, cold, seal injection water is provided, or cooling water flow is maintained to the RCP thermal barrier to cool any reactor coolant leakage through the seal. The AP600 designers felt that other types of RCPs should be considered since a basic design premise of the AP600 plant design was to maintain safety and respond to accident situations without reliance on ac power. Providing seal injection or thermal barrier cooling to the shaft seal RCPs for an extended time following the postulated loss of all ac power would be difficult to accomplish using only passive, natural forces.

A potential design option for the AP600 plant was the use of sealless motor pumps. It is noted that the AP600 required forced RCS circulation for normal operation at power, as natural circulation would be inadequate.

Sealless RCPs have been used in non-commercial nuclear applications. Sealless pumps used in these applications have been demonstrated to be highly reliable and represented a RCP solution with no possibility of coolant leakage since they have no seals to leak. The selection was made to use a sealless motor type pump for the AP600 design, based on simplicity, reliability, and experience with similarly sized motors. The pump is not claimed to function post-accident, and its pressure boundary is continuous, without any leakage during normal or fault conditions. The larger power rating of the AP1000 design required a significant upscaling of the pump/motors.

Advantages and Disadvantages

The following advantages result from choosing sealless pumps:

- No risk of a RCP seal LOCA through failure of the shaft seals or shaft damage following a loss of all ac power event, thereby significantly enhancing safety.

- Because the motor and the pump bearings are within the coolant boundary, the canned-motor pump also allows the designer to eliminate the shaft seal pump support systems, such as seal injection, seal leakoff, and lubricating oil system. In addition, the FPS can be simplified since no provisions for mitigating a lubricating oil fire are required. This avoids complexity and results in lower overall cost.

- Higher intrinsic reliability than shaft seal pumps.

- Reduced fire risk, because there is no lubricating oil system.

- Reduced radioactive effluent, because there is no shaft seal leak-off flow to collect and process.

- The decision to attach the pumps directly to their SG, eliminates the crossover leg required for shaft seal pumps. This also eliminates the high/low stagnation portion of the crossover, thus promoting natural circulation for post-accident cooling, and there is no depression of the water level in the reactor vessel caused by the loop seal clearing following postulated cold leg LOCAs.

- Reduced pump maintenance.

- Lower maintenance dose due to the avoidance of maintenance time in the vicinity of the SGs resulting from the need to remove the entire pump and motor.

The following disadvantages result from choosing sealless motor pumps:

- They are not as efficient as shaft seal pumps.

- Unlike shaft seal pumps, sealless pumps cannot be repaired in situ, requiring the plant design to accommodate the ability for quick removal and replacement of an entire RCP(s).

- Unlike shaft seal pumps, canned-motor pumps of the size required for the AP1000 design had not been built before. This required that large sealless pump designs be developed and that an extensive test programme be conducted as part of the design verification.

- Sealless RCPs slow down quickly when electrical power is removed as compared to shaft seal RCPs, which employ a large flywheel outside the RCS pressure boundary. The sealless RCPs solution to this challenge was the addition of rotating inertia to the pump in the form of a heavy flywheel inside the motor housing.

6A.3.5.2 Use of Grey Rods for Load-Following

Most nuclear power plants today are operated as base load plants but with some ability to load-follow. In typical operating PWRs, this load-following capability is achieved by means of systems that increase and decrease the boron concentration of the reactor coolant water by adding borated or unborated water while removing reactor coolant. In order to avoid releasing very large quantities of borated water, these plants often evaporate water and recycle the water and recovered boric acid, on a short time scale. This requires elaborate and complicated boron and water handling systems outside the containment, and results in restrictions on the rate of load-follow available.

The AP1000 designers recognised that there is an alternative to short-term reactivity control other than changing boron concentration in the reactor coolant, "grey" control rods. These are control rods with low-density neutron absorber, which can be moved to provide modest reactivity adjustments. The materials for grey rods are well known, and their effectiveness for partial reactivity control is easily analysed. It should be noted that grey rods are used in addition to the "black" safety rods, and are not needed for shutting the reactor down. The use of grey rods for load follow minimises the radioactive effluent from the RCS since the reactor coolant boron concentration is only slowly reduced during a plant fuel cycle to account for fuel reactivity decrease as the fuel is used. This effluent can be more easily processed and released after dilution while meeting typical environmental release regulations. Also, due to the small amount of effluent produced, the need to process and recycle water and boric acid is eliminated.

Advantages and Disadvantages

The following advantages result from choosing grey control rods as the means for providing a load-following capability:

- Results in a significant reduction in the amount of liquid radioactive effluent that must be processed during plant load follow operation and a significant simplification of the WLS.

- Potentially eliminates the need for boron recycling, because relatively little boric acid is used during power operation as load-follow is accomplished with grey rods and without changes in the RCS boron concentration.

- Reduced operator dose because the water and boric acid used for plant reactivity control has not been recycled and contains no residual radioactivity. Also, operator dose is reduced since there is no boron and water recycle equipment to operate and maintain.

- Improved operational flexibility, especially towards the end of a fuel cycle, the most difficult situation for a boron control system.

- Greater ability to load-follow than would be achievable with continual boron recycling in and out of the primary coolant.

- Reduced possibility for a reactivity excursion caused by inadvertent dilution of the reactor coolant.

The following disadvantages are apparent:

- The addition of grey rods results in additional control rod drive line penetrations through the RV head and additional RCCAs, guides, and control rod drive mechanisms.

- Potential reactivity faults caused by inadvertent grey rod withdrawal

- Operator dose resulting from maintenance of the added control rod drive mechanisms.

6A.3.5.3 Locating the Chemical and Volume Control System Purification Loop within the Containment

One of the major functions of the CVS is to remove impurities and minimise the radioactivity of the reactor coolant by demineralising and filtering the coolant during all normal operating modes.

In typical operating PWR plants today, this function is performed by a variety of CVS components, most of which are outside the containment, by taking reactor coolant out of the containment (letdown flow). The letdown flow temperature and pressure are reduced, it is demineralised and filtered, dissolved hydrogen is replenished, and it is then pumped back into the containment and the RCS (makeup flow). This process results in the contamination of the equipment and introduces potential reactor coolant leak sites outside the containment.

In the AP1000 plant, the CVS components used to continuously demineralise and filter the reactor coolant are located entirely within the containment. These components include the CVS regenerative HX, letdown HX, demineralisers, filters, and their associated valves, piping, and instrumentation; all of which are designed to operate at RCS pressure. The flow through this in-containment purification loop is driven without the need of continuously operating charging pumps, making use of the reactor coolant pump developed head to provide the motive force.

Advantages and Disadvantages

The following advantages result from locating the CVS within the containment:

- The AP1000 CVS is greatly simplified compared to other PWR designs; eliminating the need for continuously operating makeup pumps, eliminating the need for a volume control tank (VCT), eliminating control of the VCT hydrogen cover gas and fission gas removal, and greatly reducing the quantity of CVS piping and valves.

- The operation of the CVS is greatly simplified and the dose to operator and maintenance personnel is reduced by the elimination of CVS components and the amount of radioactive piping, valves, and instrumentation.

- The potential for leaks of radioactive water outside containment is greatly reduced since the need for reactor coolant letdown during power operation is virtually eliminated.

There are no disadvantages to locating the CVS within the containment.

6A.3.5.4 Zinc Addition to the Primary Coolant

The buildup of crud (typically oxides of activated metal) on component surfaces in the RCS has the potential to cause stress corrosion cracking and crud-induced power shift due to boron concentration in the crud on fuel rods. Also, this crud often becomes solubilised during reactor cooldown operations and results in increased radiation doses during reactor disassembly and refuelling operations. Operation with chemical zinc in the coolant has been demonstrated to change the oxide film on the primary system component surfaces in such a way as to significantly reduce the potential for stress corrosion cracking and crud-induced power shift. Also, zinc addition results in a significant reduction in crud related release into the reactor coolant and has resulted in occupational radiation exposure reductions of as much as 50 percent when incorporated as early as the hot functional testing. Zinc addition to the RCS has been implemented at numerous PWRs to date, with zinc concentrations ranging from 5 to 40 parts per billion (ppb).

The design of the AP1000 CVS incorporates a zinc addition subsystem. The reactor coolant water chemistry specifications for the AP1000 design specify a maximum zinc concentration of 40 ppb to maximise the benefits associated with zinc addition.

Advantages and Disadvantages

The following advantages result from adding zinc to the primary coolant:

- Reduced likelihood of stress corrosion cracking in reactor coolant system components.
- Crud-induced power shift is minimised.
- Reduces occupational radiation exposure to the operators and maintenance personnel.
- Zinc addition is based on operating plant experience and is a proven technology

There are no disadvantages to adding zinc to the primary coolant except for the slight increase in operations and cost of the required equipment.

6A.3.6 Duty Systems

6A.3.6.1 Startup Feedwater Cavitating Venturi

The startup feedwater pumps and their associated pipes and valves comprise the duty system for normal decay heat removal from the RCS at high pressure. If the system operates correctly, it obviates the need for the Class 1 safety measure, the PRHR HX. During a transient with the loss of the main feedwater supply, at least one of the two startup feedwater pumps takes suction from the condensate storage tank and delivers feedwater to the SGs.

The potential exists for excessive startup feedwater flow should the SG pressure be low. The AP1000 design employs a cavitating venturi at the discharge of each of the two startup feedwater pumps to limit the flow. The venturi is designed to cavitate at a point near pump runout; the choked flow in the throat of the venturi under such conditions prevents further flow increase. Thus, the venturi prevents a startup feedwater pump from running out past its designed maximum flow rate. Pump runout protection is important during conditions when the steam generators are at low or atmospheric pressure or following a line break downstream of the pumps. The venturis limit the pump runout such that the required NPSH does not exceed the available NPSH at maximum flow conditions. The venturis also ensure that the total flow rate from both pumps is limited so the maximum flow to the SGs is not exceeded. Thus the venturi flow elements provide a passive mean of limiting the flow. The cavitating venturi also provides the secondary function of a flow measurement signal at normal flow rates.

Advantages and Disadvantages

The following advantages result from incorporating a cavitating venturi at the outlet of the startup feedwater pumps:

- Reduced likelihood of exceeding the startup feedwater pump runout flow limit and ensures the pump NPSH requirement is always met
- Reduced likelihood of excessive cooldown of the primary circuit, thereby causing a reactivity injection
- Proven technology

The only disadvantage of incorporating a cavitating venturi is cost. However, because it also enables flow to be measured, a function that would have to be provided anyway, its net cost is negligible.

6A.3.6.2 Use of Air Diaphragm Pumps for Waste Water Duty

Wastewater needs to be transferred within the plant, from tank to tank or for processing, and ultimately it must be discharged out of the plant. This wastewater can be contaminated and nonradioactive, radioactive, or contaminated and radioactive; the contamination might be oily. In currently operating nuclear power plants, such transfers are brought about by a wide variety of pump types: centrifugal, positive displacement, air-operated, and others. Those pump types that require seals, especially rotating seals, are prone to leakage with the potential for consequent radioactive or oily effluent and accidental loss of radioactive fluid outside the containment.

It was decided to pick a pump type with no seals for wastewater pumping duty. In this type of pump, the working fluid remains fully contained inside the pump's pressure boundary, thereby eliminating any chance of seal leakage. After consideration of the available pump types, the air diaphragm pump was chosen.

Advantages and Disadvantages

The following advantages result from using all air diaphragm pumps for wastewater pumping duty:

- Less expensive than other pump types of the same capacity.
- Diaphragm pumps are simple and easy to maintain, and standardisation reduces the number and types of spare parts that must be maintained.
- As a fully contained pump, eliminates the possibility of accidental loss of radioactive fluid due to seal leakage, thereby minimising the risk of public or operator radiation exposure from wastewater leakage.

There are no disadvantages resulting from using air diaphragm pumps for wastewater pumping duty.

6A.3.6.3 ac Power Fast Bus Transfer

The onsite ac power system comprises a normal power supply, a preferred power supply, a maintenance power supply, and a standby power supply. The normal, preferred, and maintenance power supplies are included in the main ac power system. The standby power supply is included in the onsite standby power system. These power supplies provide ac at 11 kV.

During normal power generation mode, the main turbine generator supplies electric power to the plant auxiliary loads through the unit auxiliary transformers. This is the normal power supply.

When the plant is shut down or starting up, the generator breaker is open and ac power is provided from the preferred power supply. This comes from the high-voltage substation by way of the main step-up transformers (main generator transformers, in UK parlance) and the unit auxiliary transformers.

During maintenance on the main step-up transformers, power comes from the high-voltage substation by way of the two reserve auxiliary transformers (station transformers, in UK parlance). Each reserve auxiliary transformer can be used in place of a unit auxiliary transformer; that is, its output rating is the same. Bus transfer to the maintenance power supply is manual or automatic, through a fast bus transfer scheme.

Two onsite standby diesel generators power the onsite standby power system. This supplies power to selected loads in the event of the loss of the normal or the preferred ac power supplies. These loads provide defence in depth functionality. The diesel generators are automatically started and connected to their respective buses. In the event of a fast bus transfer, the diesel connection to the bus is delayed such that the fast bus and residual transfer is allowed to initiate.

The original AP1000 design had only one reserve auxiliary transformer and was vulnerable to losing ac power due to the failure any of the following:

- Any one of five large oil-filled transformers
- The 26-kV isophase bus duct
- The associated malfunction of the protective relay for the above electrical equipment

The ac power cut would last for up to approximately 2 minutes, until such time as the onsite standby diesel generators started, warmed up, and loaded; or the plant operators transferred selected loads to the single reserve auxiliary transformer. This condition would result in a reactor trip because of the loss of the four RCPs, which are powered from the unit auxiliary transformer buses.

To prevent such a reactor trip from the electrical faults mentioned above, a fast bus transfer capability was incorporated into the AP1000 design. Automating the bus transfer from the unit auxiliary transformers to the single reserve auxiliary transformer would have required shedding sufficient unnecessary loads so as to be within the rating of the reserve auxiliary transformer; this would have required a complex automatic system. Instead, it was decided to go for a simple automatic capability and second reserve auxiliary transformer to allow the transfer of loads from the unit auxiliary transformers to the reserve auxiliary transformers.

In summary, the addition of another reserve auxiliary transformer was chosen to allow for the bus transfer from the unit auxiliary transformers to the reserve auxiliary transformers.

Advantages and Disadvantages

The following advantages result from incorporating a fast bus transfer capability and a second reserve auxiliary transformer:

- Prevents a reactor trip in case of any of various electrical faults, and thereby minimises challenges to the plant shutdown cooling or safety related systems, minimises plant transients, and avoids the cost of lost electrical production.

- Results in a much simpler and more reliable automatic system than the option of a single reserve auxiliary transformer.

- Two reserve auxiliary transformers allow functionally redundant pumps or groups of loads to be supplied from separate buses.

- Two reserve auxiliary transformers allow increased operational flexibility.

The only disadvantages resulting from incorporating a fast bus transfer capability and a second reserve auxiliary transformer are an increased initial cost and ongoing maintenance costs over not installing the system at all.

6A.4 REFERENCES

6A.1 None

TABLE OF CONTENTS

TABLE OF CONTENTS (cont.)

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS AND ACRONYMS

AE	architect-engineer
ALARP	as low as reasonably practicable
ASME	American Society of Mechanical Engineers
BAT	best available technique
BPEO	best practical environmental option
BPM	best practical means
C&I	control and instrumentation
CAE	computer-aided engineering
CDM	Construction (Design and Management)
COMAH	Control of Major Accident Hazards
CV	containment vessel
DA	design authority
DAP	duly authorised person
DBA	design basis accident
DBE	design basis event
EHS	environment, health and safety
EMIT	examination, maintenance, inspection, and testing
EURATOM	European Atomic Energy Community
FME	foreign material exclusion
GDA	generic design assessment
HELB	high-energy line break
HSE	Health and Safety Executive
HVAC	heating, ventilation, and air conditioning
IAEA	International Atomic Energy Agency
IC	intelligent customer
IEEE	Institute of Electrical and Electronics Engineers
ILW	intermediate-level waste
IRR	Ionising Radiations Regulations
ISI	in-service inspection
IST	in-service testing
LLW	low-level waste
MPA	multi-party agreement
NI	nuclear island
NPP	nuclear power plant
NSSS	nuclear steam supply system
OI	operating instruction
ONR	Office for Nuclear Regulation
PCSR	Pre-Construction Safety Report
PSI	pre-service inspection
PWR	pressurised water reactor
QA	quality assurance
QMS	Quality Management System
RCP	reactor coolant pump
RCS	reactor coolant system
REPPIR	Radiation (Emergency Preparedness and Public Information) Regulations
RPV	reactor pressure vessel
SLC	site licence condition
SQEP	suitably qualified and experienced person
SSC	system, structure, or component
UK	United Kingdom

7 LIFE CYCLE ENGINEERING AND SAFETY

7.1 Introduction

This section provides an overview of the engineering and safety arrangements throughout the life cycle of the AP1000 pressurised water reactor (PWR) plant. It focuses on specific aspects of the management arrangements associated with the achievement of nuclear safety throughout the design life cycle of the plant considering the design, change control, construction, commissioning, maintenance, ageing, and degradation and decommissioning.

This chapter summarises the general arrangements for the overall project including the expectations of the engineering and safety principles and processes to be applied and implemented during the lifetime of the AP1000 plant. Design, build, test, and maintenance activities influence the safety of the AP1000 plant throughout its life. Many of these activities occur after generic design acceptance. These later activities cannot be addressed at this time since they are the responsibility of the licensee. It shall be noted that this chapter describes anticipated actions from a licensee in accordance with UK regulatory guidance. It will be the prerogative of the future utility to decide on its own processes and programmes for these topics and others.

This chapter focuses specifically on the nuclear safety aspects of the United Kingdom (UK) AP1000 plant submitted for generic design assessment (GDA). However, where there is an impact on the nuclear safety of the plant from other aspects of the UK AP1000 plant design, these are also included.

Plant ageing mechanisms need to be understood and managed to ensure the design and constructed plant remain safe and that the risks remain as low as reasonably practicable (ALARP) for the duration of the plant life cycle. As modifications are introduced into the plant design and facilities, the safety case must be revisited to ensure the modifications keep the plant operating within its safety envelope. The scope and purpose of how the safety case is developed throughout the plant life is provided in Chapter 2. As the safety case develops and the responsibility for it is handed over to the site licensee, appropriate management arrangements will need to identify how information is transferred to the licensee, who must ensure they understand the technical arguments contained in the document(s). These aspects of knowledge transfer, intelligent customer (IC), and the role of the design authority (DA) are summarised in Section 7.2. The overall management of safety is discussed in Chapter 3.

Periodic safety reviews ensure the safety case remains valid throughout the plant life, as the behaviour or nature of the plant changes over time. During the operational phase, periodic safety reviews also demonstrate that ageing and other time-related phenomena will not compromise safety, particularly before the next periodic review. There is normally a maximum time limit of 10 years before each periodic review.

The safety of pre-power operation, power operation, and post-power operation activities for the AP1000 plant (see Figure 7-1) will be based on risk reduction, dose minimisation, the ALARP principle, waste minimisation, and passive safe storage. This is ensured through the following:

- **Design** – The systems, structures, and components (SSCs) that comprise the AP1000 plant are designed to keep risk ALARP.

- **Construction Commissioning** – The AP1000 plant SSCs are built in accordance with the design and will be systematically and rigorously commissioned to demonstrate the

required functionality in accordance with the safety case and design intent. Plant facilities that provide a safety function will be appropriately configured and the required functionality will be demonstrated during commissioning.

- **Operation Maintenance** – The AP1000 reactor and any plant facilities that provide a safety function will be operated and maintained in accordance with the safety case. Activities will be controlled in a safe manner and risks demonstrated to be ALARP.

- **Decommissioning** – The AP1000 reactor and associated facilities are designed to have minimal impact on the environment at the end of its operating life. The AP1000 reactor and its facilities will be capable of being safely decommissioned in accordance with government policy for which a safety case will be prepared.

Westinghouse has developed a number of safety programmes to be used in support of the potential licensee throughout the design, construction, and operation of the AP1000 plant, a brief description of which is provided in the Plant Life Cycle Safety Report (Reference 7.1). The Plant Life Cycle Safety Report outlines the information required to demonstrate that the construction and installation activities will result in a plant of appropriate quality and that the constructed plant will be capable of being operated within safe limits. The Plant Life Cycle Safety Report also describes the process by which the knowledge within the AP1000 plant safety case can be most comprehensively transferred to the potential licensee and outlines Westinghouse's expectations for any operator management system.

7.2 Design Implementation

The Westinghouse safety management framework is discussed in Chapter 3 and notes the safety philosophy policy statement. In support of this policy, Westinghouse, as the plant designer, is committed to the following:

- Providing safe working conditions to protect the health and safety of employees and contractors

- Reducing waste, preventing pollution, conserving resources, and using energy efficiently in its operations

- Complying with the applicable environment, health, and safety (EHS) legislation and regulations, as well as any other requirements, including fire regulations

- Continually improving EHS management systems and performance by establishing and maintaining meaningful objectives and targets, taking into consideration significant EHS aspects; technological options; and legal, operational, business, and other requirements

- Establishing and maintaining procedures to identify the potential for and response to accidents and emergency situations, and to prevent and mitigate the impacts associated with them

- Training employees to work in a safe and environmentally responsible manner

- Effectively managing and promptly resolving impacts from historical operations in a manner that minimises risks and liabilities while accommodating current operations

- Periodically monitoring, auditing, and evaluating EHS performance as it relates to applicable design requirements and established objectives and targets

The way in which this policy is implemented through the design is discussed further in the Plant Life Cycle Safety Report (Reference 7.1, Section 3).

7.2.1 Knowledge Transfer

As mentioned in Chapter 3, to ensure that the knowledge transfer process is comprehensive, there must be strong interfaces with potential site licensees during the GDA process and following licence acceptance. Westinghouse has worked with potential utility licensees during the GDA process concerning submissions to the UK regulators with the purpose of ensuring that an acceptable safety case has been made for the AP1000 design. Although the utility involvement has evolved throughout the GDA there has been a high level of interactions and utilities have been invited to Level 1-4 regulatory meetings throughout GDA. This arena forms the basis for ensuring that the interested utilities are engaged in the production of the GDA safety submission and will include an understanding of the following:

- The design
- Procedures to be used during the procurement and construction phases
- Procedures for normal operation, and emergency and accident management
- Procedures required during the installation and commissioning phases
- The safe operating envelope and the operating regime required to maintain the integrity of that envelope
- Technical Specifications
- Operating instructions (OIs), including the commissioning schedules
- Maintenance schedules
- Training requirements
- Emergency preparedness
- Radiological protection arrangements
- Safety case used as the basis for the GDA submission

The aim of the knowledge transfer process is to ensure that potential licensees have the capability to secure and maintain the safety of the facility and that, where necessary, the licensee has the means to perform as an IC. Whilst it is appreciated that potential licensees are required to demonstrate their arrangements for compliance to the requirements of the site licence, sufficient information will be made available by Westinghouse to enable those organisations to enact their arrangements as per appropriate contract arrangements. The definition of an IC is defined in Reference 7.2 as follows:

> *As an IC, in the context of nuclear safety, the management of the facility should know what is required, should fully understand the need for a contractor's services, should*

specify requirements, should supervise the work and should technically review the output before, during and after implementation. The concept of IC relates to the attributes of the organisation rather than the capabilities of the individual post holders.

These aspects of demonstrating that the licensee has suitable IC capability are discussed further in the Plant Life Cycle Safety Report (Reference 7.1).

Westinghouse expects to be fully integrated into the potential licensee's management arrangements and Westinghouse's arrangements will meet and will be aligned with those of the licensee. This in itself will aid the knowledge transfer during the licensing process and later in the various plant phases.

Westinghouse will support the licensee to ensure that the knowledge of the aspects of the design, construction, commissioning, and future operability of the plant is transmitted in an effective and appropriate manner and provide visible assurance that this has been achieved. Thus, any contract between Westinghouse and a licensee is expected to define the tasks and interrelationship between the organisations. The management arrangements and the related communication processes between the licensee and Westinghouse have to be agreed within this framework.

The principles on the use and management of contractors given in Reference 7.2 have been applied by Westinghouse in the production of safety submission for the GDA process. The broad principles are as follows:

- The overall responsibility for, and the control of, the nuclear and radiological safety and security of all its business, including work carried out on its behalf by contractors, is maintained by the IC.

- The choices between sourcing work in-house or from contractors should be informed by a clear policy that takes due account of the nuclear safety implications of those choices.

- It is ensured that an IC capability is maintained for all work carried out on its behalf by contractors that may impact upon nuclear safety.

- It is ensured that the IC only lets contracts for work with nuclear safety significance to contractors with suitable competence, safety standards and resources.

- It is ensured that all contractor organisations are familiar with the nuclear safety implications of their work and interact in a well coordinated manner with their own staff.

- It is ensured in practice that the contractor's work is carried out to the required level of safety and quality.

These principles of the suitability to act as an IC will be applied to the licensee to determine if they themselves have the knowledge and depth of understanding of the overall safety of the AP1000 plant. In addition to being able to act as an IC, the licensee will have to demonstrate that they have suitable safety management arrangements in place, demonstrate compliance to those arrangements, and demonstrate that they adequately control and supervise all activities where safety may be affected, including being capable of exerting proper controls of the activities of contractors.

The arrangements for knowledge transfer will be defined and discussed in detail with the licensees and the process developed throughout the various project phases leading up to and

beyond the start of operations. These aspects are covered further in the Plant Life Cycle Safety Report (Reference 7.1).

Westinghouse has assumed the position of IC for the purposes of the GDA submission.

As discussed in the Plant Life Cycle Safety Report (Reference 7.1), one area where it will be demonstrated that suitable and sufficient information has been made available, transferred, and understood is the appointment of duly authorised persons (DAPs) and suitably qualified and experienced persons (SQEPs). These appointments are made by the licensee and are a requirement of the site licence conditions (SLCs), specifically those relating to commissioning, control, and supervision of all operations that may affect safety, including the examination, maintenance, inspection, and testing (EMIT) of safety equipment.

It must also be ensured that the potential licensees are aware of and learn from any information gained from the construction, commissioning, and operation of other AP1000 plants worldwide. To facilitate this, it is essential that Westinghouse has good processes for the management and preservation of knowledge relating to the design development of the AP1000 plant and, where appropriate, these aspects of knowledge management are transferred to the licensees. These processes and procedures are discussed further in Chapter 3.

7.2.2 Design Authority

The concept of knowledge transfer is fundamental in defining who the DA is for the AP1000 plant throughout the plant life cycle. Westinghouse will be the DA until at a suitable point this role will be transitioned over to the licensee and Westinghouse will become the responsible designer (Reference 7.3), defined as follows:

> *The organisation which has a formal responsibility for maintaining detailed, specialised knowledge of all the systems and components important to safety, and a core competence in the detailed design process.*

Design changes made by the licensee during the plant life must be made with the full knowledge and understanding of the design and safety functions that need to be provided. This knowledge is to be retained and made available by the licensee over the lifetime of the plant until it has been decommissioned.

The licensee is also responsible for maintaining the design integrity and the overall basis for safety over the plant life. Thus, the role of DA is defined in Reference 7.3 as follows:

> *The defined function of a licensee's organisation with the responsibility for, and the requisite knowledge to maintain, the design integrity and the overall basis for safety of its nuclear facilities throughout the full lifecycle of those facilities. Design Authority relates to the attributes of an organisation rather than the capabilities of individual post holders.*

Prior to a licensee being designated as the DA, the licensee must demonstrate sufficient knowledge to understand the safety case requirements for the plant and be able to assess the impact of proposed design changes on the functionality, reliability, and availability claims made in the safety case. The licensee will also need to demonstrate an understanding of any specific constraints that impact the practical use of the plant, such as restrictions on space, availability of services, and environmental considerations.

The Westinghouse design safety case for the AP1000 plant will be evaluated throughout the plant life. In this context, Westinghouse has processes in place to do the following:

- Review relevant plant modifications
- Perform design substantiation for modifications proposed
- Record and learn from operational experience across all AP1000 plants
- Communicate the need for essential plant upgrades and changes to operating constraints across all AP1000 plants

The licensee and Westinghouse will have arrangements in place to enable delivery of Westinghouse service as the responsible designer during the plant construction and commissioning, recognising that some elements may be assigned to other responsible designers. The DA is expected to demonstrate certain capability principles and, during the transfer of this role from Westinghouse to the licensee, any contractual arrangements will be in accordance with these principles, which include the following:

- Be a defined function within the licensee's organisation.
- Have the authority and responsibility to propose, approve, or reject design changes.
- Have the capability to understand the totality of the design and nuclear safety case in the context of each stage of the full plant life cycle.
- Have the resources, capability, and management processes to assess the changes to the plant's conditions, limits, and performance characteristics, and have the authority to recommend modification to or suspension of operation.
- Have appropriate and up-to-date knowledge, skills, experience, and resources.
- Regularly assess and determine the continued adequacy of the plant's design and safety case, and have the authority and responsibility to respond to the issues identified.

Where the DA does not have the detailed knowledge required of all the systems and components important to safety, it may choose to assign those responsibilities to responsible designers using the supply chain.

While Westinghouse remains the DA, design changes will be in accordance with Westinghouse's own procedures, as discussed in Chapter 3. However, the licensee will be required to have suitable arrangements in place to maintain design integrity and, throughout the licensing process, any changes will have to be made in accordance with the licensee's arrangements for making modifications to the design under construction, SLC 20 (Reference 7.4). Thus, Westinghouse's processes will align with and be integrated into the licensee's arrangements, where applicable.

7.3 Design Change Control

7.3.1 Introduction

The management of safety is outlined in Chapter 3 and discussed further in the Plant Life Cycle Safety Report (Reference 7.1).

The evolution of the design of the AP1000 plant is described in detail in the Genesis and Process of the AP1000 design document (Reference 7.5) and has been built on the design

philosophy that emphasises “safe and simple”, while recognising the benefits of a standard design to be deployed on multiple sites.

Westinghouse has considered, and continues to consider, safety in the early design of equipment and facilities, and the design review (Section 7.3.2) is one of the primary tools to capture plant lifetime nuclear and personnel safety aspects.

To ensure design change control up to and including commissioning the AP1000 plant and supporting facilities, Westinghouse operates a Quality Management System (QMS) that contains the management processes outlined below. During the licensing process and after a site licence has been granted, Westinghouse’s procedures will be aligned with the licensee’s arrangements for SLC 20 (Reference 7.4) and SLC 22 (Reference 7.6), as appropriate.

Design modifications throughout the life cycle of the plant:

- Once the design documentation for the plant has been agreed, any subsequent design changes will be subject to design change management control. The reviews, which form part of the design change process, are used to verify the completeness and adequacy of the design change to meet the design intent.

- Any proposed changes to the plant baseline design must be assessed to ensure the safety case is not undermined and the effects on adjacent systems have been considered. This process is applicable throughout the construction, commissioning, and operational phases.

Design control for facilities:

- When modifications are made to the facility reference design, a safety design change committee, or equivalent, will review the changes, in accordance with the licensee’s site licence arrangements. Where applicable, an appropriate Nuclear Site Safety Committee subcommittee, set up in accordance with the site licensee management arrangements, will review operational procedures in accordance with their safety category/classification and endorse or authorise the documents. The relationship between Westinghouse and the licensee may require Westinghouse to provide any information and support to the licensee to enable them to make informed decisions and to be able to present the case for change knowledgeably to the regulators.

- Following the granting of a site licence, the licensee will have the option to assess the impact of any changes to be carried out by Westinghouse, another third party, or the licensee’s own in-house design team. Consideration must be given to the roles and responsibilities held by Westinghouse and the licensee as responsible designer and DA and the need to demonstrate suitable IC capability where applicable.

- Records of all plant design change control will be kept in accordance with SLC 6 (Reference 7.8).

- The regulatory authorities may request visibility of any modification (Reference 7.4) and impose hold points before allowing that modification to proceed. The licensee will manage any such hold points in accordance with its management arrangements.

These processes will interface with the site licence holder’s arrangements for meeting SLC 14, SLC 19, SLC 20, SLC 21, and SLC 22 (References 7.9, 7.10, 7.4, 7.11, and 7.6, respectively) and any others deemed appropriate.

Safety of the AP1000 plant design through the life cycle of the plant will be managed in accordance with appropriate legislative requirements by Westinghouse and then the site licence holder, with their priority being to design, construct, commission, and operate the plant safely and ensure any risks to workers or the public remain ALARP and within legislative requirements.

7.3.2 Safety through Design Review

Westinghouse considers safety from the early stages in the design of equipment and facilities and throughout any modifications during the construction and commissioning stages.

The design review process (see Figure 7-2) is one of the primary tools used to ensure that plant lifetime nuclear and personnel safety considerations are properly considered when products, processes, analytical tools, systems, equipment, or servicing tools are introduced or undergo major change. This is an important aspect of the Westinghouse design verification process before or during manufacturing, construction, commissioning, and operation.

Design reviews are conducted at appropriate stages of the design development through manufacture, construction, commissioning, and operation to provide an objective overview of design adequacy, safety, performance, and cost.

Design reviews are performed when:

- A system or plant failure could result in significant risk to public safety, the environment, worker health, company finances, or customer satisfaction.
- The design is a significant departure or extrapolation from a past proven design or analytical methodology.
- The physical configuration is similar to proven designs, but there are potentially significant changes in application or acceptance criteria.
- The design involves significant changes to power plant operations, processes, or systems.
- A customer or regulatory agency stipulates a requirement (for Class 1 items, independent reviews are performed by individuals or multidisciplined review teams).

Sufficient time must be provided in the design plan to ensure that adequate reviews are performed and action items are resolved satisfactorily before the design or design change is released. Design reviews address the following as applicable:

- Correct selection of design input
- Correct incorporation of design inputs into the design
- Specification of design input and verification requirements for interfacing organisations
- Adequate identification, description, and reasonableness of assumptions
- Appropriateness of design methods
- Reasonableness of design output compared to design input

- Adequacy of critical fits and clearances and, when applicable, plant construction and equipment installation
- Plant installation
- Impact to supply base/supplier, manufacturability, and cost effectiveness

7.3.3 Maintenance

Maintainability is to be "designed in" by extensive layout reviews by the AP1000 design team. From the beginning of AP1000 development, the layout was generated in 3-D computer-aided engineering (CAE) software. As items (structure, equipment, pipeline, duct, and tray) are added to the design, it may be checked for interferences, inspection access, and maintenance access. These evaluations may be performed with site licensee involvement. Design decisions will be made to minimise maintenance time, the need to work from heights, accessibility, and other risks that occur while routine and breakdown maintenance activities are performed.

The design change control process will ensure that maintenance activities are considered when design reviews are undertaken, especially during modifications made onsite in accordance with SLC 20 (Reference 7.4). This will involve interfacing arrangements between Westinghouse and the site licence holder for EMIT and other maintenance arrangements in accordance with SLC 28 (Reference 7.12).

7.4 Construction

7.4.1 Introduction

Civil engineering construction is a major component of the Westinghouse AP1000 nuclear power plant (NPP). The plant, including the civil engineering aspects, has been designed with the intention of being capable of being sited at any reasonable location in the world without modification.

The Westinghouse AP1000 design employs construction methods and a plant layout that are conducive to safe construction. Much of the design is modular, which allows the build and test of subassemblies to be undertaken in a factory environment. The size of the plant and the number of components is also significantly less than previous generations of PWRs. These approaches will reduce site construction work and hence the risks from those activities. Modular construction in a factory environment is expected to have a positive effect on product quality and safety and can contribute to reduced maintenance requirements during the lifetime operation of the plant.

During the construction phase, responsibility for safety, health, and the environment will rest with the licensee. The licensee's arrangements will ensure that they will be compliant with Construction (Design and Management) (CDM) regulations (Reference 7.13). The licensee will determine the extent of work responsibility that they wish to hand over to Westinghouse and other contractors. As a minimum, the licensee will ensure that both Westinghouse's and the licensee's management arrangements permit access to the relevant Westinghouse knowledge and support necessary to ensure health and safety of people, and environmental protection onsite during construction and subsequent commissioning and operation of the plant. Throughout the construction phase, Westinghouse will work closely with the licensee to provide the necessary technical information to enable the development of the appropriate safety case documentation. Westinghouse's construction arrangements will align with and be delivered under the licensee's arrangements. These will need to be confirmed as acceptable

by the licensee, i.e., that they meet the expectations of the UK regulators. These aspects are discussed further in the Plant Life Cycle Safety Report (Reference 7.1).

For justification of the civil engineering structures, supporting information can be found in Chapter 16, based on the structure's relevant categorisation and classification identified in Appendix 15A.

The use of a steel-concrete composite construction method for some structures where concrete is placed between two steel plates that provide the reinforcement, instead of conventional internal reinforcement bars, is unconventional in the UK for nuclear power station construction. Therefore, the justification for SC structures has been considered in particular detail by Westinghouse, and Chapter 16 refers to this detailed information.

The adequacy of construction, installation, and preliminary operation of components and systems is verified during construction and installation commissioning. Development of the construction and installation tests is based on the engineering information for the equipment and systems installed.

The construction verification process is the means to demonstrate that the AP1000 plant is constructed to the design intent. This process provides assurance that a plant that receives a design acceptance is manufactured and the equipment installed in conformance with the accepted design.

An equivalence study has been carried out to ensure that any codes and standards used in the above construction verification programme have been demonstrated to be acceptable for use in the UK. This is provided in the AP1000 Equivalence/Maturity Study of U.S. Codes and Standards (Reference 7.15).

7.4.2 Overview of Construction Verification Process

During the design process, systems are designed and optimised to provide the highest degree of nuclear safety to ensure worker and public protection and compliance with all appropriate standards.

Principal design criteria establish the necessary design, fabrication, construction, testing, and performance requirements for SSCs important to safety; that is, SSCs that provide plant protection such that the power plant can be operated throughout its life cycle with minimised risk to the health and safety of the public and workers.

The safety of the nuclear plant is governed by the necessity to reduce risks to be ALARP and to ensure worker and public protection. This is achieved by conservative design to meet regulatory criteria and established industry codes and standards. The design process then proceeds following approved engineering practices and procedures using verified computer codes and test information. From the design activities, items required for verification of the design are logged and records kept.

7.4.3 Construction Objectives

The construction verification process follows the hierarchical objectives (shown in Figure 7-3) with verification of these objectives ensuring that the construction of the plant is in accordance with the design.

The licensee will ensure that prior to construction and installation adequate safety arrangements will be made and implemented, including the following:

- Procedures will be in place to ensure that, insofar as safety can be affected, the construction and installation of the plant is controlled, supervised, and carried out by an SQEP in accordance with written procedures.

- Roles and responsibilities relevant to the construction and installation of the plant will be defined.

- Relevant safety-related CDM regulations (Reference 7.13) appointments will be identified and adequate arrangements will be made and implemented.

- Where other contractors are employed on the construction and installation activities, adequate arrangements will be made to cover the work; for example, quality assurance (QA) programmes on the interaction between Westinghouse, the contractor, and the licensee.

- Records of the construction, installation, and testing undertaken will be retained by the licensee and, where appropriate, by Westinghouse in accordance with the licensee's arrangements.

Any construction activities undertaken on the licensed site will be in accordance with the licensee's arrangements. The licensee will assess the contractor's arrangements, including those of Westinghouse. Where necessary, modifications may be made to Westinghouse's arrangements to demonstrate acceptance by the licensee. Part of this process will involve the production of a construction and installation schedule in accordance with the arrangements outlined above.

7.5 Commissioning

7.5.1 Introduction

During commissioning, responsibility for the safety of the plant and the environment will rest with the licensee. Commissioning of the AP1000 PWR NPP follows the construction and installation phase. Commissioning verifies that the construction, installation, and operation of the plant behave according to their design intent and the assumptions made in the safety case.

Westinghouse will ensure that prior to commissioning adequate arrangements are made, implemented, and aligned with the licensee's arrangements. Westinghouse's arrangements will include the following:

- Procedures are in place to ensure that, insofar as safety can be affected, the commissioning of the plant is controlled, supervised, and carried out by an SQEP in accordance with written procedures.

- Roles and responsibilities relevant to the commissioning of the plant will be identified.

- Relevant safety-related CDM regulations (Reference 7.13) appointments will be made and implemented.

- Where other contractors are employed on commissioning activities, adequate arrangements will be made to cover the work.

- Records of commissioning undertaken will be retained by Westinghouse and provided to the licensee.

- Suitable safety-related hold points will be introduced.

In addition, documents to describe the commissioning tests (for example, method statements) will be prepared, authorised, and issued as appropriate. Local procedures to cover commissioning requirements, including any handover processes (for example, from construction to commissioning), will be made. These arrangements need to be confirmed as acceptable by the licensee.

Upon successful commissioning, the following claims made within the safety case can be justified:

- The plant has been designed so that all risks are ALARP.
- The plant has been built in accordance with the design.
- The plant has been fully commissioned to allow validation of the safety case assumptions.
- The plant can be safely operated and maintained in accordance with the safety case throughout its life cycle.

The main purpose of commissioning tests is to ensure that the assumptions made in the Pre-Construction Safety Report (PCSR) and other safety documentation are proven, such that the plant can operate safely. Commissioning tests serve as a progressive transition between the construction, equipment installation and the start of normal operation of the various plant systems. These tests may take place in-factory (as the AP1000 reactor is a modular design), on specific test facilities, or onsite. The choice depends on the type of equipment, the level of a system's integration that can be simulated offsite (e.g., control and instrumentation (C&I) systems), and the ability to obtain specific conditions onsite (e.g., for qualification tests or accident transients).

The method for defining commissioning tests is chosen to ensure that all operational aspects of system functions are tested, including safety-classified functions, taking into account offsite tests, where relevant.

As noted above a comprehensive commissioning programme will be prepared for implementation on the licensed site. This programme will be structured to include hold points at key milestones, at which the acceptability of the commissioning tests results will be verified (with particular focus on demonstrating that the plant will meet the appropriate design safety requirements) before entering into the next phase of commissioning.

7.5.2 Overview of Construction Testing Process

Equipment and construction specifications are developed to describe construction details such as welding methods and the necessary inspections and tests to ensure the quality of the welding. Principal design criteria establish the necessary design, fabrication, construction, testing, and performance requirements for SSCs important to safety, i.e., SSCs that provide assurance that the power plant can be operated such that the risk to the health and safety of the public and workforce can be shown to be ALARP.

7.5.3 Commissioning Phases

Commissioning follows the verification phase in a progressive test programme similar to that shown in Figure 7-4. This figure shows a typical PWR commissioning high-level test

programme profile broken down into manageable stages. The following subsections provide a brief overview of each stage. Note that due to the modular and staged construction schedule for the AP1000, the phases of Figure 7-4 will overlap by plant area. Each area of the plant will follow the progression of Figure 7-4.

The AP1000 test programme refers to the testing phases as "construction and installation tests" (typically, Phases 1 and 2, Figure 7-4), "pre-operational tests" (typically, Phases 3 and 4), and "startup tests" (typically, Phase 5 and onwards).

7.5.3.1 Safety Commissioning and Safety Commissioning Schedule

The site licensee and Westinghouse will produce the AP1000 plant safety commissioning schedule. This is a definitive record of requirements and evidence of the tests conducted in order to substantiate the claims and assumptions made within the plant safety case. The test results will demonstrate that the as-built plant is acceptable for safe operation.

The AP1000 commissioning strategy will be based on the following key objectives that will ensure the safe conduct of commissioning:

- Identify processes, systems, and equipment to be commissioned, as well as their interfaces, safety functions, and performance requirements.
- Identify processes, systems, and equipment that cannot be safely commission tested, and ensure that an appropriate justification for not undertaking commissioning tests and inspections is provided.
- Describe commissioning tests, including statements that the tests will demonstrate the required performance of the plant and meet their safety justifications in accordance with the safety category and classifications.
- Identify the limits and conditions of plant operation so that operating rules can be established in accordance with SLC 23 (Reference 7.16).
- Make reference to the operating conditions and limits and OIs that will apply to the commissioning stage in accordance with SLC 24 (Reference 7.17).
- Make reference to the stages into which the commissioning will be split (e.g., phase permissioning hold points) (see Figure 7-4 as an example).
- Align with the site licensee safety management arrangements for commissioning.
- Define the following aspects, with respect to safety management during commissioning:
  - Linkages to and interfaces with relevant safety documentation, e.g., fault schedules, probabilistic safety assessment design justification reports, and PCSR.
  - Interfaces between organisations participating in the commissioning programme.
  - Ownership and responsibility (e.g., from the site owner, site licensee, construction organisation, and commissioning organisation), whilst at all times ensuring that the site licensee retains overall responsibility for safety and the environment.

  - Discharge of responsibility for safety as a result of completed tests.
  - Handover arrangements for the transfer of responsibilities between the construction organisation and the commissioning organisation.

- Demonstrate that sufficient and appropriate commissioning tests have been undertaken to confirm the assumptions made in the safety case.
- Provide verification that the plant has been constructed in accordance with the design intent.

7.5.4 Phase 1: Initial Plant Testing

Phase 1 commissioning starts with the inspection, setting to work of support systems, and component-level activities such as instrument calibration, setting to work motorised valves, motors, and pumps.

The intent is to define activities that will be undertaken to verify that the as-built system conforms to the design features and characteristics defined in the design description of the plant. Construction and installation tests are performed to verify the adequacy of construction, installation, and preliminary operation of components and systems. Various electrical and mechanical tests are performed, including cleaning and flushing, hydrostatic testing, electrical checks, operability checks, and instrumentation calibration. The completion of the construction and installation test programme demonstrates that the system is ready for pre-operational testing.

7.5.5 Phase 2: Cold Functional Testing

During Phase 2 testing, whole systems are run for the first time (for example, the flushing of pipework systems). Typically the integrity of the containment system is proven and an integrated leak test is performed to demonstrate the leakage integrity of the primary containment to withstand the calculated design basis accident (DBA) peak pressure. Another example is that the cold pressure testing also takes place for the rest of the reactor primary circuit.

7.5.6 Phase 3: Hot Functional Testing

This involves the plant being run as a totally integrated system for the first time with the whole of the nuclear steam supply system (NSSS) intact, and with all the necessary supporting nuclear and conventional plant systems commissioned but without fuel in the core. The reactor coolant system (RCS) will be progressively run up to full operating conditions from energy input from the reactor coolant pumps (RCPs).

The main purpose of the pre-operational testing is to operate the primary circuit at temperature in order to pre-condition the internal surfaces of the reactor vessel and primary circuit. During the test conditions all reactor protection functions are gradually introduced. For example, during the gradual heat up and subsequent cool-down, thermal expansion and vibration of pipework is measured to confirm compliance with the plant design and demonstrate that systems operate within design limits. Additionally, integrated operation of plant systems under pre-core hot functional conditions is demonstrated

This phase can prove useful for the staff of the licensee in helping to gain operating experience alongside Westinghouse personnel with the plant under hot conditions. This is

part of the knowledge transfer process and helps to demonstrate compliance with the licensee's arrangements for SLC 10 and SLC 12 (References 7.18).

7.5.7 Phase 4: Preparations for Fuel Load

This is the final commissioning of the systems that support fuel loading. Before the receipt of fuel; construction, preoperational testing, flushing and room turnover are sufficiently completed to successfully receive and store the fuel assemblies needed for initial core load. Conditions in the auxiliary building fuel handling area are made ready to prevent damage to the fuel assemblies. There is a turnover of the fuel handling machine, rail car bay crane and cask crane, as well as complete preoperational testing.

Component testing, flushing and preoperational flow testing on systems that interface with the spent fuel pool prior to fuel receipt are a necessity. Once these are complete, necessary controls are put into place to ensure the spent fuel pool remains dry until initial core load. The spent fuel pool could serve as a storage function before fuel load. The use of the spent fuel pool in this function depends on the number of fuel assemblies that the new fuel storage vault holds.

Due to the introduction of nuclear fuel on site, zones will be established and maintained for security, access, administrative controls and Foreign Material Exclusion (FME).

Prior to fuel receipt, the operators are trained to receive, inspect, and place nuclear fuel. Phases 3 and 4 are the pre-operational testing of the plant, some of which only apply to the first AP1000 plant tests (see Table 7-1). It is anticipated that first plant tests will have been performed outside the UK.

7.5.8 Phase 5: Fuel Load

Fuel assemblies together with inserted components (control rods, burnable poison assemblies, and primary and secondary neutron sources) are placed in the reactor vessel, according to an established and approved sequence.

During and following the insertion of each fuel assembly, until the last fuel assembly has been loaded, the response of the neutron detectors is observed and compared with previous fuel loading data or calculations to verify that the observed changes in core reactivity are as expected. Specific instructions are provided if unexpected changes in reactivity are observed.

Because of the unique conditions that exist during initial fuel loading, temporary neutron detectors may be used in the reactor vessel to provide additional reactivity monitoring. Credit for the use of temporary detectors may be taken in meeting Technical Specification requirements on the number of operable source range channels.

Once fuel loading is complete, the upper reactor internals are loaded and the integrated head package moved into position. Once all the head closure bolts are tightened, the reactor is in Mode 5.

7.5.9 Phase 6: Pre-Critical and Low-Power Physics Tests

During this phase the fully assembled core is exposed to the full RCS conditions taking the plant from Mode 5 (cold shutdown, ambient conditions) to Mode 2 (startup).

Surveillance test procedures are demonstrated at this time and further analysis of pipework thermal growth and vibration is performed.

The reactor power is gradually increased but remains under 5 percent, and physics tests are undertaken.

Following criticality and prior to operation at power levels greater than 5 percent of rated power, physics tests are performed to verify that the operating characteristics of the reactor core are consistent with design predictions. During these tests, values are obtained for the reactivity worth of control and shutdown rod banks, isothermal temperature coefficients, and critical boron concentration for selected rod bank configurations.

Other tests at low power include verification of the response of the nuclear instrumentation system and radiation surveys.

For each test, the test procedure presents a general description for the test objective, test prerequisites, test description, and test performance criteria, where applicable. In describing a test, the operating and safety significant characteristics of the plant to be tested and evaluated are identified.

Following successful completion of the initial criticality tests, low-power tests are conducted, typically at power levels less than 5 percent, to measure physical characteristics of the reactor system, and to verify the operability of the plant systems at low-power levels.

7.5.10 Phase 7: Raise Power

The overall objective of the raise power phase is to demonstrate the safe and reliable operation and performance of the plant under both steady-state and transient conditions. It is also designed to verify the adequacy of the operating procedures for normal and abnormal operating conditions.

Major transient tests such as reactor trips and load rejections are carried out during this phase with a variety of procedures being carried out on the conventional plant and systems.

After low-power testing is completed, testing is performed at specified elevated power levels to demonstrate that the plant operates in accordance with design during normal steady-state operations.

During power ascension, tests are performed to obtain operational data and to demonstrate the operational capabilities of the plant.

7.5.11 First-Time-Only Tests and the First Three Plant Tests

The AP1000 plant as a standard design will undergo the same test programmes for the same SSCs in some key areas with only the local environment changing between sites. It is anticipated that first-time-only and the first three plant tests will be performed on plants outside the UK and will not be performed on the UK AP1000 plants. These tests are shown in Table 7-1.

7.6 Examination, Maintenance, Inspection, and Testing

7.6.1 Introduction

The purpose of the AP1000 UK Safety Categorisation and Classification Methodology (Reference 7.20) is to categorise safety functions required to maintain safety in the event of specific fault sequences, identifying which SSCs deliver these safety functions, and classifying them accordingly.

The classification scheme helps to define the quality management requirements placed on SSCs during the design, manufacture, commissioning and through-life operations, including EMIT, as part of a comprehensive preventative maintenance programme. In particular, the safety class of a given SSC can be used to determine what maintenance considerations are appropriate to that SSC to ensure it operates on demand.

The AP1000 UK Safety Categorisation and Classification of Systems, Structures and Components (see Appendix 15A) forms the basis of the engineering schedule for the AP1000 plant, providing the classification of the SSCs based on their safety function category. Information identifying how the safety category and safety class are determined is presented in Chapter 5.

Class 1 passive systems are the principal means of providing Category A safety functions and must have the highest levels of integrity, performance, and availability. The EMIT provisions identified in the engineering schedule for such SSCs will be commensurate with this safety importance. The same applies to the Class 1 systems that provide supporting functionality, such as Class 1 power supplies and C&I.

The active systems that are claimed to provide backup or alternative means to the passive systems are not Class 1 systems; they are appropriately classified within the EMIT programme. This will ensure these systems operate on demand and underpin the deterministic and probabilistic claims identified within the safety case.

7.6.2 Examination, Maintenance, Inspection, and Testing Process

It is a requirement that the licensee must provide EMIT schedules in accordance with SLC 28 (Reference 7.12) to ensure that appropriate maintenance is provided to ensure nuclear safety functions are met on demand.

The EMIT process will be part of the site licensee management arrangements supported by the licensee quality programme that will interface with the Westinghouse QMS.

This will ensure that appropriate instructions and methods have been followed in support of the EMIT programme and that these instructions and methods remain valid during any changes or modifications throughout the plant life cycle.

The instructions and methods for carrying out EMIT will describe the criteria for identifying the safety significance of all plant items and systems, and identify the safety significance of all examination, inspection, maintenance, and test activities.

The EMIT schedule may comprise a single document, but most likely will contain several parts. If this is the case, the schedule should be produced in a tiered format, with a hierarchy indicating the specific nuclear safety significance of the maintenance activities. The engineering schedule in Appendix 15A will be further developed during site-specific licensing to form the basis of the EMIT schedule.

Some activities specified in the EMIT schedule will only be able to be carried out during shutdown periods. On this basis, the maximum operating period between shutdowns will need to be identified and any tolerances for the EMIT activity to be included in the schedule. All EMIT activities will be undertaken by a SQEP.

Intervals in the EMIT schedule of work should be carried out in accordance with the specified time interval, to ensure reliability of the SSCs demanded within the safety case.

If any Class 1 SSC is determined not to have operated on demand or identified as faulty during maintenance activities then this occurrence must be reported and investigated by the licensee under their arrangements made to satisfy SLC 7 (Reference 7.21). In addition if this occurs during the commissioning phase, Westinghouse will also be required to be involved in the investigation process.

Records of any EMIT will be made and kept by the licensees in accordance with their arrangements. Any such EMIT undertaken by Westinghouse will be recorded, and the information will be provided to the licensees.

7.6.3 Examination, Maintenance, Inspection, and Testing Schedules

EMIT schedules are to be prepared by the site licensee on the premise that the plant and equipment in use will retain the reliability claimed in the safety case, thus ensuring that the risk of failure associated with the process is kept ALARP. The reliability of the AP1000 plant will be maintained by a process of planned maintenance procedures, including replacement, based upon a sound understanding of the plant and equipment's ageing mechanisms supported by the programme of EMIT.

The EMIT programme should be implemented in accordance with the requirements of the maintenance schedule and related procedures and instructions produced by the site licensee.

EMIT activities undertaken on SSCs with nuclear or radiological implications will be identified in the plant maintenance programme and classified according to the methodology described earlier. Each task in the schedule will be classified according to its nuclear safety significance using the classification scheme. This is necessary to ensure that such equipment is maintained to appropriate standards, thereby providing confidence that the SSC will fulfil its safety functional requirements if called upon, and the plant remains within its operating limits and conditions.

EMIT schedules will be written by the site licensee, with guidance from the design engineers (Westinghouse and other suppliers). At a system level, the items that need to be included in the EMIT schedule are those on which the nuclear safety case imposes performance and/or availability requirements.

It is a requirement that the EMIT schedules should take into account the requirement that the redundancy or diversity assumed in the safety case remains consistent with its nuclear safety significance based on the classification scheme, even whilst the corresponding system is being maintained or tested, in some cases during plant operation.

Generically the EMIT schedules will be developed from the testing undertaken during plant startup and commissioning. They will be maintained throughout the operational phases of the plant remaining a "live" document. This in turn being updated as changes and modifications are made to the plant.

7.7 Operational Phase

The safety management during the operation of the plant will be the responsibility of the licensee within the operating organisation. The primary safety management responsibility of the licensee is the protection of the public and the operators from harm arising from ionising radiation or other causes. The licensee will operate and maintain the plant in accordance with the licence granted by the Office for Nuclear Regulation (ONR) and will comply with relevant UK legislation.

However, in moving into the operational phase, Westinghouse will be involved with the licensee in providing guidance and information on what may be included in their arrangements and procedures. Further discussion is provided in the Plant Life Cycle Safety Report (Reference 7.1, Section 9), which is summarised in the following sections.

7.7.1 Operating Instructions

Where appropriate, written OIs will be provided to the licensee for operations that may affect safety during all phases of the plant life. These will be written, validated, and approved by an SQEP. Such information will aid the knowledge transfer process. Specifically these will include the OIs necessary to ensure that the limits and conditions identified in the safety case remain valid. These instructions are expected to be vast and very comprehensive.

Any records of training or demonstration that the OIs have been followed will be in accordance with the licensee's arrangements and where appropriate integrated into Westinghouse's processes.

7.7.2 Manning Levels

Westinghouse will provide recommended information relating to the preparation and plans for the operation of the AP1000 plant to the licensee. The purpose is to provide reasonable assurance that the licensee will establish and maintain manning levels and technical competences that reasonable assurance of adequate protection of public health and safety is provided. The licensee will demonstrate to the ONR that suitable arrangements are in place for compliance to the requirements of SLC 36 (Reference 7.22).

Such manning levels will also include those levels needed to respond to an onsite and offsite emergency.

Where there is reliance upon the services of Westinghouse contracted personnel, the structure of that part of Westinghouse, the authorities, responsibilities, and interfaces with the licensees will be provided, and suitable instructions and procedures will be established.

7.7.3 Training

Personnel who have responsibility for an action that may affect safety have to be adequately trained for that purpose. This is a requirement not only of the site licence, but also other UK legislation, including The Ionising Radiations Regulations (IRRs) (Reference 7.23) and Management of Health and Safety at Work Regulations (Reference 7.24).

Westinghouse identifies the need to ensure that all people employed on behalf of Westinghouse are suitably qualified (for example, trained) and experienced for the tasks they are to perform. The appropriate Westinghouse procedures relating to training will also be applied, as discussed in Chapter 3.

In addition, Westinghouse will align their training requirements with the arrangements of the licensee and align the procedure for maintaining appropriate training records with those of the licensee. Implementation of the above arrangements will ensure that all personnel associated with the construction, installation, and commissioning of the AP1000 plant will be SQEPs.

Where appropriate, Westinghouse will provide training to licensee personnel in the safe operation and maintenance of the AP1000 plant to assist the licensee in accordance with its requirements to ensure that only SQEPs perform any duties that may affect safety. This is also an essential part of the knowledge transfer process and ensures that the licensee can demonstrate its ability to act as an IC and as a DA.

In addition, the licensee will be expected to identify DAPs to either carry out or directly supervise operations of the highest safety significance. If required, Westinghouse will assist in the training of DAPs.

7.7.4 Emergency Procedures and Services

Westinghouse states that all facilities must be operated within their safe operating parameters so that they do not present a hazard to employees, the public, or the environment. In addition, all plants and facilities require an appropriate emergency plan to control and mitigate the impact of unforeseen circumstances. Procedures will be developed to establish an integrated emergency response and crisis management at the project level. The licensee is responsible for making and implementing emergency arrangements and will ensure that Westinghouse's procedures align. The procedures will ensure suitable consideration has been given to compliance with the Radiation (Emergency Preparedness and Public Information) Regulations (REPPIR) 2001 (Reference 7.25) and Control of Major Accident Hazards (COMAH) Regulations (Reference 7.26).

These procedures address the implementation of an effective response to any minor onsite incident ranging through to a major offsite incident. Where appropriate, external bodies whose assistance, cooperation, or services are required to fulfil those arrangements will be consulted during the preparation.

Further information regarding emergency preparedness is provided in Chapter 25 and refers to the need for both an onsite and an offsite emergency plan and the emergency response facilities.

7.7.5 Radiological Protection

The AP1000 design incorporates radiation exposure reduction principles to keep the worker and public doses ALARP. Chapter 24 discusses the normal operational radiological aspects of the design and operation of the AP1000 plant.

7.7.6 Nuclear Material Arrangements

Prior to any active commissioning, as part of the licensing requirements, the licensee must have adequate arrangements in place to ensure that the introduction and storage of any nuclear materials is controlled (Reference 7.27). If specified by the ONR, consent must be obtained prior to any nuclear matter being brought on to the site. Such arrangements must be in place for the operations with new and spent fuel and radioactive waste. Such arrangements will include ensuring that there is an adequate safety case, suitable records of the nature of the material, and its storage location on plant. Such facilities are required to have appropriate criticality safety controls in place. This is normally achieved using criticality certificates that detail the safety measures in place to prevent an accidental criticality outside of the reactor

core. Where appropriate, the European Atomic Energy Community (EURATOM) will be informed of any imports/exports, and arrangements will be expected to be in place for EURATOM verification. While this is clearly a requirement of the licensee, Westinghouse will support the licensee as necessary to ensure compliance to these requirements during commissioning activities.

7.8 Ageing and Degradation

7.8.1 Introduction

Ageing management is defined as engineering, operations, and maintenance actions to control ageing degradation of SSCs within acceptable limits.

To provide for the timely detection and mitigation of ageing degradation of SSCs important to safety, NPP owners/operators should have in place a systematic ageing management programme, which takes account of regulatory policy and guidance.

Ageing management, as a part of its input to life cycle management, should consider the benefits to the plant of maintaining SSCs in good working order.

The AP1000 plant has been designed to operate for 60 years; this claim is to be justified within the safety case or relevant SSCs within the plant footprint will be identified that can be easily repaired in situ or replaced if they become obsolete. Consideration is given to the ageing process affecting the following:

- The SSCs that make up the primary and secondary circuits, for example, electrical and mechanical systems.

- The SSCs that make up the nuclear island (NI) facilities and supporting auxiliary buildings, for example, the civil structures.

All the SSCs with a nuclear safety function are maintained within the EMIT programme, and any other supporting SSCs will be maintained via the licensed site maintenance plan. The EMIT programme will ensure the required reliability of those SSCs with a safety function to operate on demand, but eventually there will be a time when an SSC can no longer be maintained or repaired, i.e., it is beyond its operable life. This is also applicable to those systems that do not have a direct nuclear safety function but would impact nuclear safety if they failed.

The site licensee should consider within its management arrangements how stores will be procured to avoid obsolescence and how modifications to replace failed or faulty parts will be undertaken. This impacts the stores' policy and whether like-for-like parts will continue to be available over the plant's 60-year life cycle.

Consideration will also be required of the safety implications of new parts and modifications, along with how they will be assessed to confirm safe operation within the existing plant.

This section of the PCSR identifies how the ageing process is justified within the safety case and the Westinghouse approach to justifying the claim for a 60-year design life of the plant.

7.8.2 Background

Westinghouse has designed, developed, and manufactured nuclear facilities since the 1950s. Beginning with the world's first large central station nuclear plant (Shippingport), which produced power from 1957 until 1982, Westinghouse has designed and delivered more than 100 commercial NPPs worldwide, including the design of Sizewell B, with a combined electrical generating capacity in excess of 90,000 MW. The design of the AP1000 plant is therefore supported by decades of successful plant operating experience that have accumulated many operating years without significant issue. Westinghouse has substantial proven experience, knowledge, and capability to design, manufacture, and furnish technical assistance for the installation, startup, and service of NPPs.

The AP1000 plant is of similar design to that of the earlier Westinghouse designs that use similar proven materials and manufacturing processes in the construction and commissioning of the plant.

Records of safe operating experience are insufficient to directly support reliability claims for a new build project in the UK, but they provide confidence that similar materials, standards, and codes have been successfully operating in existing plants. Materials in existing plants will experience similar behaviour when exposed to ageing and degradation mechanisms in the AP1000 plant. Understanding the in-service performance of these materials has aided design, manufacture, and the management and mitigation of through-life ageing and degradation issues in the AP1000 plant.

7.8.3 Methodology

A structured safety argument to demonstrate that the plant is fit for purpose for the required design lifetime of 60 years is presented in Volume 4 of the PCSR.

The structural integrity of large vessels and components is substantiated in Chapter 20. A four-legged approach is used to justify the incredibility of failure argument composed of the following:

- Leg 1 Interpolation/Extrapolation of Experience – Good Design and Manufacture
- Leg 2 Functional Testing
- Leg 3 Failure Analysis
- Leg 4 Forewarning of Failure

Compliance with the appropriate American Society of Mechanical Engineers (ASME) standards for Class 1 components provides the basic demonstration of fitness for purpose and is generally inferred as providing substantiation for a component frequency of failure of 10^{-5}/yr.

Additional qualitative arguments are presented in the component safety reports in Chapter 20 to demonstrate evidence of defence in depth and to substantiate component reliability commensurate with the classification for the lifetime of the SSCs.

This approach is used for other items, namely the electrical and mechanical systems. Additional high-integrity SSCs requiring further justification have further supplementary measures to ensure high quality.

7.8.4 Codes and Standards

The plant is designed, fabricated, and installed in accordance with the codes, standards, and regulations identified in Volume 4 of the PCSR. Complying with such proven and established codes, standards, and regulations minimises the level of design and manufacturing uncertainty. For example, compliance with the ASME Boiler and Pressure Vessel Code provides assurance over a wide range of issues from material procurement, component design, selection of manufacturing consumables, qualification of welders, specification of heat treatment, manufacturing quality checks and nondestructive examination, testing, installation, pre-service inspection (PSI), and in-service inspection (ISI) requirements (see Chapter 20). The extensive body of experience that is embodied within the ASME Code and the successful operation of a significant number of pressure vessels (both nuclear and non-nuclear) means that compliance with the code provides assurance that the vessel reliability will remain high for the design life of the component.

Similarly this level of assurance is claimed for both the primary and secondary SSCs within Volume 4 of the PCSR.

7.8.5 Component Manufacture

The quality of the component manufacture makes a significant contribution in ensuring that the AP1000 plant materials maintain proven service performance. The materials are selected to meet or exceed ASME or equivalent specifications based on the following:

- Tight control on chemical composition is enforced to minimise the effects of irradiation embrittlement or thermal ageing to ensure that materials remain ductile when stressed.

- Materials are compatible with each other and with the environment and are resistant to environmental degradation over the life of the plant. Degradation characteristics are known and understood.

- Material testing is sufficient to demonstrate that the material properties are compliant with the relevant specifications.

The materials selected for use in the plant will be compatible with the full range of internal and external environmental conditions that may be encountered over the plant life and are predicted not to degrade to an unacceptable degree in that time. These environmental conditions include temperature, humidity, radiation, chemistry of fluid or materials in contact, and other external conditions that may affect the performance of a material.

To ensure the selected materials support the design life of the plant, the AP1000 equipment qualification programme is in place that relies on the Institute of Electrical and Electronics Engineers (IEEE) 323 (Reference 7.32) definition for design life.

7.8.6 Ageing Evaluation Programme for Safety-Related Electrical and Mechanical Equipment

The Ageing Evaluation Program describes methods for addressing potential age-related, common-mode failure mechanisms used in AP1000 plant equipment qualification programmes. These programmes make use of guidance from IEEE 323 and IEEE 344 (Reference 7.32 and 7.33). The approach conforms to current industry positions and makes maximum use of available data and experience in the evaluation, test, and analysis of ageing mechanisms. Specific treatment of seismic qualification, part of the qualification test sequence recommended in IEEE 323, is addressed in IEEE 344.

As stated in IEEE 323, ageing of Class 1 equipment during normal service is considered an integral part of the qualification programme. The objective is not to address random age-induced failures that occur in-service and are detected by periodic testing and maintenance programmes. The objective is to address the concern that some ageing mechanisms, when considered in conjunction with the specified design basis events (DBE), may have the potential for common-mode failure.

The approach places primary emphasis on common-mode failures due to enveloping DBEs. For example, reasonable assurance against common-mode failures being induced because of a loss of heating, ventilation, and air conditioning (HVAC) is provided by adequate design, normal maintenance, and calibration procedures. The objectives of the ageing evaluation programme are:

- To establish, where possible, the effects of the degradation due to ageing mechanisms that occur before the occurrence of an accident, when equipment are called upon to function.

- To provide increased confidence that equipment perform their safety function under the specified service condition.

The general approach to addressing ageing allocates equipment to one of two subprogrammes (A or B).

- **Subprogramme A** – Includes electrical equipment required to perform a safety function in a high-energy line break (HELB) environment. For this equipment an ageing simulation is included as part of the equipment qualification test sequence. The equipment is energised during the ageing simulation.

- **Subprogramme B** – Includes equipment required to mitigate HELBs but that, due to its location, is isolated from any adverse external environment resulting from the accident. For equipment in Subprogramme B the single DBE capable of producing an adverse environment at the equipment location is the seismic event. Ageing, for Subprogramme B, is not included in the equipment qualification test sequence. Significant ageing mechanisms are determined by evaluation of available test data. Generally, this data is from separate programmes conducted to demonstrate that aged components continue to meet manufacturer's performance specifications under applicable seismic DBE conditions and that seismic testing of unaged equipment is not invalidated by anticipated ageing mechanisms.

IEEE 627 (Reference 7.34) describes the methodology that has been adopted to qualify equipment. The two standards primarily used to demonstrate compliance with this standard are IEEE 323 and IEEE 344.

7.8.7 In-Service Inspection and Testing

In order to provide assurance the electrical and mechanical systems remain operable within the design life and to ensure that defects will be detected prior to becoming a threat to the life cycle of the plant, an extensive programme of ISI and in-service testing (IST) will help to identify degradation long before failure.

Pre-service inspection data and ISI data from other sites enables judgement of in-service defects and helps plan maintenance to extend the lifetime of the plant.

ISI and IST is the preferred method of forewarning possible failure of plant SSCs. The role of ISI and IST is to detect defects before it becomes problematic and enable the operator to take remedial action.

7.8.8 Civil Engineering Structures

The NI structures house SSCs that provide the principal means of delivering Category A safety functions. These functions must be delivered to achieve and maintain a nonhazardous, stable state for at least 72 hours of the initiating event for a DBA throughout the design life of the plant. Failure of these SSCs has the potential to lead to core damage or activity release to the environment outside design basis limits. Thus, the civil engineering structures composing the NI are all designated as A1 (Category A safety function and Class 1 contribution to this safety function.). They are also seismic Category I (see Section 5.8). Based on this classification the civil engineering structures are constructed to the highest quality standards to ensure the AP1000 plant maintains proven service performance. The materials are selected to meet or exceed specifications, and designed, fabricated, and installed in accordance with the codes, standards, and regulations identified in Volume 4 of this PCSR. Complying with such proven and established codes, standards, and regulations minimises the level of design, construction, and manufacturing uncertainty.

Selected materials are compatible with each other and with the environment and are resistant to environmental degradation over the life of the plant. Degradation characteristics are known and understood and will be suitable to meet decommissioning requirements at the end of plant life.

Materials testing based on existing Westinghouse operating plants can be used to demonstrate that the construction material properties are compliant with the relevant specifications identified in Volume 4 of this PCSR.

7.9 Decommissioning

7.9.1 Introduction

The objective of this section is to summarise the aspects of the AP1000 plant that will facilitate safe decommissioning at the end of the plant operational life and identify that the claims made regarding decommissioning within the safety case can be adequately achieved.

The fundamental objective of decommissioning is to reduce the risks associated with the plant to an acceptable level. In order to achieve this end state, radioactive and conventional wastes must be removed from the site as far as reasonably practicable and/or to achieve the criteria agreed for delicensing in accordance with government policy. This objective includes the requirements to demonstrate that the doses to workers and the public will be ALARP, and that legislation under the Environmental Protection Act will be met using best available technique (BAT) to establish acceptable methods of decommissioning.

Although decommissioning is the last stage in the overall life cycle of a facility, decommissioning must be considered at the planning and design stages and also considered during any modifications to the plant.

SLC 35 (Reference 7.28) requires the licensee to make adequate arrangements for the safe decommissioning of the site, and these will need to accord with any relevant government policy. As part of this, a decommissioning programme to implement the decommissioning strategy will be required along with the decommissioning safety case.

Further decommissioning details and evidence to support the decommissioning strategy and end-of-life aspects of the plant are identified within Chapter 27. The main claims justified within the safety case regarding the decommissioning of the plant are the following:

- That the environmental impact of the plant during decommissioning will be minimised and will be within authorised limits and operational targets.
- That the plant design will allow for the proper management of radioactive waste and spent fuel.
- That the plant can be decommissioned safely.

These assumptions will be managed by the site licence holder in accordance with its own processes and procedures, and in accordance with relevant legislation and licence conditions. The site licence holders will have the responsibility for the final decommissioning plan.

7.9.2 Assumptions

With regard to decommissioning on the site, the following assumptions are made within the safety case:

- Irradiated fuel from the plant is stored on the originating site in an appropriate facility for the operating life of the plant. At the end of the operating life, a decision will be made whether to continue to store irradiated fuel onsite or to dispatch it to an appropriate final disposal repository.
- Operational intermediate-level waste (ILW) is conditioned into suitable final disposal packages. The ILW will be transported to an onsite ILW store, where it will be held in a passively safe condition until a national ILW repository becomes available. This is discussed further in Chapter 27.
- The generation of low-level waste (LLW) from site operations is managed using standard waste minimisation techniques. As required, LLW packages will be dispatched from the originating site to an appropriate final disposal repository.
- Three options exist for the decommissioning of the NPP: immediate decommissioning, delayed or safe store, and entombment.

7.9.3 Decommissioning Stages

Three stages of decommissioning are identified in Chapter 27. The three stages are based on International Atomic Energy Agency (IAEA) safety standards, and briefly described in Table 7-2.

7.9.3.1 Stage 1 Decommissioning

During Stage 1 decommissioning the first contamination barrier is kept as it was during operation, but the mechanical opening systems and penetrations are permanently blocked and sealed (valves, plugs). The containment building is kept in a state appropriate to the remaining hazard, and the atmosphere inside the building is subject to appropriate control. Access to the building is subject to monitoring and surveillance procedures. The unit is under surveillance and the equipment necessary for monitoring radioactivity, both inside and outside the plant, is kept in good condition. Inspections are carried out to check that the plant remains in good condition. If necessary, checks are carried out to see that there are no leaks in the first contamination barrier and the containment building.

During this period, the work described in Chapter 27 will be implemented. The principal activities to be accomplished during Stage 1 are the following:

- Removal of fuel from the reactor to the spent fuel pool.
- Removal of radioactive inventory from the reactor system and non-decommissioning service systems
- Contamination mapping of all radioactive and potentially radioactive systems to ensure that health and safety risks associated with maintenance and dismantling of the radioactive systems are understood and the decontamination and radioactive waste treatment options can be assessed
- Post-operational clean out and in-situ decontamination (e.g., chemical decontamination of active circuits) of non-decommissioning service systems and reactor system
- Establishment of new radiation control areas based on the above actions as work progresses
- Review configuration of existing service systems and plan for their use/modification in decommissioning activities
- Removal of fuel from the spent fuel pool to the spent fuel store.

7.9.3.2 Stage 2 Decommissioning

During Stage 2 decommissioning, the first activities associated with dismantling and removal of systems and components are carried out. The contamination barrier is reduced to minimum size and all easily dismantled parts are removed. The sealing of the barrier is reinforced by physical means and the biological shield is extended if necessary so that it completely surrounds the barrier.

Depending on the extent to which other equipment is removed or decontaminated, access to the former containment building can be permitted. The non-radioactive buildings or equipment in the plant may be converted for new purposes. Surveillance around the barrier

can be relaxed, but it is desirable for periodic spot checks to be continued as appropriate, together with surveillance of the environment. External inspection of the sealed parts should also be performed.

During this period, the work described in Chapter 27 will be implemented. The principal activities to be accomplished during Stage 2 are:

- Modification of existing service systems and installation of temporary service systems to meet decommissioning requirements (e.g., shielding, monitoring, ventilation systems)
- Removal of radioactive inventory, post-operational clean out and in-situ decontamination of spent fuel pool system and fuel handling system
- Dismantling of non-radioactive systems and non-decommissioning service systems
- Conversion of fuel handling building into an interim waste storage, decontamination, waste reduction, packaging, and processing area for ILW
- Contamination mapping, dismantling, decontamination and disposal of non-decommissioning service systems
- Contamination mapping of residual radioactive and potentially radioactive systems
- Radiation and security controls

7.9.3.3 Stage 3 Decommissioning

During Stage 3 decommissioning, all materials, equipment, and parts of the plant in which activity remains significant despite decontamination will be removed as active waste.

During this period, the work described in Chapter 27 will be implemented. The principal activities to be accomplished during Stage 3 are:

- Removal, dismantling, decontamination and disposal of the reactor pressure vessel (RPV) and internals
- Removal of radioactive inventory, post-operational clean out, decontamination, and dismantling and disposal of residual radioactive systems
- Contamination mapping of residual radioactive and potentially radioactive decommissioning service systems, the containment building and shield building
- Cutting, processing, and removal of active concrete in the containment building and fuel handling building
- Dismantling, decontamination, and disposal of the containment building, shield building, and turbine building
- Removal of radioactive inventory, post-operational clean out, decontamination, dismantling and disposal of radioactive decommissioning service systems (temporary service systems will be supplied as required)

- Dismantling and disposal of non-radioactive decommissioning service systems (temporary service systems will be supplied as required)
- Dismantling, decontamination and disposal of the auxiliary building
- Dismantling, decontamination and disposal of the radwaste building
- Dismantling, decontamination and disposal of the temporary decommissioning service systems, waste water system, diesel generator building and annex building
- Dismantling, decontamination and disposal of the temporary decommissioning facility

The stages may be carried out by rapidly progressing from one stage to the next one, or may be carried out over a prolonged period. It is recognised that spent fuel requires considerable time to cool and that long-term storage will be required with additional time required for decommissioning the spent fuel storage facilities.

The plant and site are cleared for unrestricted use. From the point of view of radiological protection, no further surveillance, inspection, or tests will be necessary. In some cases, the whole plant, including inactive components, may be dismantled to make room for a replacement facility or other usage.

Decommissioning of Waste Stores

The ILW store design life is substantially longer than the power generation facility and as such will be a standalone structure supported by its own services and utilities. If the national ILW repository is available before end of AP1000 operations, ILW decommissioning waste could be shipped direct to the repository without interim storage onsite. Having the national ILW repository available before the end of AP1000 operations will also allow the decommissioning and dismantlement of the onsite ILW store using the decommissioning facilities created for the AP1000 plant. Once all the stored waste packages have been removed from the ILW store to offsite storage (national ILW repository or other appropriate storage facility) the building can be decommissioned.

The onsite spent fuel store will be decommissioned following the transfer of stored spent fuel to the national HLW repository (once available). On site storage up to 160 years after plant start up may be required to allow all the fuel to decay before shipment to the national HLW repository.

7.9.4 Site End Point

It is expected that the intended site end point and the subsequent management of contaminated land, if appropriate, will be addressed by the site licensee as part of their update of the decommissioning strategy. One decommissioning objective should always be to remove hazards so that the site does not present an unacceptable level of risk to human health or the wider environment. The final site end point will depend on the potential future use of the site.

The following is an example of one desirable site end point:

- Active materials will be decontaminated and removed.
- Structures, if present, will be deplanted and demolished during final site clearance.

- Buildings will be removed down to a depth of 1 m below ground level.
- Roads, car parks, and underground services will be removed.
- Active drains and outfalls will be removed. Foul and surface water drains will be removed if less than 1 m below ground level.
- Basements, if present, will be demolished to 1 m below ground level, and any remaining subsurface structures punctured to assist drainage.
- Land requiring remediation will be identified and treated appropriately.
- Surveying and sampling will be performed to demonstrate that the land is:
  - Suitable for delicensing in accordance with current regulatory guidance (Reference 7.29).
  - Not considered contaminated land as per the current regulations.
- Ground will be appropriately landscaped and land drains installed, if required.

7.9.5 Differing Approaches to Decommissioning

The IAEA have recognised the following three primary decommissioning strategies in developing safety standards:

- **Immediate Dismantling** – Dismantling commences soon after shutdown of the plant (typically within 5 years) with radioactive material above a specific level being removed. This strategy does not allow for any significant decay of radionuclides.
- **Deferred Dismantling or Safe Enclosure (Safe Store)** – Those parts of the facility containing radioactivity are processed or brought into a condition such that they can be stored and maintained in a safe manner (e.g., liquids are drained from the system and irradiated fuel and operational waste materials removed). The facility is placed in long-term storage (e.g., 50 years) prior to later dismantling. This option allows for decay of radionuclides.
- **Entombment** – As with the deferred dismantling option, liquids and waste are removed. The remaining radioactive material is encased onsite (normally in concrete). Essentially, the site becomes a near-surface waste repository.

The nature of the AP1000 design is amenable to all three options due to the fact that it is based on a modular build strategy that naturally lends itself to the immediate dismantling option. This makes decommissioning easier as these modules can be removed (and contained if necessary) to the waste processing area for further dismantlement, decontamination, packaging, and disposal.

7.9.6 Decommissioning Concept

The UK AP1000 NPP Decommissioning Plan (Reference 7.31) provides an outline decommissioning plan that demonstrates the technical and practical feasibility of one method by which the AP1000 plant can be safely decommissioned. The outline plan provides assurance that decommissioning can be safely accomplished within the currently acceptable

limits of personnel exposure to radiation and will not result in any pollution impact on the decommissioned site or wider environment. Further evidence that the safety case can be justified is given in Chapter 27.

The outline plan is based on an immediate dismantling option and adopts a staged approach, which can be seen in Table 7-2.

This outline strategy assumes that, prior to Stage 1 works commencing, temporary buildings will be provided for processing and storage of ILW and LLW generated by dismantling large-scale components.

The outline plan forms the basis for a detailed decommissioning strategy to be produced in parallel with the decommissioning safety case by the licensee and developed throughout the life cycle of the facility. As the end of the operational lifetime of the facility is approached, a detailed decommissioning plan will be produced along with the safety case. This detailed plan will expand and improve upon the outline plan and will reflect the BAT.

7.10 Health and Safety Arrangements for Project Execution

This chapter focuses on the nuclear safety aspects of the project. However, there are many other aspects of safety that can have impact on the nuclear safety of the facility. Thus, it is considered prudent to provide a brief explanation of the expectations and standards on other safety aspects that Westinghouse expects to be implemented during the construction phase. These topics are considered in more detail in the Plant Life Cycle Safety Report (Reference 7.1).

The construction scope for the AP1000 plant will typically be performed by a Westinghouse partner that is a competent and experienced architect-engineer (AE)/contractor. The AE will be expected to demonstrate its safety performance record on similar job sites and the content and application of its EHS Manual.

It is expected that the AE will develop a site-specific EHS programme to govern all aspects of protecting the environment and the health and safety of project/site employees during construction. The arrangements will have to be acceptable to the licensee and reflect their requirements.

The areas expected to be covered will include, but are not exclusive to, the following:

- Onsite medical services
- Construction fire prevention programme
- Appropriate site and material security programme
- Accident reporting and investigation to input into the continual improvement programme
- Work planning, including risk assessments, permit to work systems, safe systems of work, and method statements
- Recognition and rewards programme to provide positive reinforcement for behaviours and activities that support a strong, effective health and safety programme
- Accountability on an individual and project level

- Worker participation to ensure that both management and safety representatives encourage participation by the workforce in all aspects of programme implementation
- Audits and assessments
- Environmental safety

The UK AP1000 Environment Report (Reference 7.30) has been prepared to consolidate and summarise the environmental information presented. Other environmental aspects are covered in Chapter 26.

7.11 References

7.1 Westinghouse Report, UKP-GW-GL-737, Rev. 2, "Plant Life Cycle Safety Report," March 2011.

7.2 ONR Nuclear Safety Technical Assessment Guide, NS-TAST-GD-049, Rev. 4, "Licencee Core and Intelligent Customer Capabilities," Office for Nuclear Regulation, April 2013.

7.3 ONR Nuclear Safety Technical Assessment Guide, NS-TAST-GD-079, Rev. 2, "Licensee Design Authority Capability," Office for Nuclear Regulation, April 2013.

7.4 ONR Nuclear Safety Technical Inspection Guide, NS-INSP-GD-020, Rev. 3, "LC20: Modification to Design of Plant under Construction," Office for Nuclear Regulation, March 2013.

7.5 Westinghouse Report, APP-GW-GER-005, Rev. 1, "Safe and Simple: The Genesis and Process of the AP1000 Design," August 2008.

7.6 ONR Nuclear Safety Technical Inspection Guide, NS-INSP-GD-022, Rev. 3, "LC22: Modification or Experiment on Existing Plant," Office for Nuclear Regulation, December 2014.

7.7 Westinghouse Procedure, APP-GW-GAP-341, Rev. 0, "AP1000 Plant Program Design Change Control," January 2016.

7.8 Nuclear Safety Technical Inspection Guide, NS-INSP-GD-006, Rev. 0, LC6: "Documents, Records, Authorities and Certificates," Health and Safety Executive, October 2015.

7.9 ONR Technical Inspection Guide, NS-INSP-GD-014, Rev. 2, "LC14: Safety Documentation," Office for Nuclear Regulation, May 2013.

7.10 ONR Nuclear Safety Technical Inspection Guide, NS-INSP-GD-019, Rev. 4, "LC19: Construction or Installation of New Plant," Office for Nuclear Regulation, October 2015.

7.11 ONR Nuclear Safety Technical Inspection Guide, NS-INSP-GD-021, Rev. 3, "LC21: Commissioning," Office for Nuclear Regulation, March 2013.

7.12 ONR Nuclear Safety Technical Inspection Guide, NS-INSP-GD-028, Rev. 4, "LC28: Examination, Inspection, Maintenance and Testing," Office for Nuclear Regulation, September 2015.

7.13 UK Statutory Instrument No. 51, "The Construction (Design and Management) Regulations," 2015.

7.14 Not Used

7.15 Westinghouse Report UKP-GW-GL-045, Rev. 2, "AP1000 Equivalence/Maturity Study of the U.S. Codes and Standards," September 2011.

7.16 ONR Nuclear Safety Technical Inspection Guide, NS-INSP-GD-023, Rev. 3, "LC23: Operating Rules," Office for Nuclear Regulation, January 2013.

7.17 ONR Nuclear Safety Technical Inspection Guide, NS-TAST-GD-024, Rev. 2, "LC24: Operating Instructions," Office for Nuclear Regulation, May 2009.

7.18 ONR Nuclear Safety Technical Assessment Guide, NS-TAST-GD-027, Rev. 4, "Training and Assuring Personnel Competence" Office for Nuclear Regulation, November 2014.

7.19 Not Used.

7.20 Westinghouse Report, UKP-GW-GL-044, Rev. 1, "AP1000 UK Safety Categorisation and Classification Methodology," April 2010.

7.21 ONR Nuclear Safety Technical Inspection Guide NS-INSP-GD-007, Rev. 2, "LC7: Incidents on the Site and Other Reporting and OE Processes," 7, Incidents on Site Office for Nuclear Regulation, February 2013.

7.22 ONR Nuclear Safety Technical Assessment Guide, NS-TAST-GD-048, Rev. 4, "Organisational Capability," Office for Nuclear Regulation, March 2013.

7.23 UK Statutory Instrument No. 3232, "Ionising Radiations Regulations," 1999.

7.24 UK Statutory Instrument No. 3242, "Management of Health and Safety at Work Regulations," 1999.

7.25 UK Statutory Instrument No. 2975, "The Radiation (Emergency Preparedness and Public Information) Regulations," 2001.

7.26 UK Statutory Instrument No. 743, "The Control of Major Accident Hazards Regulations," 1999.

7.27 ONR Nuclear Safety Technical Inspection Guide, NS-INSP-GD-004, Rev. 0, "LC4: Restrictions on Nuclear Matter on the Site," Health and Safety Executive, March 2013.

7.28 Nuclear Safety Technical Inspection Guide, NS-INSP-GD-035, Rev. 3, "LC35: Decommissioning," Office for Nuclear Regulation.

7.29 HSE, "Guidance to inspectors on the interpretation and implementation of the HSE policy criterion of no danger for the delicensing of nuclear sites," Health and Safety Executive, August 2008.

7.30 Westinghouse Report, UKP-GW-GL-790, Rev. 6, "UK AP1000 Environment Report," January 2017.

7.31 Westinghouse Report UKP-GW-GL-795, Rev. 0, "UK AP1000 NPP Decommissioning Plan," March 2011.

7.32 IEEE-323-1974, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers, 1974.

7.33 IEEE 344-1987, "IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers, 1987.

7.34 IEEE 627-1980, "IEEE Standard for Design Qualification of Safety System Equipment Used in Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers, 1980.

Table 7-1. First-Time-Only Test and the First Three Plant Tests(1)

First-Time-Only Plant Tests
In-containment refuelling water storage tank heatup test
Pressuriser surge line stratification evaluation
Reactor vessel internals vibration testing
Natural circulation tests
Rod cluster control assembly out of bank measurements
Load follow demonstration
First Three Plant Tests
Core makeup tank heated recirculation tests
Automatic depressurisation system blowdown test

Note (1) All of these tests will be performed on AP1000 plants before the UK AP1000 plants startup and as a result will not have to be performed on the UK AP1000 plants.

Table 7-2. Decommissioning Stages and Estimated Timeline

Stage 1	Stage 2	Stage 3
Approx. 10 years	**Approx. 6 years**	**Approx. 6 years**
Removal of fuel from the reactor to the spent fuel pool	Modification of existing service systems and installation of temporary service systems to meet decommissioning requirements	Removal, dismantling, decontamination and disposal of the RPV and internals
Removal of radioactive inventory from the reactor system and non-decommissioning service systems	Removal of radioactive inventory, post-operational clean out and in-situ decontamination of spent fuel pool system and fuel handling system	Removal of radioactive inventory, post-operational clean out, decontamination, dismantling and disposal of residual radioactive systems
Contamination mapping of all radioactive and potentially radioactive systems	Dismantling of non-radioactive systems and non-decommissioning service systems	Dismantling and removal of remaining non-radioactive systems
Post-operational clean out and in-situ decontamination of non-decommissioning service systems and reactor system	Conversion of the fuel handling building into an interim waste storage, decontamination, waste reduction, packaging, and processing area for ILW	Contamination mapping of residual radioactive and potentially radioactive decommissioning service systems, the containment vessel (CV) and shield building
Establishment of new radiation control areas based on the above actions as work progresses	Contamination mapping, dismantling, decontamination and disposal of non-decommissioning service systems	Cutting, processing, and removal of active and clean concrete in the CV and fuel handling building
Review configuration of existing service systems and plan for their use/modification in decommissioning activities	Contamination mapping of residual radioactive and potentially radioactive systems	Dismantling, decontamination and disposal of the CV, shield building and turbine building
Removal of fuel from the spent fuel pool to the spent fuel store	Radiation and security controls	Removal of radioactive inventory, post-operational clean out, decontamination, dismantling and disposal of radioactive decommissioning service systems
		Dismantling, decontamination and disposal of the auxiliary building
		Dismantling, decontamination and disposal of the radwaste building

Table 7-2. Decommissioning Stages and Estimated Timeline (cont.)

Stage 1	Stage 2	Stage 3
Approx 10 years	**Approx 6 years**	**Approx 6 years**
		Dismantling, decontamination and disposal of the temporary decommissioning facility
		Dismantling, decontamination and disposal of the waste water system, diesel generator building and annex building

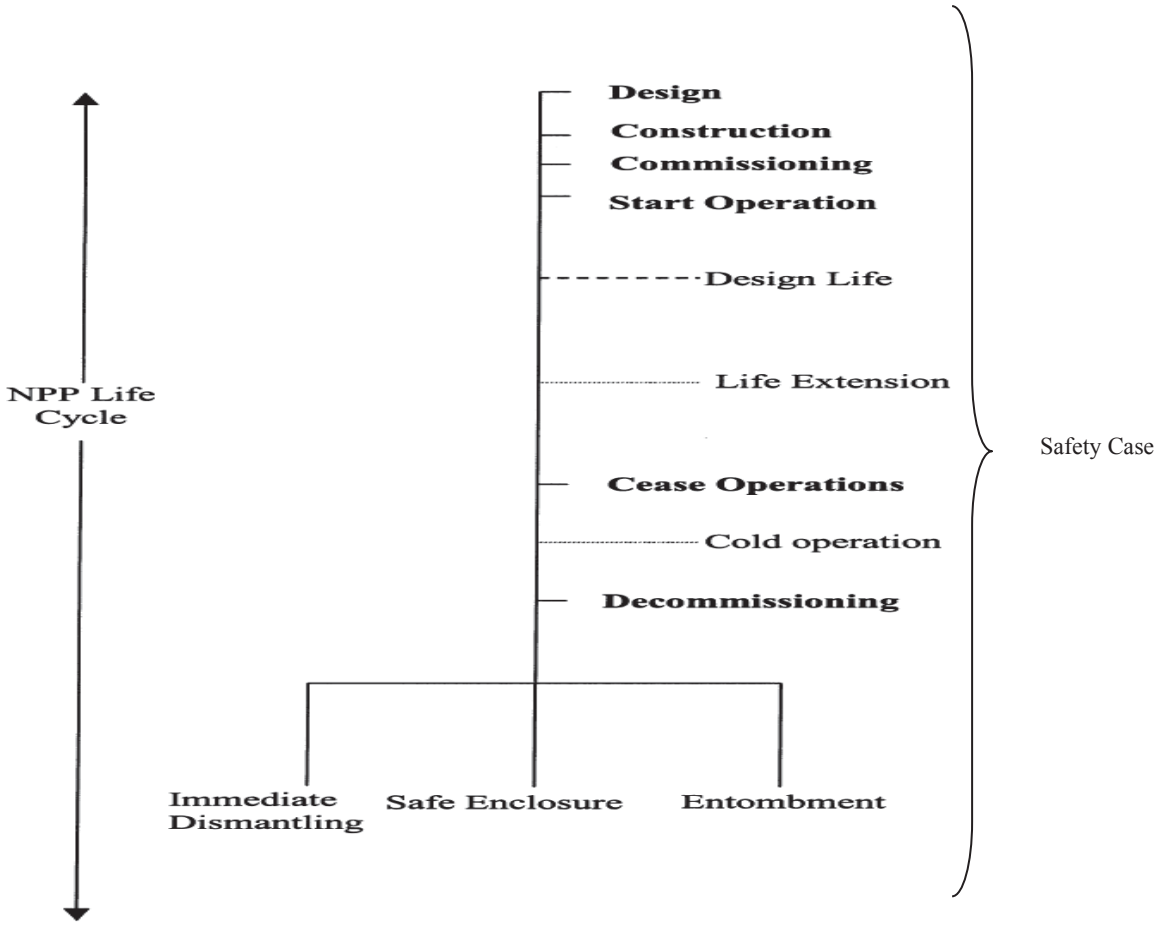


Figure 7-1. Nuclear Power Plant Life Cycle

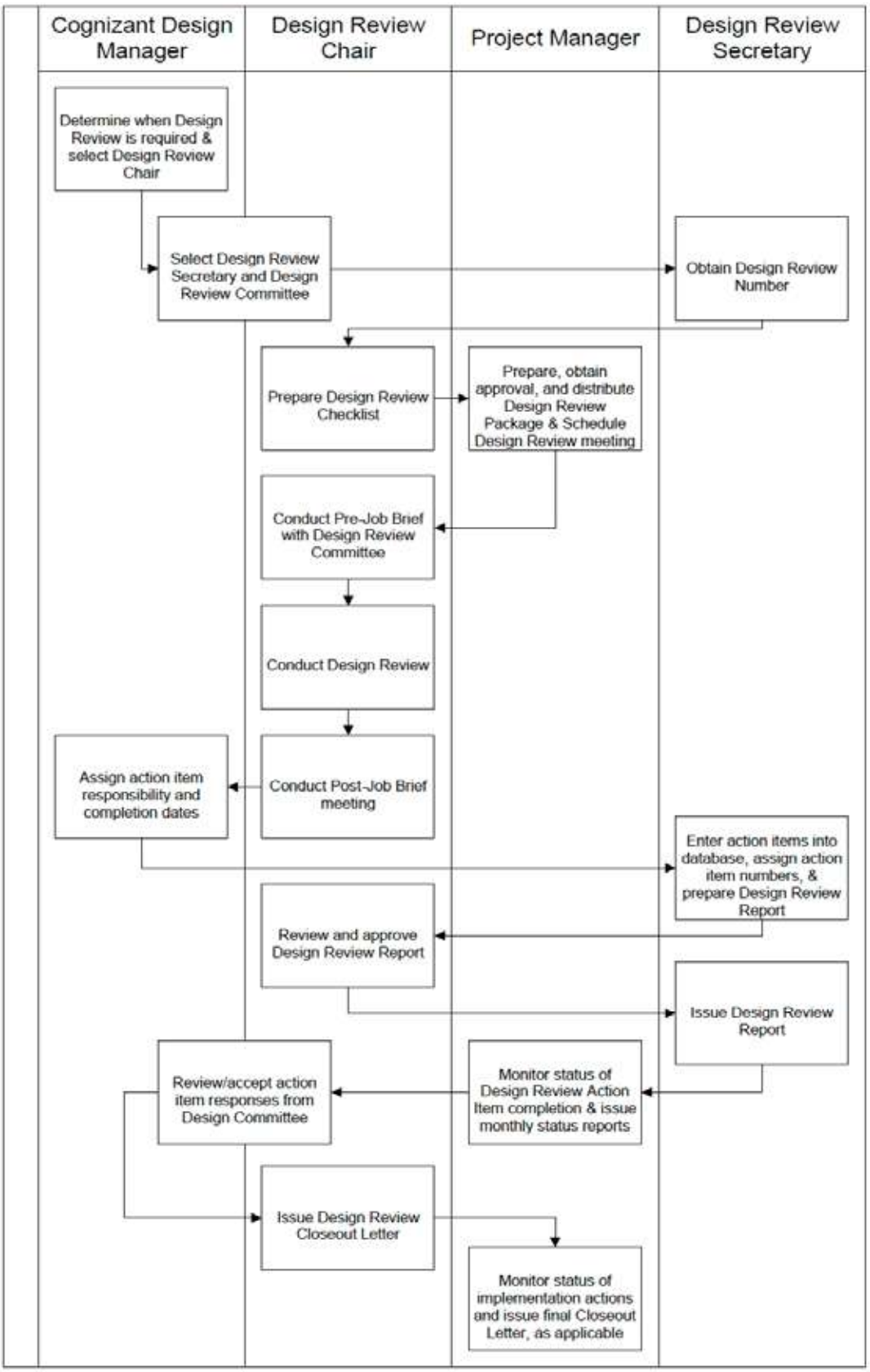


Figure 7-2. Design Review Process

Level 1	Level 2	Level 3
		Construction facilities shall be subject to production readiness inspection. This shall include assessment of facilities, processes and any hazards that the facilities present to the AP1000 plant.
		Information provided for construction shall have been subject to review.
	Construction process inputs are defined and controlled	All construction processes, including storage, handling, and manufacture shall be compatible with the achievement of design intent.
		There shall be a process in place whereby the construction team can query the design.
		Construction procedures shall be subject to an appropriate level of review and approval. This shall involve adequate arrangements for suitable training and audit of training records.
		Adequate review point arrangements shall be in place, based on the stages of construction, to gain the necessary assurance of construction quality.
The AP 1000 plant is constructed in accordance with the design intent.	Construction process is carried out in a controlled manner	It is required that defence in depth is applied to the construction assurance in a manner that is proportional to safety significance. This will involve, where appropriate, separation of ensurance and assurance functions.
		Quality oversight of construction is required.
		Construction plant and facilities shall be maintained and inspected such that they are fit for purpose in the construction of the AP1000.
		At all stages of construction the AP1000 shall be maintained in accordance with design intent.
	Construction process produces adequate evidence of design intent achievement	There shall be adequate evidence of design intent achievement for construction. This shall include required procedures, processes, process records, inspection and audit records.
	Construction non conformity of output with input is controlled	It is required that processes are in place for either concession or non conforming construction product.

Figure 7-3. Construction Objectives

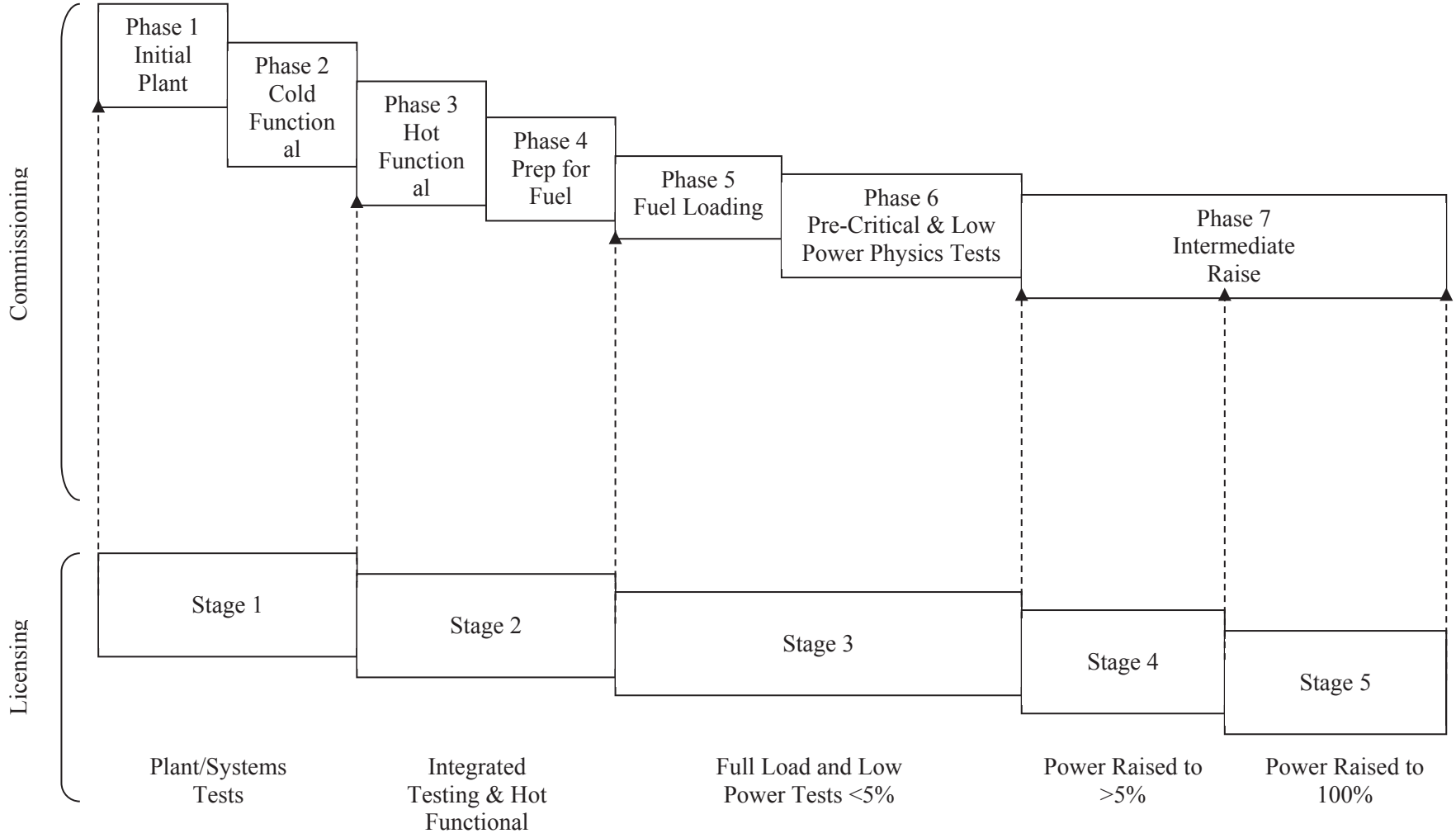


Figure 7-4. Typical Pressurised Water Reactor High-Level Commissioning Programme

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS, ACRONYMS, AND TRADEMARKS

ac	alternating current
ADS	automatic depressurisation system
ALARP	as low as reasonably practicable
AOV	air-operated valve
ASME	American Society of Mechanical Engineers
ANSI	American National Standards Institute
ATWT	anticipated transient without trip
BDB	beyond design basis
BSL	basic safety level
BSO	basic safety objective
C&I	control and instrumentation
CCF	common-cause failure
CCS	component cooling water system
CDF	core damage frequency
CI	containment isolation
CLP	cask loading pit
CMT	core makeup tank
CVS	chemical and volume control system
CWP	cask washdown pit
ΔT	temperature change
DAS	diverse actuation system
DB	design basis
DBA	design basis accident
Dc	direct current
DG	diesel generator
DNB	departure from nucleate boiling
DNBR	departure from nucleate boiling ratio
DRP	design reference point
DVI	direct vessel injection
DWS	demineralised water transfer and storage system
EMI	electromagnetic interference
EMIT	examination, maintenance, inspection, and testing
ESF	engineered safety feature
ET	event tree
FPS	fire protection system
FTC	fuel transfer canal
GNS	general non-safety
HEPA	high-efficiency particulate air
HF	human factors
HFLC	high-frequency, low-consequence
HP	health physics
HVAC	heating, ventilation, and air conditioning
HX	heat exchanger
IAEA	International Atomic Energy Agency
ID	identification
IDS	Class 1E dc and UPS system
IE	initiating event
IEF	initiating event frequency
ILW	intermediate-level waste
INPO	Institute of Nuclear Power Operations

LIST OF ABBREVIATIONS, ACRONYMS, AND TRADEMARKS (cont.)

IRR	Ionising Radiations Regulations
IRWST	in-containment refuelling water storage tank
K_{eff}	effective multiplication factor
LBLOCA	large-break loss-of-coolant accident
LLW	low-level waste
LOCA	loss-of-coolant accident
LP	low pressure
LRF	large release frequency
MBLOCA	medium-break loss-of-coolant accident
MCR	main control room
MFIV	main feedwater isolation valve
MG	motor-generator
MOV	motor-operated valve
MPC	multipurpose canister
MSIV	main steam isolation valve
NUREG/CR	Nuclear Regulatory Commission technical report designation/contractor report
PCCAWST	passive containment cooling ancillary water storage tank
PCCWST	passive containment system water storage tank
PCS	passive containment cooling system
PCSR	Pre-Construction Safety Report
PMS	protection and safety monitoring system
POCO	post operation clear out
PRHR	passive residual heat removal
PSA	probabilistic safety assessment
PWR	pressurised water reactor
PZR	pressuriser
RCCA	rod cluster control assembly
RCP	reactor coolant pump
RCS	reactor coolant system
RNS	normal residual heat removal system
SAP	safety assessment principle
SBLOCA	small-break loss-of-coolant accident
SFP	spent fuel pool
SFS	spent fuel pool cooling system
SG	steam generator
SGT	steam generator tube
SGTR	steam generator tube rupture
SSC	system, structure, or component
T_{avg}	average temperature
Tech Spec	technical specification
VFS	containment air filtration system
VWS	chilled water system
WGS	gaseous radwaste system
WSS	solid radwaste system
UK	United Kingdom
UPS	uninterruptible power supply
US	United States

8 FAULT AND ACCIDENT ANALYSIS

8.1 Introduction

Volume 3 of the Pre-Construction Safety Report (PCSR) presents the faults and accident assessment for the AP1000 design. This volume of the AP1000 design safety case aims to demonstrate that the AP1000 design and operation are tolerant to faults; that United Kingdom (UK) safety targets are met; and that the risks from AP1000 plant operation to the public, workforce, and environment are as low as reasonably practicable (ALARP). The safety case developed in these chapters is based on the demonstration that provision of Category A safety functions is sufficient to meet regulatory targets and ALARP requirements for at least the first 72 hours following any abnormal event and Category B safety functions post 72 hours.

The purpose of this chapter is to provide an overview of the faults, their class, and the key safety features credited in mitigating the faults. References are made to the accident analysis methodology and results that are presented in the following chapters of the PCSR. It is recognised that fault and accident studies underpin the entire safety case, and the methodology presented here is consistent with UK safety assessment principles (SAPs) (Reference 8.1) and best practices.

This chapter describes the fault and accident analysis process, which is based on the design reference point (DRP) defined in Reference 8.3 and expanded upon in Chapter 9 and the systems, structures, or components (SSCs) described in Chapter 6. Chapter 8 describes the methodology for fault and hazard identification. The information collected is used as input to the design basis assessment (Chapter 9), probabilistic safety assessment (PSA) (Chapter 10), internal and external hazards assessments (Chapters 11 and 12), human factors assessment (Chapter 13), and the overall ALARP assessment (Chapter 14). Engineering substantiation is given in Volume 4.

The chapter describes the identification of faults and hazards and groups them according to their evaluation in other Chapters (9 to 13). The complete fault list is given in Appendix 8A.

Chapters 9 through 13 demonstrate that the appropriate safety criteria are met and that the AP1000 design meets the regulatory targets and is ALARP. Chapter 14 of this PCSR brings together the results of Chapters 9 to 13 of this volume and demonstrates that the AP1000 design is robust with respect to all types of faults.

8.2 Overview of Fault and Accident Analysis Methodology

The methodology used in this PCSR is based on UK best practices. An overview is given in Figure 8-1. The application of the methodology ensures that the targets given in the UK SAPs (Reference 8.1) are accommodated in the design.

The elements of the methodology are summarised in the remainder of this section and shown in Figure 8-1.

8.2.1 Reference Design

The safety case begins with the definition of a reference design. For this PCSR, the reference design is contained in the PCSR, as described in the Design Reference Point document (Reference 8.3). The reference design also includes a definition of normal operations. The reference design is described in Chapter 6 of this PCSR. As part of the AP1000 design development and licensing process, a number of design alternatives have been incorporated.

This process and the design changes considered and/or made as alternatives are discussed within the ALARP assessment in Section 14.6.

The reference design documentation also includes Technical Specifications (Tech Specs) that define design limits and conditions on plant operations. These limits and conditions are inputs to the fault analysis and may also be informed by the analysis. See Section 5.6.

As described in Chapter 2, the PCSR is included in the configuration management process for the AP1000 design so that the effects of any subsequent design changes on the safety case will be assessed (see Figure 8-1).

8.2.2 Systematic Fault and Hazard Identification

The next stage of the process is a systematic, auditable, and comprehensive identification of faults. This includes internally initiated faults, internal hazards, external hazards, and human errors. It also includes all modes of normal operation of the reactor and radioactive inventories in other areas (the spent fuel in the auxiliary building and waste routes, in particular). These faults are listed in the fault schedule given in Appendix 8A and in Reference 8.4.

Some of the faults include minor variations that do not impact the SSCs used to mitigate them or their classification. In addition, there are faults that are different enough in their mitigating SSCs, event classification, or consequences that they need to be listed as separate faults.

The identification process is described in Section 8.3.1 for internally initiated faults, and Sections 8.3.2 and 8.3.3 for internal and external hazards. The identification of human errors is described in Chapter 13.

8.2.3 Design Basis Assessment

Once the faults have been identified, each is allocated to a design basis (DB) class. This allocation depends on the initiating event frequency (IEF) of the fault.

The DB classes are derived from SAP Target 4 and from the frequency limits given in the SAPs for DB faults and frequent faults (Reference 8.1) with some additional interpretations. The resulting mitigated consequences are required to be below the dose targets associated with the DB classes, as follows:

DB1 – Infrequent DB faults with an initiating event frequency between 10^{-3}/yr and 10^{-5}/yr. Consequences are limited to:

- Public dose < 10 mSv or worker dose < 200 mSv for events between 10^{-3} and 10^{-4} /yr
- Public dose < 100 mSv or worker dose < 500 mSv for events between 10^{-4} and 10^{-5} /yr

DB2 – Frequent DB faults with an initiating event frequency >10^{-3}/yr. Consequences are limited to public dose < 1 mSv or worker dose < 20 mSv.

DBL – Low probability design basis faults with an IEF between 10^{-5} and 10^{-6}/yr with consequences limited to public dose < 200 mSv or worker dose < 1000 mSv.

BDB – Beyond design basis (BDB) faults with an IEF <10^{-6}/yr, e.g., below the frequency for DBL faults. The consequences would be higher than for DBL events.

HFLC – High-frequency, low-consequence (HFLC) faults with IE frequencies $>10^{-3}$/yr with consequence limits between DB limits and normal operating limits.

DB0 – All other faults; no radiological consequences expected.

The HFLC class is formally outside the DB but it is UK best practice to consider it, since it covers frequent faults with consequences above those associated with normal operations.

The DB class, together with the categorisation and classification scheme given in Section 5.2 of this PCSR, normally defines the requirements for safety measures as follows:

DB2 – Two diverse mitigation capabilities are required for each Category A safety function. At least one capability must be Class 1. The other may be Class 2. Analysis of the plant with consideration for a common cause failure may be performed with less conservative methods and/or inputs and may apply relaxed acceptance criteria.

DB1 – One Class 1 mitigation capability is required for each Category A safety function.

DBL – One Class 1 mitigation capability is required for each Category A safety function. Analysis of the plant may be performed with less conservative methods and/or inputs and may apply relaxed acceptance criteria.

HFLC – No formal requirement, but best practice is to identify one Class 2 system for each Category B safety function.

BDB – No formal requirement except for demonstrating event considerations are ALARP.

DB0 – No formal requirement except for demonstrating event considerations are ALARP.

The AP1000 plant has been designed with consideration for the effects of fluid system pressure part failure. As such, supplemental design requirements have been applied to piping systems where improved reliability (reduction in the associated IEF) are beneficial to plant safety; worker and public radiation exposure; and plant examination, maintenance, inspection, and testing (EMIT) obligations. Refer to Section 11.4 for additional discussion of these supplemental design requirements.

The AP1000 plant has applied these supplemental requirements, combined with additional measures, to significantly reduce the probability of pressure part failures in risk important piping systems. These measures include:

- Reduced piping stresses, more restrictive than American Society of Mechanical Engineers (ASME) requirements
- Increased understanding of material stress-strain behaviour (mechanistic applications only)
- Improved piping pre-service and in-service inspections
- Reduced length of piping through the use of passive safety systems, sealless reactor coolant pumps (RCPs) and other plant simplifications
- Reduced number of welds through the use of bent piping instead of elbows

- Use of improved piping and weld materials based on industry operating experience to reduce chance of corrosion mechanisms (e.g., erosion-corrosion, galvanic corrosion, stress-cracking corrosion)
- Arrangement of piping systems to avoid thermal stripping
- Design of piping systems to avoid significant dynamic effects
- Improved sensitivity and reliability of leak detection capabilities

The result of the application of these design requirements and characteristics is a significant reduction in the likelihood of pressure part failure. Based on this reduction, such events are classified as low probability design basis events (DBL Class events). This is a reasonable approach as both the mechanistic and deterministic principles apply requirements to the design, fabrication, construction, operation, and EMIT functions for the full extent of plant life.

Because of the low probability of DBL faults, the analysis of such faults can have reduced margins (although still conservative) and the consequences can be greater (i.e., higher dose limits), compared with what is used for more probable design basis events (DB1, DB2).

For internally initiated faults (faults originating within the reactor, safety systems, or balance of plant) the DB analysis consists of a deterministic assessment of the initiating fault and the corresponding safety measures (i.e., SSCs) provided by the design. Transient or other calculations using conservative initial conditions, assumptions, and methods demonstrate that the consequences of the DB faults are below the limits listed at the beginning of this section for the corresponding DB class. Conservative assumptions include the assumption of failure of all non-claimed systems and a single failure, as well as conservative initial conditions. In addition, for frequent faults (DB2 class), a single common cause failure is assumed instead of a single failure. Generally only limited DB analysis is undertaken for HFLC events and none for DB0 or BDB events, although they are all considered in the PSA.

The DB analysis may depend explicitly or implicitly on a number of limits and conditions. Generally for the AP1000 plant, the limits and conditions do not allow for Class 1 SSCs to be removed from service for planned maintenance when the reactor is at power or at hot standby conditions, such that SSC unavailability due to maintenance need not be considered. During shutdown, the same situation is true for SSCs required to be operable; however, as the plant is brought to lower operating Modes, some SSCs are permitted to be removed from service for planned maintenance and inservice testing / inspection. These limits and conditions fall into three main groups: limits and conditions that identify the initial conditions for transient analysis, limits and conditions that are assumed for the operation of SSCs important for safety, and limits and conditions imposed by the analysis to limit effective doses either to the public or to the workforce. The limits and conditions that are assumed for the operation of SSCs include such things as water inventory, water temperature, or boron concentration. They also include the availability of SSCs such as valves. These limits and conditions are listed as being important to the safety case. Most will be associated with Tech Specs applied to Class 1 SSCs or with short-term availability controls applied to Class 2 SSCs; some may be candidates for operating rules or to have operating rules associated with them (see Chapter 5). The link between the DB analysis and the Tech Specs is shown in Figure 8-1.

The SSCs identified in the DB assessment and their safety classifications are listed in Appendix 15A “engineering schedule”. The role of each SSC in the DB assessment leads to its classification as described in Chapter 5.

In addition to the above, any operator actions identified in the assessment are also listed. These operator actions fall into two groups: those required to actuate or realign SSCs as part of the response to the fault, and those identified to reduce operator dose such as the requirement to evacuate on the activation of a gamma alarm. Such operator actions are classified in a similar manner to SSCs, as described in Chapter 5 and are consolidated in Chapter 13.

The DB assessment of internally initiated faults is provided in Chapter 9.

8.2.4 Design Basis Assessment of Internal and External Hazards

For internal hazards, the DB1 hazards are the most severe accidents within the normal design basis of the plant that could occur on site, taking such things as fire loading or water inventories into account. An SSC not designed or evaluated to survive a DB hazard is assumed to fail and then it is demonstrated that there are sufficient remaining SSCs to provide all Category A safety functions. Demonstration of the capability of achieving safe shutdown is required following a hazard that directly causes a plant trip or that disables SSCs that are required to be operable by Technical Specifications that require the plant to shutdown if the SSCs are in-operable beyond the specified time period. Failure of an SSC as a result of an internal hazard initiating event where the hazard does not also initiate a reactor fault would simply require the reactor to be manually shut down using the duty systems.

Required diverse mitigation of frequent internal hazards varies based on the initiating hazard. Section 4.0 of Table 8A-2 provides only a primary mitigation capability for most hazard faults, as most of the faults with a "frequent" intensity level would not be onerous enough to induce a reactor trip or controlled shutdown. If they would require such mitigation, they are assumed to already be tagged to the appropriate frequent faults via the individual hazard schedules presented in Chapter 11. Internal frequent fires pose the most onerous impact to diverse mitigation, and as such are discussed in detail in Section 8.2.4.1. In nearly all cases, diverse actuation of passive Class 1 SSCs is available via Class 2 Control & Instrumentation (C&I) diverse actuation system (DAS). All other internal hazard categories are briefly covered in the list below.

- Pressure Part Failure events are categorised based on their likelihood of pipe gross failure, and as such, frequent fault events are already captured within the line break scenarios presented in Sections 1-3 of Table 8A-2. For example, fault 1.4.2, a small break loss-of-coolant accident (LOCA) 2" or smaller is considered a cliff edge frequent fault, and is analysed as such.

- Internal frequent flooding events either identify frequent fault pressure part failure scenarios, or a generic internal flooding scenario that would not compromise the ability of DAS to provide diverse mitigation.

- Internal explosions are generally limited to compartments, and as such, frequent fault internal explosions are already bounded by frequent internal fire events; however, explosions are not postulated at locations that could compromise DAS. Therefore, diverse mitigation of DAS for a reactor trip is possible for all scenarios.

- Dropped load events are evaluated similarly to pressure part failure events, where bounding line break faults are identified and diversity is demonstrated as applicable. For a "frequent" dropped load event, the size of the dropped load, the impact zone of influence, and the mitigation capability of the structures and interacting components can be given more credit such that there is no frequent fault dropped load event that

would be expected to compromise the ability of DAS to provide diverse mitigation to a generic reactor trip event.

- Biological agent frequent faults would not pose any unique impact compared to a more onerous infrequent fault event. This fault would not compromise the DAS automatic functionality, and as such, diverse mitiation is available.

- Onsite transport frequent faults can only occur at specific locations on the grounds of the plant. Based on the separate locations of the primary DAS panel in the main control room and the redundant location in the security room, there is no infrequent limiting event, let alone frequent event, that could damage both locations and preclude diverse mitigation of SSCs.

- A release of toxic, corrosive, or flammable material frequent fault is already covered by one of the other internal hazard events (e.g., biological agent, internal fire, or onsite transport), as the consequences would be the same.

- Electromagnetic interference frequent faults are not considered to have any additional compromise to diverse mitigation equipment due to the electromagnetic interference requirements for the diverse C&I system (DAS); See Chapter 19.

The DB analysis for internal hazards is given in Chapter 11.

For external hazards, DB1 hazards are those with an IE frequency $>10^{-4}$/yr. Any SSC not specifically designed to survive a DB hazard is assumed to fail. The DB analysis consists of demonstrating that sufficient SSCs are available to provide all Category A safety functions after the event. In some cases, more frequent, less severe DB hazards are also listed (DB2). For these frequent internal hazard faults, two diverse mitigation capabilities are required as is discussed for internal events in Section 8.2.3.

Finally, in some cases there is a risk that the maximum DB1 hazard may be exceeded. For these DBL external hazards, analyses and/or evaluations are performed to demonstrate that there is a reasonable likelihood that sufficient SSCs will be available to mitigate the event. For these DBL hazards, the analysis may be performed with relaxed acceptance criteria and with less conservative methods/inputs.

The DB analysis for external hazards is given in Chapter 12.

8.2.4.1 Internal Fire

The initiation of an internal fire is considered a frequent fault. In accordance with Section 8.2.3, two diverse mitigation capabilities should be provided. Note that an internal fire fault is similar to a frequent intact circuit fault with respect to the SSCs that are credited to provide both primary and diverse mitigation. All of the credited SSCs are Class 1 except for the DAS C&I. All of the Class 1 SSCs have fire separation, and as a result can still meet their safety functions after a fire. Also, all of the mechanical SSCs that provide the primary mitigation of an intact circuit fault are fail safe, which reduces the probability of being disabled by a fire. As a result, for an internal fire plus a common cause failure (CCF), the AP1000 design would generally provide diverse Class 1 mitigation.

However, there is a limited exception to the AP1000 diverse capability for fires; that is a specific fire could completely disable the DAS since it is a Class 2 system and does not have

fire separation. This exception is considered acceptable because of the following AP1000 design features:

- DAS is a small system with only a few sensors, cables and cabinets. As a result the probability of a fire that might disable DAS is low since there are a limited number of challenging fire initiation locations.

- Fire induced hot shorts causing spurious automatic depressurisation system (ADS) component actuations are considered beyond design basis events; such a fire needs to start in a DAS cabinet, propagate to second DAS cabinet, cause spurious signals in at least two specific controllers before operators respond to fire alarms and de-energize DAS.

- Spurious plant trip caused by fire in DAS actuation cabinets that might cause a spurious reactor trip is considered an infrequent fault; such a fire needs to start and propagate to short wires or to cause processors to malfunction and cause spurious signals. DAS is an energize-to-actuate design that requires two spurious signals to generate an automatic actuation.

- A fire could disable DAS without causing spurious reactor trip; such a fire is considered a frequent fault (DB2). The availability controls on DAS do not require plant to be shutdown if DAS is unavailable. Therefore in case a fire disabled DAS, the plant should be assumed to continue to operate and would not have to transition to safe shutdown.

Furthermore, the PSA shows that the AP1000 design has a low core damage frequency for internal fire initiators. The PSA considers the potential for fires to propagate beyond the fire area of inception and thus affect more than one division of Class 1 SSCs delivering a Category A safety function, coincident with failures in the unaffected SSCs. The assessment shows that, under such conditions, the core damage frequency is below the Target 8 BSO.

Based on this discussion, Fault 4.1.1 of Table 8A-2 lists fires as frequent faults, and provides diverse mitigation capabilities; however, it notes that the diverse cases do not apply to fires located at limited locations that could disable DAS.

8.2.5 Human Factors

Human factors play a significant role in fault analysis. Since the methodology for human error analysis is specific for that purpose, operator actions or errors identified in the fault analysis elsewhere are considered in Chapter 13 along with specific human error identification and assessment.

In the DB assessments, any operator action identified as necessary for the provision of a Category A safety function (or the provision of a Category B safety function in some cases) is identified. Failure of the operators to perform these actions is then assessed in Chapter 13.

8.2.6 Probabilistic Safety Assessment

The PSA for the AP1000 design is discussed in Chapter 10. The PSA consists of a complete Level 1 and Level 2 PSA and an indicative Level 3 PSA for internally initiated faults with a discussion of seismic margins. The existing PSA addresses internal hazards, including fire and internal floods, in a simplified manner.

The Level 1 PSA uses best-estimate assumptions to consider the DB initiating events as well as other initiating events. It also considers combinations of failures of SSCs based on their probabilities. The SSCs credited in the PSA include those identified in the DB analysis as principal and defence in depth means of providing Category A safety functions for the reactor. Additional SSCs beyond these are also credited. These combinations of failures are represented as a series of event trees (ETs) with "nodes" corresponding to the failure of a particular SSC. The probability of failure of each of these systems is justified in Chapters 17, 18, and 19 of this PCSR. The end points of the Level 1 PSA fall into two groups: those that do not result in damage to the core, and those that result in core damage states. One of the major outputs of the study is the core damage frequency (CDF). Another major output is the relative importance of different SSCs. The Level 1 PSA is used in the fault and accident analysis to assess the adequacy of the reliability claims made for the SSCs identified in the DB analysis.

The SAPs (Reference 8.1) give targets for the individual risk of death of 10^{-4}/yr basic safety level (BSL) and 10^{-6}/yr basic safety objective (BSO) in Targets 5 and 7 for workers and members of the public, respectively. Individual risk of death cannot be directly obtained from the PSA.

An overview of the PSA is shown in Figure 8-2.

8.2.7 Severe Accident Assessment

Severe accidents are defined as fault sequences that lead to major core damage and containment releases (exceeding the DB dose levels given in Target 4) resulting from an initiating event and a sequence of failures of mitigating measures (including principal and defence in depth features). The analysis of severe accidents for the AP1000 plant is part of the Level 2 and 3 PSA in this PCSR and is presented in Chapter 10.

The Level 2 PSA takes each of the core damage states from the Level 1 PSA and performs a best-estimate analysis of these severe accident sequences to follow the progression of the core damage. The analysis uses best-estimate techniques to assess the contribution of various severe accident phenomena to failure of the containment function to assess the possible characteristics of any release of radioactivity. The following phenomena are assessed:

- Core heatup, melting, and relocation
- In-core zirconium-water reaction
- In-vessel retention of molten core debris in the lower plenum
- Fission product release and transport and offsite doses
- In-vessel steam explosion
- High pressure core melt phenomena
- Ex-vessel steam explosion
- Molten core concrete interaction
- Long-term containment pressurisation with failure of passive containment cooling system (PCS) cooling and alternative sources of water cooling

- Hydrogen combustion
- Equipment survivability

The possible releases from core damage events are grouped into different damage states based on:

- the size of the release from the core/RCS,
- the radioactive inventory in the containment,
- the height/energy/rate and magnitude of the release from the containment,
- the timing of the release.

The sum of the frequencies of all these major releases is the large release frequency (LRF). The use of this severe accident assessment to identify risk-reduction measures is described in Section 14.6.3.

The source terms coming from the Level 2 PSA are further analysed in the indicative Level 3 PSA, which considers pathways back to the human population surrounding the site and emergency counter-measures to estimate societal risk. The Level 3 PSA is only indicative, since a full Level 3 PSA can only be done once a specific site is in view, since population densities, prevailing weather, probabilistic weather variations, and planned emergency countermeasures are all site specific. A more detailed Level 3 PSA would form part of a site-specific PCSR. In the absence of a detailed Level 3 PSA, the LRF is used as a surrogate for the risk of 100 deaths or more in the comparison with the societal risk target in SAP Target 9.

An overview of the PSA is shown in Figure 8-2.

8.2.8 Assessment that Risks are As Low As Reasonably Practicable

The DB assessment and PSA provide insights for use in the design of the safety measures used to provide the Category A safety functions (Category B for HFLC events) to meet DB and probabilistic targets.

It is an additional requirement in the UK that the risks from faults to the public, workforce, and environment should be ALARP. As part of the assessment of each fault, an assessment is made of other measures that might be claimed to decrease the risk from the fault. Whether or not these measures are claimed is based on whether to do so would be ALARP.

Chapter 14 provides a summary of the full ALARP assessment for the AP1000 plant. Each chapter in volume 3 (9 – 13) provides specific ALARP assessments for individual faults.

8.2.9 Engineering Substantiation

Appendix 15A “Engineering Schedule” provides a detailed picture of the requirements placed on engineered systems to provide safety functions during fault and accident conditions.

The safety case is dependent upon these engineered systems meeting their designated requirements. Engineering substantiation provides the evidence that each system can meet these requirements (with a suitable level of confidence) and provides details of the maintenance and testing regime that is required to ensure that they remain able to do so

throughout the life of the plant. The evidence and maintenance and testing requirements are added to the engineering schedule shown in Figure 8-1.

Engineering substantiation is discussed in Volume 4.

8.3 Fault and Hazard Identification

Fault and hazard identification, together with the corresponding fault schedule, form an important part of the safety assessment, as they are the basis of demonstrating the tolerance of the design to faults and hazards.

The main requirement for fault and hazard identification is that it should be systematic, auditable, and comprehensive. In particular, the fault and hazard identification must cover all normal operating conditions and all inventories of radioactivity, whether they are in the reactor, fuel route, waste routes or other parts of the plant.

Faults and hazards fall into one of the following types:

- Internally initiated faults
- Internal hazards
- External hazards
- Human errors

The methodology for identifying all of the faults and hazards in these groups is slightly different, and the methodology adopted in this PCSR is described below for each group. These faults are listed in the fault schedule given in Appendix 8A which also includes other data arising from subsequent stages of the process.

8.3.1 Internally Initiated Faults

The approach to fault identification is to start with the faults identified in the standard AP1000 design. This has been supplemented by separate systematic studies to demonstrate completeness of the AP1000 standard design for reactor faults and to include faults in systems and operations outside the reactor.

In the first instance, internally initiated faults have been identified by application of the checklist of categorised initiating faults specified in American National Standards Institute (ANSI) N18.2 (Reference 8.7). This document presents a checklist of categorised hazards that have been drawn from assessment of United States (US) nuclear plant SSC failure Modes and from many years of operating experience.

The application of the ANSI N18.2 checklist has been reviewed against the AP1000 design and PSA and has been appropriately updated to reflect the plant-specific design features. In particular, the fault list was augmented by design-specific faults, such as spurious actuation of the passive residual heat removal (PRHR) system.

This identification of initiating faults is also supported by a review of operating experience documented in Nuclear Regulatory Commission technical report designation/contractor report (NUREG/CR)-2300 (Reference 8.8, Section 5-4.1) and NUREG/CR-5750 (Reference 8.9), as well as the Institute of Nuclear Power Operations (INPO) and Westinghouse databases. A more recent review using NUREG/CR-6928 (Reference 8.6) has identified no additional hazards that need to be addressed.

The application of the ANSI N18.2 checklist has also been reviewed against relevant good practice in hazard identification. As a result of this, bounding initiating faults relating to shutdown states are identified, as are bounding initiating faults relating to spent fuel handling and storage.

It is recognised, however, that the above approach is not completely systematic and therefore does not fully meet UK requirements for fault identification. Further, the ANSI N18.2 checklist only considers single events as initiators of a fault sequence and does not consider combinations of events that might contribute at a frequency greater than 10^{-5}/yr.

The ANSI N18.2 checklist does not include faults or hazards in parts of the plant other than the reactor itself. There is a need to identify faults and hazards as they may apply to the fuel route, waste routes, and any other part of the plant where there are inventories of radioactive material.

The ANSI N18.2 checklist does include anticipated transient without trip (ATWT) faults. If these are considered as initiating events, their frequency puts them outside the DB for the AP1000 design, and therefore they would not be considered. However, it is UK practice to consider potential ATWT events for all frequent fault initiating events or transients followed by a common cause failure in a principal safety function. On this basis, ATWT events are not identified as initiating events but are included as part of the assessment of frequent faults.

A top-down assessment was undertaken to demonstrate that the list of faults and hazards for the reactor is comprehensive and to provide a list of faults for systems outside the reactor. This top-down assessment relied on the observation that all initiating events correspond to the loss or degradation of one of the following principle safety functions:

- Control of nuclear criticality
- Removal of heat from nuclear fuel
- Confinement (containment) of radioactive material
- Shielding of personnel from direct radiation

Each of these safety functions was applied in turn to the primary and secondary side of the reactor, to all parts of the fuel route, to the radwaste routes, and to any other part of the plant where there is radioactive material. In each case, all normal operating conditions were reviewed.

The application of this methodology did not reveal any significant omissions from the list of reactor faults already identified but did supplement the list with faults in areas other than the reactor.

8.3.2 Internal Hazards

Internal hazards are those hazards to plant and structures that originate within the site boundary but that are external to the nuclear or active systems. The licensee has control over the initiating events to some extent.

The internal hazards identified in Chapter 11 are as follows:

- Fire
- Internal flooding
- Pressure part failure, including:
  - Water spray

  - Jets
  - Steam leakage
  - Pipe whip effects
- Explosions
- Missiles
- Releases of toxic, corrosive and flammable material
- Collapsing, falling or mishandling loads
- Biological agents
- Onsite transport accidents
- Electromagnetic interference (EMI)

Combinations of the hazards and the potential for consequential failures are assessed in Chapter 11 of this PCSR.

8.3.3 External Hazards

External hazards are those hazards to a site and facilities that originate externally to both the site and its processes, i.e., the licensee may have very little or no control over the initiating event. External hazards fall into two main groups: naturally occurring events such as extreme weather or earthquakes, and man-made events such as explosions or aircraft crash. The identification and analysis of external hazards is given in Chapter 12.

Through structured technical review, the following list of external hazards has been identified as applicable for assessment:

- Seismic events
- External flooding
- Aircraft impact
- External explosions
- Extreme temperature
- Drought
- Extreme wind
- External fire
- External missiles
- Biological fouling
- EMI and lightning

8.3.4 Human Errors

The AP1000 design is designed to minimise the impact that operator errors can have on plant safety. However, three types of human errors are identified and classified consistent with those defined in the International Atomic Energy Agency (IAEA) guidance, “Human Reliability Analysis in Probabilistic Safety Assessment for Nuclear Power Plants: A Safety Practice” (Reference 8.2).

- **Type A** – Unrevealed maintenance errors that might compromise the performance of a safety system when it is demanded.

- **Type B** – Maintenance or operator errors that could cause an initiating fault.

- **Type C** – Operator errors that affect the course of an accident in a detrimental way.

A systematic study has been undertaken to identify all such errors that might have a significant effect on the safety of the AP1000 design. A number of initiating faults identified as internally initiated faults have a contribution from Type B errors. Similarly, the progression of a number of internally initiated faults may be affected by Type C errors. These are covered further in Chapter 13.

Human error contributions to internally initiated faults (Type B errors) are included in the relevant fault in the fault list in Appendix 8A. Where operator actions are required in the DB analysis, they are identified and the failure of operators to properly execute them is included in the list of Type C errors addressed in Chapter 13.

The identification of human errors and the screening and assessment of these errors is summarised in Chapter 13 of this PCSR.

8.4 Fault Schedule

The faults and hazards identified by the various processes described above are listed in the fault schedule given in Table 8A-2. However, there are numerous individual faults, and many of them are similar to one another. The usual practice is to group variations of similar faults so that the results of any variation of a given fault describe the limiting consequences. Each fault identified has a limiting transient analysed in the DB assessment. The radiological consequences presented are meant to bound the most limiting case for a particular fault.

From the DB point of view, several of the PSA events can be grouped together since the only difference is the point of release, which leads to different consequences but not to differences in the requirements for the provision of safety functions. Alternatively, some PSA events need to be split as the provision of safety functions is different, although, from a PSA point of view, the release points and timescales are the same. Table 8A-2 breaks down the faults for both DB and PSA use.

Table 8A-2 also includes faults for non-power operation conditions (shutdown and refuelling operating conditions). In the PSA, most of these events are assumed to be bounded by the corresponding power operation event where applicable. In some cases, separate calculations are presented. Table 8A-2 also includes faults outside the reactor, which are not included in the PSA.

8.5 References

8.1 "Safety Assessment Principles for Nuclear Facilities," Rev. 0, Office for Nuclear Regulation, 2014.

8.2 IAEA Safety Series No. 50-P-10, "Human Reliability Analysis in Probabilistic Safety Assessment for Nuclear Power Plants: A Safety Practice," International Atomic Energy Agency, January 1996.

8.3 Westinghouse Report UKP-GW-GL-060, Rev. 10, "AP1000 Design Reference Point for UK GDA," January 2017.

8.4 Westinghouse Report UKP-GW-GLR-003, Rev. 2, "AP1000 Fault Schedule for the United Kingdom," January 2017.

8.5 Westinghouse Report UKP-GW-GL-067, Revision 1, "AP1000 Assessment of Diverse Mitigation of Frequent Faults for the UK," December 2011

8.6 NUREG/CR-6928, "Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants," U.S. Nuclear Regulatory Commission, February 2007.

8.7 ANSI N18.2, "Nuclear Safety Criteria for the Design of Stationary Pressurized Water Reactor Plants," American National Standards Institute, August 1973.

8.8 NUREG/CR-2300, "PRA Procedures Guide: A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants," U.S. Nuclear Regulatory Commission, February 2010.

8.9 NUREG/CR-5750, "Rates of Initiating Events at U.S. Nuclear Power Plants: 1987-1995," U.S. Nuclear Regulatory Commission, 1999.

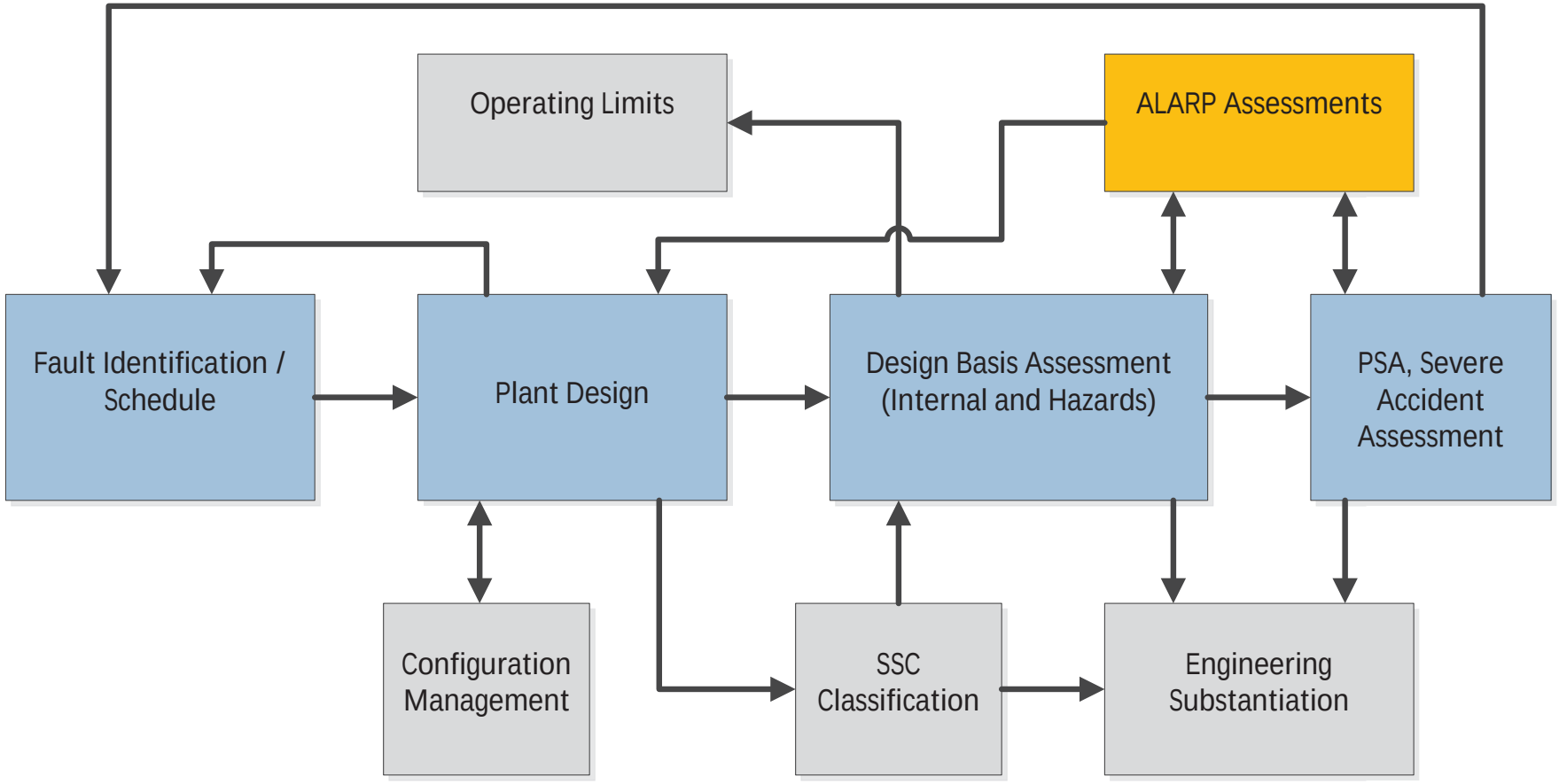


Figure 8-1 Fault and Accident Analysis Overview

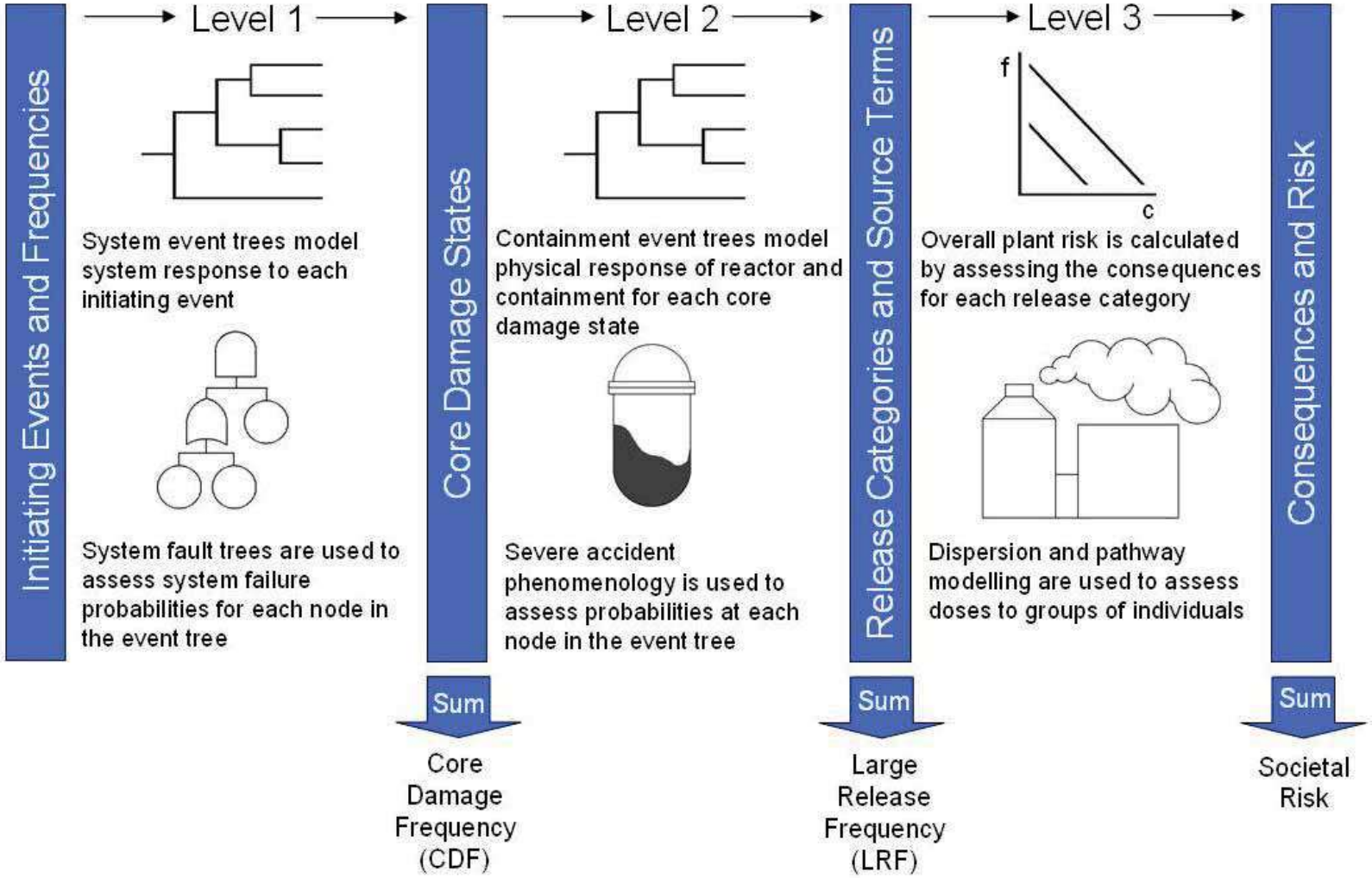


Figure 8-2 Probabilistic Safety Assessment Overview

APPENDIX 8A
FAULT AND ACCIDENT ANALYSIS
AP1000 COMPOSITE FAULT LIST

8A.1 Background

The fault list, presented as Tables 8A-2 and 8A-3 in this appendix, covers the full set of initiating faults that are addressed throughout the safety justification provided within this Pre-Construction Safety Report (PCSR). This fault list is based on a systematic fault identification study, undertaken using the methodology described earlier in this chapter, particularly those associated with reactor operations outside of the reactor coolant system (RCS) boundary.

The fault list for reactor internal faults in Table 8A-2 has been structured in a manner which demonstrates that the list of design basis faults can be reconciled with equivalent faults identified in the probabilistic safety assessment (PSA) and that all the faults identified in the PSA, which fall within the design basis, are covered by the design basis assessment (DBA). To this end, the fault list itself has been prepared by organising and consolidating the faults identified from all document sources under the appropriate initiating event category defined in the PSA. Section 1.0 is titled "Reactor Internal Events," and contains all design basis initiating events that originate at-power (i.e., Modes 1-2), and have a direct consequence on the reactor system. Section 1.0 also evaluates the design basis events initiating at-power for all modes of operation. Section 2.0 "Additional Reactor Internal Faults" contains design basis initiating events that originate only at lower operational power modes, but have direct consequences on the reactor system. Section 3.0 "Non-Reactor Faults" are design basis initiating events that may originate at any time, but do not have direct consequences on the reactor system; rather, they result in radiological consequences due to some malfunction during a maintenance activity or impact the ability of the spent fuel pool (SFP) to provide adequate protection of spent fuel.

Hazard schedules exist as identified in Chapters 11 and 12, and an appropriate linkage to the fault schedule entries in Table 8A-2 are provided therein. If the consequences of a particular internal or external hazard results in an already identified fault, reference is provided to fault IDs within Sections 1-3, and the appropriate mitigation claims are provided in Table 8A-2 in addition to the hazard protection claims provided in the referencing hazard schedule entry. If the hazard fault is not already contained within Sections 1-3, a unique entry is provided in Section 4.0 of Table 8A-2 for internal hazards and in Section 5.0 of Table 8A-2 for external hazards. These sections address all major hazard categories as discussed in Chapters 11 and 12, and provide appropriate linkage to the detailed hazard evaluations presented in those chapters, which cover the safety justification for the plant in the context of these hazards. The approach to demonstrating safety for external and internal hazards is based on justifying the resilience of the essential structures, systems and components to defend against fault sequences initiated by external or internal events. The demonstration of resilience is based on arguments relating to withstand, diversity, and segregation. The PSA also focuses on the impact of internal and external hazards on the availability of safety features in event trees.

Information on the document source(s) for each fault and identification reference(s) used within the source(s) for each fault are documented in Reference 8.4. This allows full traceability of each fault back to its relevant source(s), including the human factors (HF) assessment topic report for those faults which involve HF initiators.

8A.2 Fault Schedule Structure

- Fault Identification (ID) – A discrete identification number is provided for each fault entry. Separate faults may be identified for the same initiating event occurring during different operating mode(s), or in different locations within the plant where unique consequences may result.

- Initiating Event (Fault and Consequences) - A brief description of each initiating fault and the unmitigated consequences of the fault progression are given. The fault consequence column provides a description of the state of the plant following the initiating fault. The information in this column does not provide details of how the fault is mitigated, which is provided in following columns.

- Initiating Event Frequency (IEF) / Design Basis (DB) Class - This column provides the initiating event frequency information for the fault and the event classification (refer to Section 8.2.3). The IEFs are in most cases obtained directly from the PSA (See Chapter 10); however, if generated independently because the discrete fault is not contained in the same manner within the PSA, clarification is given in the "comments" column. General Notes regarding IEFs:

  1. The probabilities used in this table are based on the AP1000 plant PSA (see Chapter 10). These event probabilities are only one of the tools to identify an appropriate accident class for the event. Other factors are considered as discussed in section 8.2.3. In several cases, these IEFs are conservatively high, especially for events that are not a significant contributor to the overall PSA safety metrics (e.g., CDF). In other cases, the probabilities would put events into the beyond design basis class since their IEF is under 1E-06/yr, as discussed in Section 8.2.3. In some cases, these events are included in the design basis as DBL events because of uncertainties in the IEF. An example is a postulated large break loss-of-coolant accident (LBLOCA); as indicated in the fault schedule, this fault has an IEF of ~8E-07 per year, which would lead to it being classified in the BDB class. However, in the AP1000 design fault schedule it is classified as a DBL event and analysed to DBL assumptions, methods and consequences.

  2. Since most of the faults in shutdown mode are significantly less limiting then at power, the PSA does not provide the probability for all of shutdown events[1]. For these analysed in the PSA, associated probabilities will be used in the fault schedule. For the faults in shutdown Modes not defined in the PSA, the following logic is applied when the reactor is shut down; the probability of any event in shutdown Modes is significantly smaller that the conservative probabilities estimated for at power modes. This is due to both the limited time at risk (for all of the shutdown Modes combined [3-6]), and the lower pressure and temperature in these modes. The time at risk is on the order of 5% of the cycle time. For the sake of this fault schedule, probabilities are estimated to be 1/20th of the frequency estimated for at power faults. This is considered extremely conservative, as it does not take credit for the effect of the reduced pressure and temperature conditions. Also, this probability is cumulative to all shutdown Modes combined, and is used herein as bounding.

[1] A more detailed low power and shutdown PSA is expected to be performed during site licensing; at that time, these IEFs would be reassessed.

- Possible Modes Affected - The fifth column indicates the reactor operational Modes where the fault is applicable. The six operational Modes are identified in Table 8A-1 below, and discussed in more detail in Section 6.2. Different Modes of operation may be pertinent to different faults, and as such, the fault list in Table 8A-2 includes faults that are specific to shutdown Modes as a separate group.

- Engineered Safety Functions (ESFs) – This set of columns is intended to provide the claimed protection and/or mitigation functions and the associated actuation systems and signals, as applicable. This section is intended to be in alignment with sections titled "…SSCs credited" for primary DBA and diversity analyses presented throughout Chapter 9. Additional details on the format and content of this section is provided in the "Systems, Structures, or Components" section below.

    - Actuation/Indication Signals – The AP1000 plant C&I logic is designed such that multiple actuation signals could lead to a single ESF actuation. All of the potential ESFs for a DBA analysis and their associated signals are identified in Table 9.0-10. The typical approach in Table 8A-2 is to present the SSCs and actuation/indication signals identified in the limiting design basis analysis referenced in Chapter 9. A C&I system may be identified without a specific signal for manual ESF actuations, which are assumed to occur at a specific conservative point in time rather than immediately after the first indication is provided to the operator or after a number of indications are provided to the operator.

    - Short term reactivity control – This set of columns is intended to identify rapid reactivity control protection, which in almost all cases is provided by the rod breakers or the rod motor-generator (MG) set field breakers. Long term reactivity control is discussed either in the comments section or within the referenced detailed evaluation of the fault. For some faults, additional clarification is provided in the comments column due to a limiting analysis covering both at-power and shutdown conditions although the different operational modes may have different initial positioning of the control rods.

    - Safe Shutdown - Note that the SSCs listed are sufficient to mitigate the faults as well as to bring the plant to a safe shutdown. Refer to Appendix 9C for additional details on the operation of these SSCs as well as their performance capabilities in the long term.

- Comments – Clarifications, nuances, exceptions, and any additional detail not contained within the other columns is included in this column.

- Further Assessment of Fault –The last column in the table serves to provide traceability of the fault to its subsequent assessment description elsewhere in Volume 3 where the fault is discussed in more detail. These references are provided for deterministic and PSA analysis, as applicable. Note that the PSA analysis usually considers a range of similar initiating faults as well as more failures and fewer mitigating SSCs than considered in deterministic analyses.

8A.3 Systems, Structures, or Components

Methodology

The central columns in Table 8A-2 provide information on the front line SSCs that are claimed in order to maintain the engineered safety functions of reactivity control, heat removal, and containment of radioactive material within each fault progression. Each fault may contain one or more of the following:

- White (no shade) rows contain the primary design basis safety case engineered safety functions credited. As discussed in section 8.2.3, the primary mitigation of all faults only credits Class 1 SSCs.

- Grey shaded rows present diverse core cooling engineered safety functions for DB2 frequent faults. As discussed in section 8.2.3, the mitigation of these faults relies mainly on Class 2 C&I actuation of Class 1 passive SSCs. Class 2 mitigation SSCs are also credited on a limited exception basis.

- Blue shaded rows present diverse anticipated transient without trip (ATWT) engineered safety functions for DB2 frequent faults. As discussed in section 8.2.3, the mitigation of these faults relies mainly on Class 2 C&I actuation of Class 1 passive SSCs. Class 2 mitigation SSCs are also credited on a limited exception basis.

Additional discussion is provided below on unique mitigating safety functions, and how they may be presented in the "engineered safety functions" section of Table 8A-2:

- Support SSCs
- Pressure Control
- Containment Cooling
- Containment Isolation

Support SSCs

The AP1000 plant Class 1 SSCs require few support systems to allow them to provide their safety functions. Table 8A-4 lists the front line SSCs listed in Table 8A-2 and their necessary support systems. For example, the Class 1 equipment is supported by the essential electrical supply system (Class 1 direct current (dc) and UPS system [IDS]). The IDS provides reliable power for the Class 1 equipment required for the plant instrumentation, control, monitoring, and other vital functions needed to shut down the plant. In addition, the IDS provides power to the normal and emergency lighting in the main control room (MCR) and at the remote shutdown workstation. The IDS is capable of providing reliable power for the safe shutdown of the plant without the support of battery chargers during a loss of all alternating current (ac) power sources coincident with a design basis accident. The system is designed so that no single failure will result in a condition that will prevent the safe shutdown of the plant.

The front line SSCs listed in the central columns in Table 8A-2 are mostly Class 1 passive SSCs and are capable of providing for at least 72 hours of operation. After this time, a few additional SSCs are required to continue their operation. This long-term support of the passive SSCs can be provided by installed "ancillary" equipment or by offsite SSCs which can be transported to the plant and installed within the 72 hours available. Table 8A-5 lists these SSCs.

Heating, ventilation, and air conditioning (HVAC) SSCs are noted when their operation is necessary to provide cooling to support SSC operation. The HVAC transfers heat to the chilled water system (VWS) for this cooling. Although both the PMS and DAS are supported by an HVAC system during normal plant operation, neither require HVAC cooling post accident. The PMS relies upon passive heat sinks (room walls and ceilings) to limit the temperature rise for the first 72 hours. Afterwards, fans are credited to circulate outside air. The fans can either be the installed ancillary fans powered by the installed ancillary diesel generators (DGs) or they can be fans and DGs from offsite. The DAS has a limited operational time post accident and the temperature rise during that time (without HVAC) is acceptable. The DAS room may contain backup plant security equipment. If this option is used then there would be additional heat input to the room, however in this case the room would be continuously manned and that person would have procedures to take actions to prevent excessive heat rise (open doors, turn off the backup security equipment).

Pressure Control

For all of the faults discussed in Table 8A-2, the primary safety case RCS pressure control is provided by the spring-operated passive pressuriser safety valves or is not applicable (i.e., depressurisation events such LOCAs); as such, it is not listed for any fault. The diverse cases require no pressure relief or valve actuation. The AP1000 plant pressuriser size is large enough that frequent faults do not require the opening of the pressuriser safety valves to prevent over-pressurising the RCS. There are no pressuriser power operated relief valves in the AP1000 design. In addition, normal operations rely on pressuriser (PZR) sprays, turbine bypass system, and rapid power reduction system to control RCS pressure.

Containment Cooling

As indicated above, diversity is required in the safety functions credited in mitigating frequent faults. Table 8A-4 lists the features that provide this diversity. Note that the ultimate heat sink is provided by the PCS for both the primary and diverse cases. This is acceptable because there is no CCF that can cause the PCS to fail to meet its diversity requirements. The following outlines the reasons for this (a more detailed discussion is provided in Appendix A of Reference 8.5):

- The drain of water from the PCS water storage tank is diverse:
  - The water drain from the PCS water storage tank uses three 100 percent capacity paths and the valves that initiate water flow are diverse; there are two air-operated valves (AOVs) and one motor-operated valve (MOV) as shown on Figure 8A-1.
  - The actuation of the PCS valves uses diverse power supplies; the AOVs are self-powered (springs) and the MOV uses Class 1 dc power. The AOVs open on loss of instrument air pressure or loss of power to the air control solenoids.
  - The control of these valves uses diverse C&I systems; all three actuation valves are actuated by both the protection and safety monitoring system (PMS) and the DAS.
- If water fails to drain from the PCS water storage tank, then air-only cooling of the outside of the containment is sufficient for at least 24 hours. During this time the operators will be able to manually align another water supply; both the fire protection system and the demineralised water system (DWS) have installed connections to provide water to the outside of the containment shell. Chapter 10 provides analysis of PCS air-only cooling. Figure 8A-1 shows these alternate water supplies.

- Other postulated failure mechanisms are not credited. These mechanisms include:
  - Blockage of the air flow path. This is not credited because the total area is enormous, the inlets are located in a 360 degree radius at the top of the shield building cylinder and blockage of significant portion of the inlets would not cause the passive cooling process to fail. In addition, even if the inlets were greatly blocked and the air flow path reduced, water drain from the PCS without any air flow would adequately cool the containment.
  - Inadequate heat transfer through the containment shell. Extensive testing has been performed to support the design of the PCS. Three different facilities/scales were used. The PCS performance has been confirmed by independent analysis. In addition, for frequent faults the demands on the PCS heat transfer are less than they are for the limiting DBAs (large-break loss of coolant accident (LOCA) and double-ended guillotine steam line break).

Containment Isolation

Containment isolation (CI) valves form part of the containment pressure boundary and provide a means for fluid penetrations not serving accident consequence limiting systems to be provided with two isolation barriers. These isolation devices are either passive or active (automatic). Manual valves, de-activated automatic valves secured in their closed position (including check valves with flow through the valve secured), blind flanges, and closed systems are considered passive devices. Check valves, or other automatic valves designed to close without operator action following an accident, are considered active devices. Two barriers in series are provided for each penetration so that no single credible failure or malfunction of an active component can result in a loss of isolation or leakage that exceeds limits assumed in the fault studies. One of these barriers may be a closed system. Faults which require CI are indicated by the inclusion of CI as a safety function device.

The primary means of providing CI is by automatic closure Class 1 valves actuated by the Class 1 PMS. This capability applies to both LOCA and non-LOCA faults. These features are single failure tolerant and automatically actuated. The Class 2 DAS provides a diverse capability to actuate the risk important CI valves (Class 1). The risk important CIs include lines that connect to the RCS or the containment atmosphere and are greater than 2.54 cm (1 inch) in diameter.

In addition to diverse actuation of CI valves, diversity is provided for a common cause failure (CCF) of CI valves, where the same design is used for the inside and outside valves. Some containment penetration lines have diverse valves (such as an air operated valve outside and a check valve inside); such lines would not be subject to a CCF. For lines that use the same valve type inside and outside, a diverse containment isolation capability is provided to deal with a CCF that could fail both valves. The largest containment line that could be subject to a CCF is a containment air filtration system (VFS) line which is 40.6 cm (16 inch). If this line remained open due to a CCF, some containment atmospheric inventory (steam and air) would be lost out through the un-isolated path. Over a few hours, the loss of containment inventory would decrease and then stop as the air concentration in the containment atmosphere decreased. This behaviour is the result of the PCS heat transfer improving as the concentration of air decreases in the containment until all of the decay heat can be removed by the PCS with the containment pressure at atmospheric pressure. The amount of containment atmosphere lost is limited such that, on a best estimate basis (appropriate for sequences with a CCF), long term passive residual heat removal or small LOCA containment recirculation operation can continue for an extended time. Chapter 9 provides additional information. Note that in the fault schedule shown in Table 8A-2, CI is always shown as

being provided by valve closure, either by PMS or DAS actuation. The diverse means (without valve closure) discussed in this paragraph is a variation that applies to the diverse core cooling cases shown in Table 8A-2 for DB2 frequent faults.

8A.4 Conclusions

The information presented in Table 8A-2 is intended to address the requirement raised by the Office for Nuclear Regulation at Step 3 of the GDA process that *"There is a need to demonstrate that the list of design basis initiating events is complete and can be reconciled with the list of faults in the PSA"*.

Future decommissioning and spent fuel management arrangements are considered later in the PCSR. In regards to spent fuel management, Westinghouse proposes using dry fuel storage system for longer term storage of spent fuel. After cooling in the pool, fuel would be retrieved and dried before being transferred into dry storage. Subsequently the fuel would be consigned for disposal into the planned geological disposal facility. Although Westinghouse expects that operators may wish to follow a different strategy, it is presently considered as the reference design. Given the longer term nature of decommissioning operations and the uncertainty regarding the preferred option for spent fuel management, a more generic list of faults has been identified and is presented in Table 8A-3.

The fault schedule provided in Table 8A-2 along with this introductory text shows that the AP1000 design provides sufficient SSCs with appropriate classification to meet regulatory targets and demonstrate an ALARP design.

Table 8A-1 Definition of Operational Modes

Mode	Title	Reactivity Condition (K_{eff})	% Rated Thermal Power (1)	Average Reactor Coolant Temperature °C (°F)
1	Power Operation	≥ 0.99	> 5	N/A
2	Start-up	≥ 0.99	≤ 5	N/A
3	Hot Standby	< 0.99	N/A	> 216 (420)
4	Safe Shutdown(2)	< 0.99	N/A	216 (420) ≥ T_{avg}(4) > 93 (200)
5	Cold Shutdown(2)	< 0.99	N/A	≤ 93 (≤ 200)
6	Refuelling(3)	N/A	N/A	N/A

Notes:

1. Excluding decay heat
2. All reactor vessel head closure bolts fully tensioned
3. One or more reactor vessel head closure bolts less than fully tensioned
4. Average Temperature

Table 8A-2 AP1000 PCSR Composite Fault List for Reactor Internal and Non-internal Events and Internal and External Hazards[1]

Fault ID	Initiating Event		Initiating Event Frequency/ DB Class	Possible Modes Affected	Engineered Safety Functions[2]				Comments	Further Assessment of Fault
					Reactivity Control (short term)		Safety Functions			
	Fault	Consequences			Signals	Devices	Signals	Devices		
1. Reactor Internal Events										
1.1 Reactor Pressure Vessel Rupture										
1.1.1	Rupture of RPV due to random failure event	Excessive loss of RCS inventory beyond makeup capabilities. Core damage and large fission product release.	3.2E-08 per reactor year BDB	1-6	N/A	Voids(C1)	N/A	Emergency cooling assumed to be inadequate due to severity of event	Limiting scenario assumes break below core level. Not assumed to be a credible event when the RCS is open in Modes 5-6 with the RCS open due to lack of pressurisation.	BDB Fault. Included in PSA (Chapter 10).
1.2 Large LOCA										
1.2.1	Large break loss of coolant accident (LBLOCA)	Rapid loss of coolant, with concurrent de-pressurisation of the RCS.	8.4E-07 per reactor year DBL	1-2	N/A	Voids(C1)	PMS(A,C1) – Low-2 Pressuriser Pressure	CMT(C1) (Core makeup tank) CI(C1)	Note that Rod Breakers are tripped on the PMS Low-2 pressuriser pressure signal. Break is >9" (22.9cm) in RCS primary circuit pipe due to random failure event. Break size range for LBLOCA is as adopted in the PSA. Large break in a pipe is assumed to bound other faults identified involving a major rupture in individual items of primary circuit plant (i.e. PZR shell, SG bottom head, Pump failure (bowl or motor casing). ASTRUM methodology used in DB analysis. Break area is treated as a statistical parameter.	Modes 1 and 2 are discussed in Section 9.6.4, "Large Break Loss of Coolant Accident". This fault is also discussed in Section 10.4.
							N/A	ACCUM(C1)		
							PMS (A,C1) – Low CMT Level	ADS(C1) IRWST(C1)		
							PMS(A,C1) – Low IRWST Level	RECIRC(C1)		
							PMS(A,C1) – High-2 Containment Pressure	PCS(C1)		
1.2.2	Large break loss of coolant accident (LBLOCA)	Rapid loss of coolant, with concurrent de-pressurisation of the RCS.	4.2E-08 per reactor year (See Note 1 in 8A.1) DBL/BDB	3,4 and 5 with RCS intact	N/A	Rods already inserted	PMS(A,C1) – High-2 Containment Pressure	CMT(C1) CI(C1) PCS(C1)	Mode 3 analysis performed in Section 9.8.4.6.4, assuming accumulators out of service confirms that fault in shutdown mode is significantly less limiting then at power, even when equipment availability in different modes is considered. A LBLOCA is increasingly unlikely as the plant transitions to lower modes, and is not credible in Mode 5 due to lower pressures and temperatures.	Modes 3, 4, 5, and 6 are discussed in Section 9.8.4.6.4, "Loss-of-Coolant Accident Events in Shutdown Modes". This fault is also discussed in Section 10.4.
							PMS(A,C1) – Low CMT Level	ADS(C1) IRWST(C1)		
							PMS(A,C1) – Low IRWST Level	RECIRC(C1)		

[1] Table 8A-2 is a summary of internal and external faults and hazards presented throughout the PCSR. As such, abbreviations and acronyms are not defined throughout the table.

[2] For information regarding RCS pressure control, see Section 8A-3, "Pressure Control".

Table 8A-2 AP1000 PCSR Composite Fault List for Reactor Internal and Non-internal Events and Internal and External Hazards (cont.)

Fault ID	Initiating Event		Initiating Event Frequency/ DB Class	Possible Modes Affected	Engineered Safety Functions				Comments	Further Assessment of Fault
	Fault	Consequences			Reactivity Control(short term)		Safety Functions			
					Signals	Devices	Signals	Devices		
1.2.3	Large break loss of coolant accident (LBLOCA)	N/A	BDB	5 with RCS open, 6	N/A	Rods already inserted	See Comments		Mode 5 and 6 with RCS open, CMTs are not required to be available, RCS makeup function is provided by in-containment refuelling water storage tank (IRWST). No analysis is required since a LBLOCA in Mode 5 with the RCS open and in Mode 6 is not considered credible. In the event of a line break due a dropped load, the consequences are bounded by Faults 2.3.2 and 2.3.3, but there is no loss of inventory outside of containment.	Modes 5 and 6 are discussed in Section 9.8.4.6.4, "Loss-of-Coolant Accident Events in Shutdown Modes".
1.3 Interfacing System LOCA										
1.3.1	Interfacing system LOCA due to random failures of the low/high pressure boundaries between low pressure (LP) systems and the RCS	May lead to an un-isolable loss of coolant outside the containment. Similar to LBLOCA.	<1E-06 per reactor year BDB	1-6	N/A	Voids(C1)	N/A	Emergency cooling assumed to be inadequate due to large loss of primary coolant outside containment	In lower modes, this event would not overpressurise the interfacing system, and therefore would not result in an uncontrolled loss of coolant.	BDB Fault. Included in PSA, see Section 10.4.8.9.
1.4 Medium LOCA										
1.4.1	Medium break loss-of-coolant accident	Loss of coolant with a concurrent de-pressurisation of the RCS.	6.8E-06 per reactor year DBL	1-2	PMS(A,C1) – Low-2 Pressuriser Pressure	Rod breakers (C1)	PMS(A,C1) – Low-2 Pressuriser Pressure	PRHR(C1) CMT(C1) CI(C1)	Bounding case models a 10-inch (25.4 cm) break in the bottom of a cold leg, connected to the balance line of CMT-1. Probability is calculated for a break range between 4” (10.2 cm) and 9” (22.9 cm) in the RCS primary circuit due to random failure event.	Modes 1 and 2 are discussed in Section 9.6.5.3.6, "MBLOCA - 254 mm (10-inch) Cold Leg Break Results". This fault is also discussed in Section 10.4.
							N/A	ACCUM(C1)		
							PMS(A,C1) – Low CMT Level	ADS(C1) IRWST(C1)		
							PMS(A,C1) – Low IRWST Level	RECIRC(C1)		
							PMS(A,C1) – High-2 Containment Pressure	PCS(C1)		
1.4.2	Medium break loss-of-coolant accident	Loss of coolant with a concurrent de-pressurisation of the RCS.	3.4E-07 per reactor year (See Note 1 in 8A.1) DBL/BDB	3,4,5 with RCS intact	N/A	Rods already inserted	PMS(A,C1) – High-2 Containment Pressure	PRHR(C1) CMT(C1) CI(C1) PCS(C1)	A medium-break loss-of-coolant accident (MBLOCA) is increasingly unlikely as the plant transitions to lower modes, and is not credible in Mode 5 due to lower pressures and temperatures.	Modes 3, 4, 5, and 6 are discussed in Section 9.8.4.6.4, "Loss-of-Coolant Accident Events in Shutdown Modes". This fault is also discussed in Section 10.4.
							PMS(A,C1) – Low CMT Level	ADS(C1) IRWST(C1)		
							PMS(A,C1) – Low IRWST Level	RECIRC(C1)		

Table 8A-2 AP1000 PCSR Composite Fault List for Reactor Internal and Non-internal Events and Internal and External Hazards (cont.)

Fault ID	Initiating Event		Initiating Event Frequency/ DB Class	Possible Modes Affected	Engineered Safety Functions				Comments	Further Assessment of Fault
	Fault	Consequences			Reactivity Control(short term)		Safety Functions			
					Signals	Devices	Signals	Devices		
1.4.3	Medium break loss-of-coolant accident	N/A	3.4E-07 per reactor year (See Note 1 in 8A.1) BDB	5 with RCS open, 6	N/A				A MBLOCA is not credible when RCS is open. In the event of a line break due a dropped load, the consequences are bounded by Faults 2.3.2 and 2.3.3, but there is no loss of inventory outside of containment.	Modes 3, 4, 5, and 6 are discussed in Section 9.8.4.6.4, "Loss-of-Coolant Accident Events in Shutdown Modes". This fault is also discussed in Section 10.4.
1.5 Spurious Actuation of ADS										
1.5.1	Failures (false signals, human errors or mechanical ruptures) that result in inadvertent operation of ADS 4	Rapid loss of coolant, with concurrent de-pressurisation of the RCS. Less limiting than large LOCAs in fault 1.2 Challenges structural design of ADS stage 4 pipes and supports.	<1E-07 per reactor year BDB	1-6	See Comments				The potential for a failure to initiate spurious ADS stage 4 flow is so low it is a BDB event. All failures are considered including mechanical ruptures and inadvertent actuation signals. Note that spurious failures not due to software are assumed to be less than 1E-05 events per year. Failures that could cause spurious squib valve opening are discussed in PCSR Chapters 10.4, 17.5 and 19.2. Additional information is available in the Squib Valve Safety Case, UKP-GW-GL-200. Consequences acceptable in Modes 4-6.	This beyond design basis fault is discussed in Section 10.4.
1.5.2	Failures (false signals, human errors or mechanical ruptures) that result in inadvertent operation of ADS 1-3 Inadvertent Opening of a Pressuriser Safety Valve	Inadvertent depressurisation of the reactor coolant system which results in a rapidly decreasing reactor coolant system pressure and a decrease in moderator density feedback.	<1E-07 per reactor year DB1/BDB	1-5 with RCS Intact	PMS(A,C1) – Low-2 Pressuriser Pressure or PMS(A,C1) – OTΔT	Rod breakers (C1)	PMS(A,C1) – Low-2 Steam Generator (SG) narrow range (NR) level coincident with Low-2 startup feedwater (SFW) flow	PRHR(C1)	The potential for a failure to initiate spurious ADS stage 1-3 flow is so low it is a BDB event. Note that spurious failures not due to software are assumed to be less than 1E-05 events per year. Inadvertent pressuriser safety opening has an IEF of 3.9E-04 events per reactor year, and is therefore categorized as a DB1. Therefore, this fault is analysed as a DB1 event and covers both the spurious ADS 1-3 as well as inadvertent pressuriser safety valve opening. This event is also considered in PSA. Failures that could cause spurious are discussed in PCSR Sections 10.4, 17.5 and 19.2. Additional information is available in the Squib Valve Safety Case, UKP-GW-GL-200. These events are not credible in Modes 5 and 6 with the RCS open.	Modes 1 and 2 are discussed in Section 9.6.1, "Inadvertent Opening of a Pressuriser Safety Valve or Inadvertent Operation of the ADS". Modes 3, 4, 5, and 6 are discussed in Section 9.8.4.6.1, "Inadvertent Opening of a Pressuriser Safety Valve or Inadvertent Operation of the Automatic Depressurisation System". This fault is also discussed in Section 10.4.
							PMS(A,C1) – Low-2 Cold Leg Temperature	CMT(C1) CI(C1)		
							N/A	ACCUM(C1)		
							PMS(A,C1) – Low CMT Level	ADS(C1) IRWST(C1)		
							PMS(A,C1) – Low IRWST Level	RECIRC(C1)		
							PMS(A,C1) – High-2 Containment Pressure	PCS(C1)		

Table 8A-2 AP1000 PCSR Composite Fault List for Reactor Internal and Non-internal Events and Internal and External Hazards (cont.)

Fault ID	Initiating Event		Initiating Event Frequency/ DB Class	Possible Modes Affected	Engineered Safety Functions				Comments	Further Assessment of Fault
	Fault	Consequences			Reactivity Control(short term)		Safety Functions			
					Signals	Devices	Signals	Devices		
1.6 CMT Line Break										
1.6.1	Core Makeup Tank Inlet Line Break	Similar to a MBLOCA (Fault 1.4.1), loss of coolant with a subsequent de-pressurisation of the RCS and pressure decrease in the pressuriser.	5.4E-07 per reactor year DBL	1-2	PMS(A,C1) – Low-2 Pressuriser Pressure	Rod breakers (C1)	PMS(A,C1) – Low 2 Pressuriser Pressure	PRHR(C1) CMT(C1) CI(C1)	Fault is considered to bound possible failures of the Core Makeup Tank itself. Fault assessed as a separate group because of non-availability of CMT as a consequence. Section 9.6.5.3.8 argues that fault is bounded by the limiting DVI line and the MBLOCA breaks. For Modes 3-6, CMT line break is bounded by MBLOCA (see Fault 1.4.2-1.4.3).	Modes 1 and 2 are discussed in Section 9.6.5.3.8, "Core Makeup Tank Line Break Results". Modes 3, 4, 5, and 6 are discussed in Section 9.8.4.6.1, "Loss-of-Coolant Accident Events in Shutdown Modes". This fault is also discussed in Section 10.4.
							N/A	ACCUM(C1)		
							PMS(A,C1) – Low CMT Level	ADS(C1) IRWST(C1)		
							PMS(A,C1) – Low IRWST Level	RECIRC(C1)		
							PMS(A,C1) – High-2 Containment Pressure	PCS(C1)		
1.7 Direct Vessel Injection Line Break										
1.7.1	Direct vessel injection (DVI) line break	Similar to a MBLOCA (Fault 1.4.1), loss of coolant with a subsequent de-pressurisation of the RCS and pressure decrease in the Pressuriser.	1.4E-06 per reactor year DBL	1-2	PMS(A,C1) – Low-2 Pressuriser Pressure	Rod breakers (C1)	PMS(A,C1) – Low 2 Pressuriser Pressure	PRHR(C1) CMT(C1) CI(C1)	Fault includes any rupture occurring in one of the safety injection lines including the DVI line and lines that connect the CMT, accumulator, or IRWST to DVI. Fault differs from MBLOCA because one CMT, one accumulator, one injection line, and one recirculation line spill to containment without injecting to the RCS. For Modes 3-6, DVI line break is bounded by MBLOCA (see Fault 1.4.2-1.4.3).	Modes 1 and 2 are discussed in Section 9.6.5.3.5, "Direct Vessel Injection Line Break Results". Modes 3, 4, 5, and 6 are discussed in Section 9.8.4.6.1, "Loss-of-Coolant Accident Events in Shutdown Modes". This fault is also discussed in Section 10.4.
							N/A	ACCUM(C1)		
							PMS(A,C1) – Low CMT Level	ADS(C1) IRWST(C1)		
							PMS(A,C1) – Low IRWST Level	RECIRC(C1)		
							PMS(A,C1) – High-2 Containment Pressure	PCS(C1)		
1.8 Small LOCA										
1.8.1	Small break loss-of-coolant accident	Loss of coolant with a subsequent de-pressurisation of the RCS and pressure decrease in the Pressuriser.	>1E-04 per reactor year DB1	1-2	PMS(A,C1) – Low-2 Pressuriser Pressure	Rod breakers (C1)	PMS(A,C1) – Low 2 Pressuriser Pressure	PRHR(C1) CMT(C1) CI(C1)	Frequency determination is presented in UKP-GW-GL-797. This fault is applicable to larger small break LOCAs, greater than cliff edge small LOCAs (2 inch/ 5.1 cm) and less than medium LOCAs (4 inch / 10.2 cm).	Modes 1 and 2 are discussed in Section 9.6.5.3.4, "SBLOCA - 50.8 mm (2-inch) Cold Leg Break Results". This fault is also discussed in Section 10.4.
							PMS(A,C1) – Low CMT Level	ADS(C1) IRWST(C1)		
							PMS(A,C1) – Low IRWST Level	RECIRC(C1)		
							PMS(A,C1) – High-2 Containment Pressure	PCS(C1)		
							N/A	ACCUM(C1)		

Table 8A-2 AP1000 PCSR Composite Fault List for Reactor Internal and Non-internal Events and Internal and External Hazards (cont.)

Fault ID	Initiating Event		Initiating Event Frequency/ DB Class	Possible Modes Affected	Engineered Safety Functions				Comments	Further Assessment of Fault
					Reactivity Control(short term)		Safety Functions			
	Fault	Consequences			Signals	Devices	Signals	Devices		
1.8.2	Small break loss-of-coolant accident	Loss of coolant with a subsequent de-pressurisation of the RCS and pressure decrease in the pressuriser.	1E-04 per reactor year DB2 Cliff Edge	1, 2	PMS(A,C1) – Low-2 Pressuriser Pressure	Rod breakers (C1)	PMS(A,C1) – Low 2 Pressuriser Pressure	PRHR(C1) CMT(C1) CI(C1)	Frequency determination is presented in UKP-GW-GL-797. This fault is applicable to LOCAs greater than RCS leaks (0.95 cm [3/8 inch]) and less than infrequent fault small LOCAs (5.1 cm [2 inches]). Small-break loss-of-coolant accident (SBLOCA) fault is also considered to bound break in chemical and volume control system (CVS) make-up or let down line. Note that five sets of mitigating SSCs are listed for this event. The first one contains all of the C1 equipment that would normally actuate to mitigate the event. The next three sets of equipment demonstrate the capability of the AP1000 plant to tolerate a CCF and still provide adequate core cooling. For the third diverse core cooling case, the use of the ADS stages 1-3 is credited although it may not be necessary depending on the magnitude of the impact of nitrogen discharge from the accumulators. The RCS pressure is calculated to remain at the accumulator empty pressure such that a limited amount of nitrogen is expected to discharge from the accumulators. In this situation the PRHR heat exchanger (HX) is expected to work well enough to keep the RCS pressure low enough to allow for normal residual heat removal system (RNS) injection. However, crediting operation of ADS stages 1-3 removes any such uncertainty. The last set of equipment demonstrates the capability of the plant to tolerate a PMS CCF ATWT event and still shutdown the reactor. Note that a mechanical CCF of the rods is bounded by this this C&I CCF (See Supporting Analysis).	Modes 1 and 2 are discussed in Section 9.6.5.3.4, "SBLOCA - 50.8 mm (2-inch) Cold Leg Break Results". This fault is also discussed in Section 10.4.
							PMS(A,C1) – Low CMT Level	ADS(C1) IRWST(C1)		
							PMS(A,C1) – Low IRWST Level	RECIRC(C1)		
							PMS(A,C1) – High-2 Containment Pressure	PCS(C1)		
							N/A	ACCUM(C1)		
					PMS(A,C1) – Low-2 Pressuriser Pressure	Rod breakers (C1)	PMS(A,C1) – Low-2 Pressuriser Pressure	PRHR(C1) CMT(C1) CI(C1)		
							PMS(A,C1) – Low CMT Level	ADS 4(C1) IRWST(C1)		
							PMS(A,C1) – Low IRWST Level	RECIRC(C1)		
							PMS(A,C1) – High-2 Containment Pressure	PCS(C1)		
					PMS(A,C1) – Low-2 Pressuriser Pressure	Rod breakers (C1)	PMS(A,C1) – Low-2 Pressuriser Pressure	CMT(C1) CI(C1)		
							PMS(A,C1) – Low CMT Level	ADS 1-4(C1) IRWST(C1)		
							PMS(A,C1) – Low IRWST Level	RECIRC(C1)		
							PMS(A,C1) – High-2 Containment Pressure	PCS(C1)		
					DAS(A,C2) - Low-2 Pressuriser Level	Rod MG Set breakers (C2)	DAS(A,C2) – Low-2 Pressuriser Level	PRHR(C1)		
							N/A	ACCUM(C1)		
							DAS(M,C2)	ADS 1-3(C1) RECIRC(C1)		
							PLS(M,C2)	RNS Injection(C2)		
							DAS(A,C2) – High Containment Temperature	PCS(C1) CI(C1)		
					DAS(A,C2) - High Hot Leg Temperature	Rod MG Set breakers (C2)	DAS(A,C2) – Low-2 Pressuriser Level	PRHR(C1) CMT(C1)		
							DAS(MC2)	ADS (C1) IRWST (C1) RECIRC(C1)		
							DAS(A,C2)- High Containment Temperature	PCS(C1) CI(C1)		

Table 8A-2 AP1000 PCSR Composite Fault List for Reactor Internal and Non-internal Events and Internal and External Hazards (cont.)

Fault ID	Initiating Event		Initiating Event Frequency/ DB Class	Possible Modes Affected	Engineered Safety Functions				Comments	Further Assessment of Fault
					Reactivity Control(short term)		Safety Functions			
	Fault	Consequences			Signals	Devices	Signals	Devices		
1.8.3	Small break loss-of-coolant accident	Loss of coolant with a subsequent de-pressurisation of the RCS and pressure decrease in the pressuriser.	1.4E-04 per reactor year (See Note 1 in 8A.1) DB1	3,4 and 5 with RCS Intact	N/A	Rods already inserted	PMS(A,C1) – Low 2 Pressuriser Level	PRHR(C1) CMT(C1) CI(C1)	In shutdown modes, both accumulators are isolated at 6.895 MPa. (1000 psia) or less. In MODE 5 one CMT can be isolated. Since the probability of being in these MODEs is less than at power, the max LOCA size would be reduced (ignored in this assessment). There is no need to consider ATWT event in shutdown, since rods already inserted.	Modes 3, 4, and 5 are discussed in Section 9.8.4.6.1, "Loss-of-Coolant Accident Events in Shutdown Modes". This fault is also discussed in Section 10.4.
							PMS(A,C1) – Low CMT Level	ADS(C1) IRWST(C1)		
							PMS(A,C1) – Low IRWST Level	RECIRC(C1)		
							PMS(A,C1) – High-2 Containment Pressure	PCS(C1)		
1.8.4	Small break loss-of-coolant accident	N/A	N/A	5 with RCS Open, 6	N/A				In these MODEs the RCS is at atmospheric pressure such that a LOCA is no longer considered a credible fault. In the event of a line break due a dropped load in this Mode, the consequences are bounded by Faults 2.3.2 and 2.3.3, but there is no loss of inventory outside of containment.	Modes 5 and 6 are discussed in Section 9.8.4.6.1, "Loss-of-Coolant Accident Events in Shutdown Modes". This fault is also discussed in Section 10.4.
1.9 Reactor Coolant Leakage										
1.9.1	Reactor coolant leakage	Loss of coolant, smaller than limiting SBLOCA (Fault 1.8.1).	1.4E-03 per reactor year HFLC	1-6	N/A (See Comments)				Under normal operating conditions the plant will "ride the transient out" without generating a reactor trip. If fault progresses, the mitigation SSCs would be consistent with frequent fault SBLOCA (Fault 1.8.2) In MODEs 3-6 the rods are already inserted. The description in this row considers a scenario where the safety class 2 CVS does not perform its intended function, thus loss of CVS is initiating event. Very low rate of coolant loss from RCS (up to 22.71m^3/hr [100 gpm]), eventually leading to low-2 pressuriser level indication. For Modes 4-6, the IEF is 7.0 E-05, making it an infrequent fault (See Note 1 in 8A.1), with low consequences. Regardless, the consequences are bounded by a SBLOCA (Faults 1.8.3-1.8.4).	Modes 1 and 2 are discussed in Section 9.6.5.3.10, "Reactor Coolant Leakage Results". Modes 3, 4, 5, and 6 are discussed in Section 9.8.4.6.1, "Loss-of-Coolant Accident Events in Shutdown Modes". This fault is also discussed in Section 10.4.
1.9.2	Failure of small lines carrying primary coolant outside containment	Activity release outside of containment to the environment. The loss of coolant reduces pressuriser level and creates a demand for makeup.	>1E-03 per reactor year DB2	1-6	N/A (See Comments)				The mitigation SSCs are consistent with frequent fault SBLOCA (Fault 1.8.2) This leakage event is assumed to be detected and isolated within 30 minutes of event initiation based on availability of Class 1 Radiation Monitoring System (RMS) alarm and plant emergency operating procedures. For Modes 4-6, the IEF is 5.0 E-05, making it a DB1 infrequent fault (See Note 1 in 8A.1). Thus, the consequences are bounded by a SBLOCA (Faults 1.8.3-1.8.4).	Mode 1 is discussed in Section 9.6.2, "Failure of Small Lines Carrying Primary Coolant Outside Containment" and Modes 2, 3, 4, and 5 are discussed in Section 9.8.4.6.2, "Failure of Small Lines Carrying Primary Coolant Outside Containment"

Table 8A-2 AP1000 PCSR Composite Fault List for Reactor Internal and Non-internal Events and Internal and External Hazards (cont.)

Fault ID	Initiating Event		Initiating Event Frequency/ DB Class	Possible Modes Affected	Engineered Safety Functions				Comments	Further Assessment of Fault
	Fault	Consequences			Reactivity Control(short term)		Safety Functions			
					Signals	Devices	Signals	Devices		
1.9.3	Failures (false signals, human errors or mechanical ruptures) that result in inadvertent operation of the IRWST injection squib valves	Opening of these squib valves would result in leakage through upstream check valve pressure balance holes. In addition, these check valves are assumed to be in-operable (stuck closed) following this fault because of the large load applied.	<1E-07 BDB	1-6	See Comments				The potential for a failure to spuriously open IRWST injection squib valves is so low it is a BDB event. All failure modes are considered including mechanical ruptures and inadvertent actuation signals. Note that spurious failures not due to software are assumed to be less than 1E-05 events per year. Failures that could cause spurious squib valve opening are discussed in PCSR Sections 10.4, 17.5 and 19.2. Additional information is available in the Squib Valve Safety Case, UKP-GW-GL-200. Consequences acceptable in MODEs 4, 5, 6.	This beyond design basis fault is discussed in Section 10.4.
1.10 PRHR Tube Rupture										
1.10.1	Passive residual heat removal tube rupture	Loss of coolant, smaller than limiting SBLOCA (Fault 1.8.1).	1.1E-04 per reactor year DB1	1-5 with RCS Intact	N/A (See Comments)				If CVS operation or PRHR isolation fail, fault progression and mitigation SSCs is similar to SBLOCA (depending on the size of the break). PRHR system performance would be degraded by a break in PRHR tube(s); however, sufficient functionality to support fault mitigation would still be available. Event is not a credible initiator in Modes 5 and 6 with the RCS open, as there is no pressure on the PRHR tubing.	Modes 1 and 2 are discussed in Section 9.6.5.3.9, "Passive Residual Heat Removal Tube Rupture Results". Modes 3, 4, 5, and 6 are discussed in Section 9.8.4.6.1, "Loss-of-Coolant Accident Events in Shutdown Modes". This fault is also discussed in Section 10.4.
1.11 SGTR										
1.11.1	Steam Generator Tube Rupture (SGTR)	Increase in contamination of the secondary system due to leakage of radioactive coolant from the RCS and a subsequent release of activity to the atmosphere.	3.3E-03 per reactor year DB2	1, 2	PMS(A,C1) – Low-2 Pressuriser Level	Rod breakers (C1)	PMS(A,C1) – Low 2 Pressuriser Level	PRHR(C1) CMT(C1)	The IEF for this fault is based on historical data, and the SG tubes for the AP1000 plant are manufactured in accordance with relevant good practice, which incorporates improved materials and processes. No ruptures have been experienced since these major improvements were made. As such, the initiating event frequency is realistically expected to be below 1E-03 events per reactor year, but is still evaluated as a frequent fault event. Fault due to random failure event. Limiting case is a single tube rupture compared to multiple tube ruptures. The analysis presented in Section 9.6.3.2.3 assumes a loss of offsite power at the start of the event resulting in rod insertion. For diverse core cooling scenario, loss of normal feedwater fault is bounding (Fault 1.16.1).	Modes 1 and 2 are discussed in Section 9.6.3, "Steam Generator Tube Rupture". This fault is also discussed in Section 10.4. Note that the diversity case has not been explicitly analysed, and will be addressed during site licensing. It is explained in Section 9.6.3.3.1 why the scenario is expected to be mitigated adequately.
							PMS(A,C1) – Low-2 Steamline Pressure	CI(C1)		
							PMS(A,C1) – High-2 Containment Pressure	PCS(C1)		
					DAS(A,C2) - Low-2 SG WR Level	Rod MG Set breakers (C2)	N/A	ACCUM(C1)		
							DAS(M,C2)	ADS(C1) IRWST(C1) RECIRC(C1)		
							DAS(A,C2) – High Containment Temperature	PCS(C1) CI(C1)		
					DAS(A,C2) – Low Pressuriser Level	Rods fail to insert	DAS(A,C2) – Low Pressuriser Level	CMT(C1) PRHR(C1)		
							DAS(A,C2) –High Containment Temperature	PCS(C1) CI(C1)		

Table 8A-2 AP1000 PCSR Composite Fault List for Reactor Internal and Non-internal Events and Internal and External Hazards (cont.)

Fault ID	Initiating Event		Initiating Event Frequency/ DB Class	Possible Modes Affected	Engineered Safety Functions				Comments	Further Assessment of Fault
					Reactivity Control(short term)		Safety Functions			
	Fault	Consequences			Signals	Devices	Signals	Devices		
1.11.2	Steam Generator Tube Rupture (SGTR)	Increase in contamination of the secondary system due to leakage of radioactive coolant from the RCS and a subsequent release of activity to the atmosphere.	1.7E-04 per reactor year (See Note 1 in 8A.1) DB1	3-5 with RCS Intact	N/A	Rods already inserted	PMS(A,C1) – Low 2 Pressuriser Level	CMT(C1) PRHR(C1)	Fault due to random failure event. There is no need to consider ATWT event in shutdown, since rods already inserted.	Modes 3, 4, 5, and 6 are discussed in Section 9.8.4.6.3, “Steam Generator Tube Rupture in Lower Modes". Also discussed in Chapter 10.4.
							PMS(A,C1) – High-2 Containment Pressure	PCS(C1) CI(C1)		
1.11.3	Steam Generator Tube Rupture (SGTR)	N/A	N/A	5 with RCS Open, 6	N/A	Rods already inserted	N/A		In Modes 5 and 6, the RCS pressure and temperature are reduced, thus, a SGTR event is not credible.	Modes 3, 4, 5, and 6 are discussed in Section 9.8.4.6.3, “Steam Generator Tube Rupture in Lower Modes". Also discussed in Chapter 10.4.
1.12 Transient with Main Feed water										
1.12.1	Inadvertent operation of the core makeup tanks	Significant core makeup tank injection flow leading to a boration of the RCS.	>1E-03 per reactor year DB2	1-2	PMS(A,C1) – High 3 Pressuriser Level	Rod breakers (C1)	PMS (M,C1) - High-2 Pressuriser Level	Head Vent(C1)	Fault is caused by operator error, false electrical signal or a valve malfunction. Fault is assessed individually in ‘Transient With Main Feed-water Available’ Section in Chapter 9 because of assumed difference regarding availability of one CMT post fault. Pressuriser safety valve is credited in the analysis for reactor coolant system pressure control. For ATWT, this event is bounded by Fault 1.13.1a “Complete loss of forced reactor coolant flow”	Modes 1 and 2 are discussed in Section 9.5.1, "Inadvertent Operation of the Core Makeup Tanks during Power Operation".
							PMS(A,C1) – High 3 Pressuriser Level	PRHR(C1)		
							PMS(A,C1) – Low-2 Cold Leg Temperature	CMT(C1) CI(C1)		
							PMS(A,C1) – High-2 Containment Pressure	PCS(C1)		
					DAS(M,C2)	Rod MG Set breakers (C2)	DAS(M,C2)	ADS(C1) IRWST(C1) RECIRC(C1)		
							N/A	ACCUM(C1)		
							DAS(A,C2) – High Containment Temperature	PCS(C1) CI(C1)		
1.12.2	Inadvertent operation of the core makeup tanks	Significant core makeup tank injection flow leading to a boration of the RCS.	>1E-03 per reactor year DB2	3-5 with RCS Intact	N/A	Rods already inserted	PMS (M,C1) - High-2 Pressuriser Level	Head Vent (C1)	The limiting case is initiated from shutdown with rods already inserted, which produces minimum initial shutdown margin. Fault is caused by operator error, false electrical signal or a valve malfunction. In shutdown modes, assume both accumulators isolated at 6.895 MPa. After RNS cut in, RNS relief valves may provide relief in lieu of head vent valves. There is no need to consider ATWT event in shutdown, since rods already inserted.	Modes 3, 4, 5, and 6 are discussed in Section 9.8.4.5, "Increase in Reactor Coolant Inventory".
							PMS(A,C1) – High 3 Pressuriser Level	PRHR(C1)		
							PMS(A,C1) – Low Cold Leg Temperature	CMT(C1) CI(C1)		
							PMS(A,C1) – High-2 Containment Pressure	PCS(C1)		
					N/A	Rods already inserted	DAS(M,C2)	ADS(C1) IRWST(C1) RECIRC(C1)		
							DAS(A,C2) – High Containment Temperature	PCS(C1) CI(C1)		
1.12.3	Inadvertent operation of the core makeup tanks	N/A	N/A	5 with RCS Open, 6	N/A				Fault is not credible in Mode 5 with RCS pressure boundary open and in Mode 6 due to the CMTs being isolated.	Modes 3, 4, 5, and 6 are discussed in Section 9.8.4.5, "Increase in Reactor Coolant Inventory".

Table 8A-2 AP1000 PCSR Composite Fault List for Reactor Internal and Non-internal Events and Internal and External Hazards (cont.)

Fault ID	Initiating Event		Initiating Event Frequency/ DB Class	Possible Modes Affected	Engineered Safety Functions				Comments	Further Assessment of Fault
					Reactivity Control(short term)		Safety Functions			
	Fault	Consequences			Signals	Devices	Signals	Devices		
1.12.4	Chemical and volume control system malfunction that increase reactor coolant inventory	Injection of highly borated water into the RCS from one or both of the CCS pumps.	>1.0x10-3 per reactor year DB2	1-4 prior to RNS alignment	PMS(A,C1) – Low-2 Cold Leg Temperature	Rod breakers (C1)	PMS (M,C1) - High-2 Pressuriser Level	Head Vent (C1)	Note that in the PSA, CVS malfunction is part of the core power excursion, not transient with main feedwater. Pressuriser safety valve is credited in the analysis for reactor coolant system pressure control. For ATWT, this event is bounded by Fault 1.12.8 .	Modes 1 and 2 are discussed in Section 9.5.2, "Chemical and volume control system malfunction that increase reactor coolant inventory". Modes 3, 4, 5, and 6 are discussed in Section 9.8.4.5, "Increase in Reactor Coolant Inventory".
							PMS(A,C1) – High 3 Pressuriser Level	PRHR(C1)		
							PMS(A,C1) – Low-2 Cold Leg Temperature	CMT(C1) CI(C1)		
							PMS(A,C1) – High-2 Containment Pressure	PCS(C1)		
					DAS(M,C2)	Rod MG Set breakers (C2)	Same Mitigation SSCs as Fault 1.12.8			
1.12.4a	Chemical and volume control system malfunction that increase reactor coolant inventory	Injection of highly borated water into the RCS from one or both of the CCS pumps. Overpressurisation could result in RCS coolant being relieved via RNS relief valves.	>5E-05 per reactor year (See Note 1 in 8A.1) DB1	4 after RNS alignment, 5 with RCS Intact	N/A	Rods already inserted	PMS(M,C1)	PRHR(C1)	Frequency of occurrence at lower modes reduced to DB1 fault. Operators would be expected to be monitoring RNS conditions continuously during these MODEs. Further analysis to substantiate these claims will be performed during site licensing. Should RCS inventory swell beyond the volume of the RCS/RNS, the RNS spring-operated relief valves would provide pressure relief. Radiological consequences are bounded by RNS line break, see Fault 2.3.1. Expected to be lower releases due to no break.	Modes 3, 4, 5, and 6 are discussed in Section 9.8.4.5, "Increase in Reactor Coolant Inventory".
							PMS(M,C1)	CMT(C1) CI(C1)		
							PMS(A,C1) – High-2 Containment Pressure	PCS(C1)		
1.12.5	Chemical and volume control system malfunction that increase reactor coolant inventory	None, RCS pressure boundary open, no potential for over pressurisation.	N/A	5 with RCS Open, 6	N/A				This event is not credible when the RCS pressure boundary is open.	Modes 3, 4, 5, and 6 are discussed in Section 9.8.4.5, "Increase in Reactor Coolant Inventory".

Table 8A-2 AP1000 PCSR Composite Fault List for Reactor Internal and Non-internal Events and Internal and External Hazards (cont.)

Fault ID	Initiating Event		Initiating Event Frequency/ DB Class	Possible Modes Affected	Engineered Safety Functions				Comments	Further Assessment of Fault
					Reactivity Control(short term)		Safety Functions			
	Fault	Consequences			Signals	Devices	Signals	Devices		
1.12.6	Inadvertent operation of pressuriser heaters	Potential to cause over-pressurisation of the reactor coolant system (RCS).	>1E-03 per reactor year DB2	1-5 RCS Pressure Boundary Intact	PMS(A,C1) – High-2 Pressuriser Pressure or Overtemperature ΔT or Low-2 RCP speed	Rod breakers (C1)	PMS(A,C1) - Low-2 SG NR Level coincident with Low-2 SFW flow	PRHR(C1)	This fault is bounded by the loss of load/turbine trip fault (Fault 1.12.8). For this transient, the sole concern would be over-pressurising the RCS. [ ] Based on this comparison, it can be concluded that the inadvertent operation of the pressuriser heaters would not challenge RCS pressure limits or PSV pressure relief capacity. For the primary safety case, eventually the reactor would be tripped on high RCS pressure and the PSVs are available to limit the RCS pressure transient caused by the heat load from the pressuriser heaters.	See Loss of Load / Turbine Trip discussion presented in Section 9.2.3 “Turbine Trip”. This fault will be examined in more detail to confirm claims and arguments presented during site licensing.
							PMS(A,C1) – Low Cold Leg Temperature	CMT(C1) CI(C1)		
							PMS(A,C1) – High-2 Containment Pressure	PCS(C1)		
					DAS(A,C2)- High Hot Leg Temperature	Rod MG Set breakers (C2)	N/A	ACCUM(C1)		
							DAS(M,C2)	ADS(C1) IRWST(C1) RECIRC(C1)		
							DAS(A,C2) - High Containment Temperature	PCS(C1) CI(C1)		
					DAS(A,C2)- High Hot Leg Temperature	Rods fail to insert	PMS(A,C2) – Low-2 SG NR Level coincident with Low-2 SFW flow	PRHR(C1)		
							DAS(A,C2) - Low-2 SG WR Level	CMT(C1)		
							PMS(A,C1) – High-2 Containment Temperature	PCS(C1) CI(C1)		
1.12.7	Inadvertent operation of pressuriser heaters	N.A	N.A	5 with RCS Open, 6	N/A				RCS overpressurisation is not a concern when the RCS pressure boundary is open.	N/A

Table 8A-2 AP1000 PCSR Composite Fault List for Reactor Internal and Non-internal Events and Internal and External Hazards (cont.)

Fault ID	Initiating Event		Initiating Event Frequency/ DB Class	Possible Modes Affected	Engineered Safety Functions				Comments	Further Assessment of Fault
					Reactivity Control(short term)		Safety Functions			
	Fault	Consequences			Signals	Devices	Signals	Devices		
1.12.8	Turbine trip Loss of external electrical load	Loss of steam flow from SGs and decrease in heat removal. Loss of major load on the plan where the AC power remains available to operate major plant components.	>1E-03 per reactor year DB2	1-2	PMS(A,C1) – High-2 Pressuriser Pressure or Overtemperature ΔT or Low-2 RCP speed	Rod breakers (C1)	PMS(A,C1) - Low-2 SG NR level coincident with Low-2 SFW flow	PRHR(C1)	Turbine bypass accommodates up to 40% of rated steam flow during normal (power) operation. With Rapid Power Reduction System, this event is not expected to result in Reactor Trip or Safety Valve Actuation. PZR spray limits increase in coolant pressure. If automatic turbine bypass fails (or if condenser unavailable) the PZR and SG safety valves are sized to protect RCS and SG. Even assuming turbine bypass not available, the “normal” plant response (with class 2 systems available) Steam generator + SFW(A,C2)+CVS(A,C2), followed by RNS(M,C2). AC power from offsite or, from standby diesel generators Two diverse cases listed. First one is for core cooling. Second one is for anticipated transient without trip (ATWT). ATWT turbine trip is bounded by ATWT loss of normal feedwater (Fault 1.16.1) for peak RCS pressure and by ATWT complete loss of flow for core damage (Fault 1.13.1a). ATWT systems available for this event are reported; however, limiting ATWT case which models mechanical rod insertion failure reaches safe stable steady-state condition but a manual action would be required to terminate event. This ATWT case bounds the ATWT case assuming a PMS common cause failure (which only credits DAS protection functions). ATWT core cooling is aided by steam relief from the RCS via the safety relief valves and from the secondary loop via the steam generator PORVs.	Mode 1 is discussed in Section 9.2.3, "Turbine Trip".
							PMS(A,C1) – Low-2 Cold Leg Temperature	CMT(C1) CI(C1)		
							PMS(A,C1) – High-2 Containment Pressure	PCS(C1)		
					DAS(A,C2) - High Hot Leg Temperature	Rod MG Set breakers (C2)	N/A	ACCUM(C1)		
							DAS(M,C2)	ADS(C1) IRWST(C1) RECIRC(C1)		
							DAS(A,C2) - High Containment Temperature	PCS(C1) CI(C1)		
					DAS(A,C2)- High Hot Leg Temperature	Rods fail to insert	PMS(A,C2) – Low-2 SG NR Level coincident with Low-2 SFW flow	PRHR(C1)		
							DAS(A,C2) - Low-2 SG WR Level	CMTC1)		
							PMS(A,C1) – High-2 Containment Temperature	PCS(C1) CI(C1)		
1.12.9	Loss of load and turbine trip	None, turbine already tripped.	N/A	3-6	N/A				N/A	Modes 2, 3, 4, 5, and 6 are discussed in Section 9.8.4.2.1, "Loss of Load and Turbine Trip".
1.12.10	Not Used									
1.12.11	Reactor trip – spurious, or initiated by human error, or in response to progression of fault sequences initiated by events identified elsewhere in this list.	Increase in reactor fuel and coolant temperatures and coolant pressure.	<1E00 per reactor year DB2	1-2	Spurious Reactor Trip		See Comments		Same Mitigation SSCs as frequent fault Loss of Load / Turbine Trip (Fault 1.12.8)This fault is not applicable to Modes 3, 4, 5 and 6 since the reactor is already tripped.	See Section 9.2.3, "Turbine Trip".

Table 8A-2 AP1000 PCSR Composite Fault List for Reactor Internal and Non-internal Events and Internal and External Hazards (cont.)

Fault ID	Initiating Event		Initiating Event Frequency/ DB Class	Possible Modes Affected	Engineered Safety Functions				Comments	Further Assessment of Fault
					Reactivity Control(short term)		Safety Functions			
	Fault	Consequences			Signals	Devices	Signals	Devices		
1.13 Loss of RCS Flow										
1.13.1	Partial loss of forced reactor coolant flow	Increase in reactor fuel and coolant temperatures and coolant pressure	1.7E-02 per reactor year DB2	1-2	PMS(A,C1) – Low-2 RCS Flow	Rod Breakers (C1)	PMS(A,C1) – Low-2 SG NR Level coincident with Low-2 SFW flow	PRHR(C1)	The IEF presented is the failure of power supply to the RCPs and includes a number of initiating events resulting in a loss of flow and covers faults such as a loss of component cooling. Partial loss of forced reactor coolant flow is due to: failure of power supply to the RCP, random failure of pump variable speed controller, flow blockage, pumps cavitation during startup, or operator error. Pressuriser safety valve is credited in the analysis for reactor coolant system pressure control. Anticipated transient without trip (ATWT) partial loss of forced reactor coolant flow is bounded by ATWT loss of normal feedwater (Fault 1.16.1) for peak RCS pressure and by ATWT complete loss of forced reactor coolant flow (Fault 1.13.1a) for core damage. ESF systems available for this event are reported; however, limiting ATWT reaches safe stable steady-state condition but a manual action would be required to terminate event.	Modes 1 and 2 are discussed in Section 9.3.1, "Partial Loss of Forced Reactor Coolant Flow".
							PMS(A,C1) – Low-2 Cold Leg Temperature	CMT(C1) CI(C1)		
							PMS(A,C1) – High-2 Containment Pressure	PCS(C1)		
					DAS(A,C2)- High Hot Leg Temperature	Rod MG Set breakers (C2)	N/A	ACCUM(C1)		
							DAS(M,C2)	ADS(C1) IRWST(C1) RECIRC(C1)		
							DAS(A,C2) - High Containment Temperature	PCS(C1) CI(C1)		
					DAS(A,C2)- High Hot Leg Temperature	Rods fail to insert	DAS(A,C2) - High Hot Leg Temperature	PRHR(C1)		
							DAS(A,C2) – Low-2 SG WR Level	CMT(C1)		
							DAS(A,C2) - High Containment Temperature	PCS(C1) CI(C1)		
1.13.1a	Complete loss of forced reactor coolant flow	Increase in reactor fuel and coolant temperatures and coolant pressure.	1.7E-02 per reactor year DB2	1-2	PMS(A,C1) – Low-2 RCP Speed	Rod Breakers (C1)	PMS(A,C1) – Low-2 SG NR Level coincident with Low-2 SFW flow	PRHR(C1)	The IEF presented is the failure of power supply to the RCPs and includes a number of initiating events resulting in a loss of flow and covers faults such as a loss of component cooling. Complete loss of forced reactor coolant flow is due to: maintenance or operator error, loss of electrical supply, common cause failure of pump bearings due to gas build-up during startup. Pressuriser safety valve is credited in the analysis for reactor coolant system pressure control. Two diverse cases listed. First one is for core cooling. Second one is for Anticipated transient without trip (ATWT). ATWT complete loss of forced reactor coolant flow is bounded by ATWT loss of normal feedwater (Fault 1.16.1) for peak RCS pressure and is the limiting ATWT event for core damage. ESF systems available for this event are reported; however, limiting ATWT case does not credit trip rod cluster control assembly (RCCA) insertion or actuation of PRHR and CMT. As discussed in Section 9.3.2.3.1.3, the DAS trip on High hot leg temperature initiates a turbine trip, with a consequent reduction in reactivity for this case. The plant reaches safe stable steady-state condition and manual action would be required to terminate event.	Modes 1 and 2 are discussed in Section 9.3.2, "Complete Loss of Forced Reactor Coolant Flow".
							PMS(A,C1) – Low-2 Cold Leg Temperature	CMT(C1) CI(C1)		
							PMS(A,C1) – High-2 Containment Pressure	PCS(C1)		
					DAS(A,C2)- High Hot Leg Temperature	Rod MG Set breakers (C2)	N/A	ACCUM(C1)		
							DAS(M,C2)	ADS(C1) IRWST(C1) RECIRC(C1)		
							DAS(A,C2) - High Containment Temperature	PCS(C1) CI(C1)		
					DAS(A,C2) - High Hot Leg Temperature	Rods fail to insert	DAS(A,C2) - High Hot Leg Temperature	PRHR(C1)		
							DAS(A,C2) – Low-2 SG WR Level	CMT(C1)		
							DAS(A,C2) - High Containment Temperature	PCS(C1) CI(C1)		

Table 8A-2 AP1000 PCSR Composite Fault List for Reactor Internal and Non-internal Events and Internal and External Hazards (cont.)

Fault ID	Initiating Event		Initiating Event Frequency/ DB Class	Possible Modes Affected	Engineered Safety Functions				Comments	Further Assessment of Fault
					Reactivity Control(short term)		Safety Functions			
	Fault	Consequences			Signals	Devices	Signals	Devices		
1.13.2	Partial and complete loss of forced RCS flow	None	N/A	3-5 with RCS Intact	N/A				Below Mode 2, forced RCS flow is not needed because margin to departure from nucleate boiling (DNB) is not an issue	Modes 3, 4 and 5 are discussed in Section 9.8.4.3.1, "Partial and Complete Loss of Forced RCS Flow".
1.13.3	Partial and complete loss of forced RCS flow	None	N/A	5 with RCS Open, 6	N/A				RCP's are not running in these modes.	N/A
1.13.4 – 1.13.10	Not Used									
1.13.11	Reactor coolant pump shaft seizure (Locked Rotor)	Pump flywheel and shaft would be disengaged from the shaft and the motor is assumed to continue running. Rapid reduction in flow, resulting in reactor trip on low flow signal. Combine with 1.13.12 if possible.	<1E-04 per reactor year DB1	1-2	PMS(A,C1) – Low-2 RCS Flow	Rod Breakers (C1)	PMS(A,C1) – Low-2 SG NR Level coincident with Low-2 SFW flow	PRHR(C1)	Since the initial rate of reduction of coolant flow is greater for the reactor coolant pump rotor seizure event, this is taken to be the most limiting fault condition for mechanical failure of an RCP. Pressuriser safety valve is credited in the analysis for reactor coolant system pressure control. This event at any shutdown mode is less limiting than the at-power conditions for which a DB is analysed.	Modes 1 and 2 are discussed in Section 9.3.3, "Reactor Coolant Pump Shaft Seizure (Locked Rotor)". Mode 2 is discussed in Section 9.8.4.3.2, " Reactor Coolant Pump Shaft Seizure or Break ".
							PMS(A,C1) – Low-2 Cold Leg Temperature	CMT(C1) CI(C1)		
							PMS(A,C1) – High-2 Containment Pressure	PCS(C1)		
1.13.11a	Reactor coolant pump shaft seizure (Locked Rotor)	Pump flywheel and shaft would be disengaged from the shaft and the motor is assumed to continue running. Rapid reduction in flow, resulting in reactor trip on low flow signal.	N/A	3-6	N/A				This event at any shutdown mode is less limiting than the at-power conditions for which a DB is analysed. RCPs are not operated in Mode 6.	Modes 3, 4, 5, and 6 are discussed in Section 9.8.4.3.2, " Reactor Coolant Pump Shaft Seizure or Break ".
1.13.12	Reactor Coolant Pump Shaft Break	Impeller is assumed to be free to rotate. Flow through affected loop is rapidly reduced.	<1E-04 per reactor year DB1	1-2	PMS(A,C1) – Low-2 RCS Flow	Rod Breakers (C1)	PMS(A,C1) – Low-2 SG NR Level coincident with Low-2 SFW flow	PRHR(C1)	This event at any shutdown mode is less limiting than the at-power conditions for which a DB is analysed.	Modes 1 and 2 are discussed in Section 9.3.4, "Reactor Coolant Pump Shaft Break".
							PMS(A,C1) – Low-2 Cold Leg Temperature	CMT(C1) CI(C1)		
							PMS(A,C1) – High-2 Containment Pressure	PCS(C1)		
1.13.12a	Reactor Coolant Pump Shaft Break	Impeller is assumed to be free to rotate. Flow through affected loop is rapidly reduced.	N/A	3-6	N/A				This event at any shutdown mode is less limiting than the at-power conditions for which a DB is analysed. RCPs are not operated in Mode 6.	Modes 3, 4, 5, and 6 are discussed in Section 9.8.4.3.2, " Reactor Coolant Pump Shaft Seizure or Break ".

Table 8A-2 AP1000 PCSR Composite Fault List for Reactor Internal and Non-internal Events and Internal and External Hazards (cont.)

Fault ID	Initiating Event		Initiating Event Frequency/ DB Class	Possible Modes Affected	Engineered Safety Functions				Comments	Further Assessment of Fault
					Reactivity Control(short term)		Safety Functions			
	Fault	Consequences			Signals	Devices	Signals	Devices		
1.15 Core Power Excursions										
1.15.1	Uncontrolled rod cluster control assembly bank withdrawal from a subcritical or low-power startup condition	Uncontrolled addition of reactivity to the reactor core.	<1E-02 per reactor year DB2	2	PMS(A,C1) – Power Range High Neutron Flux (low setting)	Rod Breakers (C1)	PMS(A,C1) – Low-2 SG NR Level coincident with Low-2 SFW flow	PRHR(C1)	The ATWT uncontrolled RCCA withdrawal from sub-critical or low power condition is bounded by RCCA withdrawal at power (Fault 1.15.4).	Mode 2 is discussed in Section 9.4.1, "Uncontrolled Rod Cluster Control Assembly Bank Withdrawal from a Subcritical or Low-Power Startup Condition".
							PMS(A,C1) – Low-2 Cold Leg Temperature	CMT(C1) CI(C1)		
							PMS(A,C1) – High-2 Containment Pressure	PCS(C1)		
					DAS(A,C2) – High Hot Leg Temperature	Rod MG Set breakers (C2)	N/A	ACCUM(C1)		
							DAS(M,C2)	ADS(C1) IRWST(C1) RECIRC(C1)		
							DAS(A,C2) - High Containment Temperature	PCS(C1) CI(C1)		
1.15.2	Uncontrolled rod cluster control assembly bank withdrawal from a subcritical or low-power startup condition	Uncontrolled addition of reactivity to the reactor core.	<1E-02 per reactor year DB2	3-5	PMS(A,C1) – Power Range High Neutron Flux (low setting)	Rod Breakers (C1)	PMS(A,C1) – Low-2 SG NR Level coincident with Low-2 SFW flow	PRHR(C1)	The limiting case is initiated from shutdown with rods already inserted, which produces minimum initial shutdown. Note that rods are already inserted at the beginning of the event for lower modes; event is caused from a withdrawal of an assembly bank which would be stopped by reactor trip.	Modes 3, 4, and 5 are discussed in Section 9.8.4.4.1, "Uncontrolled RCCA Bank Withdrawal from a Subcritical Condition".
							PMS(A,C1) – Low-2 Cold Leg Temperature	CMT(C1) CI(C1)		
							PMS(A,C1) – High-2 Containment Pressure	PCS(C1)		
					DAS(A,C1) – High Hot Leg Temperature	Rod MG Set breakers (C2)	DAS(M,C2)	ADS(C1) IRWST(C1) RECIRC(C1)		
							DAS(A,C2) - High Containment Temperature	PCS(C1) CI(C1)		
1.15.3	Uncontrolled rod cluster control assembly bank withdrawal from a subcritical or low-power startup condition	None	N/A	6	N/A	Rods already inserted	N/A		Rod control is not applicable in Mode 6.	Modes 3, 4, and 5 are discussed in Section 9.8.4.4.1, "Uncontrolled RCCA Bank Withdrawal from a Subcritical Condition".

Table 8A-2 AP1000 PCSR Composite Fault List for Reactor Internal and Non-internal Events and Internal and External Hazards (cont.)

Fault ID	Initiating Event		Initiating Event Frequency/ DB Class	Possible Modes Affected	Engineered Safety Functions				Comments	Further Assessment of Fault
					Reactivity Control(short term)		Safety Functions			
	Fault	Consequences			Signals	Devices	Signals	Devices		
1.15.4	Uncontrolled rod cluster control assembly bank withdrawal at power	Increase in core heat flux and reactor coolant temperature.	<1E-02 per reactor year DB2	1	PMS(A,C1) – OTΔT or OPΔT or High Power Range Positive Flux Rate	Rod Breakers (A,C1)	PMS(A,C1) – Low-2 SG NR Level coincident with Low-2 SFW flow	PRHR(C1)	Bounding case is taken to be the uncontrolled withdrawal of a single RCCA when the reactor is operating at power. Two diverse cases listed. First one is for core cooling. Second one is for Anticipated transient without trip (ATWT). ATWT RCCA withdrawal at power is bounded by ATWT loss of normal feedwater (Fault 1.16.1) for peak RCS pressure and by ATWT complete loss of flow (Fault 1.13.1a) for core damage. ATWT Safety functions available for this event are reported; however, limiting ATWT case terminates event after DAS reactor trip.	Mode 1 is discussed in Section 9.4.2, "Uncontrolled Rod Cluster Control Assembly Bank Withdrawal at Power". Not applicable by definition in Modes 2, 3, 4, 5, and 6.
							PMS(A,C1) – Low-2 Cold Leg Temperature	CMT(C1) CI(C1)		
							PMS(A,C1) – High-2 Containment Pressure	PCS(C1)		
					DAS(A,C2) – High Hot Leg Temperature	Rod MG Set breakers (C2)	N/A	ACCUM(C1)		
							DAS(M,C2)	ADS(C1) IRWST(C1) RECIRC(C1)		
							DAS(A,C2) - High Containment Temperature	PCS(C1) CI(C1)		
					DAS(A,C2) – High Hot Leg Temperature	Rod MG Set breakers (C2)	DAS(A,C2) - High Hot Leg Temperature	PRHR (C1)		
							DAS(A,C2) - Low-2 SG WR Level	CMT (C1)		
							DAS(A,C2) - High Containment Temperature	PCS (C1) CI(C1)		
1.15.5	Rod cluster control assembly misalignment due to system malfunction or operator error (Statically Misaligned RCCA)	Altered radial and axial power distribution.	<1E-02 per reactor year DB2	1	N/A (See Comments)				The most severe static misalignments do not require any automatic mitigation as DNB would not be reached; thus, no SSCs are credited. Following the identification of an RCCA group misalignment condition by the operator, they would take action as required by the plant Technical Specifications and operating instruction to restore the plant to an acceptable condition.	Mode 1 is discussed in Section 9.4.3, "Rod Cluster Control Assembly Misalignment (System Malfunction or Operator Error)".
1.15.5a	Rod cluster control assembly misalignment due to system malfunction or operator error (Dropped RCCA or RCCA Bank)	Rod control system response leads to power overshoot and adverse power shapes in the core.	<1E-02 per reactor year DB2	1	PMS(A,C1) – Low-2 Pressuriser Pressure	Rod Breakers (C1)	PMS(A,C1) – Low-2 SG NR Level coincident with Low-2 SFW flow	PRHR(C1)	The ATWT diversity case did not credit reactor trip or function of the P-17 rod block function. It concludes that ATWT acceptance criteria are met for all feasible scenarios. Since ATWT diversity case reaches safe stable steady-state condition, no engineered safety functions are specified. Operator action would be required to terminate the event.	Mode 1 is discussed in Section 9.4.3, "Rod Cluster Control Assembly Misalignment (System Malfunction or Operator Error)".
							PMS(A,C1) – Low-2 Cold Leg Temperature	CMT(C1) CI(C1)		
							PMS(A,C1) – High-2 Containment Pressure	PCS(C1)		
					Not Credited (See Comments)		N/A	ACCUM(C1)		
							DAS(M,C2)	ADS(C1) IRWST(C1) RECIRC(C1)		
							DAS(A,C2) - High Containment Temperature	PCS(C1) CI(C1)		

Table 8A-2 AP1000 PCSR Composite Fault List for Reactor Internal and Non-internal Events and Internal and External Hazards (cont.)

Fault ID	Initiating Event		Initiating Event Frequency/ DB Class	Possible Modes Affected	Engineered Safety Functions				Comments	Further Assessment of Fault
					Reactivity Control(short term)		Safety Functions			
	Fault	Consequences			Signals	Devices	Signals	Devices		
1.15.5b	Rod cluster control assembly misalignment due to system malfunction or operator error (Single rod cluster control assembly withdrawal)	Increase in core power and reactor coolant temperature leads to DNB and core damage.	<1E-04 per reactor year DB1	1-2	PMS(A,C1) - Low-2 Pressuriser Pressure or OTΔT	Rod Breakers (C1)	PMS(A,C1) – Low-2 SG NR Level coincident with Low-2 SFW flow	PRHR(C1)	A more realistic initiating event frequency of less than 1E-04 events per year is assumed for this fault and not determined by PSA. Multiple failures (either electrical or operator error) would be required for single RCCA withdrawal. This frequency is estimated based on the probability of an open wire (or terminal) failure being 1.6E-08 faults per hour per MIL-HDBK-217F, which can be converted to 1.4E-04 events per year. Additional coincident failures (electrical or operator detection based) would be required, and as such those would drop the frequency below 1E-04 and therefore make this event an infrequent fault, classified as a DB1 fault. A Mode 2 event is less limiting than the at-power conditions for which a DB is analysed.	Mode 1 is discussed in Section 9.4.3, "Rod Cluster Control Assembly Misalignment (System Malfunction or Operator Error)".
							PMS(A,C1) – Low-2 Cold Leg Temperature	CMT(C1) CI(C1)		
							PMS(A,C1) – High-2 Containment Pressure	PCS(C1)		
1.15.5c	Rod cluster control assembly misalignment due to system malfunction or operator error (all types)	N/A	N/A	2-6	N/A				Misaligned RCCAs have no effect in the absence of a critical neutron flux and are not a concern below Mode 2. Mode 2 for Fault 1.15.15b addressed by that fault entry.	Modes 2, 3, 4, 5, and 6 are discussed in Section 9.8.4.4.3, "RCCA Misalignment".
1.15.6	Startup of an inactive reactor coolant pump at an incorrect temperature	Cooler water entering core could lead to insertion of positive reactivity.	N/A	N/A	N/A				The Technical Specifications require all RCPs to be operating while the plant is in operating modes 1 and 2. For lower modes, the reactor will initially be subcritical. There will be no increase in core power and therefore no protective action is required.	Modes 1 and 2 are discussed in Section 9.4.4, "Startup of an Inactive Reactor Coolant Pump at an Incorrect Temperature". Modes 3, 4, 5, and 6 are discussed in Section 9.8.4.4.4, "Startup of an Inactive Reactor Coolant Pump at an Incorrect Temperature".
1.15.7	Chemical and volume control system malfunction that results in a decrease in the boron concentration in the reactor coolant	Insertion of positive reactivity to the core.	<1E-02 per reactor year DB2	1-2	PMS(A,C1) – OTΔT or High Source Range Neutron Flux	Rod Breakers (C1) and Isolation of dilution sources (C1)	PMS(A,C1) – Low-2 SG NR level coincident with Low-2 SFW flow	PRHR(C1)	Boron dilution can be due to controller, operator, or mechanical failure of CVS. Two diverse cases listed. First one is for core cooling. Second one is for Anticipated transient without trip (ATWT). The limiting ATWT boron dilution event is presented here. In some analysed scenarios, manual action would be required to terminate the boron dilution event (isolate dilution source). In addition, CMT manual actuation is available for mechanical failures that prohibit rod insertion.	Modes 1, 2, 3, 4, and 5 are discussed in Section 9.4.6, "Chemical and Volume Control System Malfunction that Results in a Decrease in the Boron Concentration in the Reactor Coolant".
							PMS(A,C1) – Low-2 Cold Leg Temperature	CMT(C1) CI(C1)		
							PMS(A,C1) – High-2 Containment Pressure	PCS(C1)		
					DAS(A,C2) – High Hot Leg Temperature	Rod MG Set breakers (C2)	N/A	ACCUM(C1)		
							DAS(M,C2)	ADS(C1) IRWST(C1) RECIRC(C1)		
							DAS(A,C2) - High Containment Temperature	PCS(C1) CI(C1)		
					DAS(A,C2) – High Hot Leg Temperature	Rods fail to insert	DAS(A,C2) - High Hot Leg Temperature	PRHR(C1)		
					PMS(A,C1) – OTΔT	Isolation of dilution sources (C1)	DAS(A,C2) - High Containment Temperature	PCS(C1) CI(C1)		

Table 8A-2 AP1000 PCSR Composite Fault List for Reactor Internal and Non-internal Events and Internal and External Hazards (cont.)

Fault ID	Initiating Event		Initiating Event Frequency/ DB Class	Possible Modes Affected	Engineered Safety Functions				Comments	Further Assessment of Fault
					Reactivity Control(short term)		Safety Functions			
	Fault	Consequences			Signals	Devices	Signals	Devices		
1.15.8	Chemical and volume control system malfunction that results in a decrease in the boron concentration in the reactor coolant	Insertion of positive reactivity to the core.	<1E-02 per reactor year DB2	3-5	N/A	Rods Already Inserted	N/A		Three diverse cases listed. First one is for core cooling. Second one is for ATWT. The third one is for a Xenon decay transient. The limiting ATWT boron dilution event assuming common cause PMS failure is presented here. For all cases, the DAS Intermediate Range trip results in isolation of CVS and RNS and trip of RCPs in addition to CMT actuation. These actions have been shown to be adequate to prevent core power reaching the point of adding heat. As noted in section 9.4.6.3.1.3.2, simplified boron dilution calculations have shown that cases with only RNS pumps operating are not as challenging as cases with the RCPs running. Results reported apply to cases with RCPs running.	Modes 1, 2, 3, 4, and 5 are discussed in Section 9.4.6, "Chemical and Volume Control System Malfunction that Results in a Decrease in the Boron Concentration in the Reactor Coolant".
					PMS(A,C1) – High source range neutron flux	Isolation of dilution sources (C1)				
					PMS(A,C1) - Flux Doubling	Isolation of dilution sources (C1)	PMS(A,C1) – Low-2 Cold Leg Temperature	CMT(C1) CI(C1)		
							PMS(A,C1) – High-2 Containment Pressure	PCS(C1)		
					DAS (A, C2) – High Intermediate Range Nuclear Detector	Isolation of dilution sources (C1)	N/A	ACCUM(C1)		
							DAS(M,C2)	ADS(C1) IRWST(C1) RECIRC(C1)		
							DAS(A,C2)- High Containment Temperature	PCS(C1) CI(C1)		
					DAS (A, C2) – High Intermediate Range Nuclear Power	Isolation of dilution sources (C1) Rod MG Set breakers (C2)	DAS(A, C2) – High Intermediate Range Nuclear Detector	CMT(C1) RNS isolation (C1)		
1.15.9	Chemical and volume control system malfunction that results in a decrease in the boron concentration in the reactor coolant	N/A	N/A	6	N/A				Boron dilution transient cannot occur during mode 6 due to administrative controls.	Mode 6 is discussed in Section 9.4.6, "Chemical and Volume Control System Malfunction that Results in a Decrease in the Boron Concentration in the Reactor Coolant" and 9.8.4.4.5, "Chemical and Volume Control System Malfunction that Results in a Decrease in the Boron Concentration in the Reactor Coolant".
1.15.10	Inadvertent loading and operation of a fuel assembly in an improper position	Increased heat fluxes in the core.	DB0	1-6	N/A				In the unlikely event that a loading error occurs, analyses confirm that resulting power distribution effects are either readily detected by the online core monitoring system prior to reaching full power, or cause a sufficiently small perturbation to be acceptable within the uncertainties allowed between nominal and design power shapes. This event is not applicable in the subcritical modes, Modes 3 through 6.	Modes 1 and 2 are discussed in Section 9.4.7, "Inadvertent Loading and Operation of a Fuel Assembly in an Improper Position". Modes 3, 4, 5, and 6 are discussed in Section 9.8.4.4.6, "Inadvertent Loading of a Fuel Assembly in an Improper Position".

Table 8A-2 AP1000 PCSR Composite Fault List for Reactor Internal and Non-internal Events and Internal and External Hazards (cont.)

Fault ID	Initiating Event		Initiating Event Frequency/ DB Class	Possible Modes Affected	Engineered Safety Functions				Comments	Further Assessment of Fault
					Reactivity Control(short term)		Safety Functions			
	Fault	Consequences			Signals	Devices	Signals	Devices		
1.15.11	Spectrum of rod cluster control assembly ejection accidents	Rapid reactivity insertion causing a rapid rise in the reactor power, which would also cause a breach in the RCS pressure boundary resulting in a subsequent depressurisation and loss of reactor coolant.	<1E-04 per reactor year DB1	1-2	PMS(A, C1) – High Power Range Positive Flux Rate	Rod Breakers (C1)	PMS(A,C1) – Low-2 SG NR Level coincident with Low-2 SFW flow	PRHR(C1)	While the group comprises a single fault, the ejection of an RCCA assembly form the core, analysis has been performed to establish the most limiting conditions for the fault. Pressuriser safety valve is credited in the analysis for reactor coolant system pressure control.	Modes 1 and 2 are discussed in Section 9.4.8, "Spectrum of Rod Cluster Control Assembly Ejection Accidents".
							PMS(A,C1) – Low-2 Cold Leg Temperature	CMT(C1) CI(C1)		
							PMS(A,C1) – Low CMT Level	ADS(C1)		
							N/A	ACCUM(C1)		
							PMS(A,C1) – Low CMT Level	IRWST(C1)		
							PMS(A,C1) – Low IRWST Level	RECIRC(C1)		
							PMS(A,C1) – High-2 Containment Pressure	PCS(C1)		
1.15.12	Spectrum of rod cluster control assembly ejection accidents	Loss of coolant with a subsequent de-pressurisation of the RCS and pressure decrease in the pressuriser.	2.5E-05 per reactor year DB1	3-6	N/A				In the lower modes (3 and lower), there is not enough reactivity in a single rod that, if ejected, would cause the reactor to go critical. Rod ejection then becomes a small LOCA. See Fault 1.8.3 to 1.8.4.	Modes 3, 4, 5, and 6 are discussed in Section 9.8.4.4.7, "RCCA Ejection".
1.15.13	Feedwater system malfunctions that result in a decrease in feed water temperature	Reductions in feedwater temperature cause an increase in core power by decreasing reactor coolant temperature.	>1E-03 per reactor year DB2	1-5 with RCS Intact	Not Credited (See Comments)		PMS(A,C1) – Low-2 SG NR Level coincident with Low-2 SFW flow	PRHR(C1)	The behaviour and consequences of this fault are bounded by the 1.15.18 (Excessive load Increase). It is noted that the bounding DBA (Fault 1.15.18) does not produce a reactor trip but stabilizes in safe condition. Two diverse cases listed. First one is for core cooling. Second one is for ATWT. The ATWT result is bounded by ATWT loss of normal feedwater (Fault 1.16.1) for peak RCS pressure and by ATWT complete loss of flow (Fault 1.13.1a) for core damage. ATWT systems available for this event are reported; however, limiting ATWT case reaches safe stable steady-state condition but manual operator action would be required to end the transient.	Modes 1 and 2 are discussed in Section 9.1.1, "Feedwater System Malfunctions that Result in a Decrease in Feedwater Temperature" and Modes 3 and 4 are discussed in Section 9.8.4.1.1, "Feedwater System Malfunctions Which Increase Heat Removal from the Primary System"
							PMS(A,C1) – Low-2 Cold Leg Temperature	CMT(C1) CI(C1)		
							PMS(A,C1) – High-2 Containment Pressure	PCS(C1)		
					DAS(A,C2) - Pressuriser Level	Rod MG Set breakers (C2)	N/A	ACCUM(C1)		
							DAS(M,C2)	ADS(C1) IRWST(C1) RECIRC(C1)		
							DAS(A,C2) - High Containment Temperature	PCS(C1) CI(C1)		
					DAS(A,C2) - High Hot Leg Temperature	Rod MG Set breakers (C2)	DAS(A,C2) - High Hot Leg Temperature	PRHR(C1)		
							DAS(A,C2) - Low-2 SG WR Level	CMTC1)		
							DAS(A,C2) - High Containment Temperature	PCS(C1) CI(C1)		
1.15.13a	Feedwater system malfunctions that result in a decrease in feed water temperature	Reductions in feedwater temperature cause an increase in core power by decreasing reactor coolant temperature.	N/A	5 with RCS Open, 6	N/A				RCS is borated and effectively isolated for secondary system in Modes 5 and 6 that such a cooldown-induced power excursion cannot be postulated.	Modes 5 and 6 are discussed in Section 9.8.4.1.1, "Feedwater System Malfunctions Which Increase Heat Removal from the Primary System"

Table 8A-2 AP1000 PCSR Composite Fault List for Reactor Internal and Non-internal Events and Internal and External Hazards (cont.)

Fault ID	Initiating Event		Initiating Event Frequency/ DB Class	Possible Modes Affected	Engineered Safety Functions				Comments	Further Assessment of Fault
					Reactivity Control(short term)		Safety Functions			
	Fault	Consequences			Signals	Devices	Signals	Devices		
1.15.14	Feedwater system malfunctions that result in an increase in feed water flow	Increase in feedwater flow causes an increase in core power by decreasing reactor coolant temperature.	>1E-03 per reactor year DB2	1-5 with RCS Intact	PMS(A,C1) – High-3 SG NR Level	Rod breakers (C1)	PMS(A,C1) – Low-2 SG NR Level coincident with Low-2 SFW flow	PRHR(C1)	Two diverse cases listed. First one is for core cooling. Second one is for ATWT. The ATWT result is bounded by ATWT loss of normal feedwater (Fault 1.16.1) for peak RCS pressure and by ATWT complete loss of flow (Fault 1.13.1a) for core damage. ATWT systems available for this event are reported; however, limiting ATWT case would transition to the loss of normal feedwater upon turbine trip for high SG level.	Modes 1 and 2 are discussed in Section 9.1.2, "Feedwater System Malfunctions that Result in an Increase in Feedwater Flow" and Modes 3and 4 are discussed in Section 9.8.4.1.1, "Feedwater System Malfunctions Which Increase Heat Removal from the Primary System"
							PMS(A,C1) – Low-2 Cold Leg Temperature	CMT(C1) CI(C1)		
							PMS(A,C1) - High-3 SG NR Level	MFIVs(C1) (Feedwater Isolation Valves)		
							PMS(A,C1) – High-2 Containment Pressure	PCS(C1)		
					DAS(A,C2) - Low-2 SG WR Level	Rod MG Set breakers (C2)	N/A	ACCUM(C1)		
							DAS(M,C2)	ADS(C1) IRWST(C1) RECIRC(C1)		
							DAS(A,C2) - High Containment Temperature	PCS(C1) CI(C1)		
					DAS(A,C2) - High Hot Leg Temperature	Rods fail to insert	PMS(A,C2) - Low-2 SG NR Level coincident with Low-2 SFW flow	PRHR(C1)		
							DAS(A,C2) – Low-2 SG WR Level	CMT(C1)		
							PMS(A,C2) – High-2 Containment Temperature	PCS(C1) CI(C1)		
1.15.14a	Feedwater system malfunctions that result in an increase in feed water flow	Increase in feedwater flow causes an increase in core power by decreasing reactor coolant temperature.	N/A	5 with RCS Open, 6	N/A				RCS is borated and effectively isolated for secondary system in Modes 5 and 6 that such a cooldown-induced power excursion cannot be postulated.	Modes 5 and 6 are discussed in Section 9.8.4.1.1, "Feedwater System Malfunctions Which Increase Heat Removal from the Primary System"
1.15.15	Inadvertent operation of PRHR heat exchanger	Re-circulation of cooler water back into the RCS causes reactivity insertion.	>1E-03 per reactor year DB2	1-2	PMS(A,C1) – PRHR Valve Position	Rod Breakers (C1)	N/A (Actuation is the Initiating Event)	PRHR(C1)	Two diverse cases listed. First one is for core cooling. Second one is for ATWT. The ATWT result is bounded by ATWT loss of normal feedwater (Fault 1.16.1) for peak RCS pressure and by ATWT complete loss of flow (Fault 1.13.1a) for core damage. ATWT systems available for this event are reported; however, limiting ATWT case reaches safe stable steady-state condition but manual operator action would be required to end the transient. Steamline, feedline, and SFW isolation occurs on Low-2 Cold Leg Temperature “S” signal.	Modes 1 and 2 are discussed in Section 9.1.7, "Inadvertent Operation of the PRHR Heat Exchanger"
							PMS(A,C1) – Low Cold Leg Temperature	CMT(C1) CI(C1)		
							PMS(A,C1) – High Containment Pressure	PCS(A,C1)		
					DAS(A,C2) - Low-2 SG WR Level	Rod MG Set breakers (C2)	N/A	ACCUM(C1)		
							DAS(M,C2)	ADS(C1) IRWST(C1) RECIRC(C1)		
							DAS(A,C2) - High Containment Temperature	PCS(C1) CI(C1)		
					DAS(A,C2)- Low Pressuriser level	Rod MG Set breakers (C2)	DAS(A,C2) - High Hot Leg Temperature	PRHR(C1)		
							DAS(A,C2) -Low Pressuriser level	CMTC1)		
							DAS(A,C2) - High Containment Temperature	PCS(C1) CI(C1)		

Table 8A-2 AP1000 PCSR Composite Fault List for Reactor Internal and Non-internal Events and Internal and External Hazards (cont.)

Fault ID	Initiating Event		Initiating Event Frequency/ DB Class	Possible Modes Affected	Engineered Safety Functions				Comments	Further Assessment of Fault
					Reactivity Control(short term)		Safety Functions			
	Fault	Consequences			Signals	Devices	Signals	Devices		
1.15.16	Inadvertent operation of PRHR heat exchanger	Re-circulation of cooler water back into the RCS causes reactivity insertion.	>1E-03 per reactor year DB2	3-5 with RCS Intact	N/A	Rods already inserted	N/A (Actuation is the Initiating Event)	PRHR(C1)	Steamline isolation also occurs on Low-2 Cold Leg Temperature "S" signal.	Modes 3, 4, 5 are discussed in Section 9.8.4.1.4, "Inadvertent PRHR HX Operation"
							PMS(A,C1) – Low-2 Cold Leg Temperature	CMT(C1) CI(C1)		
							PMS(A,C1) – High Containment Pressure	PCS(A,C1)		
					N/A	Rods already inserted	DAS(M,C2)	ADS(C1) IRWST(C1) RECIRC(C1)		
							DAS(A,C2)- High Containment Temperature	PCS(C1) CI(C1)		
1.15.17	Inadvertent operation of PRHR heat exchanger	None	N/A	5 with RCS Open, 6	N/A				RCS is borated and effectively isolated for secondary system in Modes 5 and 6 that such a cooldown-induced power excursion cannot be postulated.	Modes 5 and 6 are discussed in Section 9.8.4.1.4, "Inadvertent PRHR HX Operation"
1.15.18	Excessive increase in secondary steam flow	Mismatch between reactor core power and steam generator load demand. Cooling of primary circuit by excessive increase in heat removal via secondary side, could cause positive reactivity insertion.	>1E-03 per reactor year DB2	1-5 with RCS Intact	Not Credited (See Comments)		PMS(A,C1) – Low-2 SG NR Level coincident with Low-2 SFW flow	PRHR(C1)	Fault could result from either an administrative violation or an equipment malfunction in the steam dump control or turbine speed control. It is noted that the DBA does not produce a reactor trip but stabilizes in safe condition. Two diverse cases listed. First one is for core cooling. Second one is for ATWT. The ATWT analyses do not credit reactor trip or any other engineered safety functions and demonstrate that coolable core geometry, RCS pressure boundary and containment vessel integrity are demonstrated. The limiting ATWT cases reach stable steady-state condition and manual operator action would be required to end the transient.	Mode 1 is discussed in Section 9.1.3, "Excessive Increase in Secondary Steam Flow" and Modes 2, 3, 4, and 5 are discussed in Section 9.8.4.1.2, "Excessive Increase in Secondary Steam Flow"
							PMS(A,C1) – Low-2 Cold Leg Temperature	CMT(C1) CI(C1)		
							PMS(A,C1) – High-2 Containment Pressure	PCS(C1)		
					DAS(A,C2) - Pressuriser Level	Rod MG Set breakers (C2)	N/A	ACCUM(C1)		
							DAS(M,C2)	ADS(C1) IRWST(C1) RECIRC(C1)		
							DAS(A,C2) - High Containment Temperature	PCS(C1) CI(C1)		
					Not credited (See Comments)		DAS(M,C2)	PRHR(C1) CMTC1) PCS(C1) CI(C1)		
1.15.18a	Excessive increase in secondary steam flow	Mismatch between reactor core power and steam generator load demand. Cooling of primary circuit by excessive increase in heat removal via secondary side, could cause positive reactivity insertion.	N/A	5 with RCS Open, 6	N/A				RCS is borated at modes 5 and 6 that such a cooldown-induced power excursion cannot be postulated.	Modes 5 and 6 are discussed in Section 9.8.4.1.2, "Excessive Increase in Secondary Steam Flow"

Table 8A-2 AP1000 PCSR Composite Fault List for Reactor Internal and Non-internal Events and Internal and External Hazards (cont.)

Fault ID	Initiating Event		Initiating Event Frequency/ DB Class	Possible Modes Affected	Engineered Safety Functions				Comments	Further Assessment of Fault
					Reactivity Control(short term)		Safety Functions			
	Fault	Consequences			Signals	Devices	Signals	Devices		
1.15.19	Failure of the turbine generator casing	Similar to steam line break (Faults 1.21.1 and 1.21.2), steam release from SG leads to heat removal from the RCS and a concomitant reduction in coolant temperature. This cool down causes insertion of positive reactivity.	>1E-03 per reactor year DB2	1-4	PMS(A,C1) – Low-2 Steam Line Pressure	Rod breakers (C1)	PMS(A,C1) – Low-2 SG NR Level	PRHR(C1)	The diversity ATWT case of 1.15.18 "Excessive increase in secondary steam flow" bounds this ATWT case. RCS is borated at modes 5 and 6 that such a cooldown-induced power excursion cannot be postulated.	Fault is mentioned in Section 9.1.0.1, "Increase in Heat Removal Faults (Excluding MSLB)".
							PMS(A,C1) – Low-2 Cold Leg Temperature	CMT(C1) CI(C1)		
							PMS(A,C1) – High-2 Containment Pressure	PCS(C1)		
					DAS(A,C2) - Pressuriser Level	Rod MG Set breakers (C2)	N/A	ACCUM(C1)		
							DAS(M,C2)	ADS(C1) IRWST(C1) RECIRC(C1)		
							DAS(A,C2) - High Containment Temperature	PCS(C1) CI(C1)		
1.15.20	Flooding of water from IRWST causes external cooling of RCS.	Cooling of RCS could cause negative reactivity insertion.	N/A	N/A	N/A				Fault not considered credible. Since the RCS components are thermally insulated, external flooding of the lower RCS components in this event would only cause a slight increase in heat loss from the RCS, and lead to a very minor temperature perturbation.	Fault is not addressed further.
1.15.21	Pump speed fault leading to higher than expected primary coolant flow rate	Excess cooling of RCS could cause positive reactivity insertion.	<1E-02 per reactor year DB2	1-2	Not Credited (See Comments)		PMS(A,C1) – Low-2 SG NR Level coincident with Low-2 SFW flow	PRHR(C1)	This fault is bounded by the excessive load increase fault (Fault 1.15.18). In comparison to the excessive load increase fault, an increase in RCS flow fault would not result in a sustained power demand increase; therefore, any reactor power increase would be transitory (eventually, primary power would match the normal steam load demand). [ ]	Fault is discussed in Section 9.1.0.1, "Increase in Heat Removal Faults (Excluding MSLB)". This fault will be examined in more detail to confirm claims and arguments presented during site licensing.
							PMS(A,C1) – Low-2 Cold Leg Temperature	CMT(C1) CI(C1)		
							PMS(A,C1) – High-2 Containment Pressure	PCS(C1)		
					DAS(A,C2) - Pressuriser Level	Rod MG Set breakers (C2)	N/A	ACCUM(C1)		
							DAS(M,C2)	ADS(C1) IRWST(C1) RECIRC(C1)		
							DAS(A,C2) - High Containment Temperature	PCS(C1) CI(C1)		
					Not credited (See Comments)		DAS(M,C2)	PRHR(C1) CMTC1) PCS(C1) CI(C1)		
1.15.22	Pump speed fault leading to higher than expected primary coolant flow rate	None.	<1E-04 per reactor year DB1	3-5 with RCS Intact	N/A				Due to reactor being shut down and rods inserted upon event initiation, the resultant flow rate increase would not induce any transient requiring protection.	N/A
1.15.23	Pump speed fault leading to higher than expected primary coolant flow rate	None. Pumps are not running in these Modes.	N/A	5 with RCS Open, 6	N/A				RCPs do not operate in these MODEs	N/A

Table 8A-2 AP1000 PCSR Composite Fault List for Reactor Internal and Non-internal Events and Internal and External Hazards (cont.)

Fault ID	Initiating Event		Initiating Event Frequency/ DB Class	Possible Modes Affected	Engineered Safety Functions				Comments	Further Assessment of Fault
					Reactivity Control(short term)		Safety Functions			
	Fault	Consequences			Signals	Devices	Signals	Devices		
1.16 Loss of Feedwater to both SGs										
1.16.1	Loss of normal feedwater flow	Loss of capability to remove heat from reactor core	8.9E-02 per reactor year DB2	1-2	PMS(A,C1) – Low-2 SG NR Level	Rod breakers (C1)	PMS (M,C1) - High-2 Pressuriser Level	Head Vent (C1)	Loss of main feed water to both SGs is due to: flow instability/operator error, steam generator tube blockage or bypass, and mechanical issues. Pressuriser safety valve is credited in the analysis for reactor coolant system pressure control. Two diverse cases listed. First one is for core cooling. Second one is for Anticipated transient without trip (ATWT). ATWT loss of normal feedwater is the limiting ATWT event for peak RCS pressure and is listed here. This event is bounded by ATWT complete loss of flow (Fault 1.13.1a) for core damage.	Modes 1 and 2 are discussed in Section 9.2.7, "Loss of Normal Feedwater Flow"
							PMS(A,C1) – Low-2 SG NR Level coincident with Low-2 SFW flow	PRHR(C1)		
							PMS(A,C1) – Low-2 Cold Leg Temperature	CMT(C1) CI(C1)		
							PMS(A,C1) – High-2 Containment Pressure	PCS(C1)		
					DAS(A,C2) – Low-2 SG WR Level	Rod MG Set breakers (C2)	N/A	ACCUM(C1)		
							DAS(M,C2)	ADS(C1) IRWST(C1) RECIRC(C1)		
							DAS(A,C2) - High Containment Temperature	PCS(C1) CI(C1)		
					DAS(A,C2) - High Hot Leg Temperature	Rods fail to insert	PMS(A,C1) – Low-2 SG NR Level coincident with Low-2 SFW flow	PRHR(C1)		
							DAS(A,C2) – Low-2 SG WR Level	CMT(C1)		
							PMS(A,C1) – High-2 Containment Temperature	PCS(C1) CI(C1)		
1.16.2	Loss of normal feedwater	Loss of capability to remove heat from reactor core.	4.45E-03 per reactor year (See Note 1 in 8A.1) DB2	3-4 before RNS alignment	N/A	Rods already inserted	PMS(A,C1) – Low-2 NR Level coincident with Low-2 SFW flow	PRHR(C1)	Loss of main feed water to both SGs is due to: flow instability/operator error, SGT blockage or bypass, and mechanical issues. Following reactor trip, the PRHR HX is activated for decay heat removal. Automatic PRHR HX actuation on low steam generator level is available in Modes 1 to 3 and in Mode 4 when the RCS is not being cooled by the RNS. Assume here that both accumulators are isolated (at 6.895 MPa) There is no need to consider ATWT event in shutdown, since rods already inserted.	Section 9.8.4.2.3, "Loss of Normal Feedwater"
							PMS(A,C1) – Low-2 Cold Leg Temperature	CMT(C1) CI(C1)		
							PMS(A,C1) – High-2 Containment Pressure	PCS(C1)		
					N/A	Rods already inserted	DAS(M,C2)	ADS(C1) IRWST(C1) RECIRC(C1)		
							DAS(A,C2) - High Containment Temperature	PCS(C1) CI(C1)		
1.16.3	Loss of normal feedwater	N/A	N/A	4 after RNS alignment, 5-6	N/A				In Mode 4 after RNS alignment and Modes 5 and 6, the feedwater system is not used; therefore loss of feedwater events is irrelevant. The corresponding shutdown event is loss of RNS cooling. See fault 2.2.	Modes 3, 4, 5, and 6 are discussed in Section 9.8.4.2.3, "Loss of Normal Feedwater"
1.16.4 – 1.16.6	Not Used									

Table 8A-2 AP1000 PCSR Composite Fault List for Reactor Internal and Non-internal Events and Internal and External Hazards (cont.)

Fault ID	Initiating Event		Initiating Event Frequency/ DB Class	Possible Modes Affected	Engineered Safety Functions				Comments	Further Assessment of Fault
					Reactivity Control(short term)		Safety Functions			
	Fault	Consequences			Signals	Devices	Signals	Devices		
1.16.7	Inadvertent closure of Main Steam Isolation Valves (MSIVs)	Rapid reduction in steam flow from the steam generators and a heat up of the primary side.	>1E-03 per reactor year DB2	1-6	PMS(A,C1) – High-2 Pressuriser Pressure or Overtemperature ΔT or Low-2 RCP speed	Rod breakers (C1)	PMS(A,C1) - Low-2 SG NR level coincident with Low-2 SFW flow	PRHR(C1)	Inadvertent closure of the main steam isolation values leads to a turbine trip with no credit for the turbine bypass system. Main feedwater flow is lost. Bounded by Fault 1.12.8. Two diverse cases listed. First one is for core cooling. Second one is for anticipated transient without trip (ATWT). This fault leads to an ATWT turbine trip (Fault 1.2.8), which is bounded by ATWT loss of normal feedwater (Fault 1.16.1) for peak RCS pressure and by ATWT complete loss of flow (Fault 1.13.1a) for core damage. ATWT systems available for this event are reported; however, limiting ATWT case reaches safe stable steady-state condition but a manual action would be required to terminate event. Event in Modes 2, 3, or 4 are bounded by Fault 1.12.8 at full power. In Modes 5 and 6, the event is not applicable.	Mode 1 is discussed in Section 9.2.4, "Inadvertent Closure of Main Steam Isolation Valves" and Modes 2 through 6 are discussed in Section 9.8.4.2.1, "Loss of Load, Turbine Trip, Inadvertent MSIV closure, and Loss of Condenser Vacuum"
							PMS(A,C1) – Low-2 Cold Leg Temperature	CMT(C1) CI(C1)		
							PMS(A,C1) – High-2 Containment Pressure	PCS(C1)		
					DAS(A,C2) - High Hot Leg Temperature	Rod MG Set breakers (C2)	N/A	ACCUM(C1)		
							DAS(M,C2)	ADS(C1) IRWST(C1) RECIRC(C1)		
							DAS(A,C2) - High Containment Temperature	PCS(C1)		
					DAS(A,C2) - High Hot Leg Temperature	Rods fail to insert	PMS(A,C2) – Low-2 SG NR Level coincident with Low-2 SFW flow	PRHR(C1)		
							DAS(A,C2) - Low-2 SG WR Level	CMTC1)		
							PMS(A,C1) – High-2 Containment Temperature	PCS(C1) CI(C1)		
1.16.8	Feedwater system pipe break	Loss of feedwater flow to both SGs with blowdown of faulted SG after reactor trip.	6.6E-04 per reactor year DBL/DB1	1-2	PMS(A,C1) – Low-2 SG NR Level	Rod breakers (C1)	PMS(A,C1) – Low-2 SG NR Level	PRHR(C1)	The IEF presented is documented in LTR-AP1000-PRA-16-041. This fault represents a non-isolatable break. Isolatable feedline breaks are included in fault 1.16.1. The DBL class applies to the larger breaks in the spectrum, up to full double ended breaks. Smaller break sizes would be in the DB1 class; however, the credited mitigation equipment and limiting DB analysis presented would bound all break sizes. The following worst limiting case is considered. After reactor trip, a full double-ended rupture of the feed water line is assumed between the check valve and the SG such that the faulted steam generator blows down through the break and no main feed water is delivered to the intact steam generator. Pressuriser safety valve is credited in the analysis for reactor coolant system pressure control.	Modes 1 and 2 are discussed in Section 9.2.8, "Feedwater System Pipe Break"
							PMS(A,C1) – Low-2 Steamline Pressure	CMT(C1) CI(C1)		
							PMS(A,C1) – High-2 Containment Pressure	PCS(C1)		
1.16.9	Feedwater system pipe break	Loss of feedwater flow to both SGs.	3.3E-05 per reactor year (See Note 1 in 8A.1) DBL/DB1	3-4 before RNS alignment	N/A	Rods already inserted	PMS(A,C1) – Low-2 SG NR Level	PRHR(C1)	This fault represents a non-isolatable break. Isolatable feedline breaks are included in fault 1.16.2. The DBL class applies to the larger breaks in the spectrum, up to full double ended breaks. Smaller break sizes would be in the DB1 class; however, the credited mitigation equipment and evaluation presented would bound all break sizes.	Modes 3, 4, 5, and 6 are discussed in Section 9.8.4.2.4, "Feedwater System Pipe Break"
							PMS(A,C1) – Low-2 Steamline Pressure	CMT(C1) CI(C1)		
							PMS(A,C1) – High-2 Containment Pressure	PCS(C1)		

Table 8A-2 AP1000 PCSR Composite Fault List for Reactor Internal and Non-internal Events and Internal and External Hazards (cont.)

Fault ID	Initiating Event		Initiating Event Frequency/ DB Class	Possible Modes Affected	Engineered Safety Functions				Comments	Further Assessment of Fault
	Fault	Consequences			Reactivity Control(short term)		Safety Functions			
					Signals	Devices	Signals	Devices		
1.16.10	Feedwater system pipe break	N/A	N/A	4 after RNS alignment, 5-6	N/A				In Mode 4 after RNS alignment and Mode 5,6, the feedwater system is not used, therefore loss of feedwater events is irrelevant. The corresponding shutdown event is failure of RNS. See faults 2.1.2-2.1.4 and 2.2.1-2.2.3.	Modes 3, 4, 5, and 6 are discussed in Section 9.8.4.2.4, "Feedwater System Pipe Break"
1.17 Loss of Feedwater to One SG										
1.17.1	Loss of main feed water to one SG	Loss of capability to remove heat from primary circuit leads to increase in reactor coolant temperature and pressure, increasing risk of loss of RCS integrity and discharge of primary coolant into the containment.	1.9E-01 per reactor year DB2	1-4	PMS(A,C1) – Low-2 SG NR Level	Rod breakers (C1)	PMS(A,C1) – Low-2 NR Level coincident with Low-2 SFW flow	PRHR(C1)	Loss of main feed water to one SG is due to: flow instability/operator error, SG tube blockage or bypass, and mechanical issues. The diversity ATWT case of 1.16.1 “Loss of normal feedwater” bounds this ATWT case. The corresponding shutdown event in Modes 5 to 6 is failure of RNS. See faults 2.1.2-2.1.4 and 2.2.1-2.2.3.	Fault is discussed in Section 9.2.0.1, "Decrease in Heat Removal Faults".
							PMS(A,C1) – Low-2 Cold Leg Temperature	CMT(C1) CI(C1)		
							PMS(A,C1) – High-2 Containment Pressure	PCS(C1)		
					DAS(A,C2) - Low-2 SG WR Level	Rod MG Set breakers (C2)	N/A	ACCUM(C1)		
							DAS(M,C2)	ADS(C1) IRWST(C1) RECIRC(C1)		
							DAS(A,C2) - High Containment Temperature	PCS(C1) CI(C1)		
1.18 Loss of Condenser										
1.18.1	Loss of condenser vacuum and other events resulting in turbine trip	Prevents the use of steam dump to the condenser and precludes the use of the turbine bypass.	1.1E-01 per reactor year DB2	1-4	PMS(A,C1) – High-2 Pressuriser Pressure or Overtemperature ΔT or Low-2 RCP speed	Rod breakers (C1)	PMS(A,C1) - Low-2 SG NR level coincident with Low-2 SFW flow	PRHR(C1)	Initiator for Fault 1.12.8, "Turbine trip". Other events resulting in a turbine trip include: condenser leakage, loss of circulating water, and loss of ultimate heat sink . The diversity ATWT case of 1.12.8 “Turbine Trip” bounds this ATWT case and those results are reported herein. Event in Modes 2, 3, or 4 are bounded by Fault 1.12.8 at full power. In Modes 5 and 6, the event is not applicable.	Mode 1 is discussed in Section 9.2.5, "Loss of Condenser Vacuum and Other Events Resulting in Turbine Trip" and Modes 2 through 6 are discussed in Section 9.8.4.2.1, "Loss of Load, Turbine Trip, Inadvertent MSIV closure, and Loss of Condenser Vacuum"
							PMS(A,C1) – Low-2 Cold Leg Temperature	CMT(C1) CI(C1)		
							PMS(A,C1) – High-2 Containment Pressure	PCS(C1)		
					DAS(A,C2) - High Hot Leg Temperature	Rod MG Set breakers (C2)	N/A	ACCUM(C1)		
							DAS(M,C2)	ADS(C1) IRWST(C1) RECIRC(C1)		
							DAS(A,C2) - High Containment Temperature	PCS(C1) CI(C1)		
					DAS(A,C2) - High Hot Leg Temperature	Rods fail to insert	PMS(A,C2) – Low-2 SG NR Level coincident with Low-2 SFW flow	PRHR(C1)		
							DAS(A,C2) - Low-2 SG WR Level	CMTC1)		
							PMS(A,C1) – High-2 Containment Temperature	PCS(C1) CI(C1)		

Table 8A-2 AP1000 PCSR Composite Fault List for Reactor Internal and Non-internal Events and Internal and External Hazards (cont.)

Fault ID	Initiating Event		Initiating Event Frequency/ DB Class	Possible Modes Affected	Engineered Safety Functions				Comments	Further Assessment of Fault
					Reactivity Control(short term)		Safety Functions			
	Fault	Consequences			Signals	Devices	Signals	Devices		
1.19 Loss of Offsite Power										
1.19.1	Loss of ac power to plant auxiliaries	Loss of capability to remove heat from primary circuit.	3.3E-02 per reactor year DB2	1-4 before RNS alignment	PMS(A,C1) – Low-2 RCP speed	Rod breakers (C1)	PMS(A,C1) – Low-2 SG NR level coincident with Low-2 SFW flow	PRHR(C1)	Anticipated transient without trip (ATWT) loss of ac power is bounded by the ATWT loss of normal feedwater event for peak RCS pressure and by the ATWT complete loss of flow for core damage. Loss of normal feedwater ATWT results are reported herein.	Modes 1 and 2 are discussed in Section 9.2.6, "Loss of ac Power to the Plant Auxiliaries" and modes 3, 4, 5, and 6 are discussed in Section 9.8.4.2.2, "Loss of ac Power"
							PMS(A,C1) – Low-2 Cold Leg Temperature	CMT(C1) CI(C1)		
							PMS(A,C1) – High-2 Containment Pressure	PCS(C1)		
					DAS(A,C2) – Low-2 SG WR Level	Rod MG Set breakers (C2)	N/A	ACCUM(C1)		
							DAS(M,C2)	ADS(C1) IRWST(C1) RECIRC(C1)		
							DAS(A,C2) - High Containment Temperature	PCS(C1) CI(C1)		
					DAS(A,C2) - High Hot Leg Temperature	Rods fail to insert	PMS(A,C1) – Low-2 SG NR Level coincident with Low-2 SFW flow	PRHR(C1)		
							DAS(A,C2) – Low-2 SG WR Level	CMT(C1)		
							PMS(A,C1) – High-2 Containment Temperature	PCS(C1) CI(C1)		
1.19.2	Loss of ac power to plant auxiliaries	Loss of capability to remove heat from primary circuit.	1.7E-03 per reactor year (See Note 1 in 8A.1) DB2	4 after RNS alignment, 5-6	N/A				Mitigation SSCs, discussion of analysis, and radiological consequences are included in faults 2.1.2-2.1.4 since RNS is aligned.	Modes 3-6 are discussed in Section 9.8.4.2.2, "Loss of ac Power"

Table 8A-2 AP1000 PCSR Composite Fault List for Reactor Internal and Non-internal Events and Internal and External Hazards (cont.)

Fault ID	Initiating Event		Initiating Event Frequency/ DB Class	Possible Modes Affected	Engineered Safety Functions				Comments	Further Assessment of Fault
					Reactivity Control(short term)		Safety Functions			
	Fault	Consequences			Signals	Devices	Signals	Devices		
1.20 Loss of Compressed Air										
1.20.1	Loss of compressed air	Loss of capability to remove heat from the reactor core.	3.4E-02 per reactor year DB2	1-4 before RNS alignment	PMS(A,C1) – Low-2 SG NR Level	Rod breakers (C1)	PMS(A,C1) – Low-2 SG NR Level coincident with Low-2 SFW flow	PRHR(C1)	Initiator for Loss of Main Feedwater to both SGs, Fault 1.16.1. The diversity ATWT case of 1.16.1 “Loss of normal feedwater flow” bounds this ATWT case and those results are reported herein. Fault may lead to inadvertent PRHR or CMT (Faults 1.15.15 and 1.12.1) ahead of loss of normal feedwater. All of these faults bound the loss of compressed air event, and are DB2 frequent faults. Initiating event frequency for this fault is considered separately from any of the linked faults noted above, but radiological consequences and compliance with SAP Target 4 limits are not impacted as a result.	Fault is mentioned in Section 9.2.0, "Introduction and Overview of Faults", which lists faults that decrease heat removal by the secondary system.
							PMS(A,C1) – Low-2 Cold Leg Temperature	CMT(C1) CI(C1)		
							PMS(A,C1) – High-2 Containment Pressure	PCS(C1)		
					DAS(A,C2) – Low-2 SG WR Level	Rod MG Set breakers (C2)	N/A	ACCUM(C1)		
							DAS(M,C2)	ADS(C1) IRWST(C1) RECIRC(C1)		
							DAS(A,C2) - High Containment Temperature	PCS(C1) CI(C1)		
					DAS(A,C2) - High Hot Leg Temperature	Rods fail to insert	PMS(A,C1) – Low-2 SG NR Level coincident with Low-2 SFW flow	PRHR(C1)		
							DAS(A,C2) – Low-2 SG WR Level	CMT(C1)		
							PMS(A,C1) – High-2 Containment Temperature	PCS(C1) CI(C1)		
1.20.2	Loss of compressed air	Loss of capability to remove heat from the reactor core	1.8E-03 per reactor year (See Note 1 in 8A.1) DB2	4 after RNS alignment, 5-6	N/A				Mitigation SSCs, discussion of analysis, and radiological consequences are included in faults 2.1.2-2.1.4 since RNS is aligned.	N/A
1.21 Main Steam Line Break										
1.21.1	Main steam line break outside containment, downstream/ upstream of MSIV	Increase in heat removal from primary circuit causes an insertion of positive reactivity.	9.3E-03 (Downstream) 9.3E-04 (Upstream) per reactor year DBL/DB2	1	PMS(A,C1) – OPΔT or Low-2 Steamline Pressure	Rod Breakers (C1)	PMS(A,C1) – Low-2 SG NR Level coincident with Low-2 SFW flow	PRHR(C1)	Larger breaks in spectrum are DBL, and the smaller breaks are DB2; mitigating SSCs and associated analysis are the same for the primary case. Demonstration of frequent fault diversity is included with other excessive load increase events (Fault 1.15.18). Fault 1.21.1a in Mode 2 represents the most limiting condition with respect to core protection for the time following reactor trip. This Mode 1 fault is evaluated separately to demonstrate that core protection is maintained before and immediately following the reactor trip.	Fault in discussed in Section 9.1.6 “Steam System Piping Failure at Full Power”
							PMS(A,C1) – Low-2 Cold Leg Temperature	CMT(C1) CI(C1)		
							PMS(A,C1) – High-2 Containment Pressure	PCS(C1)		

Table 8A-2 AP1000 PCSR Composite Fault List for Reactor Internal and Non-internal Events and Internal and External Hazards (cont.)

Fault ID	Initiating Event		Initiating Event Frequency/ DB Class	Possible Modes Affected	Engineered Safety Functions				Comments	Further Assessment of Fault
	Fault	Consequences			Reactivity Control(short term)		Safety Functions			
					Signals	Devices	Signals	Devices		
1.21.1a	Main steam line break outside containment, downstream/ upstream of MSIV	Increase in heat removal from primary circuit causes an insertion of positive reactivity.	9.3E-03 (Downstream) 9.3E-04 (Upstream) per reactor year DBL/DB2	2	PMS(A,C1)	Rod Breakers (C1) (See Comments)	PMS(A,C1) – Low-2 Steamline Pressure	CMT(C1) CI(C1)	Larger breaks in spectrum are DBL, and the smaller breaks are DB2; mitigating SSCs and associated analysis are the same for the primary case. Demonstration of frequent fault diversity is included with other excessive load increase events (Fault 1.15.18). DBA analysis conservatively assumes immediate PRHR actuation, to maximize cooldown transient. In reality, the PRHR would actuate automatically later to facilitate long-term cooldown. The limiting DBA case produces the maximum post-trip return-to-power and models rods inserted at start of event. Mode 2 cases with rods withdrawn are bound by Fault 1.21.1 for response prior to reactor trip and by the DBA analysis post- reactor trip. Feedline and Steamline isolation assumed to occur with containment isolation on Low-2 Steamline Pressure “S” signal.	Fault in discussed in Section 9.1.5 “Steam System Piping Failure at Hot Zero Power”
							PMS(A,C1) – Low-2 SG NR Level	PRHR(C1)		
							PMS(A,C1) – High-2 Containment Pressure	PCS(C1)		
1.21.2	Main steam line break outside containment, downstream/ upstream of MSIV	Increase in heat removal from primary circuit causes an insertion of positive reactivity.	4.7E-04 (Downstream) 4.7E-05 (Upstream) per reactor year (See Note 1 in 8A.1) DBL/DB1	3-4	N/A	Rods already inserted	PMS(A,C1) – Low-2 Cold Leg Temperature	CMT(C1) CI(C1)	Larger breaks in spectrum are DBL, and the smaller breaks are DB1; mitigating SSCs and associated analysis are the same. Main Steam System is not pressurised in Modes 5 or 6. Feedline, Steamline, and SFW isolation assumed to occur with containment isolation on Low-2 Steamline Pressure “S” signal.	Fault in Modes 3, 4, 5 and 6 is discussed in Section 9.8.4.1.3 “Steamline Breaks”
							PMS(A,C1) – Low-2 SG NR Level coincident with Low-2 SFW flow	PRHR(C1)		
							PMS(A,C1) – High-2 Containment Pressure	PCS(C1)		
1.21.3	Main steam line break inside containment, upstream of MSIV	Increase in heat removal from primary circuit causes an insertion of positive reactivity.	1.9E-04 per reactor year DBL/DB2	1-4	N/A				This Fault is included with the spectrum of outside containment steamline breaks (Faults 1.21.1-1.21.2), as the radiological consequences are limiting for outside containment breaks. Main Steam System is not pressurised in Modes 5 or 6	N/A

Table 8A-2 AP1000 PCSR Composite Fault List for Reactor Internal and Non-internal Events and Internal and External Hazards (cont.)

Fault ID	Initiating Event		Initiating Event Frequency/ DB Class	Possible Modes Affected	Engineered Safety Functions				Comments	Further Assessment of Fault
					Reactivity Control(short term)		Safety Functions			
	Fault	Consequences			Signals	Devices	Signals	Devices		
1.22 Main Steam Line Stuck Open Safety Valve										
1.22.1	Inadvertent opening of a steam generator relief or safety valve.	Steam release from SG leads to heat removal from the RCS and a concomitant reduction in coolant temperature.	2.4E-03 per reactor year DB2	1-2	PMS(A,C1)	Rod Breakers (C1) (See Comments)	PMS(A,C1) – Low-2 SG NR Level coincident with Low-2 SFW flow	PRHR(C1)	Fault covers the spurious actuation of a main steam line safety valve for Modes 1 and 2. The limiting case analysed is initiated from shutdown (Mode 2) with rods already inserted, which bounds the less limiting case in Mode 1. Two diverse cases listed. First one is for core cooling. Second one is for ATWT. The ATWT result is bounded by ATWT loss of normal feedwater (Fault 1.16.1) for peak RCS pressure and by ATWT complete loss of flow (Fault 1.13.1a) for core damage. ATWT systems available for this event are reported; however, limiting ATWT case reaches safe stable steady-state condition similar to excessive load increase. No reactor trip is required for plant protection and manual operator action would be required to end the transient.	Modes 1 and 2 are discussed in Section 9.1.4, "Inadvertent Opening of a Steam Generator Relief or Safety Valve".
							PMS(A,C1) – Low-2 Cold Leg Temperature	CMT(C1) CI(C1)		
							PMS(A,C1) – High-2 Containment Pressure	PCS(C1)		
					DAS(A,C2) – Low-2 SG WR Level	Rod MG Set breakers (C2)	N/A	ACCUM(C1)		
							DAS(M,C2)	ADS(C1) IRWST(C1) RECIRC(C1)		
							DAS(A,C2) - High Containment Temperature	PCS(C1) CI(C1)		
					DAS(A,C2) - High Hot Leg Temperature	Rod MG Set breakers (C2)	DAS(A,C2) – Low-2 SG WR Level	PRHR(C1)		
							DAS(A,C2)-SG Low SG 1 and 2 Level	CMTC1)		
							DAS(A,C2) - High Containment Temperature	PCS(C1) CI(C1)		
1.22.2	Inadvertent opening of a steam generator relief or safety valve.	Steam release from SG leads to heat removal from the RCS and a concomitant reduction in coolant temperature.	1.2E-04 per reactor year (See Note 1 in 8A.1) DB2	3-4	N/A	Rods Already Inserted	PMS(A,C1) – Low-2 SG NR Level coincident with Low-2 SFW flow	PRHR(C1)	Fault covers the spurious actuation of a main steam line safety valve for Modes 3 and 4. There is no need to consider ATWT event in shutdown, since rods already inserted.	Modes 3, 4, 5, and 6 are discussed in Section 9.8.4.1.3, "Steamline Breaks".
							PMS(A,C1) – Low-2 Cold Leg Temperature	CMT(C1) CI(C1)		
							PMS(A,C1) – High-2 Containment Pressure	PCS(C1)		
					N/A	Rods Already Inserted	DAS(M,C2)	ADS(C1) IRWST(C1) RECIRC(C1)		
							DAS(A,C2)- High Containment Temperature	PCS(C1) CI(C1)		
1.22.2a	Inadvertent opening of a steam generator relief or safety valve.	Steam release from SG leads to heat removal from the RCS and a concomitant reduction in coolant temperature.	N/A	5-6	N/A				RCS is borated and effectively isolated for secondary system in Modes 5 and 6 that such a cooldown-induced power excursion cannot be postulated.	Modes 3, 4, 5, and 6 are discussed in Section 9.8.4.1.3, "Steamline Breaks".

Table 8A-2 AP1000 PCSR Composite Fault List for Reactor Internal and Non-internal Events and Internal and External Hazards (cont.)

Fault ID	Initiating Event		Initiating Event Frequency/ DB Class	Possible Modes Affected	Engineered Safety Functions				Comments	Further Assessment of Fault
	Fault	Consequences			Reactivity Control(short term)		Safety Functions			
					Signals	Devices	Signals	Devices		
2. Additional Reactor Internal Faults										
2.1 Failure of RNS During Shutdown Conditions										
2.1.1	Not Used									
2.1.2	Failure of normal residual heat removal system	Loss of decay heat removal.	1E-03 per reactor year DB2	4-5 with RCS Intact	N/A	Rods already inserted	PMS(A,C1) – Low-2 Pressuriser Level	PRHR(C1) CMT(C1) CI(C1)	RNS is not aligned until Mode 4; therefore event is not possible during Modes 1-3. Includes various initiators, including loss of offsite power, pump failures, loss of component cooling water, loss of service water, and loss of compressed air. Manual PRHR actuation at 30 minutes, no actuation of ADS/IRWST injection occurs. Without manual actuation, CMT/PRHR would still automatically actuate at approximately 2.2 hours after loss of RNS on Low Pressuriser Level. Note that overpressure protection is provided by RNS relief valves. There is no need to consider ATWT event in shutdown, since rods already inserted.	Fault is discussed in Section 9.8.5.1, "Loss of RNS During Mode 4 and 5, with RCS Intact". Diversity cases to be analysed during site licensing.
							PMS(A,C1) – Low CMT Level	ADS(C1) IRWST(C1)		
							PMS(A,C1) – Low IRWST Level	RECIRC(C1)		
							PMS(A,C1) – High-2 Containment Pressure	PCS(C1)		
					N/A	Rods Already Inserted	PMS(A,C1) – Low-2 Pressuriser Level	CMT(C1) CI(C1)		
							PMS(A,C1) – Low CMT Level	ADS(C1) IRWST(C1)		
							PMS(A,C1) – Low IRWST Level	RECIRC(C1)		
							PMS(A,C1) – High-2 Containment Pressure	PCS(C1)		
					N/A	Rods Already Inserted	DAS(M,C2)	PRHR(C1)		
							DAS(A,C2) – High Containment Temperature	PCS(C1) CI(C1)		
2.1.3	Failure of normal residual heat removal system	Loss of decay heat removal.	<1E-04 per reactor year DB1	5 with RCS Open	N/A	Rods already inserted	PMS(A,C1) - Low Hot Leg Level	ADS(C1) IRWST(C1)	Includes various initiators, including loss of offsite power, pump failures, loss of component cooling water, loss of service water, and loss of compressed air. ADS 1-3 is already open in Modes 5 and 6 with RCS open. Only 1 ADS-4 is assumed available for actuation. Diverse manual actuation of Class 1 SSCs presented via DAS is available.	Fault is discussed in Section 9.8.5.2, "Loss of RNS During Mode 5 and 6, with RCS Open".
							PMS(A,C1) - Low IRWST Level	RECIRC(C1)		
							PMS(A,C1) – High Containment Pressure	PCS(C1) CI(C1)		
2.1.4	Failure of normal residual heat removal system	Loss of decay heat removal.	<1E-04 per reactor year DB1	6	N/A	Rods already inserted	PMS(A,C1) – High-2 Containment Pressure	PCS(C1) CI(C1)	Includes various initiators, including loss of offsite power, pump failures, loss of component cooling water, loss of service water, and loss of compressed air. Diverse manual actuation of Class 1 SSCs presented via DAS is available.	Fault is discussed in Section 9.8.5.2, "Loss of RNS During Mode 5 and 6, with RCS Open".
2.2 Not Used										

Table 8A-2 AP1000 PCSR Composite Fault List for Reactor Internal and Non-internal Events and Internal and External Hazards (cont.)

Fault ID	Initiating Event		Initiating Event Frequency/ DB Class	Possible Modes Affected	Engineered Safety Functions				Comments	Further Assessment of Fault
					Reactivity Control(short term)		Safety Functions			
	Fault	Consequences			Signals	Devices	Signals	Devices		
2.3 LOCA Events Involving RNS										
2.3.1	Rupture of the normal residual heat removal system piping	Loss-of-coolant accident.	1.6E-05 per reactor year DB1	4-5 with RCS Intact	N/A	Rods already inserted	PMS(A,C1) - Low-2 Pressuriser Level	CMT(C1)	RNS is not aligned until Mode 4; therefore event is not possible during Modes 1-3. Breaks inside containment would be bounded by this fault, but with reduced radiological consequences. Fault includes additional initiators, such as inadvertent or spurious operation of RNS-V024. RNS isolation provided by containment isolation signal on Low CMT level.	Fault is discussed in Section 9.8.5 3, "Loss of Coolant Accidents Involving RNS".
							PMS(A,C1) - Low CMT Level	ADS(C1) IRWST(C1) CI(C1) RNS Isolation (C1)		
							PMS(A,C1) - Low IRWST Level	RECIRC(C1)		
							PMS(A,C1) – High-2 Containment Pressure	PCS(C1)		
2.3.2	Rupture of the normal residual heat removal system piping	Loss-of-coolant accident.	1.6E-05 per reactor year DB1	5 with RCS Open	N/A	Rods already inserted	PMS(A,C1) - Low Hot Leg Level	ADS 4(C1) IRWST(C1) CI(C1) RNS Isolation(C1)	Breaks inside containment would be bounded by this fault, but with reduced radiological consequences. ADS-4 and IRWST injection are actuated after a 25 minute delay upon reaching Low Hot Leg Level setpoint. Fault includes additional initiators, such as inadvertent or spurious operation of RNS-V024, or over-draining of RCS while going to mid-loop level. RNS isolation provided by containment isolation signal on Low CMT level.	Fault is discussed in Section 9.8.5 3, "Loss of Coolant Accidents Involving RNS".
							PMS(A,C1) - Low IRWST Level	RECIRC(C1)		
							PMS(A,C1) – High-2 Containment Pressure	PCS(C1)		
2.3.3	Rupture of the normal residual heat removal system piping	Loss-of-coolant accident.	1.6E-05 per reactor year DB1	6	N/A	Rods already inserted	PMS(M,C1)	RNS Isolation (C1) ADS 4(C1) IRWST(C1) RECIRC(C1)	Breaks inside containment would be bounded by this fault, but with reduced radiological consequences. ADS-4 is only needed if the reactor internals are installed; otherwise, sufficient vent area exists. Fault includes additional initiators, such as inadvertent or spurious operation of RNS-V024, or over-draining of RCS while going to mid-loop level. RNS isolation assumed to be actuated manually prior to High-2 containment pressure signal.	Fault is discussed in Section 9.8.5 3, "Loss of Coolant Accidents Involving RNS".
							PMS(A,C1) – High-2 Containment Pressure	PCS(C1) CI(C1)		
2.4 Reactor Internal Events Specific to Refuelling Operations										
2.4.1	Uncontrolled rod cluster control assembly bank withdrawal during refuelling	None	N/A	6	N/A				Keff for a fully fuelled core in mode 6 is maintained at, or below, 0.95 with control rods and soluble boron. The core is maintained sufficiently sub-critical, that removal of rod cluster control assemblies will not result in criticality. Control rod breakers are required to be open preventing uncontrolled withdrawal. No difference from Fault 1.15.3.	Modes 3, 4, and 5 are discussed in Section 9.8.4.4.1, "Uncontrolled RCCA Bank Withdrawal from a Subcritical Condition".
2.4.2	Inadvertent loading of a fuel assembly in an improper position in core during refuelling.	None	N/A	6	N/A				Shutdown margin with borated coolant and RCCAs fully inserted will exceed any local reactivity perturbation caused by fuel misloading. Only a potential issue on return to power. Included in Fault 1.15.10.	Section 9.8.4.4.6, "Inadvertent Loading of a Fuel Assembly in an Improper Position".

Table 8A-2 AP1000 PCSR Composite Fault List for Reactor Internal and Non-internal Events and Internal and External Hazards (cont.)

Fault ID	Initiating Event		Initiating Event Frequency/ DB Class	Possible Modes Affected	Engineered Safety Functions				Comments	Further Assessment of Fault
	Fault	Consequences			Reactivity Control(short term)		Safety Functions			
					Signals	Devices	Signals	Devices		
2.4.3	Loss or reduction of boration in refuelling cavity due to: -faulty boron concentration measurement - uncontrolled dilution/addition of unborated water (e.g. from fire protection system (FPS))	Criticality Event	N/A	6	N/A				Criticality assessment demonstrates that complete loss of boron in the refuelling cavity would not result in a criticality event. See related Fault 1.15.9.	Fault not considered further.
2.4.4	Loss of configuration of reactor core due to dropped loads (including integrated head package, or above core internals)	Criticality Event	N/A	6	N/A				Large, heavy loads such as the integrated head package, or above core internals, would not fit within the open RPV and damage to fuel would be restricted to the uppermost regions. In such cases the consequences would only be radiological see Fault 2.4.7 below. The criticality risks posed by smaller dropped loads, due to assembly deformation, are considered to be bounded by a dropped load onto fuel assemblies in the Spent Fuel Pool – see Fault 3.2.2. Assessment shows this fault has no criticality consequences.	Fault not considered further.
2.4.5	Dropped fuel assembly (spent or new) onto, or into reactor core	Criticality Event	N/A	6	N/A				The boron concentration is maintained sufficiently high during refuelling to prevent criticality. A dropped assembly would result in geometry less conducive to approaching criticality than the standard configuration. The consequences of the event are therefore negligible regarding criticality; fuel damage is considered in Fault 2.4.9.	Fault not considered further.
2.4.6	Displacement of control rods (e.g. seismic)	Criticality Event	N/A	6	N/A				During refuelling, core inserts remain in the fuel assemblies and travel with the fuel to the spent fuel racks in the Auxiliary Building. Also, core boron concentration is kept at 2700 ppm to keep the core 5 percent $\Delta k/k$ subcritical during refuelling operations. This fault is therefore not a credible event.	Fault not considered further.
2.4.7	Damage to reactor core due to dropped loads (including integrated head package, or above core internals)	Radioactivity release	N/A	6	N/A				The polar crane is designed according to NUREG-0554, supplemented by ASME NOG-1 for a Type I failure proof crane. The crane is single failure proof, and is designed to stop and hold a critical load following the credible failure of a single component. A heavy loads analysis is performed to evaluate postulated load drops from heavy load handling systems located in safety-related areas of the plant, specifically the nuclear island. No evaluations are required for critical loads handled by the containment polar crane, the cask handling crane, the containment equipment hatch hoist, and the containment maintenance hatch hoist since a load drop is unlikely.	Fault not considered further.

Table 8A-2 AP1000 PCSR Composite Fault List for Reactor Internal and Non-internal Events and Internal and External Hazards (cont.)

Fault ID	Initiating Event		Initiating Event Frequency/ DB Class	Possible Modes Affected	Engineered Safety Functions				Comments	Further Assessment of Fault
	Fault	Consequences			Reactivity Control(short term)		Safety Functions			
					Signals	Devices	Signals	Devices		
2.4.8	Start of refuelling operations before fuel is adequately cooled	Potential for fuel overheating and damage.	N/A	6	N/A				Initiating event not considered credible. Higher than expected average decay heat levels in core would have been recognized earlier by coolant temperature/pressure remaining above expected levels. Commencement of refuelling operations requires RCS to have been cooled down to (140 F/60 C) in mode 5, with RNS operative. Refuelling operations would be deferred until these conditions are met.	Fault not considered further.
2.4.9	Damage to fuel assembly/core following drop of assembly on reactor core	Potential fuel damage and radioactivity release.	<1E-03 Per reactor year DB1	6	Same Mitigation SSC as infrequent dropped fuel assembly in spent fuel assembly in spent fuel pool (Fault 3.2.11)				Radioactivity release Consequences < BSL for Target 4 for both onsite and offsite doses. Bounded by Fault 3.2.11. Frequency is assessed in Section 9.14.5.6.	This fault is discussed in Section 9.9.5, "Dropped Fuel Assembly onto Other Fuel".
3. Non-Reactor Faults										
3.1 Faults Involving Fuel (Spent/New) Transfer Route										
3.1.1	Loss of water from refuelling cavity (failure of seal between RPV and reactor cavity, cracking of wall due to seismic event)	Loss of coolant	DB0	6	N/A				Both the refuelling cavity and the permanent cavity seal ring are seismic category 1, so this event is extremely unlikely. Nonetheless, adequate inventory would remain in the spent fuel pool area to keep the spent fuel covered for a minimum of 72 hours, depending on the amount of fuel transferred to the spent fuel pool from the core. The spent fuel pool-transfer canal weir gate or the transfer tube valve may also be closed to isolate the spent fuel pool from the refuelling cavity. Should an assembly be in the cavity or transfer canal at the time of the event, the fuel handling machine would remain operable and would transfer the assembly to a safe position in the spent fuel pool area. Should a single failure coincident with the loss of water event cause a loss of power to the fuel handling machines, manual operator action is available to transfer the assembly.	Fault not considered further.
3.1.2	Element stuck in fuel handling machine	Restriction in convective cooling over extended period	DB0	6	N/A				Refuelling machine mast is designed to support natural convection cooling of a fuel assembly. A stuck fuel assembly would pose no radiological concerns as long as the refuelling cavity water level is maintained at the minimum operating level for fuel movement. Further, all fuel handling equipment drive motors are equipped with hand wheels to support manual operation.	Fault not considered further.
3.1.3	Element stuck in transfer tube	Restriction in convective cooling over extended period	DB0	6	N/A				The fuel transfer car basket is designed to support natural convection cooling of a fuel assembly. A stuck fuel assembly would pose no radiological concerns as long as the refuelling cavity water level is maintained at the minimum operating level for fuel movement. Further, all fuel handling equipment drive motors are equipped with hand wheels to support manual operation.	Fault not considered further.

Table 8A-2 AP1000 PCSR Composite Fault List for Reactor Internal and Non-internal Events and Internal and External Hazards (cont.)

Fault ID	Initiating Event		Initiating Event Frequency/ DB Class	Possible Modes Affected	Engineered Safety Functions				Comments	Further Assessment of Fault
	Fault	Consequences			Reactivity Control(short term)		Safety Functions			
					Signals	Devices	Signals	Devices		
3.1.4	Damage to fuel assembly (spent or new) due to drop in refuelling cavity	Potential fuel damage and radioactivity release.	<1E-03 per reactor year DB1	6	Same Mitigation SSC as infrequent dropped fuel assembly in spent fuel assembly in spent fuel pool (Fault 3.2.11)				Bounded by Fault 3.2.11.	Fault is discussed in Section 9.9.5, "Dropped Fuel Assembly onto Other Fuel".
3.1.5	Operator falls into flooded refuelling cavity	Operator radiation exposure, dose < BSO	DB0	6	N/A					Fault is discussed in Section 9.10.4, "Operator Falls into Flooded Refuelling Cavity or Fuel Storage Pool".
3.1.6	Water level fall in refuelling cavity (shielding lost)	Operator radiation exposure, dose < BSO	DB0	6	N/A					Fault is discussed in Section 9.10.5, "Water Level Fall in the Refuelling Cavity or Storage Pool".
3.1.7	Over-raising fuel in refuelling cavity (shielding lost)	Operator radiation exposure, dose < BSO	DB0	6	N/A				Design of RM mast places a geometric constraint on the height to which a fuel assembly can be raised. Fault is precluded by design.	Fault screened out Table 9.10-1, "Screened-out Faults" in Section 9.10, "Operator Exposure Faults".
3.1.8	Flooding of new fuel with un-borated water or oil: - in new fuel assembly inspection area (with concrete reflection) - in new fuel storage rack (dry buffer store)	Criticality event	N/A	N/A	N/A				For a single fuel assembly in the inspection area flooded or sprayed with water and with concrete reflection on both sides, the reactivity is expected to be less than that for a fully loaded new fuel storage rack covered in water.	Fault not considered further.
3.1.9	Dropped fuel cask in rail car bay	Potential damage to cask seals and fuel content.	DB0	N/A	N/A				There is no release for this fault. Drop could occur due to operator error or failure of lifting equipment. Risk considered to be ALARP.	This fault is discussed in Section 9.9.4, "Dropped Fuel Cask in Rail Car Bay".

Table 8A-2 AP1000 PCSR Composite Fault List for Reactor Internal and Non-internal Events and Internal and External Hazards (cont.)

Fault ID	Initiating Event		Initiating Event Frequency/ DB Class	Possible Modes Affected	Engineered Safety Functions				Comments	Further Assessment of Fault
	Fault	Consequences			Reactivity Control(short term)		Safety Functions			
					Signals	Devices	Signals	Devices		
3.2 Spent Fuel Pool Faults										
3.2.1	Loss or reduction of boration in spent fuel pool due to: -faulty boron concentration measurement - uncontrolled dilution/addition of unborated water (e.g. from FPS)	Criticality event Radiation doses < Target 4 BSL	N/A	N/A	N/A				Boron is not credited in criticality analysis.	Fault is screened out deterministically in Section 9.7.1.2,
3.2.2	Loss of configuration of fuel in storage racks (e.g. seismic or dropped load) - dropped fuel assembly lying on top of rack (toppled) -.vertical misalignment of fuel assembly relative to neutron absorbing panels - change in rod pitch to a more reactive configuration (possibly outside rack) - distortion of rack geometry (e.g. bringing fuel assemblies closer together) - displacement of racks closer together, or with more concrete reflection	Criticality event	N/A	N/A	N/A				PSCR Section 9.11 concludes that there is no reactivity increase and therefore no release for a fuel assembly dropped on top of the rack. For other faults, there would only be an activity rise if there was a coincident boron dilution event, which is screened out on frequency grounds.	Fault is screened out deterministically in Section 9.7.1.2,
3.2.3	Misplaced fuel assembly in spent fuel pool: - in space next to fuel racks - placed in wrong region (R1 instead of R2) - vertical misalignment of fuel assembly relative to neutron absorber panels	Criticality event	N/A	N/A	N/A				PCSR Section 9.11 concludes that there is no increase in activity since the design is for all fresh fuel anyway.	Fault is screened out deterministically in Section 9.7.1.2,

Table 8A-2 AP1000 PCSR Composite Fault List for Reactor Internal and Non-internal Events and Internal and External Hazards (cont.)

Fault ID	Initiating Event		Initiating Event Frequency/ DB Class	Possible Modes Affected	Engineered Safety Functions				Comments	Further Assessment of Fault
	Fault	Consequences			Reactivity Control(short term)		Safety Functions			
					Signals	Devices	Signals	Devices		
3.2.4	Increased reactivity after incomplete repair of fuel assembly (some fuel rods removed but not replaced)	Criticality event	N/A	N/A	N/A				Fault involves the disassembly and incorrect re-assembly of a fuel assembly in the SFP. Even if this happened, a number of sequential errors would have to occur before there was any criticality event.	Fault is screened out deterministically in Section 9.7.1.2,
3.2.5	Loss of water from spent fuel storage pool. Class 2 8 inch SFS suction/return pipe break	Loss of cooling water	<1E-05 per reactor year DB1	N/A	N/A		Spent fuel pool cooling system (SFS)(C1) – Low-2 SFP Water Level	SFP(C1) FTC(C1) Cask washdown pit (CWP)(C1) cask loading pit (CLP) (C1) passive containment system water storage tank (PCCWST(C1))	The 8” Class 2 SFS suction and return piping connections to the SFP are the only non-Class 1 connections. The SFS return line has a 1-inch hole that is 3 ft (.61 m) below the operating deck that acts as a siphon break to prevent the pool from draining. A break in the SFS suction connection to the SFP will cause the water level to drop to the bottom of the SFS suction piping. Since the RNS suction and return connections are below the SFS connections, an RNS pump/HX train can be used to cool the pool. Any of the signals listed will alert the operator of decreased inventory. The amount of makeup required to maintain a safe level in the SFP depends on the time in the fuel cycle that the event occurs. During the majority of time in a typical fuel cycle, the water inventory in the SFP and fuel transfer canal (FTC) after the break is sufficient to maintain level for at least 72 hours after the break.	Fault discussed in section 9.7.2.4 “Postulated Loss of Water Inventory from the SFP”
3.2.6	Loss of water from spent fuel storage pool. Class 1 8 inch RNS suction/return pipe break	Loss of cooling water	<1E-05 per reactor year DBL	N/A	N/A		SFS(A,C1) – Low-2 SFP Water Level	SFP(C1) FTC(C1) CWP(C1) CLP(C1) PCCWST(C1)*	Analysed as a DB1 design basis infrequent fault. The RNS return line to the SFP has a hole that is below the operating deck that acts as a siphon break to prevent the pool from draining. A break in the RNS suction line will cause the SFP water level to drop to the bottom of the RNS suction connection, resulting in a loss of cooling scenario. Conservative analysis shows that the operator will have at least 24 hours available to align any of the sources of makeup listed. Any of the signals listed will alert the operator of decreased inventory. The amount of makeup required to maintain a safe level in the SFP depends on the time in the fuel cycle that the event occurs. During the majority of time in a typical fuel cycle, the water inventory in the SFP and FTC after the break is sufficient to maintain level for at least 72 hours after the break. *Water from the PCCWST (and passive containment cooling ancillary water storage tank (PCCAWST)) must be aligned to the SFP through the Class 2 spray lines.	Fault discussed in section 9.7.2.4 “Postulated Loss of Water Inventory from the SFP”

Table 8A-2 AP1000 PCSR Composite Fault List for Reactor Internal and Non-internal Events and Internal and External Hazards (cont.)

Fault ID	Initiating Event		Initiating Event Frequency/ DB Class	Possible Modes Affected	Engineered Safety Functions				Comments	Further Assessment of Fault
					Reactivity Control(short term)		Safety Functions			
	Fault	Consequences			Signals	Devices	Signals	Devices		
3.2.7	Loss of water from spent fuel storage pool. Class 1 6 inch FTC drain line pipe break	Loss of cooling water	<1E-05 per reactor year BDB	N/A	N/A		See Fault 3.2.5		Analysed as a DB1 design basis infrequent fault. A break in the 6" Class 1 FTC drain line will drain the pool to the gate elevation if the FTC gate is open to the SFP. If instrument air is available, the FTC gate can be closed to prevent further SFP draining. Assuming the SFP drains to the gate level, the operator will have at least 2 hours to align a makeup source during normal operation before boiling occurs and at least 1 hour during a refuelling outage.	Fault discussed in section 9.7.2.4 "Postulated Loss of Water Inventory from the SFP"
3.2.8	Loss of water from spent fuel storage pool. Class 1 6 inch CLP pipe break	Loss of cooling water	<1E-05 per reactor year BDB	N/A	N/A		See Fault 3.2.5		Analysed as a DB1 design basis infrequent fault. Bounded by larger diameter pipe breaks.	Fault discussed in section 9.7.2.4 "Postulated Loss of Water Inventory from the SFP"
3.2.9	Loss of water from spent fuel storage pool. Class 1 instrument line pipe break	Loss of cooling water	N/A	N/A	N/A		See Fault 3.2.5		Bounded by larger diameter pipe breaks.	Fault discussed in section 9.7.2.4 "Postulated Loss of Water Inventory from the SFP"
3.2.10	Loss of spent fuel storage pool cooling due to equipment failure, loss of offsite power or station blackout.	Loss of fuel decay heat removal	4.4E-03 per reactor year DB1	N/A	N/A		See Fault 3.2.5		The loss of SFP cooling is bounded by loss of cooling water scenarios where the level drops below the SFS suction connections and cooling capability is therefore lost with less water inventory in SFP. The high temperature alarm will alert the operator of a loss of cooling. If there is an extended loss of cooling, boiling will occur and the water level will begin to drop. The signals and devices available are then equivalent to those outlined in 3.2.5.	Fault discussed in section 9.7.2.3 "Loss of Spent Fuel Pool Cooling Capability".
3.2.11	Dropped fuel assembly in spent fuel storage pool	Potential fuel damage and radioactivity release.	<1E-03 per reactor year DB0	N/A	N/A		VAS(A,C3) – Activity in-air	N/A	To minimize the operator exposure to airborne activity, the fuel handling activity in-air monitor will alert operators to evacuate the area immediately. High efficiency particulate air (HEPA) filters and charcoal absorbers in the VFS reduce the dose to members of the public	This fault is discussed in Section 9.9.5, "Dropped Fuel Assembly onto Other Fuel".
3.2.12	Dropped fuel cask in spent fuel storage pool (spent or new)	Potential fuel damage and radioactivity release.	N/A	N/A	N/A				Cask handling crane is prevented from travelling over the SFP, therefore the fault cannot occur.	Fault is discussed in Section 9.9.2, "Analysis of Faults" in Section 9.9, "Dropped Loads."

Table 8A-2 AP1000 PCSR Composite Fault List for Reactor Internal and Non-internal Events and Internal and External Hazards (cont.)

Fault ID	Initiating Event		Initiating Event Frequency/ DB Class	Possible Modes Affected	Engineered Safety Functions				Comments	Further Assessment of Fault
	Fault	Consequences			Reactivity Control(short term)		Safety Functions			
					Signals	Devices	Signals	Devices		
3.2.13	Operator falls into spent fuel storage pool	Operator radiation exposure, dose < BSO	<1E-03 per reactor year DB0	N/A	N/A				DB0 due to radiological consequences less than BSO.	Fault is discussed in Section 9.10.4, "Operator Falls into Flooded Refuelling Cavity or Fuel Storage Pool".
3.2.14	Water level fall in storage pool (shielding lost)	Operator radiation exposure, dose < BSO	<1E-03 per reactor year DB0	N/A	N/A				DB0 due to radiological consequences less than BSO. Minimum allowable water depths above active fuel in a fuel assembly during fuel handling are 2.67 m in the reactor cavity and 2.67 m in the fuel transfer canal and spent fuel pool. (This limits the dose to personnel on the spent fuel pool handling machine to less than 0.025 mSv/hr for an assembly in a vertical position.)	Fault is discussed in Section 9.10.5, "Water Level Fall in the Refuelling Cavity or Storage Pool".
3.2.15	Over-raising of fuel in spent fuel storage pool (shielding lost)	Operator radiation exposure	N/A	N/A	N/A				Design of fuel handling machine places a geometric constraint on the height to which a fuel assembly can be raised. Fault is precluded by design.	Fault screened out in Table 9.10-1, "Screened-out Faults" in Section 9.10, "Operator Exposure Faults".
3.2.16	Exposure in areas contaminated by pool water (over time)	Operator radiation exposure	N/A	N/A	N/A				Assessed levels of contamination in the form of a puddle of spilt water would give very low dose rates, would be readily detectable by HP and are easily cleaned.	Fault screened out in Table 9.10-1, "Screened-out Faults" in Section 9.10, "Operator Exposure Faults".
3.3 Operator Exposure Associated with NDT, Maintenance, and Calibration Activities										
3.3.1	Unauthorized operator entry into active areas	Operator radiation exposure	N/A	N/A	N/A				Ingress and egress of plant operating personnel to radiologically restricted areas will be strictly controlled and monitored in accordance with HP principles. The arrangements will be as effective as, or better than, at existing operational pressurised water reactor (PWR) plant in general.	Fault screened out in Table 9.10-1, "Screened-out Faults" in Section 9.10, "Operator Exposure Faults".
3.3.2	Inappropriate handling or use of other sources (e.g. radiography, neutron and HP calibration sources)	Operator radiation exposure	N/A	N/A	N/A				No significant neutron or radioactive sources are present outside of the reactor fuel. All other radioactive sources required for use on the station such as X-ray machines for radiography or test sources for radiation monitoring equipment will be subject to controls as required by the Ionising Radiations Regulations (IRR). All such radiation sources would be held and used only under the local control of Health Physics (HP).	Fault screened out in Table 9.10-1, "Screened-out Faults" in Section 9.10, "Operator Exposure Faults".
3.4 Faults in CVS and WLS (All Plant States)										
3.4.1	Failure of small lines carrying primary coolant outside containment	Limited release of primary coolant outside containment.	>1E-03 per reactor year HFLC	1-6	N/A				Bounded by Fault 1.9.2	Fault is discussed in Section 9.6.2, "Failure of Small Lines Carrying Primary Coolant Outside Containment"

Table 8A-2 AP1000 PCSR Composite Fault List for Reactor Internal and Non-internal Events and Internal and External Hazards (cont.)

Fault ID	Initiating Event		Initiating Event Frequency/ DB Class	Possible Modes Affected	Engineered Safety Functions				Comments	Further Assessment of Fault
	Fault	Consequences			Reactivity Control(short term)		Safety Functions			
					Signals	Devices	Signals	Devices		
3.4.2	Fault in handling spent resins intermediate level waste (ILW). Leakage during transfer to collection tank, tank overfill, or tank rupture /leakage solid radwaste system (WSS)	Local contamination/ loss of shielding, dose < BSO	<1E-03 per reactor year DB0	N/A	N/A				DB0 due to radiological consequences less than BSO	Fault is discussed in Section 9.12.16, "Loss of Containment of Spent Resin".
3.4.3	Fault in handling spent resins low level waste ((LLW) and WSS)	Local contamination, dose < BSO	<1E-03 per reactor year DB0	N/A	N/A				DB0 due to radiological consequences less than BSO	Fault is discussed in Section 9.12.16, "Loss of Containment of Spent Resin".
3.4.4	Fault in handling wet activated carbon gaseous radwaste system (WGS)	Possible airborne contamination and loss of shielding, dose < BSO	6.7E-04 per reactor year DB0	N/A	N/A				DB0 due to radiological consequences less than BSO	Fault is Discussed in Section 9.12.7, "Radioactive Exchangeable Items (Filters and Charcoal Absorbers)".
3.4.5	Fault in handling Steam Generator blowdown material (resins) (WLS)	Local contamination/ loss of shielding, dose < BSO	6.7E-04 per reactor year DB0	N/A	N/A				DB0 due to radiological consequences less than BSO	Fault is Discussed in Section 9.12.7, "Radioactive Exchangeable Items (Filters and Charcoal Absorbers)".
3.4.6	Fault in handling Steam Generator blowdown material (membranes) (WLS)	Local contamination/ loss of shielding, dose < BSO	6.7E-04 per reactor year DB0	N/A	N/A				DB0 due to radiological consequences less than BSO	Fault is Discussed in Section 9.12.7, "Radioactive Exchangeable Items (Filters and Charcoal Absorbers)".
3.4.7	Fault in handling spent filters (higher activity)	Potential for airborne release, local contamination and loss of shielding	6.7E-04 per reactor year DB0	N/A	N/A				DB0 due to radiological consequences less than BSO	Fault is Discussed in Section 9.12.7, "Radioactive Exchangeable Items (Filters and Charcoal Absorbers)".
3.4.8	Fault in handling spent filters (higher activity)	Potential for airborne release, local contamination, dose < BSO	6.7E-04 per reactor year DB0	N/A	N/A				DB0 due to radiological consequences less than BSO	Fault is Discussed in Section 9.12.7, "Radioactive Exchangeable Items (Filters and Charcoal Absorbers)".

Table 8A-2 AP1000 PCSR Composite Fault List for Reactor Internal and Non-internal Events and Internal and External Hazards (cont.)

Fault ID	Initiating Event		Initiating Event Frequency/ DB Class	Possible Modes Affected	Engineered Safety Functions				Comments	Further Assessment of Fault
	Fault	Consequences			Reactivity Control(short term)		Safety Functions			
					Signals	Devices	Signals	Devices		
3.4.9	Unauthorised operator entry into areas of high dose	Operator radiation exposure	N/A	N/A	N/A				Comments similar to those for Fault 3.3.1.	Fault screened out in Table 9.10-1, "Screened-out Faults" in Section 9.10, "Operator Exposure Faults".
3.4.10	Failure to adequately control chemistry to manage dose rates	Operator radiation exposure	N/A	N/A	N/A				Operators required to work in potentially active areas for water chemistry will be monitored and access will be controlled. Individual doses will be controlled by HP arrangements (see also Faults 3.3.1 and 3.4.9)	Fault screened out in Table 9.10-1, "Screened-out Faults" in Section 9.10, "Operator Exposure Faults".
3.5 HVAC Faults										
3.5.1	Failure of HVAC filter	Potential external release of radioactivity, dose < BSO	DB0	N/A	N/A				DB0 due to radiological consequences less than BSO. Bounded by Fault 3.5.6.	Fault is discussed in Section 9.11.6, "Failure of Filters in the Heating, Ventilation, and Air Conditioning System".
3.5.2	Blockage of HVAC filter	Increase in air radioactivity level in affected working area, dose < BSO	DB0	N/A	N/A				DB0 due to radiological consequences less than BSO. Bounded by Fault 3.5.6.	Fault is discussed in Section 9.11.8, "Reduced Airflow".
3.5.3	Failure of HVAC fans	Increase in air radioactivity level in affected working area, dose < BSO	DB0	N/A	N/A				DB0 due to radiological consequences less than BSO. Bounded by Fault 3.5.6.	Fault is discussed in Section 9.11.8, "Reduced Airflow".
3.5.4	Failure of HVAC dampers	Increase in air radioactivity level in certain areas, dose < BSO	DB0	N/A	N/A				DB0 due to radiological consequences less than BSO. Bounded by Fault 3.5.6.	Fault is discussed in Section 9.11.8, "Reduced Airflow".
3.5.5	Leakage	Increase in air radioactivity level in certain areas, dose < BSO	DB0	N/A	N/A				DB0 due to radiological consequences less than BSO. Filters are designed with replaceable cells clamped in place. When replaced, the filters are pressure tested to ensure that are seated correctly to maintain pressure. Alarms will sound if filters are incorrectly stalled, thus leakage is not considered a fault.	Fault is discussed in Section 9.11.4, "Analysis of Faults" in Section 9.11, "Safety Assessment of Heating, Ventilation, and Air Conditioning Faults".

Table 8A-2 AP1000 PCSR Composite Fault List for Reactor Internal and Non-internal Events and Internal and External Hazards (cont.)

Fault ID	Initiating Event		Initiating Event Frequency/ DB Class	Possible Modes Affected	Engineered Safety Functions				Comments	Further Assessment of Fault
	Fault	Consequences			Reactivity Control(short term)		Safety Functions			
					Signals	Devices	Signals	Devices		
3.5.6	Fire	Potential external release of radioactivity, dose < BSO	DB0	N/A	N/A				DB0 due to radiological consequences less than BSO. Release of trapped activity from filters if involved in fire. Breakdown of filters and volatilization of deposited activity on ductwork.	Fault is discussed in Section 9.11.6, "Failure of Filters in the Heating, Ventilation, and Air Conditioning System".
3.5.7	Dropped filters	Release, suspension and dispersal of radioactivity, dose < BSO	DB0	N/A	N/A				DB0 due to radiological consequences less than BSO. Dropped filters can occur during handling (filter exchange, transfer to, or processing in radwaste building	Fault is discussed in Section 9.11.7, "Dropped Filters".
3.5.8	Failure of gaseous radwaste system beds	Potential release of radioactive gas, dose < BSO	DB0	N/A	N/A				DB0 due to radiological consequences less than BSO.	Fault is discussed in Section 9.11.6, "Failure of Filters in the Heating, Ventilation, and Air Conditioning System".
3.5.9	Failure of stack monitoring system	Inability to monitor routine discharges, dose < BSO	DB0	N/A	N/A				DB0 due to radiological consequences less than BSO. Fault is not a sequence initiator in its own right. Fault is an operability issue that does not result in any abnormal discharges.	Fault is discussed in Section 9.11.4, "Analysis of Faults" in Section 9.11, "Safety Assessment of Heating, Ventilation, and Air Conditioning Faults".
3.6 Waste Management										
3.6.1	Drop/impact of solid waste (LLW and WSS)	Potential release, suspension and dispersal of radioactivity, dose < BSO	6.7E-04 per reactor year DB0	N/A	N/A				DB0 due to radiological consequences less than BSO.	Fault is Discussed in Section 9.12.7, "Radioactive Exchangeable Items (Filters and Charcoal Absorbers)".
3.6.2	Drop/impact of solid waste (ILW and WSS)	Potential release, suspension and dispersal of radioactivity, dose < BSO	6.7E-04 per reactor year DB0	N/A	N/A				DB0 due to radiological consequences less than BSO.	Fault is Discussed in Section 9.12.7, "Radioactive Exchangeable Items (Filters and Charcoal Absorbers)".
3.6.3	Setting fire to solid waste	Contamination, airborne release of radioactivity in open air. Potential off-site release	N/A	N/A	N/A				Fault screened out. Potential for a fire is controlled by good housekeeping procedures, ensuring a lack of combustible materials stored near potential sources of ignition.	Fault is discussed in Section 9.12.4, "Analysis of Faults" in Section 9.12, "Radioactive Waste Handling".

Table 8A-2 AP1000 PCSR Composite Fault List for Reactor Internal and Non-internal Events and Internal and External Hazards (cont.)

Fault ID	Initiating Event		Initiating Event Frequency/ DB Class	Possible Modes Affected	Engineered Safety Functions				Comments	Further Assessment of Fault
	Fault	Consequences			Reactivity Control(short term)		Safety Functions			
					Signals	Devices	Signals	Devices		
3.6.4	Operator exposure from stored waste due to inadequate shielding or waste consignment error.	Operator radiation exposure	N/A	N/A	N/A				Shielding is provided as necessary for the waste storage areas to meet radiation zone and access requirements. HP will control the monitoring of radwaste.	Fault screened out in Table 9.10-1, "Screened-out Faults" in Section 9.10, "Operator Exposure Faults".
3.6.5	Incorrect consignment of waste due to assessment, clerical or sampling errors.	Operator radiation exposure	N/A	N/A	N/A				Packaging is done in accordance with local and national requirements. HP will control the monitoring of radwaste.	Fault screened out in Table 9.10-1, "Screened-out Faults" in Section 9.10, "Operator Exposure Faults".
3.6.6	Spills of liquid waste (leak to ground from vessel or pipe work)	Contamination to environment, potential dose to public	N/A	N/A	N/A				Fault screened out. Includes leaks from the spent fuel cooling system pumps and liquid radwaste system.	Fault is discussed in Section 9.12.4, "Analysis of Faults" in Section 9.12, "Radioactive Waste Handling".
3.6.7	Spills of liquid waste (leak to drain)	Contamination to environment, potential dose to public	N/A	N/A	N/A				Fault screened out.	Fault is discussed in Section 9.12.4, "Analysis of Faults" in Section 9.12, "Radioactive Waste Handling".
3.6.8	Un-authorized discharge of gaseous waste	Contamination to environment, potential dose to public	N/A	N/A	N/A				Fault screened out.	Fault is discussed in Section 9.12.4, "Analysis of Faults" in Section 9.12, "Radioactive Waste Handling".
3.6.9	Un-authorized discharge of liquid waste	Higher activity (than routine or permitted) discharges via routine discharge route. Contamination to environment / dose to public	N/A	N/A	N/A				Fault screened out.	Fault is discussed in Section 9.12.4, "Analysis of Faults" in Section 9.12, "Radioactive Waste Handling".
3.6.10	Mispackaging of waste for off-site disposal	Potential dose to operator and public. Also potential for contamination to environment if package integrity is inadequate and compromised.	N/A	N/A	N/A				Fault screened out.	Fault is discussed in Section 9.12.4, "Analysis of Faults" in Section 9.12, "Radioactive Waste Handling".

Table 8A-2 AP1000 PCSR Composite Fault List for Reactor Internal and Non-internal Events and Internal and External Hazards (cont.)

Fault ID	Initiating Event		Initiating Event Frequency/ DB Class	Possible Modes Affected	Engineered Safety Functions				Comments	Further Assessment of Fault
	Fault	Consequences			Reactivity Control(short term)		Safety Functions			
					Signals	Devices	Signals	Devices		
4. Internal Hazards										
4.1 Internal Fires										
4.1.1	Design Basis Fire	Fire is assumed to fail all SSCs in area (zone) of fire unless otherwise specified. Spurious actuations need to be considered unless evidence is provided that shows otherwise. See comments.	>1E-04 per reactor year DB2	1-6	PMS(A,C1) - Low-2 SG NR Level	Rod breakers (C1)	PMS(A,C1) – Low-2 SG NR Level coincident with Low-2 SFW flow	PRHR(C1)	Diversity is not claimed for fires in locations that would compromise DAS; this is discussed and justified in Section 8.2.4.1.	See Sections 10.16 (PSA Internal Fire Analysis) and 11.2 (Internal Hazards Internal Fire) for additional details on this hazard.
							PMS(A,C1) – Low-2 Cold Leg Temperature	CMT(C1) CI(C1)		
							PMS(A,C1) – High-2 Containment Pressure	PCS(C1)		
					DAS(A,C2) – High Hot Leg Temperature	Rod MG Set Breakers (C2)	N/A	ACCUM(C1)		
							DAS(M,C2)	ADS(C1) IRWST(C1) RECIRC(C1)		
							DAS(A,C2) - High Containment Temperature	PCS(C1) CI(C1)		
					DAS(A,C2) – High Hot Leg Temperature	Rod MG Set Breakers (C2)	DAS(A,C2) - High Hot Leg Temperature	PRHR(C1)		
							DAS(A,C2) - Low-2 SG WR Level	CMT(C1)		
							DAS(A,C2) - High Containment Temperature	PCS (C1) CI(C1)		
4.1.2	Fire in Main Control Room	MCR is abandoned	<1E-04 per reactor year DB1	1-6	PMS(M,C1)	Rod Breakers (C1)	PMS(A,C1) – Low-2 SG NR Level coincident with Low-2 SFW flow	PRHR(C1)	Operators perform manual RT in MCR before leaving. They also de-energize MCR controls after leaving and proceeding to Remote Shutdown Room. This is the only credible initiator that causes MCR evacuation; independent initiating events do not occur during MCR evacuation. RSR provides Class 1 displays to allow operators to verify plant is safe. RSR provides Class 1 system level controls in case Class 1 automatic controls fail to function properly.	See Section 11.2 for additional details on this hazard.
							PMS(A,C1) – Low-2 Cold Leg Temperature	CMT(C1) CI(C1)		
							PMS(A,C1) – High-2 Containment Pressure	PCS(C1)		
4.2 Internal Floods										
4.2.1	Flooding inside containment	Dependent on individual scenario	DB1/DB2	1-6	PMS(A,C1) - Low-2 SG NR Level	Rod breakers (C1)	PMS(A,C1) – Low-2 SG NR Level coincident with Low-2 SFW flow	PRHR(C1)	Specific scenarios are linked to fault entries as shown in the internal flooding hazard schedules (See Tables 11.3-3). Scenarios that do not directly result in a fault presented in the fault schedule could lead to (if at power) either a controlled plant shutdown or a reactor trip.	See Sections 10.15 (PSA Internal Flooding Analysis) and 11.3 (Internal Hazards Internal Flood) for additional details on this hazard.
							PMS(A,C1) – Low-2 Cold Leg Temperature	CMT(C1) CI(C1)		
							PMS(A,C1) – High-2 Containment Pressure	PCS(C1)		
4.2.2	Flooding outside containment	Dependent on individual scenario	<1E-04 per reactor year DB1	1-6	PMS(A,C1) - Low-2 SG NR Level	Rod breakers (C1)	PMS(A,C1) – Low-2 SG NR Level coincident with Low-2 SFW flow	PRHR(C1)	Specific scenarios are linked to fault entries as shown in the internal flooding hazard schedules (See Tables 11.3-3). Scenarios that do not directly result in a fault presented in the fault schedule could lead to (if at power) either a controlled plant shutdown or a reactor trip.	See Sections 10.15 (PSA Internal Flooding Analysis) and 11.3 (Internal Hazards Internal Flood) for additional details on this hazard.
							PMS(A,C1) – Low-2 Cold Leg Temperature	CMT(C1) CI(C1)		
							PMS(A,C1) – High-2 Containment Pressure	PCS(C1)		

Table 8A-2 AP1000 PCSR Composite Fault List for Reactor Internal and Non-internal Events and Internal and External Hazards (cont.)

Fault ID	Initiating Event		Initiating Event Frequency/ DB Class	Possible Modes Affected	Engineered Safety Functions				Comments	Further Assessment of Fault
	Fault	Consequences			Reactivity Control(short term)		Safety Functions			
					Signals	Devices	Signals	Devices		
4.2.3	Failures (false signals, human errors or mechanical ruptures) that result in inadvertent operation of IRWST recirculation squib valves	Draining of IRWST and flooding of sump into reactor vessel cavity	<1E-07 Per reactor year BDB	1-6	See Comments				The potential for a failure to initiate spurious IRWST recirculation is so low it is a BDB event. All failures are considered including mechanical ruptures and inadvertent actuation signals. Note that spurious failures not due to software are assumed to be less than 1E-05 events per year. Failures that could cause spurious squib valve opening are discussed in PCSR Chapters 10.4, 17.5 and 19.2. Additional information is available in the Squib Valve Safety Case, UKP-GW-GL-200. Consequences acceptable in all Modes. Operators will likely be able to mitigate transient quickly by closing adjacent MOV to squib valve.	This beyond design basis fault is discussed in Section 10.4.
4.3 Other Internal Hazards										
4.3.1	Pressure Part Failure	Dependent on individual scenario	Dependent on individual scenario	1-6	See Comments				Specific scenarios are linked to fault entries as shown in the pressure part failure hazard schedules (See Tables 11.4-1 and 11.4-2).	See Section 11.4 for additional details on this hazard
4.3.2	Internal Explosions	Dependent on individual scenario	DB1	1-6	PMS(A,C1) - Low-2 SG NR Level	Rod breakers (C1)	PMS(A,C1) – Low-2 SG NR Level coincident with Low-2 SFW flow	PRHR(C1)	Specific scenarios are linked to fault entries as shown in the explosions hazard schedule (See Table 11.5-2). Scenarios that do not directly result in a fault presented in the fault schedule could lead to (if at power) either a controlled plant shutdown or a reactor trip.	See Section 11.5 for additional details on this hazard
							PMS(A,C1) – Low-2 Cold Leg Temperature	CMT(C1) CI(C1)		
							PMS(A,C1) – High-2 Containment Pressure	PCS(C1)		
4.3.3	Internal Missiles	Dependent on individual scenario	DB1	1-6	PMS(A,C1) - Low-2 SG NR Level	Rod breakers (C1)	PMS(A,C1) – Low-2 SG NR Level coincident with Low-2 SFW flow	PRHR(C1)	Specific scenarios are linked to fault entries as shown in the missiles hazard schedule (See Table 11.6-1). Scenarios that do not directly result in a fault presented in the fault schedule could lead to (if at power) either a controlled plant shutdown or a reactor trip.	See Section 11.6 for additional details on this hazard
							PMS(A,C1) – Low-2 Cold Leg Temperature	CMT(C1) CI(C1)		
							PMS(A,C1) – High-2 Containment Pressure	PCS(C1)		
4.3.4	Release of toxic, corrosive, or flammable material	Reduction in personnel to minimum staffing levels; controlled shutdown possible	DB1	1-6	PMS(A,C1) - Low-2 SG NR Level	Rod breakers (C1)	PMS(A,C1) – Low-2 SG NR Level coincident with Low-2 SFW flow	PRHR(C1)	Assumed that operators would remain in MCR and utilise emergency ventilation systems as necessary. No direct impact to any credited Class 1 SSCs. A frequent fault version of this event would result in less onerous consequences than the infrequent fault limiting case presented. Additionally, the diverse mitigation capabilities and safety functions of Fault 1.12.8 “Turbine Trip / Loss of External Electrical Load” would not be prevented due to this event.	See Section 11.7 for additional details on this hazard
							PMS(A,C1) – Low-2 Cold Leg Temperature	CMT(C1) CI(C1)		
							PMS(A,C1) – High-2 Containment Pressure	PCS(C1)		

Table 8A-2 AP1000 PCSR Composite Fault List for Reactor Internal and Non-internal Events and Internal and External Hazards (cont.)

Fault ID	Initiating Event		Initiating Event Frequency/ DB Class	Possible Modes Affected	Engineered Safety Functions				Comments	Further Assessment of Fault
	Fault	Consequences			Reactivity Control(short term)		Safety Functions			
					Signals	Devices	Signals	Devices		
4.3.5	Dropped loads and load mishandling	Possible damage to equipment and structures in direct load path	DB1	1-6	PMS(A,C1) - Low-2 SG NR Level	Rod breakers (C1)	PMS(A,C1) – Low-2 SG NR Level coincident with Low-2 SFW flow	PRHR(C1)	Credible (i.e., design basis) dropped load events inside containment are only postulated during modes 5 and 6 (operation of cranes in containment is prevented by administrative control during higher modes). Specific drop scenarios are linked to fault entries in as shown in the dropped loads hazard schedule (See Table 11.8-3). Dropped load events outside containment that do not directly result in a fault presented in the fault schedule could lead to (if at power) either a controlled plant shutdown or a reactor trip. For all modes, in the event of any dropped load impacting the SFP, actions would be initiated to maintain SFP water level.	See Section 11.8 for additional details on this hazard
							PMS(A,C1) – Low-2 Cold Leg Temperature	CMT(C1) CI(C1)		
							PMS(A,C1) – High-2 Containment Pressure	PCS(C1)		
4.3.6	Biological Agents	Reduction in personnel to minimum staffing levels; controlled shutdown possible	DB1	1-6	PMS(A,C1) - Low-2 SG NR Level	Rod breakers (C1)	PMS(A,C1) – Low-2 SG NR Level coincident with Low-2 SFW flow	PRHR(C1)	Assumed that operators would remain in MCR and utilise emergency ventilation systems as necessary. No direct impact to any credited Class 1 SSCs. A frequent fault version of this event would result in less onerous consequences than the infrequent fault limiting case presented. Additionally, the diverse mitigation capabilities and safety functions of Fault 1.12.8 “Turbine Trip / Loss of External Electrical Load” would not be prevented due to this event.	See Section 11.9 for additional details on this hazard
							PMS(A,C1) – Low-2 Cold Leg Temperature	CMT(C1) CI(C1)		
							PMS(A,C1) – High-2 Containment Pressure	PCS(C1)		
4.3.7	Onsite Transport	No breach of containment, but damage to auxiliary and other supporting buildings possible	DB1	1-6	PMS(A,C1) - Low-2 SG NR Level	Rod breakers (C1)	PMS(A,C1) – Low-2 SG NR Level coincident with Low-2 SFW flow	PRHR(C1)	Consequences bounded by total compartment loss evaluations (e.g., internal fire or flood) A frequent fault version of this event would result in less onerous consequences than the infrequent fault limiting case presented. Additionally, the diverse mitigation capabilities and safety functions of Fault 1.12.8 “Turbine Trip / Loss of External Electrical Load” would not be prevented due to this event.	See Section 11.10 for additional details on this hazard
							PMS(A,C1) – Low-2 Cold Leg Temperature	CMT(C1) CI(C1)		
							PMS(A,C1) – High-2 Containment Pressure	PCS(C1)		
4.3.8	Electromagnetic Interference (EMI)	No consequences to Class 1 SSCs; reactor trip possible for significant event	DB1	1-6	PMS(A,C1) - Low-2 SG NR Level	Rod breakers (C1)	PMS(A,C1) – Low-2 SG NR Level coincident with Low-2 SFW flow	PRHR(C1)	Fail-safe nature of Class 1 SSCs would preclude impact due to EMI hazard; additionally, all applicable Class 1 SSCs have qualification requirements to preclude EMI impacts. A frequent fault version of this event would result in less onerous consequences than the infrequent fault limiting case presented. Additionally, the diverse mitigation capabilities and safety functions of Fault 1.12.8 “Turbine Trip / Loss of External Electrical Load” would not be prevented due to this event.	See Section 11.11 for additional details on this hazard
							PMS(A,C1) – Low-2 Cold Leg Temperature	CMT(C1) CI(C1)		
							PMS(A,C1) – High-2 Containment Pressure	PCS(C1)		

Table 8A-2 AP1000 PCSR Composite Fault List for Reactor Internal and Non-internal Events and Internal and External Hazards (cont.)

Fault ID	Initiating Event		Initiating Event Frequency/ DB Class	Possible Modes Affected	Engineered Safety Functions				Comments	Further Assessment of Fault
					Reactivity Control(short term)		Safety Functions			
	Fault	Consequences			Signals	Devices	Signals	Devices		
5. External Hazards										
5.1 Seismic Events										
5.1.1	Safe Shutdown Earthquake	Reactor Trip using Class 1 SSCs	<1E-04 per reactor year DB1	1-6	PMS(A,C1) - Low-2 SG NR Level	Rod breakers (C1)	PMS(A,C1) – Low-2 SG NR Level coincident with Low-2 SFW flow	PRHR(C1)	All Class 1 SSCs qualified for to perform their safety function in the event of a SSE.	See Section 12.6 for additional details on this hazard
							PMS(A,C1) – Low-2 Cold Leg Temperature	CMT(C1) CI(C1)		
							PMS(A,C1) – High-2 Containment Pressure	PCS(C1)		
5.1.2	Small earthquake	Equivalent to an operating basis earthquake; no significant damage to plant expected	>1E-03 per reactor year DB2	1-3	PMS(A,C1) - Low-2 SG NR Level	Rod breakers (C1)	PMS(A,C1) – Low-2 SG NR Level coincident with Low-2 SFW flow	PRHR(C1)	Magnitude of small earthquake is assumed to be same an OBE (1/3 SSE) Two diverse cases listed. First one is for core cooling. Second one is for Anticipated transient without trip (ATWT). ATWT during this event is bounded by ATWT loss of normal feedwater for peak RCS pressure and by ATWT complete loss of flow for core damage. ATWT Safety functions available for this event are reported; however, limiting ATWT case terminates event after DAS reactor trip.	See Section 12.6 for additional details on this hazard
							PMS(A,C1) – Low-2 Cold Leg Temperature	CMT(C1) CI(C1)		
							PMS(A,C1) – High-2 Containment Pressure	PCS(C1)		
					DAS(A,C2) – High Hot Leg Temperature	Rod MG Set Breakers (C2)	N/A	ACCUM(C1)		
							DAS(M,C2)	ADS(C1) IRWST(C1) RECIRC(C1)		
							DAS(A,C2) - High Containment Temperature	PCS(C1) CI(C1)		
					DAS(A,C2) – High Hot Leg Temperature	Rod MG Set Breakers (C2)	DAS(A,C2) - High Hot Leg Temperature	PRHR(C1)		
							DAS(A,C2) - Low-2 SG WR Level	CMT(C1)		
							DAS(A,C2) - High Containment Temperature	PCS(C1) CI(C1)		
5.1.3	Review Level Earthquake (RLE)	Damage to plant expected; however safe shutdown achievable via additional margin in necessary SSCs credited for SSE.	DBL*	1-3	PMS(A,C1) - Low-2 SG NR Level	Rod breakers (C1)	PMS(A,C1) – Low-2 SG NR Level coincident with Low-2 SFW flow	PRHR(C1)	Assumes acceleration equal to 1.67 times SSE * Probability is less than design basis earthquake, and site dependent	See Section 10.18 “Seismic Margins Assessment” and 12.6.3.4 “Seismic Margin Analysis”
							PMS(A,C1) – Low-2 Cold Leg Temperature	CMT(C1) CI(C1)		
							PMS(A,C1) – High-2 Containment Pressure	PCS(C1)		

Table 8A-2 AP1000 PCSR Composite Fault List for Reactor Internal and Non-internal Events and Internal and External Hazards (cont.)

Fault ID	Initiating Event		Initiating Event Frequency/ DB Class	Possible Modes Affected	Engineered Safety Functions				Comments	Further Assessment of Fault
					Reactivity Control(short term)		Safety Functions			
	Fault	Consequences			Signals	Devices	Signals	Devices		
5.2 Wind Loading / Missiles										
5.2.1	Design Basis Wind event	None	<1E-04 per reactor year DB1	1-6	PMS(A,C1) - Low-2 SG NR Level	Rod breakers (C1)	PMS(A,C1) – Low-2 SG NR Level coincident with Low-2 SFW flow	PRHR(C1)	Based on standard AP1000 plant design tornado (peak wind speed of 300 mph) and associated wind driven missiles	See Section 12.12 for additional details on this hazard
							PMS(A,C1) – Low-2 Cold Leg Temperature	CMT(C1) CI(C1)		
							PMS(A,C1) – High-2 Containment Pressure	PCS(C1)		
5.2.2	Small wind event	None	1E-03 per reactor year DB2	1-3	PMS(A,C1) - Low-2 SG NR Level	Rod breakers (C1)	PMS(A,C1) – Low-2 SG NR Level coincident with Low-2 SFW flow	PRHR(C1)	Based on standard AP1000 plant hurricane (peak winds at 140 mph) and associated wind driven missiles	See Section 12.12 for additional details on this hazard
							PMS(A,C1) – Low-2 Cold Leg Temperature	CMT(C1) CI(C1)		
							PMS(A,C1) – High-2 Containment Pressure	PCS(C1)		
					DAS(A,C2) – High Hot Leg Temperature	Rod MG Set Breakers (C2)	N/A	ACCUM(C1)		
							DAS(M,C2)	ADS(C1) IRWST(C1) RECIRC(C1)		
							DAS(A,C2) - High Containment Temperature	PCS(C1) CI(C1)		
					DAS(A,C2) – High Hot Leg Temperature	Rod MG Set Breakers (C2)	DAS(A,C2) - High Hot Leg Temperature	PRHR(C1)		
							DAS(A,C2) - Low-2 SG WR Level	CMT(C1)		
							DAS(A,C2) - High Containment Temperature	PCS (C1) CI(C1)		
5.2.3	Beyond design basis wind event	Dependent on the severity of the wind event	DBL*	1-6	See Comments				None defined since 5.2.1 is so conservative * Probability is less than design basis wind	See Section 12.12 for additional details on this hazard
5.3 External Floods										
5.3.1	Design basis flood	No immediate consequences, could result in a controlled shutdown	<1E-04 per reactor year DB1	1-6	PMS(A,C1) - Low-2 SG NR Level	Rod breakers (C1)	PMS(A,C1) – Low-2 SG NR Level coincident with Low-2 SFW flow	PRHR(C1)	Flood level less than plant grade	See Section 12.7 for additional details on this hazard
							PMS(A,C1) – Low-2 Cold Leg Temperature	CMT(C1) CI(C1)		
							PMS(A,C1) – High-2 Containment Pressure	PCS(C1)		

Table 8A-2 AP1000 PCSR Composite Fault List for Reactor Internal and Non-internal Events and Internal and External Hazards (cont.)

Fault ID	Initiating Event		Initiating Event Frequency/ DB Class	Possible Modes Affected	Engineered Safety Functions				Comments	Further Assessment of Fault
					Reactivity Control(short term)		Safety Functions			
	Fault	Consequences			Signals	Devices	Signals	Devices		
5.3.2	Small flood	None	1E-03 per reactor year DB2	1-3	PMS(A,C1) - Low-2 SG NR Level	Rod breakers (C1)	PMS(A,C1) – Low-2 SG NR Level coincident with Low-2 SFW flow	PRHR(C1)	Lower flood level than grade (assumed to be same level as 5.3.1)	See Section 12.7 for additional details on this hazard
							PMS(A,C1) – Low-2 Cold Leg Temperature	CMT(C1) CI(C1)		
							PMS(A,C1) – High-2 Containment Pressure	PCS(C1)		
					DAS(A,C2) – High Hot Leg Temperature	Rod MG Set Breakers (C2)	N/A	ACCUM(C1)		
							DAS(M,C2)	ADS(C1) IRWST(C1) RECIRC(C1)		
							DAS(A,C2) - High Containment Temperature	PCS(C1) CI(C1)		
					DAS(A,C2) – High Hot Leg Temperature	Rod MG Set Breakers (C2)	DAS(A,C2) - High Hot Leg Temperature	PRHR(C1)		
							DAS(A,C2) - Low-2 SG WR Level	CMT(C1)		
							DAS(A,C2) - High Containment Temperature	PCS (C1) CI(C1)		
5.3.3	Beyond design basis flood	No immediate consequences, could result in a controlled shutdown	DBL*	1-3	PMS(A,C1) - Low-2 SG NR Level	Rod breakers (C1)	PMS(A,C1) – Low-2 SG NR Level coincident with Low-2 SFW flow	PRHR(C1)	Plant is has additional mitigation features to protect against beyond design basis flooding. Flood level is 5.3 m (fast reseeding) or 2 m (sustained >72 hr) * Probability is less than design basis flood	See Section 12.7 for additional details on this hazard
							PMS(A,C1) – Low-2 Cold Leg Temperature	CMT(C1) CI(C1)		
							PMS(A,C1) – High-2 Containment Pressure	PCS(C1)		
5.4 Other External Hazards										
5.4.1	Accidental Crash of Small Aircraft	No immediate consequences, would likely result in a controlled shutdown	DB1	1-6	PMS(A,C1) - Low-2 SG NR Level	Rod breakers (C1)	PMS(A,C1) – Low-2 SG NR Level coincident with Low-2 SFW flow	PRHR(C1)	No damage to Class 1 SSCs as this fault is within the plant design basis. A frequent fault version of this event would result in less onerous consequences than the infrequent fault limiting case presented. Additionally, the diverse mitigation capabilities and safety functions of Fault 1.12.8 “Turbine Trip / Loss of External Electrical Load” would not be prevented due to this event.	See Section 12.8 for additional details on this hazard
							PMS(A,C1) – Low-2 Cold Leg Temperature	CMT(C1) CI(C1)		
							PMS(A,C1) – High-2 Containment Pressure	PCS(C1)		

Table 8A-2 AP1000 PCSR Composite Fault List for Reactor Internal and Non-internal Events and Internal and External Hazards (cont.)

Fault ID	Initiating Event		Initiating Event Frequency/ DB Class	Possible Modes Affected	Engineered Safety Functions				Comments	Further Assessment of Fault
	Fault	Consequences			Reactivity Control(short term)		Safety Functions			
					Signals	Devices	Signals	Devices		
5.4.2	Accidental Crash of Large Aircraft	No breach of containment, but damage to auxiliary and other supporting buildings possible	DBL	1-6	PMS(A,C1) - Low-2 SG NR Level	Rod breakers (C1)	PMS(A,C1) – Low-2 SG NR Level coincident with Low-2 SFW flow	PRHR(C1)	Dependent on location of damage; however, redundancy/diversity in the plant design exist for any loss of large area.	See Section 12.8 for additional details on this hazard
							PMS(A,C1) – Low-2 Cold Leg Temperature	CMT(C1) CI(C1)		
							PMS(A,C1) – High-2 Containment Pressure	PCS(C1)		
					DAS(A,C2) – High Hot Leg Temperature	Rod MG Set Breakers (C2)	N/A	ACCUM(C1)		
							DAS(M,C2)	ADS(C1) IRWST(C1) RECIRC(C1)		
							DAS(A,C2) - High Containment Temperature	PCS(C1) CI(C1)		
					DAS(A,C2) – High Hot Leg Temperature	Rod MG Set Breakers (C2)	DAS(A,C2) - High Hot Leg Temperature	PRHR(C1)		
							DAS(A,C2) - Low-2 SG WR Level	CMT(C1)		
							DAS(A,C2) - High Containment Temperature	PCS (C1) CI(C1)		
5.4.3	External Explosions	No breach of containment, but damage to auxiliary and other supporting buildings possible	DBL/DB1	1-6	PMS(A,C1) - Low-2 SG NR Level	Rod breakers (C1)	PMS(A,C1) – Low-2 SG NR Level coincident with Low-2 SFW flow	PRHR(C1)	Bounded by aircraft crash event (Faults 5.4.1-5.4.2) A frequent fault version of this event would result in less onerous consequences than the infrequent fault limiting case presented. Additionally, the diverse mitigation capabilities and safety functions of Fault 1.12.8 “Turbine Trip / Loss of External Electrical Load” would not be prevented due to this event.	See Section 12.9 for additional details on this hazard
							PMS(A,C1) – Low-2 Cold Leg Temperature	CMT(C1) CI(C1)		
							PMS(A,C1) – High-2 Containment Pressure	PCS(C1)		
5.4.4	Extreme Ambient Temperatures	No consequences for temperatures within site requirements; temperatures outside of this range would result in a controlled shutdown when tech spec conditions are violated.	DB0	1-6	No Event				Controlled shutdown directed by tech spec limits; no loss to Class 1 SSCs prior to shutdown	See Section 12.10 for additional details on this hazard
5.4.5	Meteorology	No consequences	DB0	1-6	No Event				Controlled shutdown directed by tech spec limits; no loss to Class 1 SSCs prior to shutdown	See Section 12.11 for additional details on this hazard
5.4.6	Offsite Fire and Smoke	Isolation of HVAC systems will automatically engage, and a controlled shutdown may be necessary.	DB1	1-6	PMS(A,C1) - Low-2 SG NR Level	Rod breakers (C1)	PMS(A,C1) – Low-2 SG NR Level coincident with Low-2 SFW flow	PRHR(C1)	Internal fire faults bound this external hazard as this hazard group would not result in lost Class 1 SSCs within the plant structures. A frequent fault version of this event would result in less onerous consequences than the infrequent fault limiting case presented. Additionally, the diverse mitigation capabilities and safety functions of Fault 1.12.8 “Turbine Trip / Loss of External Electrical Load” would not be prevented due to this event.	See Section 12.13 for additional details on this hazard
							PMS(A,C1) – Low-2 Cold Leg Temperature	CMT(C1) CI(C1)		
							PMS(A,C1) – High-2 Containment Pressure	PCS(C1)		

Table 8A-2 AP1000 PCSR Composite Fault List for Reactor Internal and Non-internal Events and Internal and External Hazards (cont.)

Fault ID	Initiating Event		Initiating Event Frequency/ DB Class	Possible Modes Affected	Engineered Safety Functions				Comments	Further Assessment of Fault
					Reactivity Control(short term)		Safety Functions			
	Fault	Consequences			Signals	Devices	Signals	Devices		
5.4.7	Offsite Missiles	No breach of containment, but damage to auxiliary and other supporting buildings possible	DB1	1-6	PMS(A,C1) - Low-2 SG NR Level	Rod breakers (C1)	PMS(A,C1) – Low-2 SG NR Level coincident with Low-2 SFW flow	PRHR(C1)	Bounded by aircraft crash event A frequent fault version of this event would result in less onerous consequences than the infrequent fault limiting case presented. Additionally, the diverse mitigation capabilities and safety functions of Fault 1.12.8 “Turbine Trip / Loss of External Electrical Load” would not be prevented due to this event.	See Section 12.14 for additional details on this hazard
							PMS(A,C1) – Low-2 Cold Leg Temperature	CMT(C1) CI(C1)		
							PMS(A,C1) – High-2 Containment Pressure	PCS(C1)		
5.4.8	Biological Fouling	Should fouling be significant enough, controlled shutdown may be necessary	DB1	1-6	PMS(A,C1) - Low-2 SG NR Level	Rod breakers (C1)	PMS(A,C1) – Low-2 SG NR Level coincident with Low-2 SFW flow	PRHR(C1)	Limiting scenarios would be bounded by existing analyses for loss of secondary water supplies, or tech spec limits and conditions would lead to a controlled shutdown. A frequent fault version of this event would result in less onerous consequences than the infrequent fault limiting case presented. Additionally, the diverse mitigation capabilities and safety functions of Fault 1.12.8 “Turbine Trip / Loss of External Electrical Load” would not be prevented due to this event.	See Section 12.15 for additional details on this hazard
							PMS(A,C1) – Low-2 Cold Leg Temperature	CMT(C1) CI(C1)		
							PMS(A,C1) – High-2 Containment Pressure	PCS(C1)		
5.4.9	Electromagnetic Interference (EMI) and Lighting	No consequences to Class 1 SSCs; reactor trip possible for significant event	DB1	1-6	PMS(A,C1) - Low-2 SG NR Level	Rod breakers (C1)	PMS(A,C1) – Low-2 SG NR Level coincident with Low-2 SFW flow	PRHR(C1)	Fail-safe nature of Class 1 SSC would preclude impact due to EMI hazard A frequent fault version of this event would result in less onerous consequences than the infrequent fault limiting case presented. Additionally, the diverse mitigation capabilities and safety functions of Fault 1.12.8 “Turbine Trip / Loss of External Electrical Load” would not be prevented due to this event.	See Section 12.16 for additional details on this hazard
							PMS(A,C1) – Low-2 Cold Leg Temperature	CMT(C1) CI(C1)		
							PMS(A,C1) – High-2 Containment Pressure	PCS(C1)		

Table 8A-3 AP1000 PCSR Fault List for Decommissioning and Dry Spent Fuel Storage Faults

Fault ID	Initiating Event		Comments
	Fault	Consequences	
6. Decommissioning Operations			
6.1	Refuelling faults arising during post operation clear out (POCO) activities (Stage I).	Criticality and inadvertent worker radiation exposure.	Potential range of faults is identical with and bounded by that for equivalent normal refuelling operations faults identified above under “non-reactor faults”.
6.2	Failure to contain radioactive liquid effluent during decontamination activities (Stages I and II).	Potential worker dose.	
6.3	Failure to contain radioactive solid particulate debris during cutting activities (Stages II and III).	Potential worker dose.	
6.4	Worker radiation exposure due to inadequate provision, or failure of (e.g., in a seismic event), temporary shielding during decontamination or dismantling operations (Stages I, II and III).	Potential worker dose.	
6.5	Release and dispersal of radioactive material due to aircraft impact while structures are compromised during dismantling operations (Stages II and III).	Potential radiation dose to workers and the public.	Containment/shield building and fuel handling area of auxiliary building (used as temporary decommissioning waste management facility) are removed after the bulk of the wastes (particularly ILW) have been removed. External hazard qualification of these buildings may therefore be retained.
6.6	Air suspension and release of radioactive material through ruptured temporary containment due to seismic event (Stages I, II and III).	Potential worker dose.	

Table 8A-3 AP1000 PCSR Fault List for Decommissioning and Dry Spent Fuel Storage Faults (cont.)

Fault ID	Initiating Event		Comments
	Fault	Consequences	
6.7	Decommissioning waste management faults (Stages I, II and III).	Potential worker dose.	Faults are similar to the generic waste management faults listed above under non reactor faults. Radioactive wastes include liquid and contaminated solid waste from decontamination activities and solid wastes from disassembly and cutting operations.
7. Dry Spent Fuel Storage (Proposed Holtec Hi-STORM 100 Dry Cask System)			
Cask Loading and Handling Phase			
7.1	Dropping of transfer cask into spent fuel pond or onto floor or storage overpack during handling.		
7.2	Accidental drop of fuel assembly during loading of multi-purpose canister (MPC).	Fuel damage and radioactivity release. Worker dose.	
7.3	Misloading of lower burnup fuel assembly into MPC.	Criticality. Very high local radiation doses and radioactivity release.	
7.4	Accidental spent fuel pond boron dilution prior to or during MPC loading.	Criticality	
7.5	Dropped load onto transfer cask in the cask pit.	Potential fuel damage and criticality due to distortion of fuel assemblies/MPC fuel basket.	
7.6	Fire from diesel fuel in the trackmobile used for storage cask transfer to transporter outside secondary containment.	Potential failure of overpack and internal damage or rupture of MPC. Loss of shielding.	
Cask Transfer Phase			
7.7	Failure of storage cask due to drop or tip-over onto hard surfaces.	Potential damage to MPC and fuel.	

Table 8A-3 AP1000 PCSR Fault List for Decommissioning and Dry Spent Fuel Storage Faults (cont.)

Fault ID	Initiating Event		Comments
	Fault	Consequences	
7.8	Impact from another vehicle during transfer.	Potential damage to MPC and fuel.	
7.9	Fire from diesel fuel in the transporter used for storage cask transfer to storage facility.	Potential failure of overpack and internal damage or rupture of MPC. Loss of shielding.	
Cask Storage Phase			
7.10	Abnormal external floodwater loading on the intermediate storage facility	Structural damage to installation and casks contained within.	
7.11	Impulsive loads on intermediate storage facility due to impact by heavy objects including aircraft and external vehicles.	Structural damage to installation and casks contained within.	
7.12	Shockwaves from external explosions.	Structural damage to installation and casks contained within.	
7.13	Overheating of storage casks due to vent blockage.	Thermal damage to casks.	
7.14	Lightning damage to storage casks.	Cracking of casks.	
7.15	Fire from external or site-specific fuel source. Includes aircraft crash, gas main, and forest fire.	Potential for over-pressurisation of storage casks and excessive differential thermal stresses.	
7.16	Long term corrosion of MPC in high humidity, coastal, and industrial environments.	Preferential attack on welds weakening or perforation of MPC.	

Table 8A-4 Support Systems for Front Line SSCs Listed in Table 8A-2

Function	System	Class 1 SSCs		Class 2 SSCs				
		PMS	DC	DAS	PLS	DC	AC	HVAC[5]
C&I	PMS		x					(6)
	DAS					x		(6)
	PLS					x	x	x
Reactor shutdown								
	Rod insert	x	(1)					
	Rod insert			x		x		
	Ride out (2)			x		x		
RCS makeup								
	CMTs	x	(1)					
	CMTs			x		x		
	Accumulators							
	IRWST	x	x					
	IRWST			x		x		
	Containment Recirculation	x	x					
	Containment Recirculation			x		x		
	RNS inject				x	x	x	x
	ADS 1,2,3,4	x	x					
	ADS 1,2,3,4			x		x		
RCS heat removal								
	PRHR HX	x	(1)					
	PRHR HX			x		x		
	(3)							
RCS pressure protection								
	Pressuriser Safety Valves	Passively acting SSCs						
	Pressuriser Volume(4)							
Containment cooling								
	PCS water drain	x	(1)					
	PCS water drain			x		x		
Containment isolation								
	Valve act.	x	x					
	Valve act.			x		x		

Notes:

1. These passive system functions self-actuate on loss of instrument air or Class 1 DC.
2. Plant can ride out failure to inset rods with DAS actuation of turbine trip, PRHR HX, and CMTs. Core moderator temperature coefficient helps reduce core power.
3. RCS makeup features provide diverse RCS heat removal and primary heat removal for LOCAs as indicated in Table 8A-2.
4. Pressuriser volume is sufficient to provide RCS overpressure protection.
5. HVAC transfers heat to the chilled water system (VWS) to support operation of these Class 2 SSCs.
6. PMS and DAS do not require HVAC as discussed in 8A.1.

Table 8A-5 AP1000 SSCs Used for Long-Term Passive System Support

	Component	Location	Comment
Primary Case			
Water makeup	Self-power pumps	Offsite	For PCS and SFP
Electrical power	DGs	Offsite	For PMS and fans
PMS room cooling	Fans	Offsite	Circulates outside air
MCR cooling	Fans	Offsite	Circulates outside air
Backup Case (1)			
Water makeup	PCS recirculation pumps	Installed (1)	For PCS & SFP
Electrical power	Ancillary DGs	Installed (1)	For PMS & fans
PMS room cooling	Ancillary PMS Fans	Installed (1)	Circulates outside air
MCR cooling	Ancillary MCR fans	Installed (1)	Circulates outside air

Notes:

1. These installed SSCs are considered Class 2 although they are not the primary means of providing these Class 2 functions. The offsite SSCs are the primary means of providing these long-term functions. The function of these installed SSCs is to reduce the probability that the offsite SSCs will need to be brought to the plant.

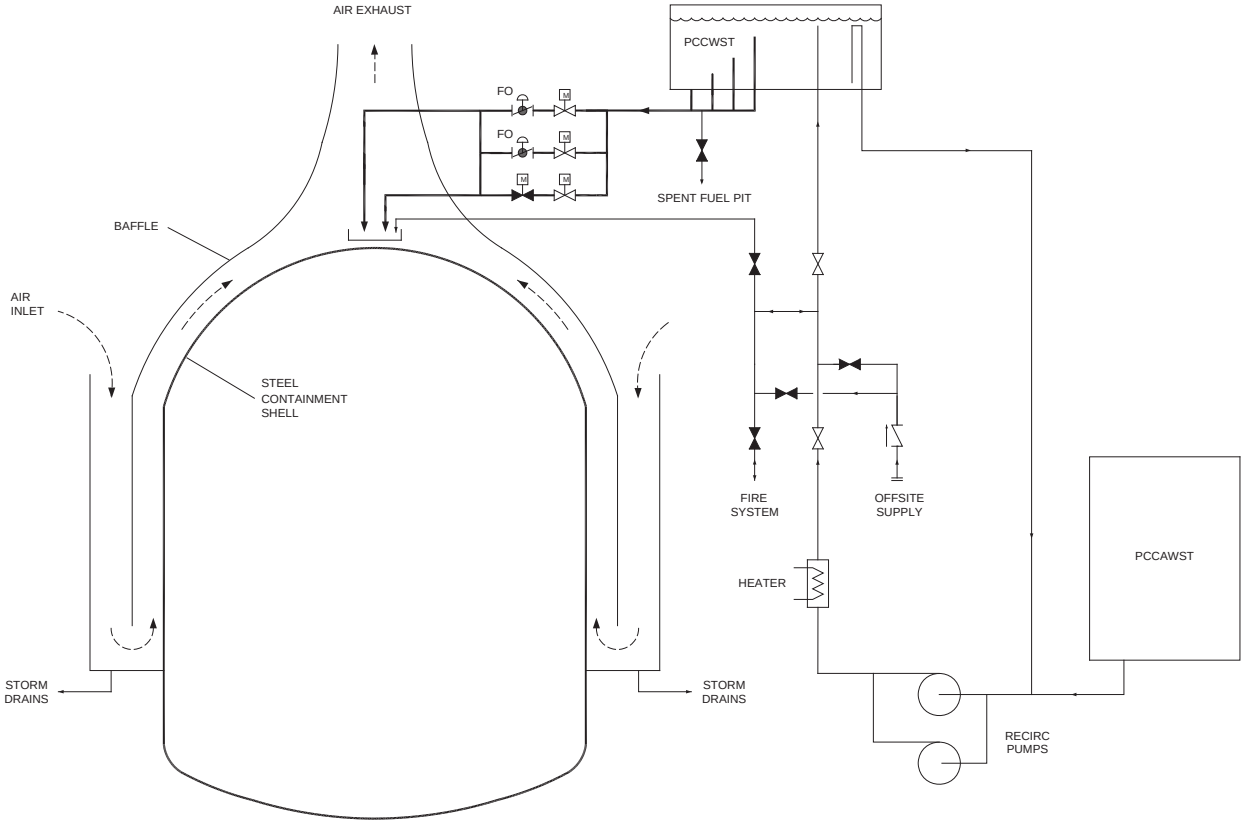


Figure 8A-1 Passive Containment Cooling System Schematic

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS, ACRONYMS, AND TRADEMARKS

ac	alternating current
Accum	accumulator(s)
ADS	automatic depressurisation system
AFD	automatic fire detection and alarm system
AHU	air handling unit
ALARP	as low as reasonably practicable
AMAD	activity median aerodynamic diameter
ANC	neutronics code
ANS	American Nuclear Society
ANSI	American National Standards Institute
AO	axial offset
AOV	air-operated valve
ASME	American Society of Mechanical Engineers
ASTRUM	automated statistical treatment of uncertainty method
ATWS	anticipated transient without scram
ATWT	anticipated transient without trip
BDB	beyond design basis
BDPS	boron dilution protection system
BDS	steam generator blowdown system
BOC	beginning of cycle
BSL	basic safety level
BSO	basic safety objective
C&I	control and instrumentation
CCF	common cause failure
CCS	component cooling water system
CEDE	committed effective dose equivalent
CFIL	Council Food Intervention level
CHF	critical heat flux
CI	containment isolation
CL	cold leg
CLOF	complete loss of flow
CLP	cask loading pit
CMT	core makeup tank
CMTLB	core makeup tank line break
COLR	Core Operating Limit Report
CRDM	control rod drive mechanism
CsI	caesium iodide
CVS	chemical and volume control system
CWO	core-wide oxidation
DAS	diverse actuation system
DB	design basis
DBA	design basis assessment
dc	direct current
DCF	decontamination factor
DECLG	double-ended, cold-leg guillotine
DEDVI	double-ended, direct vessel injection
DEHLG	double-ended, hot-leg guillotine
DEG	double-ended guillotine
DF	decontamination factor
DG	diesel generator
DiD	defence in depth

DMW	demineralised water
DNB	departure from nucleate boiling
DNBR	departure from nucleate boiling ratio
DRP	design reference point
DVI	direct vessel injection
DWS	demineralised water transfer and storage system
DWST	demineralised water storage tank
EAB	exclusion area boundary
ECCS	emergency core cooling system
ECS	main ac power system
EDE	effective dose equivalent
EDS	standby electrical supply system
EM	evaluation model
EMDAP	Evaluation Model Development and Review Process
EOC	end of cycle
ESF	engineered safety feature
FDF	fuel damage frequency
FF	frequent fault
FHA	fuel handling accident
FID	fixed incore detector
FON	fraction of nominal
FPS	fire protection system
FSG	fault sequence group
FTC	fuel transfer canal
FWS	main and startup feedwater system
GDA	generic design assessment
GDL	generalised derived limit
GNS	general non-safety
GRCA	gray rod control assembly
GSP	grab sample panel
HEM	homogeneous equilibrium
HEPA	high-efficiency particulate air
HFLC	high frequency, low-consequence
HFP	hot full power
HL	hot leg
HSE	Health and Safety Executive
HVAC	heating, ventilation, and air conditioning
HX	heat exchanger
HZP	hot zero power
ICRP	International Commission on Radiological Protection
ID	identification
IDS	essential electrical supply system
IEF	initiating event frequency
IHP	integrated head package
ILW	intermediate-level waste
IoF	incredibility of failure
IRNI	intermediate range nuclear instrumentation
IRWST	in-containment refuelling water storage tank
ITC	isothermal temperature coefficient
K_{eff}	effective multiplication factor
LBLOCA	large-break loss-of-coolant accident
LCCW	loss of component cooling/service water
LCO	limiting conditions for operations

LLW	low-level waste
LOCA	loss-of-coolant accident
LONF	loss of normal feedwater
LOOP	loss of offsite power
LRF	large release frequency
LTOP	low-temperature overpressure protection
MG	motor generator
MBLOCA	medium-break loss-of-coolant accident
MCR	main control room
MDC	moderator density coefficient
MFW	main feedwater
MFWIV	main feedwater isolation valve
MLO	maximum local oxidation
MOV	motor-operated valve
MSIV	main steam isolation valve
MSLB	main steam line break
MSS	main steam system
MSSV	main steam safety valve
MTC	moderator temperature coefficient
MTO	margin to overfill
MTTR	mean time to repair
MWD/MTU	megawatt days per metric ton of uranium
NIS	nuclear instrumentation system
NPP	Nuclear Power Plant
NPSH	net positive suction head
NR	narrow range
NRC	U.S. Nuclear Regulatory Commission
NSSS	nuclear steam supply system
OPΔT	overpower ΔT
OTΔT	overtemperature ΔT
PAMS	post-accident monitoring system
PCCAWST	passive containment cooling ancillary water storage tank
PCCWST	passive containment cooling water storage tank
PCMI	pellet clad mechanical interaction
PCS	passive containment cooling system
PCSR	Pre-Construction Safety Report
PCT	peak clad temperature
pfd	probability of failure on demand
PIRT	phenomena identification and ranking table
PLOF	partial loss of flow
PLS	plant control system
PMS	protection and safety monitoring system
PORV	power-operated relief valve
POW	person organising work
PPE	personal protective equipment
PRHR	passive residual heat removal
PRHR HX	passive residual heat removal heat exchanger
PSA	probabilistic safety assessment
PSV	pressuriser safety valve
PTLR	Pressure and Temperature Limits Report
PWR	pressurized water reactor
PXS	passive core cooling system
PZR	pressuriser

RAD	refuelling cavity
RC	refuelling cavity
RCCA	rod cluster control assembly
RCP	reactor coolant pump
RCS	reactor coolant system
RF	release fraction
RFA	robust fuel assembly
RHR	residual heat removal
RM	refuelling machine
RNS	normal residual heat removal system
RPRS	rapid power reduction system
RPV	reactor pressure vessel
RT	reactor trip
RTDP	revised thermal design procedure
RTP	rated thermal power
RV	reactor vessel
RWAP	RCCA withdrawal at power
RWS	raw water system
S signal	safeguards signal
SAL	Safety Analysis Limit
SAP	safety assessment principle
SBLOCA	small-break LOCA
SDM	shutdown margin
SFP	spent fuel pool
SFS	spent fuel pool cooling system
SFW	startup feedwater
SG	steam generator
SGS	steam generator system
SGTR	steam generator tube rupture
SI	safety injection
SI-LB	safety injection line break
SLC	site licence condition
SR	surveillance requirement
SSC	systems, structures, or components
SV	safety valve
SWS	service water system
T_{avg}	average temperature
Tech Spec	technical specification
TEDE	total effective dose equivalent
UK	United Kingdom
US	United States
Vac	voltage, alternating current
VAS	radiologically controlled area ventilation system
VBS	nuclear island nonradioactive ventilation system
VCS	containment recirculation cooling system
VES	main control room emergency habitability system
VFS	containment air filtration system
VHS	health physics and hot machine shop HVAC system
VRS	radwaste building HVAC system
VTS	turbine building ventilation system
VWS	central chilled water system
VXS	annex/auxiliary building nonradioactive HVAC system
VZS	diesel generator building heating and ventilation system

WGOTHIC	Westinghouse GOTHIC
WGS	gaseous radwaste system
WLS	liquid radwaste system
WR	wide range
WRS	radioactive waste drain system
WSS	solid radwaste system
ZAS	main generation system
ZOS	onsite standby power system

9 INTERNALLY INITIATED FAULTS

9.0 Introduction

The safety case for the AP1000 plant is required to demonstrate that regulatory targets are met and that the risks from all modes of normal operation and fault conditions are shown to be as low as reasonably practicable (ALARP). The internally initiated fault assessment presented in this chapter is central to both of these requirements and provides a foundation for the safety case.

The internally initiated fault assessment consists of a design basis assessment (DBA) for each identified fault to provide a robust demonstration that the engineering design and the provision of safety measures lead to a high degree of fault tolerance. This includes both frequent and infrequent faults as discussed below. Design basis (DB) faults are those abnormal events that have the potential to give radiation doses above the basic safety level (BSL) specified in Target 4 of the Office of Nuclear regulation (ONR) Safety Assessment Principles (SAPs) (Reference 9.0-1).

The DBA presented for each frequent and infrequent fault are directly applicable to the United Kingdom (UK) design reference point (DRP), UKP-GW-GL-060 (Reference 9.0-22). These design basis analyses are appropriately conservative to bound a significant set of potential plant conditions and are therefore considered to be appropriate to the plant safety case and UK AP1000 plant design. At this time, there are a few design changes that have been approved to resolve UK-specific issues that have not been incorporated into the design reference point and this analysis. Examples include a reactor coolant pump (RCP) from a different vendor and a revised normal residual heat removal system (RNS) design. The design change with the biggest potential to impact the presented analyses is the change to the alternate RCP vendor. The RNS change is less likely to impact the analyses since it is not credited in most of the Chapter 9 faults due to its safety classification. Key reactor coolant pump parameters used in the safety analysis, such as flow coastdown versus time, will be used as a part of the pump design specification for the future vendor to meet. As a result, it is expected that the overall conclusions of the analysis will continue to show that the AP1000 design satisfies the applicable safety criteria with appropriate margins.

In addition to the DBA analyses, diverse protection analyses are provided for the frequent faults identified in Table 8A-2 (initiating event frequencies (IEFs) $>10^{-3}$/yr). These analyses, which may use relaxed analysis assumptions and success criteria, demonstrate that diverse protection is provided to mitigate the events. For frequent faults, two different diverse analyses are provided, one for core cooling and another for reactor shutdown (anticipated transients without trip, (ATWT)). Reference 9.0-23 provides a systematic assessment of the frequent faults and identifies the systems, structures and components (SSCs) credited to provide diverse mitigation. Each frequent fault is either analysed in detail or else is shown to be bounded by another fault that is analysed in detail.

UKP-SSAR-GLR-001 (Reference 9.0-24) documents the sources of technical information providing the basis for the overall safety case of the AP1000 contained in Chapter 9 and justification for the use of these analyses. Appendix A of Reference 9.0-24 provides a listing of all AP1000 standard plant analysis documents that serve as the basis for the text in Chapter 9. Appendix B of Reference 9.0-24 provides a listing of all UK specific analysis documents that provide a basis for additional text in Chapter 9 including UK specific radiological consequences, frequent fault diversity, shutdown mode faults, spent fuel pool faults, and ATWT.

Finally, other reasonably practicable protection or mitigation measures are considered to provide additional evidence that the risks from operation and the fault conditions are ALARP. As part of the development process for the AP1000 plant design, the design adhered to the principles of ALARP by keeping the design safe, proven, and simple, without relying on alternating current (ac) power for safety functions. In addition, for the UK application of the AP1000 design a few changes to the standard AP1000 design have been determined to be ALARP and incorporated. Refer to section 9.0.15 for additional discussion on ALARP considerations with respect to internally initiated faults.

A systematic, auditable, and comprehensive identification of fault conditions is presented in the previous chapter and the fault list given in Appendix 8A. Chapter 9 provides the safety case for all internally initiated faults (that is, faults that originate within the reactor system itself or in other active systems or processes of the plant).

Internally initiated faults are typically those initiated by failures of normally operating systems or services, through inadvertent actuation of safety systems or through human errors. Internally initiated faults are distinguished from internal hazards, which, although they originate on the site, are events that may directly cause harm or damage, and consequently present a threat to fundamental safety functions. Internal hazards are discussed in Chapter 11 of the Pre-Construction Safety Report (PCSR).

This chapter covers internally initiated faults in the following areas:

- Reactor during all modes of operation
- Spent fuel handling and storage
- Radwaste management
- Active ventilation systems

For internally initiated faults in the reactor, all modes of operation are considered. These modes are shown in Table 9.0-1, taken from the AP1000 reactor fault schedule given in Appendix 8A.

In each of the fault areas itemised above, a number of faults have been identified, as described in Section 8.3. Faults that have generally similar properties (for example, reactor faults that lead to an increase in heat removal from the reactor coolant system (RCS) are allocated to a number of classes. Each fault class is the subject of a section in this chapter and presented in Table 8A-2.

Many of the faults develop in a similar way, and the protection provided to prevent their development or mitigate their consequences is the same. These faults are therefore dealt with as fault groups as described in Section 8.4 and presented in Chapter 9. Some of the fault classes consist of a single fault group, while others are subdivided into two or more groups.

The assessment of each fault has the same basic elements: a description of the fault, a design basis analysis, a diverse analysis (ATWT and core cooling) for frequent faults, and an ALARP assessment. Sections 9.1 to 9.6 describe the safety case for each fault identified in Table 8A-2 for internally initiated reactor faults initiating in at-power modes (Typically Modes 1 or 2). Each fault is first described and the initial event frequency and the design basis class are provided.

The analysed fault(s) are described in additional detail in the subsequent sections to complete the safety case for each fault, including:

- Identification of Causes and Accident Description
- Design Basis Mitigation
- Diverse Mitigation for ATWT and Core Cooling for Frequent Faults
- Assessment of the Radiological Consequences
- ALARP Assessment
- Conclusions

The safety case for each fault also includes a summary of credited SSCs for all primary DBA cases as well as all diversity cases, as applicable. These sections are meant to provide a linkage to Table 8A-2 and the listed engineered safety features (ESFs) for the detailed fault progression discussions that follow. Specific safety features are listed with Control & Instrumentation (C&I) actuation signals where applicable. Manual actuations are also identified and linked with the C&I system that would provide indication to the operator. Passively acting components, such as accumulators or pressuriser relief valves are noted, but not linked with a specific C&I system or actuation signal. For additional information regarding the treatment of credited SSCs, see Appendix 8A.

Section 9.8 provides an evaluation of faults that could be initiated during lower modes of operation. As most of these faults see the most limiting consequences during higher power modes, many of the sections of 9.8 refer back to the at-power descriptions provided in Sections 9.1-9.6. However, each section does clarify the event classification, radiological consequences, and a conclusion using the information from all valid modes where the fault may occur.

Sections 9.7 and 9.9 to 9.12 describe in detail non-reactor faults identified in Table 8A-2. Each section provides an overview of the system or systems that have the potential to present a hazard to operators or members of the public.

The fault(s) are described in additional detail in the subsequent sections to complete the safety case for each fault, including:

- Fault Description
- IEF and Design Basis Class
- Fault Progression
- Assessment of the Radiological Consequences
- ALARP Assessment
- Conclusions

9.0.1 Fault Groupings

Faults are arranged in groups to facilitate their understanding and analysis. These groupings are based on the faults having similar initiators and/or impacts on the reactor. This grouping is shown in the fault schedule within Chapter 8 and continues in the fault evaluations presented throughout Chapter 9. For each fault, an assessment is given for the unmitigated consequences (that is, without the provision of essential safety functions) and the IEF. These two parameters are used to assign the fault to a DB class, as described in Section 8.2.3.

Faults in classes BDB and DB0, as described in Section 8.2.3, are screened out and not analysed further in this chapter, as they are outside the DB. However, their contribution to the total risk is accounted for in the PSA presented in Chapter 10.

9.0.2 Design Basis Assessment

The AP1000 design has a number of SSCs designed to provide essential safety functions in the event of a fault. The DBA provides a robust, conservative, and deterministic analysis of the fault progression to demonstrate that design basis dose targets (SAP Target 4) are met with these safety provisions in place and correctly operating. The DB classes are identified and explained in Section 8.2.3. Fault sequences with various identified SSCs not operating are also identified. For the events where there may be additional acceptance criteria, this criteria identified in Table 9.0-3.

For faults in the DB1, DB2 and DBL classes, the SSCs identified as being the principal means of providing the (Category A) safety functions are designated as Class 1. For faults in the DB2 class, there is a requirement to identify a diverse means of providing the Category A safety function. A diverse protection analysis is provided for these frequent fault events.

For faults in the high frequency, low consequence (HFLC) class, a similar assessment leads to the designation of the principal means of providing the safety functions (Category B in this case) as Class 2. In these cases, further SSCs may be identified as providing defence in depth.

In addition to the above, any operator actions[1] required to actuate or realign SSCs to achieve the necessary safety functions, or to protect the operators from exposure to radiation (for example, evacuation), are identified and classified, as are any operating limits or conditions (usually, already identified in Technical Specifications (Tech Specs)) that must be met to meet the acceptance criteria and the risks have been reduced to be ALARP.

DBA dose calculations to assess radiological consequences for comparison with targets have been performed in accordance with Reference 9.0-2. The verification and validation status of the codes and methods used for the transient analyses required to complete the DBA is summarised in Appendix 9B.

9.0.2.1 Assumptions within the Design Basis Assessment

The DBA presented in this chapter relies on a large number of transient and other analyses. These analyses demonstrate that the SSCs identified are adequate to ensure that the plant remains within DB limits following any DB fault or event.

For every fault, the corresponding analysis assumes that the plant is operating within certain parameters or in specified conditions at the start of the fault. The progression of the fault and its consequences will depend critically on these assumptions. The assumptions will include those about such things as initial pressures and temperatures and about the availability and status of SSCs designated to protect the plant or mitigate the consequence of the fault.

The safety case depends critically on these assumptions since they define the bounds of the applicability of the analysis. During subsequent operation of the plant, it is necessary to ensure that operations remain within the boundaries defined by these assumptions because otherwise the safety case supported by these transient analyses may not be valid.

These assumptions fall into two groups:

- Limits and conditions that define the operating envelope of the plant and therefore define the initial conditions before any transient

1. The operator actions are summarised in Chapter 13.

- Limits and conditions that ensure that the Class 1 SSCs identified in the DB analysis operate according to their design and as assumed in the DB analysis.

These assumptions correspond to Technical Specifications.

A number of similar limits and conditions apply to the operation of Class 2 SSCs identified as providing defence in depth. These limits and conditions are defined in short-term availability controls relating to those SSCs.

The limits and conditions assumed in the safety analysis are listed in Table 9.0-4.

Further limits and conditions are identified in the fault analyses that constitute requirements for plant operations to ensure that doses from certain DB faults remain within DB limits. These are identified and listed in the corresponding fault analysis.

In addition to the limits and condition discussed above, each fault assessment also makes a number of assumptions to define a bounding case. These assumptions are usually about such things as state of the fuel cycle or pre-existing or coincident single failures that lead to conservative conditions for the analysis. As such, they do not have any implications for how the plant should be operated and are not identified as bounding limits or conditions. They are identified in the text in the corresponding fault analysis in this chapter.

9.0.2.2 Design Plant Conditions

Table 9.0-5 lists the principal power rating values assumed in the analyses performed at power. The thermal power output includes the effective thermal power generated by the reactor coolant pumps. Selected AP1000 plant loop layout elevations are shown in Figure 9.0-2 to aid in interpreting plots shown in Chapter 9 sections.

The values of other plant parameters used in the accident analyses are given in Table 9.0-7.

9.0.2.3 Initial Conditions

For most accidents that are departure from nucleate boiling (DNB) limited, nominal values of initial conditions are assumed. The allowances on power, temperature, and pressure are determined on a statistical basis and are included in the departure from nucleate boiling ratio (DNBR) design limit values (see Section 22.7.1.1), as described in WCAP-11397-P-A (Reference 9.0-4). This procedure is known as the Revised Thermal Design Procedure (RTDP).

For most accidents that are not DNB limited, or for which the revised thermal design procedure is not used, the initial conditions are obtained by adding the maximum steady-state errors to rated values. The following conservative steady-state errors are assumed in the analysis:

Core power	$\pm$ 1 percent allowance for calorimetric error.
Average reactor coolant temperature	$\pm$ 4.4°C (8.0°F) allowance for controller deadband and measurement errors
Pressuriser pressure	$\pm$ 0.34 MPa (50 psi) allowance for steady-state fluctuations and measurement errors

Initial values for core power, average reactor coolant system temperature, and pressuriser pressure are selected to minimize the initial DNBR unless otherwise stated in the sections

describing the specific accidents. Table 9.0-6 summarizes the initial conditions and computer codes used in the accident analyses.

9.0.2.4 Power Distribution

The transient response of the reactor system is dependent on the initial power distribution. The nuclear design of the reactor core minimizes adverse power distribution through the placement of fuel assemblies and control rods. Power distribution may be characterized by the nuclear enthalpy rise hot channel factor ($F_{\Delta H}$) and the total peaking factor (F_q). Unless specifically noted otherwise, the peaking factors used in the accident analyses are those presented in Chapter 22.

For transients that may be DNB limited, the radial peaking factor is important. The radial peaking factor increases with decreasing power level due to control rod insertion. This increase in $F_{\Delta H}$ is included in the core limits illustrated in Figure 9.0-1. Transients that may be departure from nucleate boiling limited are assumed to begin with an $F_{\Delta H}$, consistent with the initial power level defined in the Technical Specifications.

The axial power shape used in the DNB calculation is a chopped cosine, as discussed in Section 22.7.1.1, for transients analysed at full power and the most limiting power shape calculated or allowed for accidents initiated at non-full power or asymmetric rod cluster control assembly (RCCA) conditions.

The radial and axial power distributions just described are input to the VIPRE-01 code as described in Section 22.7.1.1.

For transients that may be overpower-limited, the total peaking factor (F_q) is important. Transients that may be overpower-limited are assumed to begin with plant conditions, including power distributions, which are consistent with reactor operation as defined in the Technical Specifications.

For overpower transients that are slow with respect to the fuel rod thermal time constant (for example, the chemical and volume control system malfunction that results in a slow decrease in the boron concentration in the reactor coolant system as well as an excessive increase in secondary steam flow) and that may reach equilibrium without causing a reactor trip, the fuel rod thermal evaluations are performed as discussed in Section 22.7.1.

For overpower transients that are fast with respect to the fuel rod thermal time constant (for example, the uncontrolled RCCA bank withdrawal from subcritical or lower power startup and RCCA ejection incident, both of which result in a large power rise over a few seconds), a detailed fuel transient heat transfer calculation is performed.

9.0.2.5 Reactivity Coefficients

The transient response of the reactor system is dependent on reactivity feedback effects, in particular, the moderator temperature coefficient and the Doppler power coefficient. These reactivity coefficients are discussed in Section 22.6.2.11.

In the analysis of certain events, conservatism requires the use of large reactivity coefficient values; while for other events, the use of small reactivity coefficient values is conservative. The values used are given in Figure 9.0-3, which shows the upper and lower bound Doppler power coefficients as a function of power, used in the transient analysis. The justification for use of conservatively large versus small reactivity coefficient values is treated on an event-by-event basis. In some cases, conservative combinations of parameters are used to bound the

effects of core life, although these combinations may not represent possible realistic situations.

9.0.2.6 Protection and Safety Monitoring System Setpoints and Time Delays to Trip

A reactor trip signal acts to open two trip breaker sets connected in series, feeding power to the control rod drive mechanisms. The loss of power to the mechanism coils causes the mechanisms to release the RCCAs, which then fall by gravity into the core. There are various instrumentation delays associated with each trip function including delays in signal actuation, in opening the trip breakers, and in the release of the rods by the mechanisms. The total delay to trip is defined as the time delay from the time that trip conditions are reached to the time the rods are free and begin to fall. Limiting trip setpoints assumed in accident analyses and the time delay assumed for each trip function are given in Table 9.0-8. Reference is made in that table to overtemperature ΔT (OTΔT) and overpower ΔT (OPΔT) trip shown in Figure 9.0-1. As mentioned in Chapter 19 and in Reference 9.0-18, the OTΔT protects the core from exceeding the DNB design limit, and the OPΔT protects the core from exceeding the design overpower limit. As shown on the figure, the OTΔT setpoint plus all error allowances tracks the core DNB design limits, except that the setpoint may include an upper limit on allowable inlet temperature.

Table 9.0-8 also summarizes the setpoints and the instrumentation delay for ESF functions used in accident analyses. Time delays associated with equipment actuated (such as valve stroke times) by ESF functions are summarized in Table 9.0-9.

The difference between the limiting setpoint assumed for the analysis and the nominal setpoint represents an allowance for instrumentation channel error and setpoint error. Nominal setpoints are specified in the plant Technical Specifications. During plant startup tests, it is demonstrated that actual instrument time delays are equal to or less than the assumed values. Additionally, protection system channels are calibrated and instrument response times are determined periodically in accordance with the plant Technical Specifications.

9.0.3 Instrumentation Drift and Calorimetric Errors

The calorimetric uncertainty is the uncertainty assumed in the determination of core thermal power as obtained from secondary plant measurements. On a daily basis, this measurement is compared with the ΔT power signal (Reference 9.0-18) and with the total ion chamber current (sum of the top and bottom currents) and those signals are adjusted if necessary for acceptable conformance with the calorimetric power measurement.

The secondary power is obtained from measurement of feedwater flow, feedwater inlet temperature to the steam generators, and steam pressure. Installed plant instrumentation is used for these measurements.

9.0.4 Plant Systems and Components Available for Mitigation of Accident Effects

The plant is designed to afford proper protection against the possible effects of natural phenomena, postulated environmental conditions, and dynamic effects of the postulated accidents. In addition, the design incorporates features that minimize the probability and effects of fires and explosions.

Chapter 5 discusses the quality assurance program that is implemented to provide confidence that the plant systems satisfactorily perform their assigned safety functions. The incorporation of these features in the plant, coupled with the reliability of the design, provides confidence

that the normally operating systems and components listed in Table 9.0-10 are available for mitigation of the events discussed in Chapter 9.

Table 9.0-12 summarizes the non-Class 1 systems assumed in the analyses to mitigate the consequences of events. Except for the cases listed in Table 9.0-12, control system action is not used for mitigation of accidents.

9.0.5 Optimisation of Control Systems

A control system setpoint study is performed prior to plant operation to simulate performance of the primary plant control systems and overall plant performance. In this study, emphasis is placed on the development of the overall plant control systems that automatically maintain conditions in the plant within the allowed operating window and with optimum control system response and stability over the entire range of anticipated plant operating conditions. The control system setpoints are developed using the nominal protection and safety monitoring system setpoints implemented in the plant. Where appropriate (such as in margin to reactor trip analyses), instrumentation errors are considered and are applied in an adverse direction with respect to maintaining system stability and transient performance. The accident analysis and plant control system setpoint study in combination show that the plant can be operated and meet both safety and operability requirements throughout the core life and for various levels of power operation.

The plant control system setpoint study is comprised of analyses of the following control systems: plant control, axial offset control, rapid power reduction, steam dump (turbine bypass), steam generator level, pressuriser pressure, and pressuriser level.

9.0.6 Rod Cluster Control Assembly Insertion Characteristics

The negative reactivity insertion following a reactor trip is a function of the acceleration of the RCCAs as a function of time and the variation in rod worth as a function of rod position. For accident analyses, the critical parameter is the time of insertion up to the dashpot entry, or approximately 85 percent of the rod cluster travel. In analyses where all of the reactor coolant pumps are coasting down prior to, or simultaneous, with RCCA insertion, a time of 2.3 seconds is used for insertion time to dashpot entry.

In Figure 9.0-4, the curve labelled “complete loss of flow transients” shows the RCCA position versus time normalized to 2.3 seconds assumed in accident analyses where all reactor coolant pumps are coasting down. In analyses where some or all of the reactor coolant pumps are running, the RCCA insertion time to dashpot is conservatively taken as 2.7 seconds. The RCCA position versus time normalized to 2.7 seconds is also shown in Figure 9.0-4.

The use of such a long insertion time provides conservative results for accidents and is intended to apply to all types of RCCAs, which may be used throughout plant life. Drop time testing requirements are specified in the Technical Specifications.

Figure 9.0-5 shows the fraction of total negative reactivity insertion versus normalized rod position for a core where the axial distribution is skewed to the lower region of the core. An axial distribution skewed to the lower region of the core can arise from an unbalanced xenon distribution. This curve is used to compute the negative reactivity insertion versus time following a reactor trip, which is input to the point kinetics core models used in transient analyses. The bottom-skewed power distribution itself is not an input into the point kinetics core model.

There is inherent conservatism in the use of Figure 9.0-5 in that it is based on a skewed flux distribution, which would exist relatively infrequently. For cases other than those associated with unbalanced xenon distributions, significantly more negative reactivity is inserted than that shown in the curve, due to the more favourable axial distribution existing prior to trip.

The normalized RCCA negative reactivity insertion versus time is shown in Figure 9.0-6. The curves shown in this figure were obtained from Figures 9.0-4 and 9.0-5. A total negative reactivity insertion following a trip of 4 percent Δk (shutdown margin) is assumed in the transient analyses except where specifically noted otherwise. This assumption is conservative with respect to the calculated trip reactivity worth available.

The normalized RCCA negative reactivity insertion versus time curve for an axial power distribution skewed to the bottom (Figure 9.0-6) is used in those transient analyses for which a point kinetics core model is used. Where special analyses require use of three-dimensional or axial one-dimensional core models, the negative reactivity insertion resulting from the reactor trip is calculated directly by the reactor kinetics code and is not separable from the other reactivity feedback effects. In this case, the RCCA position versus time of Figure 9.0-4 is used as code input.

9.0.7 Fission Product Inventories

The sources of radioactivity for release are dependent on the specific accident. Activity may be released from the primary coolant, from the secondary coolant, and from the reactor core if the accident involves fuel damage. The radiological consequences analyses use the conservative design basis source terms identified in Appendix 9A.

9.0.8 Residual Decay Heat

9.0.8.1 Total Residual Heat

Residual heat in a subcritical core is calculated for the loss-of-coolant accident (LOCA) according to the requirements as described in WCAP-10054-P-A, WCAP-12945-P-A, and WCAP-16009-P-A (References 9.0-5, 9.0-6, and 9.0-17). The large-break LOCA methodology considers uncertainty in the decay power level. The small-break LOCA events and post-LOCA long-term cooling analyses use decay heat, which assumes infinite irradiation time before the core goes subcritical to determine fission product decay energy. For all other accidents, the same models are used, except that fission product decay energy is based on core average exposure at the end of an equilibrium cycle. Margins applied to design basis analyses are as described above; for diversity analyses, this margin is often reduced to reflect a more realistic analysis with appropriately reduced uncertainties.

9.0.8.2 Distribution of Decay Heat Following a Loss-of-Coolant Accident

During a LOCA, the core is rapidly shut down by void formation, RCCA insertion, or both, and a large fraction of the heat generation considered comes from fission product decay gamma rays. This heat is not distributed in the same manner as steady-state fission power. Local peaking effects, which are important for the neutron-dependent part of the heat generation, do not apply to the gamma ray contribution. The steady-state factor, which represents the fraction of heat generated within the cladding and pellet, drops to 95 percent or less for the hot rod in a LOCA.

For example, consider the transient resulting from the postulated double-ended break of the largest reactor coolant system pipe; one-half second after the rupture, about 30 percent of the heat generated in the fuel rods is from gamma ray absorption. The gamma power shape is less

peaked than the steady-state fission power shape, reducing the energy deposited in the hot rod at the expense of adjacent colder rods. A conservative estimate of this effect on the hot rod is a reduction of 10 percent of the gamma ray contribution or 3 percent of the total heat. Because the water density is considerably reduced at this time, an average of 98 percent of the available heat is deposited in the fuel rods; the remaining 2 percent is absorbed by water, thimbles, sleeves, and grids. Combining the 3 percent total heat reduction from gamma redistribution with this 2 percent absorption produce as the net effect a factor of 0.95, which exceeds the actual heat production in the hot rod. The actual hot rod heat generation is computed during the large-break LOCA transient as a function of core fluid conditions.

9.0.9 Computer Codes Used

Summaries of some of the principal computer codes used in transient analyses are given as follows. Other codes – in particular, specialized codes in which the modelling has been developed to simulate one given accident, such as those used in the analysis of the reactor coolant system pipe rupture (see Sections 9.6.4 and 9.6.5) – are summarized in their respective accident analyses sections. The codes used in the analyses of each transient are listed in Table 9.0-6. WCAP-15644-P (Reference 9.0-13) provides the basis for use of analysis codes. Additional information is provided in Appendix 9B.

9.0.9.1 FACTRAN Computer Code

FACTRAN (Reference 9.0-7) calculates the transient temperature distribution in a cross section of a metal-clad UO_2 fuel rod and the transient heat flux at the surface of the cladding using as input the nuclear power and the time-dependent coolant parameters (pressure, flow, temperature, and density). The code uses a fuel model which simultaneously exhibits the following features:

- A sufficiently large number of radial space increments to handle fast transients
- Material properties which are functions of temperature and a sophisticated fuel-to-clad gap heat transfer calculation
- The necessary calculations to handle post-DNB transients: film boiling heat transfer correlations, zircaloy-water reaction, and partial melting of the materials

FACTRAN is further discussed in WCAP-7908-A (Reference 9.0-7).

9.0.9.2 LOFTRAN Computer Code

The LOFTRAN (Reference 9.0-8) program is used for studies of transient response of a pressurised water reactor system to specified perturbations in process parameters. LOFTRAN simulates a multi-loop system by a model containing reactor vessel, hot and cold leg piping, steam generator (tube and shell sides), and pressuriser. The pressuriser heaters, spray, and safety valves are also considered in the program. Point model neutron kinetics, and reactivity effects of the moderator, fuel, boron, and rods are included. The secondary side of the steam generator uses a homogeneous, saturated mixture for the thermal transients and a water level correlation for indication and control. The protection and safety monitoring system is simulated to include reactor trips on high neutron flux, power range high positive flux rate, overtemperature ΔT, high and low pressure, low flow, and high pressuriser level. Control systems are also simulated, including rod control, steam dump, feedwater control, and pressuriser level and pressure control. The emergency core cooling system, including the accumulators, is also modelled.

LOFTRAN is a versatile program suited to both accident evaluation and control studies as well as parameter sizing.

LOFTRAN also has the capability of calculating the transient value of DNBR based on the input from the core limits illustrated in Figure 9.0-1. The core limits represent the minimum value of DNBR as calculated for typical or thimble cell.

The LOFTRAN code is modified to allow the simulation of the passive residual heat removal (PRHR) heat exchanger, core makeup tanks, and associated protection and safety monitoring system actuation logic. A discussion of these models and additional validation is presented in WCAP-14234 (Reference 9.0-12).

LOFTTR2 is a modified version of LOFTRAN with a more realistic break flow model, a two-region steam generator secondary side, and an improved capability to simulate operator actions during a steam generator tube rupture (SGTR) event.

The LOFTTR2 code is modified to allow the simulation of the PRHR heat exchanger, core makeup tanks, and associated protection system actuation logic. The modifications are identical to those made to the LOFTRAN code. A discussion of these models is presented in WCAP-14234 (Reference 9.0-12).

9.0.9.3 TWINKLE Computer Code

The TWINKLE (Reference 9.0-9) program is a multidimensional spatial neutron kinetics code, which is patterned after steady-state codes currently used for reactor core design. The code uses an implicit finite-difference method to solve the two-group transient neutron diffusion equations in one, two, and three dimensions. The code uses six delayed neutron groups and contains a detailed multiregion fuel-clad-coolant heat transfer model for calculating pointwise Doppler and moderator feedback effects. The code handles up to 2000 spatial points and performs its own steady-state initialization. Aside from basic cross-section data and thermal-hydraulic parameters, the code accepts as input basic driving functions, such as inlet temperature, pressure, flow, boron concentration, control rod motion, and others. Various edits are provided (for example, channelwise power, axial offset, enthalpy, volumetric surge, point-wise power, and fuel temperatures).

The TWINKLE code is used to predict the kinetic behaviour of a reactor for transients that cause a major perturbation in the spatial neutron flux distribution.

9.0.9.4 VIPRE-01 Computer Code

The VIPRE-01 core model is used with the applicable DNB correlations to determine DNBR distributions along the hot channels of the reactor core under all expected operating conditions. The VIPRE-01 code is described in detail in Reference 9.0-20, including discussions on code validation with experimental data. The VIPRE-01 modelling method is described in Reference 9.0-21, including empirical models and correlations used. The effect of crud on the flow and enthalpy distribution in the core is not directly accounted for in the VIPRE-01 evaluations. However, conservative treatment by the Westinghouse VIPRE-01 modelling method has been demonstrated to bound this effect in DNBR calculations (Reference 9.0-21).

Extensive additional experimental verification of VIPRE-01 is presented in Reference 9.0-20. The VIPRE-01 analysis is based on a knowledge and understanding of the heat transfer and hydrodynamic behaviour of the coolant flow and the mechanical characteristics of the fuel elements. The use of the VIPRE-01 analysis provides a realistic evaluation of the core

performance.

VIPRE-01 is capable of transient DNB analysis. The conservation equations in the VIPRE-01 code contain the necessary accumulation terms for transient calculations. The input description can include one or more of the following time dependent arrays:

1. Inlet flow variation
2. Core heat flux variation
3. Core pressure variation
4. Inlet temperature or enthalpy variation

At the beginning of the transient, the calculation procedure is carried out as in the steady state analysis. The time is incremented by an amount determined either by the user or by the time step control options in the code itself. At each new time step the calculations are carried out with the addition of the accumulation terms which are evaluated using the information from the previous time step. This procedure is continued until a preset maximum time is reached. At time intervals selected by the user, a complete description of the coolant parameter distributions as well as DNBR is printed out. In this manner the variation of any parameter with time can be readily determined.

9.0.9.5 COAST Computer Program

The COAST computer program is used to calculate the reactor coolant flow coastdown transient for any combination of active and inactive pumps and forward or reverse flow in the hot or cold legs. The program is described in Reference 9.0-15 and was referenced in Reference 9.0-14. The program was approved in Reference 9.0-16.

The equations of conservation of momentum are written for each of the flow paths of the COAST model assuming unsteady one-dimensional flow of an incompressible fluid. The equation of conservation of mass is written for the appropriate nodal points. Pressure losses due to friction and geometric losses are assumed proportional to the flow velocity squared. Pump dynamics are modelled using a head-flow curve for a pump at full speed and using four-quadrant curves, which are parametric diagrams of pump head and torque on coordinates of speed versus flow, for a pump at other than full speed.

9.0.9.6 ANC Computer Code

The ANC computer code is used to solve the two-group neutron diffusion equation in three spatial dimensions. ANC can also solve the three-dimensional kinetics equations for six delayed neutron groups. The ANC code is described in Section 22.6.3.3.

9.0.9.7 RELAP Computer Code

Some of the events, such as loss of reactor coolant flow have small amount of steam void generated. The LOFTRAN model assumes homogeneous flow in the RCS outside the reactor vessel. The validity of the LOFTRAN model for these cases will be verified by analysis with a LOCA code such as NOTRUMP or RELAP.

For RCS depressurisation, a LOCA code such as NOTRUMP or RELAP, is used when void formation in the RCS goes beyond the point where LOFTRAN is useful.

The RELAP family of codes developed to perform analyses of postulated accidents in nuclear power plants.

The RELAP5 computer code (Reference 9.0-19) performs calculations to simulate multi-dimensional thermal-hydraulics, heat transfer, and control systems. The thermal hydraulics behaviour under single phase and two phase conditions is simulated. The hydrodynamics models track the flow of liquid, vapour and non-condensable gases. RELAP5 includes component models of valves, separators, dryers, pumps, electric heaters, turbines, and accumulators. The control system models include functions for trip logic and arithmetic functions for simulation of system filters.

RELAP has been used to analyse the diverse core cooling response to several faults during the AP1000 generic design assessment. Westinghouse has committed to update these analyses during site licensing with an appropriately benchmarked and validated analysis tool, such as NOTRUMP for SBLOCA.

9.0.10 Component Failures

9.0.10.1 Active Failures

An active failure results in the inability of a component to perform its intended function.

An active failure is defined differently for different components. For valves, an active failure is the failure of a component to mechanically complete the movement required to perform its function. This includes the failure of a remotely operated valve to change position on demand. The spurious, unintended movement of the valve is also considered as an active failure. Failure of a manual valve to change position under local operator action is included.

Spring-loaded safety or relief valves that are designed for and operate under single-phase fluid conditions are not considered for active failures to open or close when pressure rises above or reduces below the valve set point. However, when valves designed for single-phase flow are challenged with two-phase flow, such as a steam generator or pressuriser safety valve, the failure to reseat is considered as an active failure.

For other active equipment – such as pumps, fans, and rotating mechanical components – an active failure is the failure of the component to start or to remain operating.

For electrical equipment, the loss of power, such as the loss of offsite power or the loss of a diesel generator, is considered as a single failure. In addition, the failure to generate an actuation signal, either for a single component actuation or for a system-level actuation, is also considered as an active failure.

Spurious actuation of an active component is considered as an active failure for active components in safety-related passive systems. An exception is made for active components if specific design features or operating restrictions are provided that can preclude such failures (such as power lockout, confirmatory open signals, or continuous position alarms).

A single omitted operator action in response to an initiating event is also considered as an active failure; the error is limited to manipulation of safety-related equipment and does not include thought-process errors or similar errors that could potentially lead to common cause or multiple errors.

9.0.10.2 Passive Failures

A passive failure is the structural failure of a static component that limits the effectiveness of the component in carrying out its design function. A passive failure is applied to fluid systems and consists of a breach in the fluid system boundary. Examples include cracking of

pipes, sprung flanges, or valve packing leaks.

Passive failures are not assumed to occur until 24 hours after the start of the event. Consequential effects of a pipe leak – such as flooding, jet impingement, and failure of a valve with a packing leak – must be considered.

Where piping is significantly overdesigned or installed in a system where the pressure and temperature conditions are relatively low, passive leakage is not considered a credible failure mechanism. Line blockage is also not considered as a passive failure mechanism.

9.0.10.3 Limiting Single Failures

The most limiting single failure (where one exists) of safety-related equipment, is identified in each analysis description. The consequences of this failure are described therein. In some instances, because of redundancy in protection equipment, no single failure that could adversely affect the consequences of the transient is identified. The failure assumed in each analysis is listed in Table 9.0-11.

9.0.11 Operator Actions

There are several events analysed in the following sections that require operator action to terminate or mitigate the event. The loss of normal feedwater (Section 9.2.7), the inadvertent actuation of a core makeup tank (Section 9.5.1), and the chemical and volume control system malfunction (Section 9.5.2) assume operator action, after the High-2 pressuriser water level setpoint is reached, to open the safety grade reactor vessel head vent. This action prevents filling the pressuriser and allowing water to escape through the pressuriser safety valves. The analysis of the boron dilution for Mode 1 operation with automatic rod control (Section 9.4.6) relies on the operator to terminate the dilution source, after the rod insertion limit alarm, before the required shutdown margin is lost. The small line break outside containment event (Section 9.6.2) assumes the operator will isolate the break. In all cases where operator actions are credited, no operator actions are required within the first 30 minutes of the transient. For these events, before operator action is required, numerous alarms and indications would be available to the operator to diagnose the transient and ensure that the proper action is taken.

For events where the PRHR heat exchanger is actuated, the plant automatically cools down to the safe shutdown condition. Where a stabilized condition is reached automatically following a reactor trip, it is expected that the operator may, following event recognition, take manual control and proceed with orderly shutdown of the reactor using available Class 2 and 3 SSCs in accordance with the normal, abnormal, or emergency operating procedures. The exact actions taken and the time at which these actions occur depend on what systems are available and the plans for further plant operation.

However, for these events, operator actions are not required to maintain the plant in a safe and stable condition. Appendix 9C provides more details on the systems used to achieve safe shutdown.

9.0.12 Loss of Offsite ac Power

As required, accidents are analysed assuming a loss of offsite ac power. The loss of offsite power is not considered as a single failure, and the analysis is performed without changing the event category. In the analyses, the loss of offsite ac power is considered to be a potential consequence of the event.

A loss of offsite ac power will be considered a consequence of an event due to disruption of

the grid following a turbine trip during the event. Event analyses that do not result in a possible consequential disruption of offsite ac power do not assume offsite power is lost.

For those events where offsite ac power is lost, an appropriate time delay between turbine trip and the postulated loss of offsite ac power is assumed in the analyses. A time delay of 3 seconds is used. This time delay is traditionally based on the inherent stability of the offsite power grid. Following the time delay, the effect of the loss of offsite ac power on plant auxiliary equipment – such as reactor coolant pumps, main feedwater pumps, condenser, startup feedwater pumps, and RCCAs – is considered in the analyses. Turbine trip occurs 5 seconds following a reactor trip condition being reached. This delay is part of the AP1000 reactor trip system.

Design basis LOCA analyses are governed by the requirement to consider the loss of offsite power. For the AP1000 design, in which all the Class 1 systems are passive; the availability of offsite power is significant only regarding reactor coolant pump operation for LOCA events. A sensitivity study for AP1000 has shown that for large-break LOCAs, assuming the loss of offsite power coincident with the inception of the LOCA event is nonlimiting relative to assuming continued reactor coolant pump operation until the automatic reactor coolant pump trip occurs following an "S" signal less than 10 seconds into the transient. For small-break LOCA events, the AP1000 automatic reactor coolant pump trip feature prevents continued operation of the reactor coolant pumps from mixing the liquid and vapour present within a two-phase reactor coolant system inventory to increase the liquid break flow and deplete the reactor coolant system mass inventory rapidly. The automatic reactor coolant pump trip occurs early enough during AP1000 small-break LOCA transients that emergency core cooling system performance is not affected by the loss of offsite power assumption because the total break flow is approximately equivalent for reactor coolant pump trip occurring either at time zero or as a result of the safeguards, or "S" signal. Whether a loss of offsite power is postulated at the inception of the LOCA event or occurs automatically later on is unimportant in the Section 9.6.6 long-term cooling analyses because with either assumption, the reactor coolant pumps are tripped long before the long-term cooling timeframe.

The AP1000 protection and safety monitoring system and passive safeguards systems are not dependent on offsite power or on any backup diesel generators. Following a loss of ac power, the protection and safety monitoring system and passive safeguards are able to perform the safety functions and there are no additional time delays for these functions to be completed.

9.0.13 Treatment of Diverse Protection Systems

For every frequent fault two diverse analyses are performed that address the ability to shutdown the reactor core (ATWT) and the ability to cool the core. These two sets of analyses are discussed further in the following.

Summary of ATWT analysis

For all frequent faults, a conservative analysis shows that there is an alternative means of bringing the reactor to a safe shutdown if the normal means (insertion of control rods) fails. The alternative means depends on whether the failure of the normal system is due to failure within the protection and safety monitoring system (PMS) (leading to failure to generate a PMS trip signal) or to mechanical failure such as the inability of the control rods to insert. In the former case, the diverse means of shutdown is insertion of the control rods by diverse actuation system (DAS) actuation signals; in the latter case, it is operation of the core makeup tank (CMT) and the trip of the RCPs. The tripping of the RCPs results in void formation in

the core which causes a rapid reduction in the core power. The CMTs inject sufficient borated water into the primary circuit to bring about final shutdown.

In all cases, there is a significant margin to violation of any safety limit. The detailed ATWT analysis is presented in Reference 9.0-3 and summarized in the associated frequent fault sections of this PCSR chapter. The analyses show that there is no expected violation of the DNB criterion and hence no core damage; and that the primary circuit pressure never exceeds the American Society of Mechanical Engineers (ASME) service limit C level, so that the integrity of the reactor coolant circuit pressure boundary is ensured. The analysis does not consider in detail the integrity of the containment, because the early challenges to the containment from ATWT scenarios are far smaller than those from, for example, a large-break LOCA; any late challenges (arising from the slow heatup of heat sinks such as the in-containment refuelling water storage tank (IRWST)) would occur significantly later than 30 minutes after the start of the transient and could easily be prevented by operator action. Table 9.0-13 summarizes the key acceptance criteria used for the ATWT diversity analyses.

Summary of Diverse Core Cooling Analysis

Each frequent fault is shown to tolerate common cause failures (CCFs) that affect the ability of the Class 1 SSCs to provide core cooling. These frequent faults are either analysed in detail or are shown to be bounded by another fault that is analysed in detail. For each frequent fault, it is shown that the plant can tolerate a CCF affecting one of the Class 1 SSCs credited in providing core cooling and still provide adequate core cooling using diverse SSCs. The general approach is to provide two completely separate and diverse sets of SSCs including C&I out through the ultimate heat sink. However, as necessary additional sets of SSCs can be defined where they are able to meet a single CCF and they are supported by additional plant analysis.

Diverse core cooling analyses and the associated assumptions and acceptance criteria are discussed further with the individual faults.

9.0.13.1 Classification of Frequent Fault Initiating Events

In the analyses and evaluations presented here, frequent faults will include events with expected frequencies of occurrence equal to or greater than $1x10^{-3}$ per reactor year (UK class DB2).

Table 8A-2 identifies the frequent faults, for which diverse analysis is required.

9.0.13.2 Common Cause Failures Considered in ATWT Cases

Frequent faults are required to be analysed with a single CCF. Two different analyses are performed; one where the CCF affects the ability to shutdown the reactor (ATWT) and the other where the CCF affects the ability to cool the core. A CCF is the failure of two or more SSCs in the same manner or mode due to a single event or cause. Generally, the CCFs that prevent reactor scram from occurring are divided into two broad groups: electrical CCFs and mechanical CCFs. A mechanical CCF is assumed to be a mechanical fault that prevents the RCCA from inserting into the core. The electrical CCF is assumed to be either a fault of the protection system logic, sensors supplying input to the protection system or a fault in the reactor trip breakers. The CCF resulting in an ATWT is assumed to be due to one of the following groups:

1. Electrical CCF of the PMS
2. Electrical CCF of the reactor trip breakers

3. Mechanical CCF that prevents RCCA insertion

Reference 9.0-3 provides additional details regarding the unique analysis assumptions employed when performing the ATWT diversity analyses. Table 9.0-14 summarises the operability assumptions for the PMS and DAS assuming one of the above three types of CCFs occurs.

9.0.14 Description of Systems and Components Used in the Analyses

9.0.14.1 Protection and Safety Monitoring System

During normal operation, administrative procedures and plant control systems serve to maintain the reactor in a safe state, preventing damage to the three barriers (fuel clad, reactor coolant system, and reactor containment building) that prevent the spread of radioactive material to the environment. Accident conditions causing one or more of the barriers to be threatened can occur. The PMS monitors key plant parameters and will automatically initiate required protective functions to prevent violation of any of the three barriers. If violation of a barrier cannot be prevented, the PMS will maintain the integrity of the remaining barriers. This ensures that, given a design-basis event, the site boundary radiological consequences will be below design limits. The system performs its functions by actuating a variety of electrical and mechanical equipment and by monitoring the plant process using a variety of sensors and operations that perform calculations, comparisons, and logic based on the sensor inputs.

The protective functions use two basic classes of safety features to prevent damage to the reactor fuel elements and the release of radioactive material: the reactor trip feature and ESFs. The reactor trip feature uses neutron-absorbing control rods that can be rapidly inserted by gravity into the reactor core to shut down the chain reaction and dramatically reduce the power output of the reactor. In some cases, additional measures are needed to cool the reactor or containment building, isolate possible release paths for radioactive materials, prevent excessive cooling of the reactor, or prevent inadvertent core criticality. The ESFs actuate or isolate various processes to perform these functions. The PMS includes the equipment from the process sensor and manual control inputs through to the power switching devices that actuate the equipment controlled by the PMS.

9.0.14.2 Plant Control System

The plant control system (PLS) provides control and coordination of the plant during startup, ascent to power, power operation, and shutdown conditions. The PLS integrates the automatic and manual control of the reactor, reactor coolant, and various reactor support processes for required normal and off-normal conditions. The PLS also provides control of the Class 2 and Class 3 decay heat removal systems during shutdown. As a result, parts of PLS are Class 2 while other parts are Class 3. The PLS accomplishes these functions through use of the following:

- Rod control
- Pressuriser pressure and level control
- Steam generator water level control
- Turbine bypass (steam dump) control
- Rapid power reduction

The PLS provides automatic regulation of reactor and other key system parameters in response to changes in operating limits (load changes). The PLS acts to maximise margins to

plant safety limits and maximise the plant transient performance. The PLS also provides the capability for manual control of plant systems and equipment. Redundant control logic is used in some applications to increase single-failure tolerance. The PLS includes the equipment from the process sensor input circuitry through to the modulating and non-modulating control outputs, as well as the digital signals to other plant systems. Modulating control devices include valve positioners, pump speed controllers, and the control rod equipment. Non-modulating devices include motor starters for motor-operated valves and pumps, breakers for heaters, and solenoids for actuation of air-operated valves. The PLS cabinets contain the process sensor inputs and the modulating and non-modulating outputs. The PLS also includes equipment to monitor and control the control rods.

9.0.14.3 Diverse Actuation System

The DAS is a C&I system that provides a diverse backup to the PMS. This diverse backup system is included in the C&I system design to support the AP1000 plant risk goals by reducing the probability of a severe accident, which could potentially result from the unlikely coincidence of postulated transients and postulated CCF in the PMS and the PLS.

The purpose of the DAS is to lessen the probability of plant damage if the PMS fails to function when required and to reduce the frequency of the fuel core melting or containment failure in the probabilistic safety assessment (PSA). The specific functions performed by the DAS are selected based on the AP1000 plant PSA evaluation. The DAS functional requirements are based on an assessment of the protection system CCF probabilities combined with the event probability. The DAS supports both automatic and manual actuations.

9.0.14.4 Passive Core Cooling System

The passive core cooling system (PXS) is designed to perform the following major safety functions:

- Emergency RCS makeup and boration
- Safety injection
- Emergency core decay heat removal
- Post-accident containment pH control

The safety functions of the PXS provide for the integrity of the reactor coolant pressure boundary, the capability to shut down the reactor and maintain it in a safe shutdown condition, or the capability to prevent or mitigate the consequences of accidents that could result in potential offsite exposures. These safety functions are provided by Class 1 equipment with redundancy to deal with single failures, environmental qualification, and protection from external hazards. These functions are available during all normal modes of RCS operation, including hot and cold shutdowns and refuelling.

For diverse core cooling scenarios, the PXS provides the same safety functions with some exceptions. First, as it is a diversity evaluation, Class 2 SSCs are included if necessary; most notably RNS cooling. In addition, these analyses may assume CCF within the PXS to demonstrate adequate diversity with the primary case mitigation.

During an ATWT, the PXS is used to remove sufficient heat to adequately cool the plant and inject sufficient boron to shut down the core. Of particular importance to ATWT events are the emergency RCS boration (including tripping of the RCPs) and the emergency core decay

heat removal functions. Emergency boration by the PXS is performed with the CMTs during ATWT events. Emergency core heat removal is provided by the PRHR heat exchanger.

9.0.15 As Low As Reasonably Practicable Assessment

In the UK, meeting the DB and probabilistic targets alone are not sufficient to demonstrate that the plant is adequately safe. There is the additional requirement that the risk must be demonstrated to be ALARP.

The ALARP assessment determines if there are any reasonably practicable means to further reduce the risk from individual faults, including the identification of SSCs for defence in depth and in the safety case as a whole. As a result of the ALARP assessment, other SSCs may be identified as providing defence in depth or reducing risk in other ways.

Section 14.6 provides an extensive review of overall ALARP case for the AP1000 design. It reviews major design decisions taken during the evolution of the design from the previous generation of PWRs, giving a brief explanation of why certain features were selected and others rejected, to demonstrate that the evolution process has resulted in an improved design from the point of view of safety. The ALARP assessment discussed in Section 14.6 consists of a number of inputs from different phases of the development and assessment of the design. Many of these exercises have been aimed at risk reduction rather than ALARP as such, but they have led to many risk reduction measures being incorporated into the design that contribute to achieving an overall plant risk judged to be ALARP.

In addition to the discussion of the historical development activities of the AP1000 design, Section 14.6 also discusses changes incorporated into the UK AP1000 design specifically for ALARP reasons. There is also discussion of additional changes that could have been made but were rejected because they were not considered ALARP.

Note that adding additional safety SSCs can increase the overall safety of the plant. However, adding more SSCs increases the design complexity which can offset the benefits. The more complex the design, the greater the chance of additional failures of SSCs and the greater the chance of adverse interactions. More SSCs require more inservice inspection and testing which tends to increase radiation exposure to plant personnel. Thus, adding additional safety components and systems may only increase safety in small increments and possibly even decrease safety.

Finally, given that the total AP1000 plant large release frequency (refer to Chapter 10) is about an order of magnitude below the SAP Target 9 BSO (1E-7 pa), the ONR internal licensing guidance is that little additional effort should be expended to further reduce the risk.

In spite of this extensive effort already put into reducing risk in the AP1000 design, the following Chapter 9 sections include additional ALARP discussions of further improvements.

9.0.16 Conclusion

The basis for the faults analysed in this Chapter is predominantly the design basis faults identified in Table 8A-2. The faults are addressed in Sections 9.1 to 9.12. Section 9.13 contains the conclusions of the chapter.

It is noted that Sections 9.1 to 9.6 provide a discussion of faults related to reactor internally initiated events at power (Modes 1 and 2 from Table 9.0-1). Section 9.7 provides a discussion of faults associated with the spent fuel pool (SFP). All reactor faults are discussed in Sections 9.1 to 9.6 are revisited for consideration during all shutdown modes (Modes 3, 4, 5, and 6) in

Section 9.8, which also includes reactor-specific potential faults in shutdown conditions. Sections 9.9 – 9.12 provide a discussion of various faults: dropped loads; operator exposure faults; heating, ventilation, and air conditioning (HVAC) faults; and radioactive-waste-related faults.

9.0.17 References

9.0-1 ONR "Safety Assessment Principles for Nuclear Facilities," Rev. 0, Office of Nuclear Regulation, 2014.

9.0-2 HSE T/AST/045, Issue 1, Technical Assessment Guide "Radiological Analysis – Fault Conditions," Health and Safety Executive, October 2009.

9.0-3 Westinghouse Report UKP-GW-GLR-016, Rev. B, "Evaluation of ATWS Events for UK AP1000™ Pressurized Water Reactor," October 2010.

9.0-4 Westinghouse Documents WCAP-11397-P-A (Proprietary) and WCAP-11397-A (Non-Proprietary), "Revised Thermal Design Procedure," April 1989.

9.0-5 Westinghouse Documents WCAP-10054-P-A (Proprietary) and WCAP-10081-A (Non-Proprietary), "Westinghouse Small Break ECCS Evaluation Model Using the NOTRUMP Code," August 1985.

9.0-6 Westinghouse Documents WCAP-12945-P-A, Volume 1, Revision 2, and Volumes 2 through 5, Revision 1, (Proprietary) and WCAP-14747 (Non Proprietary), "Code Qualification Document for Best Estimate LOCA Analysis," 1998.

9.0-7 Westinghouse Document WCAP-7908-A, "FACTRAN A Fortran IV Code for Thermal Transients in a UO_2 Fuel Rod," December 1989.

9.0-8 Westinghouse Documents WCAP-7907-P-A, Rev. 0 (Proprietary) and WCAP-7907-A, Rev. 0 (Non-Proprietary), "LOFTRAN Code Description," April 1984.

9.0-9 Westinghouse Documents WCAP-7979-P-A, Rev. 0 (Proprietary) and WCAP-8028-A, Rev. 0 (Non-Proprietary), "TWINKLE - A Multi-Dimensional Neutron Kinetics Computer Code," January 1975.

9.0-10 Not Used.

9.0-11 Not Used.

9.0-12 Westinghouse Documents WCAP-14234, Rev. 1 (Proprietary) and WCAP-14235, Rev. 1 (Non-Proprietary), "LOFTRAN & LOFTTR2 AP600 Code Applicability Document," August 1997.

9.0-13 Westinghouse Documents WCAP-15644-P, Rev. 2 (Proprietary) and WCAP-15644-NP, Rev. 2 (Non-Proprietary), "AP1000 Code Applicability Report," March 2004.

9.0-14 "Combustion Engineering Standard Safety Analysis Report," CESSAR Docket No. STN-50-470, December 1975.

9.0-15 CENPD-98-A, "COAST Code Description," April 1973, Proprietary Information.

9.0-16 CENPD-98-A, "COAST Code Description," April 1973 (NRC Approval Letter dated December 4, 1974).

9.0-17 Westinghouse Documents WCAP-16009-P-A, Rev. 0 (Proprietary) and WCAP-16009-NP-A, Rev. 0 (Non-Proprietary), "Realistic Large-Break LOCA Evaluation Methodology Using the Automated Statistical Treatment Of Uncertainty Method (ASTRUM)," January 2005.

9.0-18 Westinghouse Document APP-GW-GLR-137, Rev. 1, "Bases of Digital Overpower and Overtemperature Delta-T (OPΔT/OTΔT) Reactor Trips," February 2011.

9.0-19 NUREG/CR-5535, EGG-2596, "RELAP5/MOD3 Code Manual," EG&G Idaho, Inc, June 1990.

9.0-20 NP-2511-CCM-A, "VIPRE-01: A Thermal-Hydraulic Code for Reactor Core," Volume 1-3 (Revision 3, August 1989), Volume 4 (April 1987), Electric Power Research Institute, Stewart, C. W., et al.

9.0-21 Westinghouse Documents WCAP-14565-P-A, Rev. 0 (Proprietary) and WCAP-15306-NP-A, Rev. 0 (Non-Proprietary), "VIPRE-01 Modeling and Qualification for Pressurized Water Reactor Non-LOCA Thermal-Hydraulic Safety Analysis," October 1999.

9.0-22 Westinghouse Report UKP-GW-GL-060, Rev. 10, "AP1000® Design Reference Point for UK GDA," January 2017.

9.0-23 Westinghouse Report UKP-GW-GL-067, Rev. 1, "AP1000 Assessment of Diverse Mitigation of Frequent Faults for the UK," December 2011.

9.0-24 Westinghouse Report UKP-SSAR-GLR-001, Rev. A, "UK Fault Studies Analysis Basis," July 2015.

Table 9.0-1. Reactor Operating Modes

Mode		Reactivity Condition (K_{eff})	% Rated Thermal Power[1]	Average Reactor Coolant Temperature
1	Power operation	≥0.99	>5	N/A
2	Startup	≥0.99	≤5	N/A
3	Hot standby	<0.99	N/A	>216°C (>420°F)
4	Safe shutdown[2]	<0.99	N/A	≤216°C (<420°F) >93°C (>200°F)
5	Cold shutdown[2]	<0.99	N/A	≤93°C (≤200°F)
6	Refuelling[3]	NA	N/A	N/A

Notes:

1. Excluding decay heat.
2. All RV head closure bolts fully tensioned.
3. One or more RV head closure bolts less than fully tensioned.

Table 9.0-2. Not Used

Table 9.0-3 (Sheet 1 of 5). Summary of Safety Analysis Events and Main Acceptance Criteria

<table>
<tr><th>Safety Analysis Group</th><th>Safety Analysis Event</th><th>Main Acceptance Criteria</th></tr>
<tr><td rowspan="5">Increase in Heat Removal from the Primary System</td><td>Feedwater System Malfunctions that Result in a Decrease in Feedwater Temperature</td><td rowspan="5">• DNBR remains above the design limit so fuel cladding integrity is maintained (refer to Sections 22.4 and 22.7 for discussion of DNBR limits)
• Pressure in the reactor coolant and main steam systems maintained below 110 percent of the design values as follows:
<table><tr><th rowspan="2">Pressure Boundary</th><th colspan="2">Design Pressure</th></tr><tr><th>USCG</th><th>(Imperial)</th></tr><tr><td>RCS</td><td>2485 psig</td><td>(17.1 MPa-g)</td></tr><tr><td>MSS</td><td>1185 psig</td><td>(8.17 MPa-g)</td></tr></table></td></tr>
<tr><td>Feedwater System Malfunctions that Result in an Increase in Feedwater Flow</td></tr>
<tr><td>Excessive Increase in Secondary Steam Flow</td></tr>
<tr><td>Inadvertent Opening of a Steam Generator Relief or Safety Valve</td></tr>
<tr><td>Inadvertent Operation of the Passive Residual Heat Removal Heat Exchanger</td></tr>
<tr><td>Steam System Piping Failure</td><td>• Fuel damage limited so doses do not exceed design limits
• Pressure in the reactor coolant and main steam system is maintained below design limits as follows:
<table><tr><th rowspan="2">Pressure Boundary</th><th colspan="2">Design Pressure</th></tr><tr><th>USCG</th><th>(Imperial)</th></tr><tr><td>RCS</td><td>2485 psig</td><td>(17.1 MPa-g)</td></tr><tr><td>MSS</td><td>1185 psig</td><td>(8.17 MPa-g)</td></tr></table></td></tr>
</table>

Table 9.0-3 (Sheet 2 of 5). Summary of Safety Analysis Events and Main Acceptance Criteria

<table>
<tr><th>Safety Analysis Group</th><th>Safety Analysis Event</th><th>Main Acceptance Criteria</th></tr>
<tr><td rowspan="8">Decrease in Heat Removal by the Secondary System</td><td>Loss of External Electrical Load</td><td rowspan="8">• DNBR remains above the design limit so fuel cladding integrity is maintained (refer to Sections 22.4 and 22.7 for discussion of DNBR limits)
• Pressure in the reactor coolant and main steam systems maintained below 110 percent of the design values as follows:
<table><tr><th rowspan="2">Pressure Boundary</th><th colspan="2">Design Pressure</th></tr><tr><th>USCG</th><th>(Imperial)</th></tr><tr><td>RCS</td><td>2485 psig</td><td>(17.1 MPa-g)</td></tr><tr><td>MSS</td><td>1185 psig</td><td>(8.17 MPa-g)</td></tr></table></td></tr>
<tr><td>Turbine Trip</td></tr>
<tr><td>Inadvertent Closure of Main Steam Isolation Valves</td></tr>
<tr><td>Loss of Condenser Vacuum and Other Events Resulting in Turbine Trip</td></tr>
<tr><td>Loss of AC Power to the Plant Auxiliaries</td></tr>
<tr><td>Loss of Normal Feedwater Flow</td></tr>
<tr><td>Feedwater System Pipe Break</td></tr>
<tr><td rowspan="2">Decrease in Reactor Coolant System Flow Rate</td><td>Partial Loss of Forced Reactor Coolant Flow</td><td rowspan="2">• DNBR remains above the design limit so fuel cladding integrity is maintained (refer to Sections 22.4 and 22.7 for discussion of DNBR limits)
• Pressure in the reactor coolant and main steam systems maintained below 110 percent of the design values as follows:
<table><tr><th rowspan="2">Pressure Boundary</th><th colspan="2">Design Pressure</th></tr><tr><th>USCG</th><th>(Imperial)</th></tr><tr><td>RCS</td><td>2485 psig</td><td>(17.1 MPa-g)</td></tr><tr><td>MSS</td><td>1185 psig</td><td>(8.17 MPa-g)</td></tr></table></td></tr>
<tr><td>Complete Loss of Forced Reactor Coolant Flow</td></tr>
<tr><td rowspan="2">Decrease in Reactor Coolant System Flow Rate</td><td>Reactor Coolant Pump Shaft Seizure (Locked Rotor)</td><td rowspan="2">• Fuel damage limited so doses do not exceed design limits
• Pressure in the reactor coolant and main steam system is maintained below design limits as follows:
<table><tr><th rowspan="2">Pressure Boundary</th><th colspan="2">Design Pressure</th></tr><tr><th>USCG</th><th>(Imperial)</th></tr><tr><td>RCS</td><td>2485 psig</td><td>(17.1 MPa-g)</td></tr><tr><td>MSS</td><td>1185 psig</td><td>(8.17 MPa-g)</td></tr></table></td></tr>
<tr><td>Reactor Coolant Pump Shaft Break</td></tr>
</table>

Table 9.0-3 (Sheet 3 of 5). Summary of Safety Analysis Events and Main Acceptance Criteria

<table>
<tr><th>Safety Analysis Group</th><th>Safety Analysis Event</th><th>Main Acceptance Criteria</th></tr>
<tr><td rowspan="4">Reactivity and Power Distribution Anomalies</td><td>Uncontrolled Rod Cluster Control Assembly Bank Withdrawal from a Subcritical or Low-Power Startup Condition</td><td rowspan="2">• DNBR remains above the design limit so fuel cladding integrity is maintained (refer to Sections 22.4 and 22.7 for discussion of DNBR limits)
• Fuel centreline temperatures do not exceed the melting point (See Section 22.5).</td></tr>
<tr><td>Uncontrolled Rod Cluster Control Assembly Bank Withdrawal at Power</td></tr>
<tr><td>Rod Cluster Control Assembly Misalignment (System Malfunction or Operator Error)</td><td>• DNBR remains above the design limit so fuel cladding integrity is maintained (refer to Sections 22.4 and 22.7 for discussion of DNBR limits)
• Fuel centreline temperatures do not exceed the melting point (See Section 22.5).
• Uniform cladding strain does not exceed 1%.</td></tr>
<tr><td>Startup of an Inactive Reactor Coolant Pump at an Incorrect Temperature</td><td>• The Technical Specifications (3.4.4) require all RCPs to be operating while in Modes 1 and 2.
• The reactor will initially be subcritical by the Technical Specification requirement.</td></tr>
<tr><td rowspan="3">Reactivity and Power Distribution Anomalies</td><td>Chemical and Volume Control System Malfunction that Results in a Decrease in the Boron Concentration in the Reactor Coolant</td><td>• DNBR remains above the design limit so fuel cladding integrity is maintained (refer to Sections 22.4 and 22.7 for discussion of DNBR limits)
• Pressure in the reactor coolant and main steam systems maintained below 110 percent of the design values as follows:
<table>
<tr><th rowspan="2">Pressure Boundary</th><th colspan="2">Design Pressure</th></tr>
<tr><th>USCG</th><th>(Imperial)</th></tr>
<tr><td>RCS</td><td>2485 psig</td><td>(17.1 MPa-g)</td></tr>
<tr><td>MSS</td><td>1185 psig</td><td>(8.17 MPa-g)</td></tr>
</table></td></tr>
<tr><td>Inadvertent Loading and Operation of a Fuel Assembly in an Improper Position</td><td>• Prevention is provided by administrative procedures.
• Loading errors are detectable by the online core monitoring system.</td></tr>
<tr><td>Spectrum of Rod Cluster Control Assembly Ejection Accidents</td><td>• Little or no possibility of fuel dispersal in the coolant, gross lattice distortion, or severe shock waves.</td></tr>
</table>

Table 9.0-3 (Sheet 4 of 5). Summary of Safety Analysis Events and Main Acceptance Criteria

<table>
<tr><th>Safety Analysis Group</th><th>Safety Analysis Event</th><th>Main Acceptance Criteria</th></tr>
<tr><td rowspan="2">Increase in Reactor Coolant Inventory</td><td>Inadvertent Operation of the Core Makeup Tanks During Power Operation</td><td rowspan="2">• DNBR remains above the design limit so fuel cladding integrity is maintained (refer to Sections 22.4 and 22.7 for discussion of DNBR limits)
• Pressure in the reactor coolant and main steam systems maintained below 110 percent of the design values as follows:
<table><tr><th rowspan="2">Pressure Boundary</th><th colspan="2">Design Pressure</th></tr><tr><th>USCG</th><th>(Imperial)</th></tr><tr><td>RCS</td><td>2485 psig</td><td>(17.1 MPa-g)</td></tr><tr><td>MSS</td><td>1185 psig</td><td>(8.17 MPa-g)</td></tr></table></td></tr>
<tr><td>Chemical and Volume Control System Malfunction That Increases Reactor Coolant Inventory</td></tr>
<tr><td rowspan="4">Decrease in Reactor Coolant Inventory</td><td>Inadvertent Opening of a Pressuriser Safety Valve or Inadvertent Operation of the Automatic Depressurisation System (ADS)</td><td>• DNBR remains above the design limit so fuel cladding integrity is maintained (refer to Sections 22.4 and 22.7 for discussion of DNBR limits)
• Pressure in the reactor coolant and main steam systems maintained below 110 percent of the design values as follows:
<table><tr><th rowspan="2">Pressure Boundary</th><th colspan="2">Design Pressure</th></tr><tr><th>USCG</th><th>(Imperial)</th></tr><tr><td>RCS</td><td>2485 psig</td><td>(17.1 MPa-g)</td></tr><tr><td>MSS</td><td>1185 psig</td><td>(8.17 MPa-g)</td></tr></table></td></tr>
<tr><td>Failure of Small Lines Carrying Primary Coolant Outside Containment</td><td>• Dose consequences do not exceed design limits</td></tr>
<tr><td>Steam Generator Tube Rupture</td><td>• DNBR remains above the design limit so fuel cladding integrity is maintained (refer to Sections 22.4 and 22.7 for discussion of DNBR limits)
• Dose consequences do not exceed design limits</td></tr>
<tr><td>Loss-of-Coolant Accidents Resulting from a Spectrum of Postulated Piping Breaks Within the Reactor Coolant Pressure Boundary</td><td>• The calculated maximum fuel element cladding temperature shall not exceed 1204°C (2200°F)
• Localized cladding oxidation shall not exceed 17 percent of the total cladding thickness before oxidation
• Changes in core geometry are such that the core remains amenable to cooling</td></tr>
</table>

Table 9.0-3 (Sheet 5 of 5). Summary of Safety Analysis Events and Main Acceptance Criteria

Safety Analysis Group	Safety Analysis Event	Main Acceptance Criteria
Radioactive Release from a Subsystem or Component	Gas Waste Management System Leak or Failure	• Failure of the gaseous radwaste system results in a minor release of activity that is not significant
	Liquid Waste Management System Leak or Failure (Atmospheric Release)	• Liquid radwaste system tanks do not contain significant levels of gaseous activity
	Release of Radioactivity to the Environment Due to a Liquid Tank Failure	• Site specific dose consequences do not exceed design limits
	Fuel Handling Accident	• Dose consequences do not exceed design limits
	Spent Fuel Cask Drop Accident	• The spent fuel cask handling crane is prevented from travelling over the spent fuel

Table 9.0-4 (Sheet 1 of 2). Limits and Conditions Assumed in Safety Case

Limit or Condition	Technical Specification Identification and Notes
Limits and conditions defining the safe operating envelope and initial conditions	
Core DNBR	2.1.1 Reactor Core Safety Limits: 2.1.1.1 The DNBR shall be maintained ≥ 1.14 for the WRB-2M DNB correlations
Core peak clad temperature	2.1.1 Reactor Core Safety Limits: 2.1.1.2 The peak fuel centreline temperature shall be maintained < 2804.44°C (5080°F), decreasing by 14.44°C (58°F) per 10,000 MWD/MTU of burn up.
RCS pressure	2.1.2 RCS Pressure Safety Limits: In Modes 1, 2, 3, 4, and 5 the RCS pressure shall be maintained ≤ 18.847 MPa gauge (2734 psig)
Shutdown margin (SDM)	3.1.1 Shutdown Margin (SDM): In Mode 2 with keff < 1.0, Modes 3, 4, and 5 SDM to be within defined limits
Shutdown rod insertion limits	3.1.5 Shutdown bank position Within insertion limits specified in the Core Operating Limit Report (COLR)
Control rod insertion limits	3.1.6 Control rod position Within insertion, sequence and overlap limits specified in the COLR
Power distribution limits	3.2.5 Peal power/length(Z), $F_{\Delta H}^{N}$, DNBR and SDM Within operating limits specified in the COLR
RCS temperature & pressure	3.4.3 RCS pressure, temperature and heatup and cooldown rates Within the limits specified in the Pressure and Temperature Limits Report (PTLR)
Steam Generator (SG) tube integrity	3.4.18 SG integrity shall be maintained and all SG tubes satisfying the tube repair criteria shall be plugged in accordance with the SG programme
Limits and Conditions determining Class 1 SSC operation	
Accumulator isolation valves open	3.5.1 Accumulators (SR 3.5.1.1)
Accumulator water volume	3.5.1 Accumulators (SR 3.5.1.2)
Accumulator nitrogen pressure	3.5.1 Accumulators (SR 3.5.1.3)
Accumulator boron concentration	3.5.1 Accumulators (SR 3.5.1.4)
CMT water temperature	3.5.2 CMTs – Operating (SR 3.5.2.1)
CMT water volume	3.5.2 CMTs – Operating (SR 3.5.2.2)

Table 9.0-4 (Sheet 2 of 2). Limits and Conditions Assumed in Safety Case

Limit or Condition	Technical Specification Identification and Notes
CMT inlet isolation valves fully open	3.5.2 CMTs – Operating (SR 3.5.2.3)
CMT boron concentration	3.5.2 CMTs – Operating (SR 3.5.2.5)
PRHR outlet isolation valve open	3.5.4 PRHR HX – Operating (SR 3.5.4.1)
PRHR inlet isolation valve open	3.5.4 PRHR HX – Operating (SR 3.5.4.2)
PRHR free from non-condensable gas	3.5.4 PRHR HX – Operating (SR 3.5.4.3)
IRWST water temperature	3.5.6 IRWST – Operating (SR 3.5.6.1)
IRWST water volume	3.5.6 IRWST – Operating (SR 3.5.6.2)
IRWST boron concentration	3.5.6 IRWST – Operating (SR 3.5.6.3)
Containment isolation valves closed	3.6.3 Containment Isolation Valves (SR 3.6.3.1)
Containment pressure	3.6.4 Containment Pressure (SR 3.6.4.1)
Passive Containment Cooling Water Storage Tank (PCCWST) water temperature	3.6.6 Passive Containment Cooling System (PCS) – Operating (SR 3.6.6.1)
PCCWST water volume	3.6.6 PCS – Operating (SR 3.6.6.2)
Essential Electrical Supply System (IDS) dc voltage	3.8.1 Direct current (DC) Sources – Operating (SR 3.8.1.1)
IDS ac voltage	3.8.3 Inverters – Operating (SR 3.8.3.1)

Note:
SR indicates a Surveillance Requirement associated with the corresponding Tech Specs.

Table 9.0-5. Nuclear Steam Supply System Power Ratings

Thermal power output (MWt)	3415
Effective thermal power generated by the reactor coolant pumps (MWt)	15
Core thermal power (MWt)	3400

Table 9.0-6 (Sheet 1 of 5). Summary Of Initial Conditions And Computer Codes Used

Section	Faults	Computer Codes Used	Reactivity Coefficients Assumed			Initial Thermal Power Output Assumed (MWt)
			Moderator Density ($\Delta k/gm/cm^3$)	Moderator Temperature (pcm/°C)	Doppler	
9.1	Increase in heat removal from the primary system					
	Feedwater system malfunctions causing a reduction in feedwater temperature	Bounded by excessive increase in secondary steam flow	–	–	–	–
	Feedwater system malfunctions that result in an increase in feedwater flow	LOFTRAN	0.470	–	Upper curve of Figure 9.0-3	0 and 3415
	Excessive increase in secondary steam flow	LOFTRAN	0.0 and 0.470	–	Upper and lower curves of Figure 9.0-3	3415
	Inadvertent opening of a steam generator relief or safety valve	LOFTRAN, VIPRE-01	Function of moderator density (see Figure 9.1.4-1)	–	See Section 9.1.4.	0 (subcritical)
	Steam system piping failure	LOFTRAN, VIPRE-01	Function of moderator density (see Figure 9.1.4-1) for zero-power case 0.470 for full-power case	–	See Section 9.1.5 for zero-power case; upper curve of Figure 9.0-3 for full-power case	0 (subcritical) and 3415
	Inadvertent operation of the PRHR heat exchanger	N/A	N/A	–	N/A	3415

Table 9.0-6 (Sheet 2 of 5). Summary Of Initial Conditions And Computer Codes Used

Section	Faults	Computer Codes Used	Reactivity Coefficients Assumed			Initial Thermal Power Output Assumed (MWt)
			Moderator Density ($\Delta k/gm/cm^3$)	Moderator Temperature (pcm/°C)	Doppler	
9.2	Decrease in heat removal by the secondary system					
	Loss of external electrical load and/or turbine trip	LOFTRAN, FACTRAN, VIPRE-01	0.470 and function of moderator density	–	Lower and upper curves of Figure 9.0-3	3415 and 3449.15 (a)
	Inadvertent closure of main steam isolation valves	Bounded by turbine trip event	–	–	–	–
	Loss of condenser vacuum and other events resulting in turbine trip	Bounded by turbine trip event	–	–	–	–
	Loss of nonemergency ac power to the plant auxiliaries	LOFTRAN	0.0	–	Lower curve of Figure 9.0-3	3449.15 (a)
	Loss of normal feedwater flow	LOFTRAN	0.0	–	Lower curve of Figure 9.0-3	3449.15 (a)
	Feedwater system pipe break	LOFTRAN	0.0	–	Lower curve of Figure 9.0-3	3449.15 (a)
9.3	Decrease in reactor coolant system flow rate					

Table 9.0-6 (Sheet 3 of 5). Summary Of Initial Conditions And Computer Codes Used

Section	Faults	Computer Codes Used	Reactivity Coefficients Assumed			Initial Thermal Power Output Assumed (MWt)
			Moderator Density ($\Delta k/gm/cm^3$)	Moderator Temperature (pcm/°C)	Doppler	
9.3	Partial and complete loss of forced reactor coolant flow	LOFTRAN, FACTRAN, COAST, VIPRE-01	0.0 and function of moderator density	–	Lower curve of Figure 9.0-3	3415
	Reactor coolant pump shaft seizure (locked rotor) and reactor coolant pump shaft break	LOFTRAN, FACTRAN, COAST, VIPRE-01	0.0 and function of moderator density	–	Lower curve of Figure 9.0-3	3415 and 3449.15 (a)
9.4	Reactivity and power distribution anomalies					
	Uncontrolled RCCA bank withdrawal from a subcritical or low power startup condition	TWINKLE, FACTRAN, VIPRE-01	–	0.0	Coefficient is consistent with a Doppler defect of -0.90%Δk	0
	Uncontrolled RCCA bank withdrawal at power	LOFTRAN	0.0 and 0.470	–	Upper and lower curves of Figure 9.0-3	10%, 60%, and 100% of 3415
	RCCA misalignment	LOFTRAN, VIPRE-01	NA	–	NA	3415
	Startup of an inactive reactor coolant pump at an incorrect temperature	NA	NA	–	NA	NA

Table 9.0-6 (Sheet 4 of 5). Summary Of Initial Conditions And Computer Codes Used

Section	Faults	Computer Codes Used	Reactivity Coefficients Assumed			Initial Thermal Power Output Assumed (MWt)
			Moderator Density ($\Delta k/gm/cm^3$)	Moderator Temperature (pcm/°C)	Doppler	
9.4	Chemical and volume control system malfunction that results in a decrease in the boron concentration in the reactor coolant	NA	NA	–	NA	0 and 3415
	Inadvertent loading and operation of a fuel assembly in an improper position	ANC	NA	–	NA	3415
	Spectrum of RCCA ejection accidents	ANC, VIPRE	Refer to Section 9.4.8	Refer to Section 9.4.8	Refer to Section 9.4.8	Refer to Section 9.4.8
9.5	Increase in reactor coolant inventory					
	Inadvertent operation of the core makeup tanks during power operation	LOFTRAN	0.0	–	Upper curve of Figure 9.0-3	3449.15 (a)
	Chemical and volume control system malfunction that increases reactor coolant inventory	LOFTRAN	0.0	–	Upper curve of Figure 9.0-3	3449.15 (a)

Table 9.0-6 (Sheet 5 of 5). Summary Of Initial Conditions And Computer Codes Used

Section	Faults	Computer Codes Used	Reactivity Coefficients Assumed			Initial Thermal Power Output Assumed (MWt)
			Moderator Density ($\Delta k/gm/cm^3$)	Moderator Temperature (pcm/°C)	Doppler	
9.6	Decrease in reactor coolant inventory					
	Inadvertent opening of a pressuriser safety valve and inadvertent operation of ADS	LOFTRAN, FACTRAN, VIPRE-01	0.0	–	Upper curve of Figure 9.0-3	3415
	Steam generator tube failure	LOFTTR2	0.0	–	Lower curve of Figure 9.0-3	3449.15 (a)
	A break in an instrument line or other lines from the reactor coolant pressure boundary that penetrate containment	NA	NA	–	NA	NA
	LOCAs resulting from the spectrum of postulated piping breaks within the reactor coolant pressure boundary	NOTRUMP WCOBRA/ TRAC	See Section 9.6.5 references	–	See Section 9.6.5 references	3434.0 (a) (b)

Notes:

a. The non-LOCA analyses assume an initial power of 101% of the nuclear steam supply system (NSSS) power (NSSS power = rated thermal power (RTP) plus 15 MWt for pump heat), and the LOCA analyses assume an initial power of 101% of RTP.

b. Section 9.6.4 describes the large-break LOCA analysis methodology, which includes treatment of the initial thermal power output uncertainty.

Table 9.0-7. Nominal Values Of Pertinent Plant Parameters Used In Accident Analyses

	RTDP With 10% Steam Generator Tube Plugging	Without RTDP[a]	
		Without Steam Generator Tube Plugging	With 10% Steam Generator Tube Plugging
Thermal output of NSSS (MWt)	3415	3415	3415
Core inlet temperature (°C/°F)	279.9 / 535.8	279.7 / 535.5	279.4 / 535.0
Vessel average temperature (°C/°F)	300.9 / 573.6	300.9 / 573.6	300.9 / 573.6
Reactor coolant system pressure (MPa/psia)	15.51 / 2250.0	15.51 / 2250.0	15.51 / 2250.0
Reactor coolant flow per loop (m^3/hr / gpm)	34250 /15.08 E+04	34046 / 14.99 E+04	33614/ 14.8 E+04
Steam flow from NSSS (kg/hr / lbm/hr)	6.79E+06 / 14.96 E+06	6.79E+06 / 14.96 E+06	6.78E+06 / 14.96 E+06
Steam pressure at steam generator outlet (MPa/psia)	5.531 / 802.2	5.612 / 814.0	5.488 / 796.0
Assumed feedwater temperature at steam generator inlet (°C/°F)	226.7 / 440.0	226.7 / 440.0	226.7 / 440.0
Average core heat flux (W/m^2 / Btu/-hr-ft^2)	6.28E+05 / 1.99 E+05	6.28E+05 / 1.99 E+05	6.28E+05 / 1.99 E+05

Note:

a. Steady-state errors discussed in Section 9.0.2 are added to these values to obtain initial conditions for most transient analyses.

Table 9.0-8 (Sheet 1 of 2). Protection And Safety Monitoring System Setpoints And Time Delay Assumed In Accident Analyses

Function	Limiting Setpoint Assumed in Analyses	Time Delays (seconds)
Reactor trip on power range high positive flux rate	15% with 60-second time constant	0.9
Reactor trip on power range high neutron flux, low setting	35%	0.9
Reactor trip on source range neutron flux reactor trip	Not applicable	0.9
Overtemperature ΔT	Variable (see Figure 9.0-1)	2.0
Overpower ΔT	Variable (see Figure 9.0-1)	1.0
Reactor trip on High-2 pressuriser pressure	16.96 MPa (2460 psia)	2.0
Reactor trip on Low-2 pressuriser pressure	12.41 MPa (1800 psia)	2.0
Reactor trip on Low-2 reactor coolant flow in either hot leg	87% loop flow	1.45
Reactor trip on reactor coolant pump under speed	90%	0.65
Reactor trip on Low-2 steam generator narrow range level	0% of span	2.0
High steam generator narrow range level coincident with reactor trip (P-4)	85% of narrow range level span	2.0 (startup feedwater isolation) 2.0 (chemical and volume control system makeup isolation)
High-3 steam generator level	95% of narrow range level span	2.0 (reactor trip) 0.0 (turbine trip) 2.0 (feedwater isolation)
Reactor trip on High-3 pressuriser water level	76% of span	2.0
PRHR actuation on Low-2 steam generator wide range level	22.3%	2.0
“S” signal and steam line isolation on Low-2 T_{cold}	260°C (500°F) lower bound 265.6°C (510°F) upper bound	2.0

Table 9.0-8 (Sheet 2 of 2). Protection And Safety Monitoring System Setpoints And Time Delay Assumed In Accident Analyses

Function	Limiting Setpoint Assumed in Analyses	Time Delays (seconds)
"S" signal and steam line isolation on Low-2 steam line pressure	2.79 MPa (405 psia) (with an adverse environment assumed)	2.0
	3.69 MPa (535 psia) (without an adverse environment assumed)	
"S" signal on Low-3 pressuriser pressure	11.721 MPa (1700 psia)	2.0
Reactor trip on PRHR discharge valves not closed	Valve not closed	1.25
"S" signal on High-2 containment pressure	0.055 MPa (8 psig)	2.0
Reactor coolant pump trip following "S"	–	5.0 5.3 (LBLOCA)
PRHR actuation on High-3 pressuriser water level	76% of span	2.0 (plus 15.0-second timer delay)
Chemical and volume control system isolation on High-2 pressuriser water level	69% of span	2.0
Chemical and volume control system isolation on high-1 pressuriser water level coincident with "S" signal	33% of span	2.0
Boron dilution block on source range flux doubling	3 over 50 minutes	80.0
ADS Stage 1 actuation on core makeup tank low level signal	67.5% of tank volume	32.0 seconds for control valve to begin to open
ADS Stage 4 actuation on core makeup tank low-low level signal	20% of tank volume	2.0 seconds for squib valve to begin to open
CMT actuation on pressuriser Low-2 water level	0% of span	2.0

Note:

1. The table includes only protection functions (reactor trip and ESF actuation) credited in the safety analysis in Chapter 9. Other protection functions are available and may act. Table 9.0-10 lists all protection functions that may act for each Chapter 9 event.

Table 9.0-9. Limiting Delay Times For Equipment Assumed In Accident Analyses

Component	Time Delays (seconds)
Feedwater isolation valve closure, feedwater control valve closure, or feedwater pump trip	10 (maximum value for non-LOCA) 5 (maximum value for mass/energy)
Steam line isolation valve closure	5
Core makeup tank discharge valve opening time	15 (maximum) 10 (nominal value for best-estimate LOCA)
Chemical and volume control system isolation valve closure	30
PRHR discharge valve opening time	15 (maximum) 10 (nominal value for best-estimate LOCA) 1.0 second (small-break LOCA value: follows a 15-second interval of no valve movement)
Demineralized water transfer and storage system isolation valve closure time	20
Steam generator power-operated relief valve block valve closure	44
Automatic depressurisation system (ADS) valve opening times	See Table 9.6.5-10.

Table 9.0-10 (Sheet 1 of 5). Plant Systems And Equipment Available For Transient And Accident Conditions

Incident	Reactor Trip Functions	ESF Actuation Functions	ESF and Other Equipment
Section 9.1			
Increase in heat removal from the primary system			
Feedwater system malfunctions that result in an increase in feedwater flow	High-3 Steam Generator Level, Power range high positive flux rate and high neutron flux, overpower ΔT, overtemperature ΔT, manual	High-3 steam generator level produced feedwater isolation and turbine trip	Feedwater isolation valves
Excessive increase in secondary steam flow	Power range high positive flux rate and high neutron flux, overtemperature ΔT, overpower ΔT, manual	–	–
Inadvertent opening of a steam generator safety valve	Power range high positive flux rate and high neutron flux, overtemperature ΔT, overpower ΔT, Low-2 pressuriser pressure, “S”, manual	Low-3 pressuriser pressure, Low-2 compensated steam line pressure, Low-2 T_{cold}, low-2 pressuriser level	Core makeup tank, feedwater isolation valves, main steam isolation valves (MSIVs), startup feedwater isolation, accumulators
Steam system piping failure	Power range high positive flux rate and high neutron flux, overtemperature ΔT, overpower ΔT, Low-2 pressuriser pressure, “S”, manual	Low-3 pressuriser pressure, Low-2 compensated steam line pressure, high-2 containment pressure, Low-2 T_{cold}, manual	Core makeup tank, feedwater isolation valves, MSIVs, accumulators, startup feedwater isolation
Inadvertent operation of the PRHR	PRHR discharge valve position	Low-3 pressuriser pressure, Low-2 T_{cold}, Low-2 pressuriser level	Core makeup tank

Table 9.0-10 (Sheet 2 of 5). Plant Systems And Equipment Available For Transient And Accident Conditions

Incident	Reactor Trip Functions	ESF Actuation Functions	ESF and Other Equipment
Section 9.2			
Decrease in heat removal by the secondary system			
Loss of external load/turbine trip	High-2 pressuriser pressure, High-3 pressuriser water level, overtemperature ΔT, overpower ΔT, Steam generator Low-2 narrow range level, Low-2 RCP speed, manual	–	Pressuriser safety valves, steam generator safety valves
Loss of nonemergency ac power to the station auxiliaries	Steam generator Low-2 narrow range level, High 2 pressuriser pressure, High-3 pressuriser level, low RCP speed, manual	Steam generator low narrow range level coincident with low startup water flow, steam generator low wide range level	PRHR, steam generator safety valves, pressuriser safety valves
Loss of normal feedwater flow	Steam generator Low-2 narrow range level, High-2 pressuriser pressure, High-3 pressuriser level, manual	Steam generator low narrow range level coincident with low startup water flow, steam generator low wide range level	PRHR, steam generator safety valves, pressuriser safety valves, reactor vessel head vent
Feedwater system pipe break	Steam generator Low-2 narrow range level, High-2 pressuriser pressure, High-3 pressuriser level, overtemperature ΔT, manual	Steam generator low narrow range level coincident with low startup feedwater flow, Steam generator low wide range level, Low-2 steam line pressure, high-2 containment pressure	PRHR, core makeup tank, MSIVs, feedline isolation, pressuriser safety valves, steam generator safety valves

Table 9.0-10 (Sheet 3 of 5). Plant Systems And Equipment Available For Transient And Accident Conditions

Incident	Reactor Trip Functions	ESF Actuation Functions	ESF and Other Equipment
Section 9.3			
Decrease in reactor coolant system flow rate			
Partial and complete loss of forced reactor coolant flow	Low flow, underspeed, manual	–	Steam generator safety valves, pressuriser safety valves
Reactor coolant pump shaft seizure (locked rotor)	Low flow, High-2 pressuriser pressure, manual	–	Pressuriser safety valves, steam generator safety valves
Section 9.4			
Reactivity and power distribution anomalies			
Uncontrolled RCCA bank withdrawal from a subcritical or low power startup condition	Source range high neutron flux, intermediate range high neutron flux, power range high neutron flux (low setting), power range high neutron flux (high setting), power range high positive flux rate, manual	–	–
Uncontrolled RCCA bank withdrawal at power	Power range high neutron flux, power range high positive flux rate, overtemperature ΔT, over-power ΔT, High-2 pressuriser pressure, High-3 pressuriser water level, manual	–	Pressuriser safety valves, steam generator safety valves
RCCA misalignment	Overtemperature ΔT, low pressuriser pressure, manual	–	–
Startup of an inactive reactor coolant pump at an incorrect temperature	Power range high positive flux rate, low flow (P-10 interlock), manual	–	–

Table 9.0-10 (Sheet 4 of 5). Plant Systems And Equipment Available For Transient And Accident Conditions

Incident	Reactor Trip Functions	ESF Actuation Functions	ESF and Other Equipment
Section 9.4 (Cont.)			
Chemical and volume control system malfunction that results in a decrease in boron concentration in the reactor coolant	Source range high flux, power range high positive flux rate, overtemperature ΔT, manual	Source range flux doubling, intermediate range high flux (Modes 3-6)	Chemical and volume control system (CVS) to RCS isolation valves, makeup pump suction isolation valves, from the demineralized water transfer and storage system
Spectrum of RCCA ejection accidents	Power range high flux, high positive flux rate, manual	–	Pressuriser safety valves
Section 9.5			
Increase in reactor coolant inventory			
Inadvertent operation of the CMT during power operation	High-2 pressuriser pressure, manual, “safeguards” trip, High-3 pressuriser level	High-3 pressuriser level, Low-2 T_{cold}	Core makeup tank, pressuriser safety valves, chemical and volume control system isolation, PRHR, steam generator safety valves, reactor vessel head vent
Chemical and volume control system malfunction that increases reactor coolant inventory	High-2 pressuriser pressure, “safeguards” trip, high pressuriser level, manual	High-3 pressuriser level, Low-2 T_{cold}, Low-2 steam line pressure	Core makeup tank, pressuriser safety valves, chemical and volume control system isolation, PRHR, reactor vessel head vent
Section 9.6			
Decrease in reactor coolant inventory			
Inadvertent opening of a pressuriser safety valve or ADS path	Low-2 pressuriser pressure, overtemperature ΔT, manual	Low-3 pressuriser pressure	Core makeup tank, accumulator

Table 9.0-10 (Sheet 5 of 5). Plant Systems And Equipment Available For Transient And Accident Conditions

Incident	Reactor Trip Functions	ESF Actuation Functions	ESF and Other Equipment
Section 9.6 (Cont.)			
Steam generator tube rupture	Low-2 pressuriser pressure, overtemperature ΔT, safeguards (“S”), manual	Low-3 pressuriser pressure, high-2 steam generator water level, high steam generator level coincident with reactor trip (P-4), Low-2 steam line pressure, Low-2 pressuriser level	Core makeup tank, PRHR, steam generator safety and/or relief valves, MSIVs, radiation monitors (air removal, steam line, and steam generator blowdown), startup feedwater isolation, chemical and volume control system pump isolation, pressuriser heater isolation, steam generator power-operated relief valve isolation
LOCAs resulting from the spectrum of postulated piping breaks within the reactor coolant pressure boundary	Low-2 pressuriser pressure, safeguards (“S”), manual	High-2 containment pressure, Low-3 pressuriser pressure	Core makeup tank, accumulator, ADS, steam generator safety and/or relief valves, PRHR, IRWST

Table 9.0-11 (Sheet 1 of 2). Single Failures Assumed In Accident Analyses

Event Description	Failure
Feedwater temperature reduction[a]	–
Excessive feedwater flow	One protection division
Excessive steam flow[a]	
Inadvertent secondary depressurisation	One core makeup tank discharge valve
Steam system piping failure	One core makeup tank discharge valve (zero-power case) One protection division (full-power case)
Inadvertent operation of the PRHR	One protection division
Steam pressure regulator malfunction[b]	–
Loss of external load	One protection division
Turbine trip	One protection division
Inadvertent closure of main steam isolation valve	One protection division
Loss of condenser vacuum	One protection division
Loss of ac power	One PRHR discharge valve
Loss of normal feedwater	One PRHR discharge valve
Feedwater system pipe break	One PRHR discharge valve
Partial loss of forced reactor coolant flow	One protection division
Complete loss of forced reactor coolant flow	One protection division
Reactor coolant pump locked rotor	One protection division
Reactor coolant pump shaft break	One protection division
RCCA bank withdrawal from subcritical	One protection division
RCCA bank withdrawal at power	One protection division
Dropped RCCA, dropped RCCA bank	One protection division
Statically misaligned RCCA[c]	–
Single RCCA withdrawal	One protection division

Notes:

a. No protection action required

b. Not applicable to AP1000

c. No transient analysis

Table 9.0-11 (Sheet 2 of 2). Single Failures Assumed In Accident Analyses

Event Description	Failure
Flow controller malfunction[b]	–
Uncontrolled boron dilution	One protection division
Improper fuel loading[c]	–
RCCA ejection	One protection division
Inadvertent CMT operation at power	One PRHR discharge valve
Increase in reactor coolant system inventory	One PRHR discharge valve
Inadvertent reactor coolant system depressurisation	One protection division
Failure of small lines carrying primary coolant outside containment[c]	–
Steam generator tube rupture	Ruptured steam generator power-operated relief valve fails open
Spectrum of LOCA Small breaks Large breaks	 One ADS Stage 4 valve One CMT valve
Post-LOCA Long-term cooling	One ADS Stage 4 valve

Notes:

a. No protection action required

b. Not applicable to AP1000 design

c. No transient analysis

Table 9.0-12. Non-Class 1 SSCs Credited For Mitigation Of Accidents

Event	Non-Class 1 System and Equipment
9.1.2 Feedwater system malfunctions that result in an increase in feedwater flow	Main feedwater pump trip
9.1.4 Inadvertent opening of a steam generator relief or safety valve	MSIV backup valves[1] Main steam branch isolation valves
9.1.5 Steam system piping failure	MSIV backup valves[1] Main steam branch isolation valves
9.2.7 Loss of normal feedwater	Pressuriser heater block
9.5.1 Inadvertent operation of the core makeup tanks during power operation	Pressuriser heater block
9.5.2 Chemical and volume control system malfunction that increases reactor coolant inventory	Pressuriser heater block
9.6.3 Steam generator tube rupture	Pressuriser heater block MSIV backup valves(1) Main steam branch isolation valves
9.6.5 Small-break LOCA	Pressuriser heater block

Note:

1. These include the turbine stop or control valves, the turbine bypass valves, and the moisture separator reheater 2nd stage steam isolation valves.

Table 9.0-13 Key Acceptance Criteria for ATWT Diversity Studies

ATWT Acceptance Criterion	Assessments used to Demonstrate Criterion is Met
Coolable geometry for reactor core is maintained	Demonstrate that DNB does not occur. As such, all ATWT core damage criteria are met.
Reactor coolant pressure boundary integrity is maintained	Calculated reactor coolant system pressure transient should be limited such that the stress does not exceed the ASME Service Level C limits. For the AP1000 plant, ASME Service Level C limits correspond to a RCS pressure of 3200 psig (22.06 MPa-g).
Containment vessel integrity is maintained	As discussed in Section 9.0.13, this criterion was not explicitly evaluated because other design transients bound ATWT events for this criterion.

Table 9.0-14. Summary of Equipment Operability Analysis Assumptions for ATWT CCF Types

Systems and Functions		CCF Group		
		PMS CCF	Reactor Trip Breakers CCF	Mechanical RCCA CCF
PMS	Reactor Trip Functions	Failed	Partial Failure (logic functions operable, RCCAs do not insert on demand from PMS)	Partial Failure (logic functions operable, RCCAs do not insert on demand from PMS)
	ESF Functions	Failed	Operable	Operable
	Turbine trip	Failed	Operable	Operable
	Manual Functions	Manual ESF Functions Failed Manual Reactor Trip Functions Operable	Partial Failure (manual functions operable except RCCAs do not insert on demand from PMS) on demand from PMS)	Partial Failure (manual functions operable except RCCAs do not insert
DAS	Diverse Reactor Trip Functions	Operable	Operable	Failed
	ESF functions	Operable	Operable	Operable
	Manual Functions	Operable	Operable	Partial Failure (manual functions operable except RCCAs do not insert on demand from DAS)

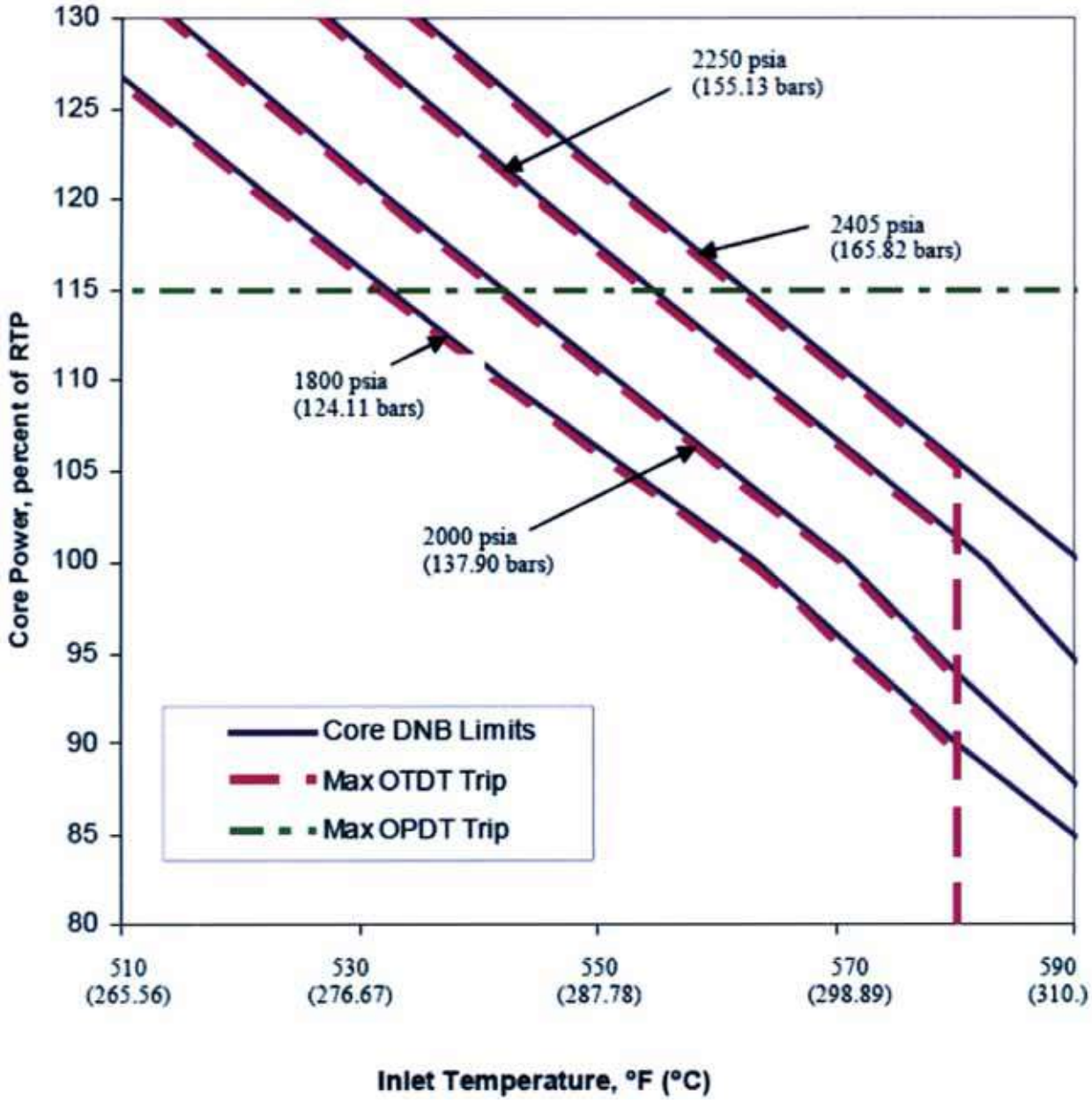


Figure 9.0-1. Overpower and Overtemperature ΔT Protection

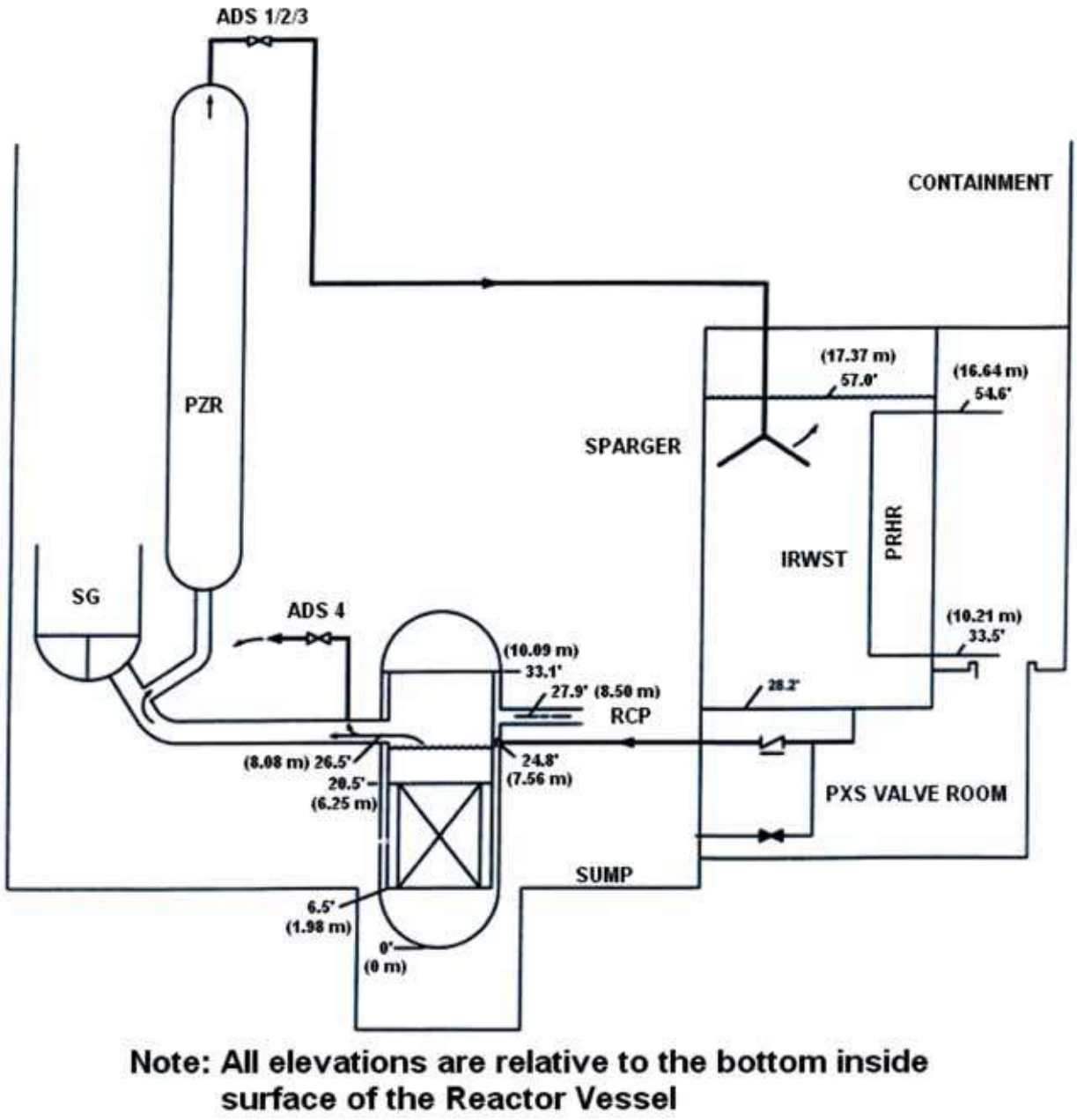


Figure 9.0-2. AP1000 Loop Layout

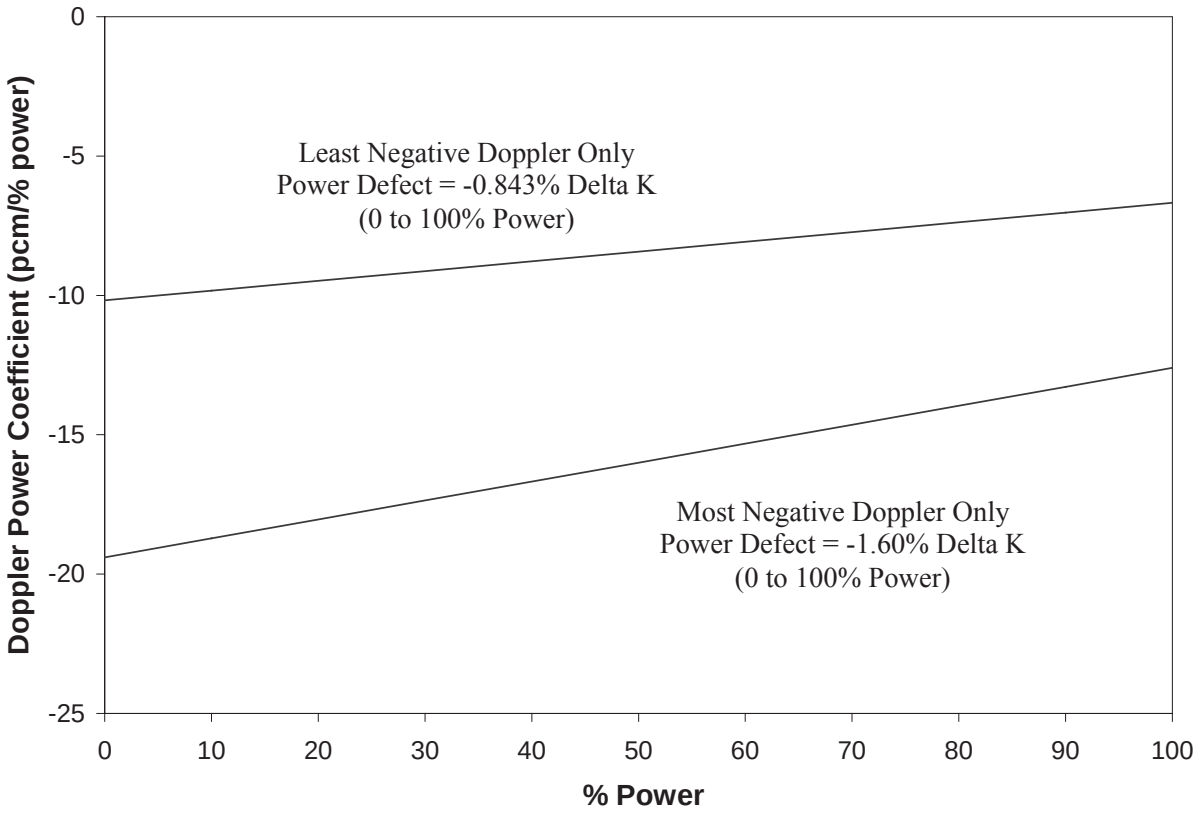


Figure 9.0-3. Doppler Power Coefficient used in Accident Analysis

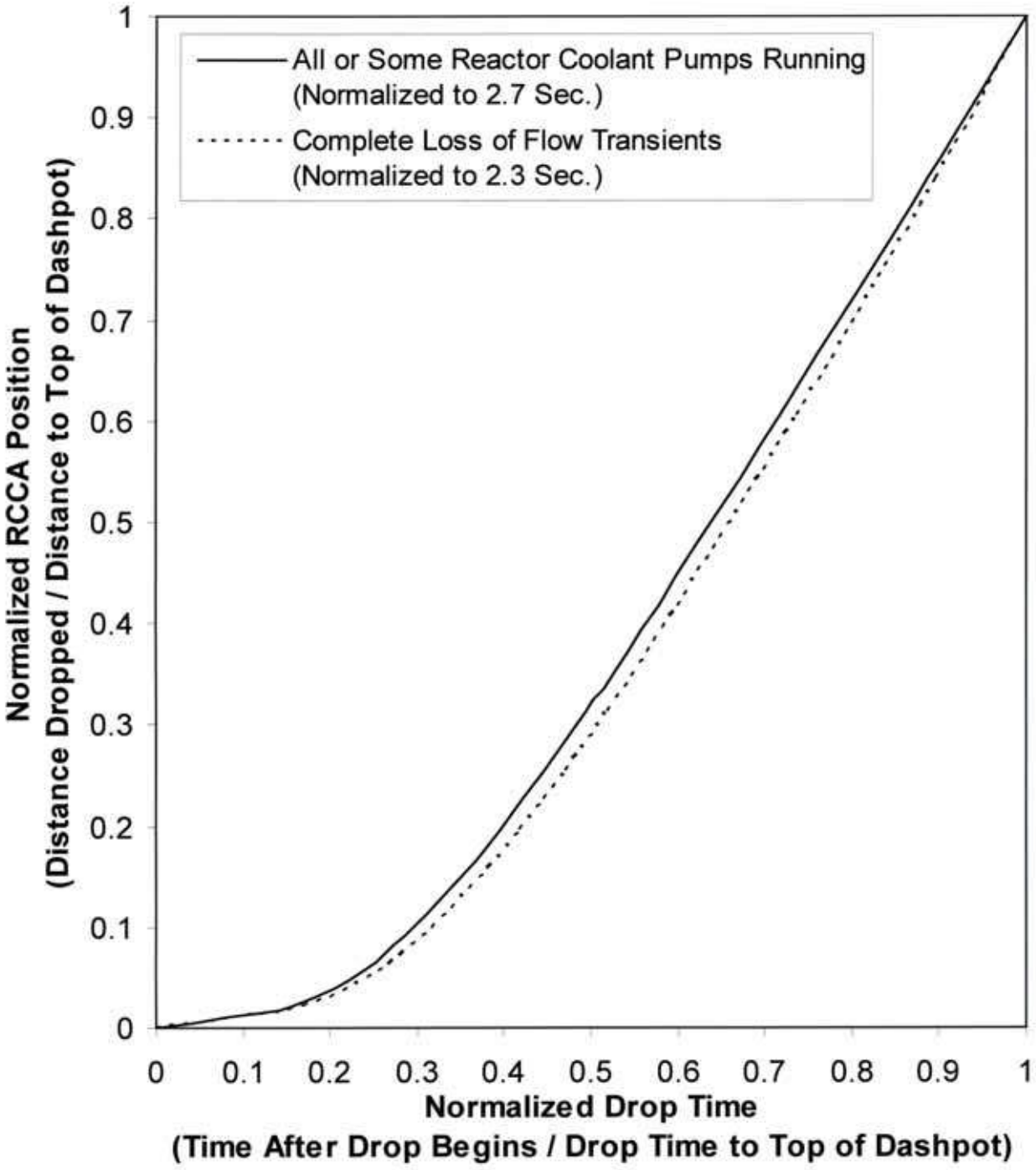


Figure 9.0-4. RCCA Position Versus Time to Dashpot

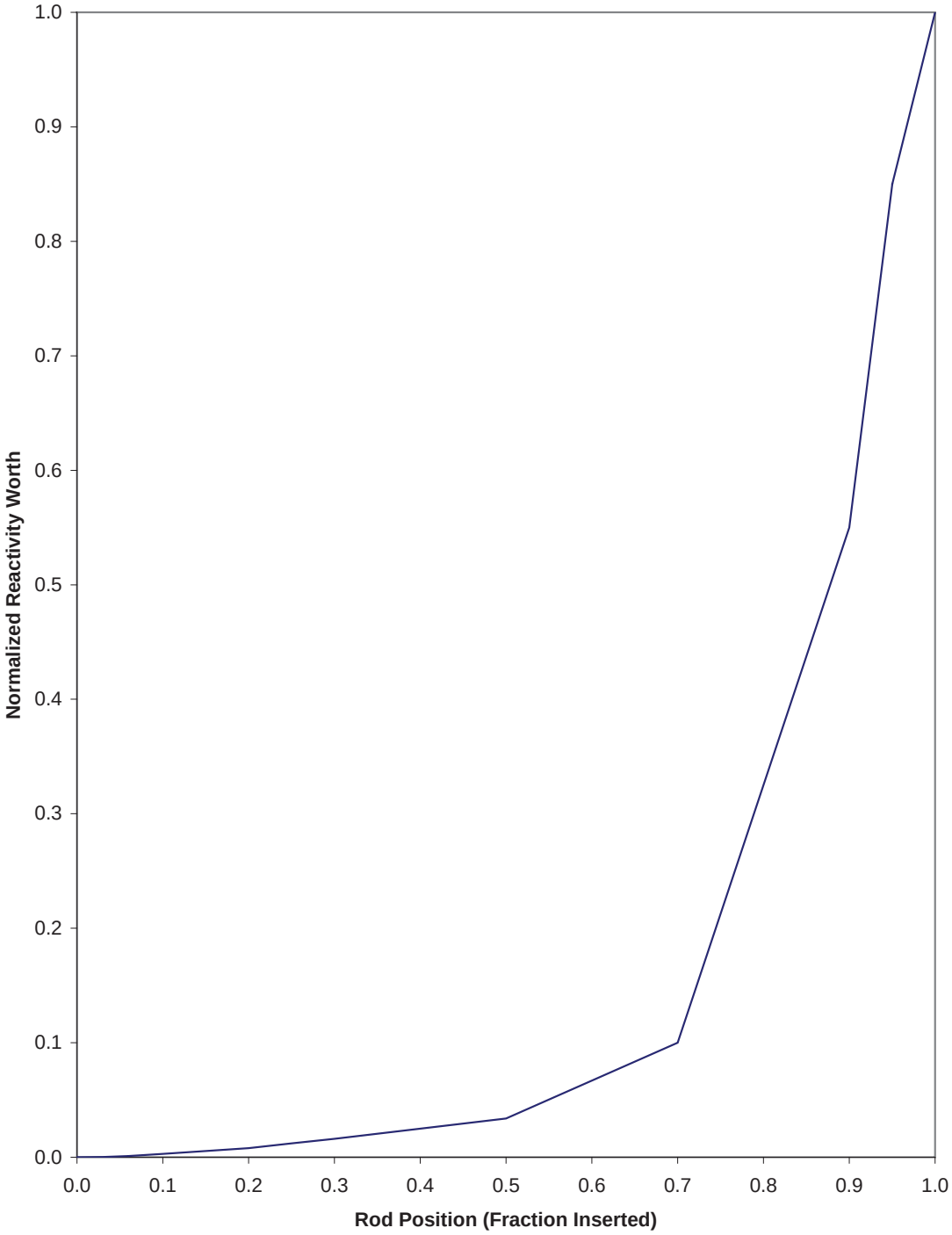


Figure 9.0-5. Normalized Rod Worth Versus Position

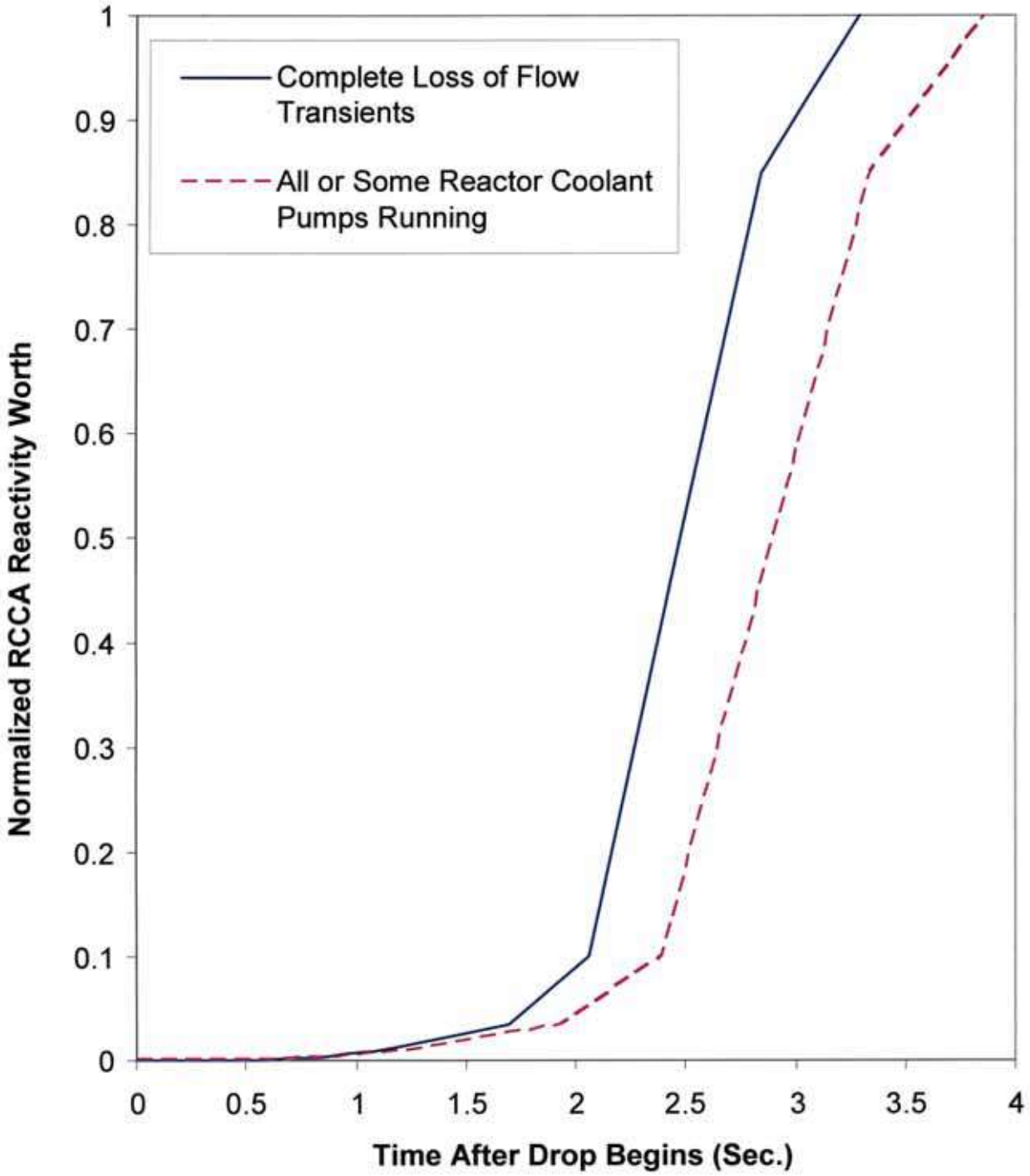


Figure 9.0-6. Normalized RCCA Bank Reactivity Worth Versus Drop Time

9.1 Increase in Heat Removal From the Primary System

A number of faults that could result in an increase in heat removal from the reactor coolant system are postulated. The events are discussed in this section. Detailed analyses are presented for the most limiting of the primary system heat removal increase events.

9.1.0 Introduction and Overview of Faults

Increase in heat removal from the reactor coolant circuit can be caused by a number of initiating faults that are split into two parts:

- Increase in heat removal events
    - Feedwater system malfunctions that result in a decrease in feed water temperature
    - Feedwater system malfunctions that result in an increase in feed water flow
    - Inadvertent operation of PRHR heat exchanger due to operator error or false actuation signal
    - Excessive increase in secondary steam flow due to administrative violation or equipment malfunction
    - Turbine generator causing random event failure
    - Pump speed fault (flow higher than demanded)
    - Power-operated relief valve (PORV) actuates prematurely and does not reclose due to human error or hardware failure
    - Spurious actuation of main steam line safety valve
- Main steam line break (MSLB)
    - Main steam line break inside containment, downstream of MSIV
    - Main steam line break outside containment, downstream of MSIV
    - Main steam line break inside containment, upstream of MSIV

Overcooling of the primary circuit causes an increase in reactor power as a result of the negative moderator temperature coefficient. Such transients are attenuated by the thermal capacity of the secondary plant and of the RCS before the overpower or overtemperature protection leads to reactor trip.

The potential reactivity injection associated with these faults may be enhanced if the effect of the cooldown is maximised (for example, if the reactor is in hot standby conditions with no significant decay heat).

The MSLB accident is considered separately, as it differs significantly from the other increase-in-heat-removal events because it involves a rapid loss of secondary coolant accompanied by a rapid cooldown of the primary circuit.

This section considers these faults in turn. Each fault is first described; the initial event frequency and the design basis class are provided and the bounding fault or faults are identified (if needed). The analysed faults are presented individually in Table 8A-2.

The analysed fault(s) are then described in additional detail in the subsequent sections to complete the safety case for each fault, including:

- Identification of Causes and Accident Description
- Design Basis Analysis of Effects and Consequences

- Assessment of the Radiological Consequences for the DBA
- Diverse Mitigation and ATWT for Frequent Faults
- ALARP Assessment
- Conclusions

ATWT analyses presented herein are based on References 9.1-5 and 9.1-10.

9.1.0.1 Increase in Heat Removal Faults (Excluding MSLB)

Description

A number of transients and accidents could increase the heat removal from the RCS. Such faults are shown below:

- Feedwater system malfunctions, causing a reduction in feedwater temperature (Fault 1.15.13)
- Feedwater system malfunctions, causing an increase in feedwater flow (Fault 1.15.14)
- Excessive increase in secondary steam flow (Fault 1.15.18)
- Inadvertent opening of a SG relief or safety valve (Fault 1.22.1)
- Inadvertent operation of the passive residual heat removal heat exchanger (PRHR HX) (Fault 1.15.15)
- Stuck-open SG relief or safety valve (effectively, a steam system piping failure, Fault 1.22.1)

Separate analyses for the non-break faults listed above are included. They are analysed separately since there may be different PMS reactor trip or Engineered Safeguards Features necessary to mitigate the consequences of each event.

Other faults that could cause an increase in heat removal are shown below:

- Failure of the turbine generator casing (Fault 1.15.19)

- Pump speed fault leading to higher than expected primary coolant flow rate (Fault 1.15.21)

Initiating Event Frequency[1]

The increase in heat removal faults, as summarised above, comprise a number of faults identified in Table 8A-2 under the "Core Power Excursion" heading, with IEFs greater than 1.0E-3/yr. It is therefore appropriate to consider the increase in heat removal faults as representative of a frequent fault (DB2).

Design Basis Class

The unmitigated consequences of increase in heat removal faults are assumed to be greater than the Target 4 BSL for frequent faults (1 mSv offsite and 20 mSv onsite). Given the IEF above, the event is in the DB2 class.

1 As discussed in Chapter 8, the frequency for initiating events from the PSA is used in both Chapters 8 and 9 with the sole purpose of supporting the categorisation of the fault to a specific DB category. As noted in Chapter 8, these probabilities should not be considered to be representative of actual frequency of the events, and for several events they can be significantly conservative. Detailed PSA results and their basis are discussed in Chapter 10 of this PCSR.

9.1.0.2 Main Steam Line Break

Description

The AP1000 design PSA considers three categories of steam system piping failure:

- MSLB MSIV
- MSLB downstream of the MSIV
- Main steam line valve stuck open

For the DBA, only major ruptures of the main steam line (i.e., MSLBs) are addressed as steam line breaks. The stuck-open safety valve and minor secondary system pipe breaks are addressed with the increase in heat removal faults, as explained previously.

Separate analyses for the MSLB faults are included to address differences in failures at hot zero power (9.1.5) and at full power (9.1.6).

Initiating Event Frequency

The fault schedule (Appendix 8A) gives the frequency of the MSLB initiating events as 5.38E-04/yr (summed values), which makes the fault an infrequent fault in the UK definition.

Design Basis Class

The unmitigated consequences of a MSLB accident are assumed to be greater than the Target 4 BSL for frequent faults (1 mSv offsite and 20 mSv onsite). Given the IEF above, the event is in the DB1 class.

9.1.1 Feedwater System Malfunctions that Result in a Decrease in Feedwater Temperature (Fault 1.15.13)

9.1.1.1 Identification of Causes and Accident Description

In the presence of a negative moderator temperature coefficient, reductions in feedwater temperature cause an increase in core power by decreasing reactor coolant temperature. Such transients are attenuated by the thermal capacity of the secondary plant and of the reactor coolant system. The overpower/overtemperature protection (high positive neutron flux rate, overtemperature, and overpower ΔT trips) prevents a power increase that could lead to a DNBR that is less than the design limit values.

A reduction in feedwater temperature may be caused by a low-pressure heater train or a high-pressure heater train out of service or bypassed. At power, this increased subcooling creates an increased load demand on the reactor coolant system.

With the plant at no-load conditions, the addition of cold feedwater may cause a decrease in reactor coolant system temperature and a reactivity insertion due to the effects of the negative moderator coefficient of reactivity. However, the rate of energy change is reduced as load and feedwater flows decrease, so the no-load transient is less severe than the full-power case. The net effect on the reactor coolant system due to a reduction in feedwater temperature is similar to the effect of increasing secondary steam flow; that is, the reactor reaches a new equilibrium condition at a power level corresponding to the new steam generator ΔT.

Appendix 9C provides discussion and analysis of long term safe shutdown for non-LOCA events.

9.1.1.2 Design Basis Mitigation

Analysis is performed to demonstrate the adequacy of the PMS to detect and mitigate the fault and show that the safety analysis criteria are satisfied including:

- No fuel failures (confirmed using minimum DNBR and fuel melt criteria),
- The RCS pressure criterion is met,
- The main steam system (MSS) pressure criterion is met, and
- The pressuriser does not fill (which could result in a LOCA).

With respect to the peak RCS and MSS pressure criteria, this event is bounded by the Turbine Trip DB analysis in Section 9.2.3 and is not explicitly verified. Also, pressuriser fill criterion is not challenged for this event, and is not explicitly verified.

9.1.1.2.1 DBA Method of Analysis

This transient is analysed by calculating conditions at the feedwater pump inlet following the removal of a low-pressure feedwater heater train from service. These feedwater conditions are then used to recalculate a heat balance through the high-pressure heaters. This heat balance gives the new feedwater conditions at the steam generator inlet.

The following assumptions are made:

- Initial plant power level corresponding to 100-percent nuclear steam supply system thermal output.

- The worst single failure in the pre-heating section of the Main Feedwater System, resulting in the maximum reduction in feedwater temperature, occurs.

Plant characteristics and initial conditions are further discussed in Section 9.0.2.

9.1.1.2.2 DBA Credited SSCs

Plant systems and equipment available to mitigate the effects of the accident are the same as for an excessive steam flow increase (Section 9.1.3) and are discussed in Section 9.0.4 and listed in Table 9.0-10.

9.1.1.2.3 DBA Results

A fault in the feedwater heaters section of the Feedwater System causes a reduction in feedwater temperature that increases the thermal load on the primary system. The maximum reduction in feedwater enthalpy, due to a single failure in the feedwater system, is bounded by the equivalent enthalpy reduction associated with the excessive increase in secondary steam flow event described in Section 9.1.3.

9.1.1.3 Diverse Mitigation

Diverse mitigation capabilities are the same as for the loss of normal feedwater fault, as described in Section 9.2.7.3.

9.1.1.3.1 Diverse Mitigation for ATWT

Because this fault will not result in a power increase sufficient to require reactor trip (i.e., No PMS or DAS setpoints are exceeded during the transient as demonstrated by the bounding DBA

analysis in Section 9.1.3), ATWT diversity is not required for this fault. The transient increase in core power does not challenge any fuel design limits. The reactor coolant pressure does not increase and challenge reactor coolant boundary design limits. There are no energy releases to containment during this event and the containment integrity is not challenged. Should the reactor operator attempt a manual trip or shutdown of the reactor and this action fails, manual reactor trip or manual actuation of the CMTs would be available via DAS.

9.1.1.3.2 Diverse Mitigation for Core Cooling

The loss of normal feedwater diverse core cooling, as analysed in Section 9.2.7.3.2, was determined to be bounding of all non-LOCA events.

9.1.1.4 Radiological Consequences

Design Basis

In the case where offsite power remains available, there is no release of activity to the environment and the Target 4 BSOs (0.01 mSv offsite and 0.1 mSv onsite) are met.

In the case where offsite power is lost, a small release of activity may occur as a result of steam dump to the atmosphere due to unavailability of the condensers. With no fuel damage and primary and secondary circuits intact, the initiating event has no impact on the doses. The doses are a consequence of the assumed loss of offsite power. Therefore, the loss of offsite power doses from Section 9.2.6.4 are presented. The calculated maximum doses for all relevant pathways (inhalation, cloudshine, and groundshine) are as follows:

- Offsite dose: 0.05 mSv Worker dose: 1.5 mSv

These doses are within the Target 4 BSL for frequent faults (1 mSv offsite and 20 mSv onsite).

Diverse Mitigation

ATWT is not applicable to this event. The diverse core cooling scenarios demonstrate that the RCS does not overpressurise and there is no significant fuel damage. For a diverse mitigation radiological consequences analysis better estimate assumptions would be credited. This would include reactor coolant system activity levels significantly lower than those modelled for the DBA and better activity retention in containment and in the steam generators. In addition better estimate atmospheric dispersion factors would be used. Therefore, a diverse mitigation radiological consequences analysis would show that the doses for the diverse core cooling scenario would be much less than for the design basis LOCA. The diverse mitigation analyses would not have to meet the Target 4 BSL for frequent faults and would meet the Target 4 BSL for infrequent faults.

9.1.1.5 As Low as Reasonably Practicable Assessment

The ALARP discussion for this event is the same as for Inadvertent Opening of a Steam Generator Relief or Safety Valve event, as described in Section 9.1.4.5.

9.1.1.6 Conclusions

The decrease in feedwater temperature transient is bounded by the excessive increase in secondary steam flow event. Based on the results presented in Section 9.1.3, the applicable evaluation criteria for the decrease in feedwater temperature event are met.

This event has also been adequately assessed with respect to ATWT considerations. This event was not explicitly analysed for the change in the current design reference point in the UK as described in Reference 9.1-9. However, the evaluation conducted to closeout FS-03 demonstrated with a subset of events (Reference 9.1-10) that there is little impact on the key analysis trends, results, and margin to the applicable acceptance criteria. Therefore, the subset of events confirmed the change in design reference point would not invalidate the conclusions presented for this event.

Diverse core cooling capabilities have been demonstrated.

DBA radiological consequences are within the Target 4 BSL for frequent faults (1 mSv offsite and 20 mSv onsite). Thus, the identification of necessary Class 1 SSCs is adequate to meet DB requirements.

It has been shown that the AP1000 plant design includes adequate systems for the protection of this fault, which limit the radiological consequences such that they are compliant with the SAPs targets and the risks have been reduced to be ALARP.

9.1.2 Feedwater System Malfunctions that Result in an Increase in Feedwater Flow (Fault 1.15.14)

9.1.2.1 Identification of Causes and Accident Description

Addition of excessive feedwater causes an increase in core power by decreasing reactor coolant temperature. Such transients are attenuated by the thermal capacity of the secondary plant and the reactor coolant system. The overpower/overtemperature protection (neutron overpower, overtemperature, and overpower ΔT trips) prevents a power increase that leads to a DNBR less than the safety analysis limit value.

An example of excessive feedwater flow is a full opening of a feedwater control valve due to a feedwater control system malfunction or an operator error. At power, this excess flow causes an increased load demand on the reactor coolant system due to increased subcooling in the steam generator.

With the plant at no-load conditions, the addition of cold feedwater may cause a decrease in reactor coolant system temperature and a reactivity insertion due to the effects of the negative moderator coefficient of reactivity.

Continuous addition of excessive feedwater is prevented by the steam generator high-3 water level signal trip, which closes the feedwater isolation valves and feedwater control valves and trips the turbine, main feedwater pumps, and reactor.

Plant systems and equipment available to mitigate the effects of the accident are discussed in Section 9.0.4 and listed in Table 9.0-10.

A loss of offsite power is assumed to occur as a consequence of the turbine trip for the excessive feedwater flow case initiated from full-power conditions. As discussed in Section 9.0.12, an excessive feedwater flow transient initiated with the plant at no-load conditions need not consider a consequential loss of offsite power. With the plant initially at zero-load, the turbine would not have been connected to the grid, so any subsequent reactor or turbine trip would not disrupt the grid and produce a consequential loss of offsite ac power.

9.1.2.2 Design Basis Mitigation

Analysis is performed to demonstrate the adequacy of the PMS to detect and mitigate the fault and show that the safety analysis criteria are satisfied including:

- No fuel failures (confirmed using minimum DNBR and fuel melt criteria),
- The RCS pressure criterion is met,
- The MSS pressure criterion is met, and
- The pressuriser does not fill (which could result in a LOCA).

With respect to the peak RCS and MSS pressure criteria, this event is bounded by the Turbine Trip DB analysis in Section 9.2.3 and is not explicitly verified. Also, pressuriser fill criterion is not challenged for this event, and is not explicitly verified.

9.1.2.2.1 DBA Method of Analysis

The excessive heat removal due to a feedwater system malfunction transient is analysed using the LOFTRAN computer code (Reference 9.1-1). LOFTRAN simulates a multiloop system, neutron kinetics, pressuriser, pressuriser safety valves, pressuriser spray, steam generator, and steam generator safety valves. The code computes pertinent plant variables, including temperatures, pressures, and power level.

The transient is analysed to demonstrate plant behaviour if excessive feedwater addition occurs because of system malfunction or operator error that allows a feedwater control valve to open fully. The following four cases are analysed assuming a conservatively large negative moderator temperature coefficient:

- Accidental opening of one feedwater control valve (single-loop) with the reactor just critical at zero-load conditions.
- Accidental opening of both feedwater control valves (multiloop) with the reactor just critical at zero-load conditions.
- Accidental opening of one feedwater control valve (single-loop) with the reactor in manual and automatic rod control at full power.
- Accidental opening of both feedwater control valves (multiloop) with the reactor in manual and automatic rod control at full power.

The reactivity insertion rate following a feedwater system malfunction is calculated with the following assumptions:

- For the feedwater control valve accident at full power, each faulted feedwater control valve is assumed to malfunction resulting in a step increase to 120 percent of nominal feedwater flow to the faulted steam generator.
- For the feedwater control valve accident at zero-load condition, a feedwater control valve malfunction occurs, which results in a step increase in flow to the faulted steam generator from 0 to 120 percent of the nominal full-load value.
- For the zero-load condition, feedwater temperature is at a conservatively low value of 120°C (248°F).
- No credit is taken for the heat capacity of the reactor coolant system and steam generator thick metal in attenuating the resulting plant cooldown.

- The feedwater flow resulting from a fully open control valve is terminated by a steam generator high-3 level trip signal, which closes feedwater control and isolation valves and trips the main feedwater pumps, the turbine, and the reactor.

Plant characteristics and initial conditions are further discussed in Section 9.0.2.

Normal reactor control systems are not required to function. The protection and safety monitoring system may function to trip the reactor because of overpower or high-3 steam generator water level conditions. No single active failure prevents operation of the protection and safety monitoring system.

The analysis assumes that the turbine trip during the case initiated from full power results in a consequential loss of offsite power that produces the coastdown of the reactor coolant pumps. As described in Section 9.0.12, the loss of offsite power is modelled to occur 3.0 seconds after the turbine trip. The excessive feedwater flow analysis conservatively delays the start of rod insertion until 2.0 seconds after the reactor trip signal is generated. Turbine trip occurs 5.0 seconds following a reactor trip condition being reached. This delay is part of the AP1000 reactor trip system. Complete rod insertion occurs in less than 5 seconds so that the loss of offsite power has no impact on the feedwater malfunction analysis.

9.1.2.2.2 DBA Credited SSCs

For the DB, all of the claimed SSCs are Class 1. The claimed Class 1 SSCs are listed in Table 9.0-10. The presented DBA ends shortly after reactor trip; however, essential safety functions for the long term safe shutdown analysis (Appendix 9C) bound safe shutdown response for this event. The primary core cooling is provided by the PRHR and passive containment cooling. Other SSCs include the CMTs, containment isolation, pressuriser safety valves (SVs) and steam generator SVs. The PMS provides the following:

- Reactor trip (RT) and Feedwater Isolation on High-3 SG narrow-range (NR) level in either SG
- PRHR actuation on Low-2 SG NR level coincident with Low-2 startup feedwater (SFW) flow
- CMTs and containment isolation on Low-2 cold leg (CL) temperature
- PCS on High-2 containment pressure

9.1.2.2.3 DBA Results

In the case of an accidental full opening of both feedwater control valves with the reactor at zero power and the preceding assumptions, the maximum reactivity insertion rate is less than the maximum reactivity insertion rate analysed in Section 9.4.1 for an uncontrolled (RCCA) bank withdrawal from a subcritical or low-power startup condition. Therefore, the results of the analysis are not presented here. If the incident occurs with the unit just critical at no-load, the reactor may be tripped by the power range high neutron flux trip (low setting) set at approximately 25-percent nominal full power, or by the power range high positive flux rate trip.

The full-power case (maximum reactivity feedback coefficients, automatic rod control, and multi-loop malfunction) results in the greatest power increase. Assuming the rod control system to be in the manual control mode results in a slightly less severe transient.

When the steam generator water level in the faulted loop reaches the high-3 level setpoint, the feedwater control valves and feedwater isolation valves are automatically closed and the main feedwater pumps are tripped. This prevents continuous addition of the feedwater. In addition, a turbine trip and a reactor trip are initiated.

Transient results show the increase in nuclear power and ΔT associated with the increased thermal load on the reactor (see Figures 9.1.2-1 and 9.1.2-2). A new equilibrium condition is reached and all the plant parameters, except for the SG water level, remain almost constant until the reactor trips on High-3 SG level. The minimum DNBR is predicted to occur before the reactor trip and the reactor coolant pump coastdown caused by the loss of offsite power. The minimum DNBR predicted is well above the design limit described in Section 22.7.1.1. Following the reactor trip, the plant approaches a stabilized and safe condition; standard plant shutdown procedures may then be followed to further cool down the plant.

Because the power level rises by a maximum of about 12 percent above nominal during the excessive feedwater flow incident, the fuel temperature also rises until after reactor trip occurs. The core heat flux lags behind the neutron flux response because of the fuel rod thermal time constant. Therefore, the peak value does not exceed 118 percent of its nominal value (the assumed overpower ΔT trip setpoint). The peak fuel temperature thus remains well below the fuel melting temperature.

The transient results show that DNB does not occur at any time during the excessive feedwater flow incident. Thus, the capability of the primary coolant to remove heat from the fuel rods is not reduced and the fuel cladding temperature does not rise significantly above its initial value during the transient.

The calculated sequence of events for this accident is shown in Table 9.1.2-1.

Appendix 9C provides discussion and analysis of long term safe shutdown for non-LOCA events**.**

9.1.2.3 Diverse Mitigation

Diverse mitigation capabilities for this event are the same as for loss of normal feedwater fault, as described in Section 9.2.7.3.

9.1.2.3.1 Diverse Mitigation for ATWT

Excessive feedwater flow events could be postulated to occur due to faults in the main feedwater system or the startup feedwater system. The flow capacity of the main feedwater system is significantly larger than that of the startup feedwater system. The evaluations presented here focus on those occurring in the main feedwater system, as discussed in the primary DBA analysis.

The following sections evaluate the consequences of an excessive feedwater event with an assumed mechanical, PMS or reactor trip breaker CCF, which prevents reactor trip from occurring.

In these cases the initial portion of the transient would be identical to the primary safety case. The core power reaches an equilibrium value equal to the steam generator heat removal. Design limits are not challenged during this period.

9.1.2.3.1.1 Diverse ATWT Method of Analysis

A number of cases were considered to address different potential CCFs that can affect the PMS and its ability to insert RCCAs. The excessive feedwater flow analyses presented in this section consider the following events:

- Excessive feedwater flow with a PMS CCF – The CCF prevents all PMS reactor trips signals and engineered safeguards features signals. The DAS is assumed to be completely operable. Offsite power and turbine bypass are also assumed available.

- Excessive feedwater flow with a PMS reactor trip breaker CCF - This failure prevents the PMS from inserting the rods; however, PMS logic continues to function, and all engineered safeguards features signals are operable. DAS is completely operable, including its capability to drop rods. Offsite power and turbine bypass are also assumed to be available.

- Excessive feedwater flow with a RCCA mechanical CCF - The PMS, DAS, and control systems are assumed to be operable except that RCCAs do not insert into the core on a trip signal.

This analysis is performed to demonstrate the adequacy of the operable portions of the PMS (considering the impact of the CCF) as well as the DAS to detect and actuate mechanical SSCs to mitigate the fault. The following ATWT acceptance criteria are applicable to this event:

- The RCS does not overpressurise due to reactor coolant heatup. The ATWT pressure limit is 22.06 MPa-rel (3200 psig).

- There is no significant fuel damage.

- The rate and duration of energy release to containment is much less than for the design basis LOCA. This demonstrates that the containment does not overpressurise due to the energy release to the containment.

9.1.2.3.1.2 Diverse ATWT Credited SSCs

For all ATWT feedwater malfunction flow increase scenarios, long-term transient response is bounded by Turbine Trip ATWT (Section 9.2.3) As noted in Section 9.2.3.3.1.2, the Turbine Trip ATWT is bounded by Section 9.2.7.3.1 which considers the turbine trip and simultaneous loss of feedwater ATWT. As such, no claimed SSCs (PMS or DAS functions) are credited to initiate passive safety features for this limiting ATWT. Instead, the plant will reach a stable steady-state power condition and ATWT criteria would be met. Ultimately, manual operator action would be required to shut down the plant. Section 9.2.7.3.1 considers the turbine trip and simultaneous loss of feedwater ATWT.

9.1.2.3.1.3 Diverse ATWT Results

Feedwater System Malfunctions that Result in an Increase in Feedwater Flow with a Mechanical CCF

This section discusses a main feedwater system malfunction that results in an increase in flow with an assumed RCCA mechanical CCF. The PMS is assumed to be operable in this case;

however, the RCCAs do not insert when a trip signal is generated. The DAS is also operable; however, the mechanical failure also prevents rod insertion on a DAS reactor trip signal.

The additional feedwater flow causes the steam generator level to increase until the PMS High-3 steam generator level setpoint is exceeded. The PMS High-3 steam generator level function generates a signal to trip the turbine, to isolate all feedwater flow by closing control and isolation valves and to trip the feedwater pumps. The High-3 steam generator level function also generates a reactor trip signal. However, in this case, due to the assumed mechanical CCF, the RCCAs do not insert.

From this point on, the transient will behave similarly to the turbine trip scenario where feedwater flow is lost (see Section 9.2.7.3.1). The excessive feedwater scenario, which leads to a turbine trip, will be less severe than the turbine trip cases because at the time the turbine is tripped and feedwater flow is terminated, fluid inventory in the steam generators is significantly above the nominal operating amount. As discussed in Section 9.2.7.3.1, for turbine trip cases with feedwater lost and a mechanical CCF that prevents reactor trip, the design limits for a turbine trip with a loss of feedwater are not exceeded.

Feedwater System Malfunctions that Result in an Increase in Feedwater Flow with a PMS CCF

This section discusses an excessive feedwater flow transient with an assumed PMS CCF that prevents reactor trip from occurring. The PMS is inoperable in this scenario. The DAS is operable, and RCCAs are assumed to be able to insert on a DAS reactor trip signal.

When steam generator level reaches the PMS High-2 setpoint, a turbine trip will not occur because of the PMS failure.

The operator can then terminate the power excursion transient by using DAS to manually trip the reactor. In the event that excessive feedwater flow continues and the turbine is not tripped, then liquid entrainment in the steam lines will increase and will eventually lead to accelerated turbine wear/erosion and likely turbine damage. A turbine trip, such as on turbine vibration, is an expected result. Once turbine trip has occurred, the transient is similar to the turbine trip events addressed in Section 9.2.3.3.1.

Feedwater System Malfunctions that Result in an Increase in Feedwater Flow with a Reactor Trip Breaker CCF

This section discusses an excessive feedwater flow transient with an assumed reactor trip breaker CCF that prevents reactor trip from occurring. The PMS is assumed to be operable in this case; however, the RCCAs do not insert when a trip signal is generated, The DAS is also operable, and RCCAs are assumed to be able to insert on a DAS reactor trip signal.

The additional feedwater flow causes the steam generator level to increase until the PMS High-3 steam generator level setpoint is exceeded. The PMS High-3 steam generator level function generates a signal to trip the turbine, isolate all feedwater flow by closing control and isolation valves and by tripping of feedwater pumps. The High-3 steam generator level function also generates a reactor trip signal. However, in this case, due to the assumed reactor trip breaker CCF, the RCCAs will not insert at this time. From this point on, the transient will behave similarly to the turbine trip scenario where feedwater flow is lost with an assumed trip breaker CCF (see turbine trip case in Section 9.2.7.3.1). The excessive feedwater scenario, which leads to a turbine trip, will be less severe than the turbine trip cases presented in Section 9.2.7.3.1, because at the time the turbine is tripped and feedwater flow is terminated, the steam generators will have a fluid

inventory significantly above nominal amounts. As discussed in Section 9.2.7.3.1, the RCCAs will be inserted when the DAS automatically trips the MG sets on low wide range steam generator level. For turbine trip cases with feedwater lost and a reactor trip breaker CCF that prevents reactor trip, design limits for a turbine trip with a loss of feedwater are not exceeded.

9.1.2.3.2 Diverse Mitigation for Core Cooling

The loss of normal feedwater diverse core cooling, as analysed in Section 9.2.7.3.2, was determined to be bounding of all non-LOCA events.

9.1.2.4 Radiological Consequences

Design Basis

In the case where offsite power remains available, there is no release of activity to the environment and the Target 4 BSOs (0.01 mSv offsite and 0.1 mSv onsite) are met.

In the case where offsite power is lost, a small release of activity may occur as a result of steam dump to the atmosphere due to unavailability of the condensers. With no fuel damage and primary and secondary circuits intact, the initiating event has no impact on the doses. The doses are a consequence of the assumed loss of offsite power. Therefore, the loss of offsite power doses from Section 9.2.6.4 are presented. The calculated maximum doses for all relevant pathways (inhalation, cloudshine, and groundshine) are as follows:

- Offsite dose: 0.05 mSv Worker dose: 1.5 mSv

These doses are within the Target 4 BSL for frequent faults (1 mSv offsite and 20 mSv onsite).

Diverse Mitigation

Both the diverse ATWT and diverse core cooling scenarios demonstrate that the RCS does not overpressurise and there is no significant fuel damage. For a diverse mitigation radiological consequences analysis better estimate assumptions would be credited. This would include reactor coolant system activity levels significantly lower than those modelled for the DBA and better activity retention in containment and in the steam generators. In addition better estimate atmospheric dispersion factors would be used. Therefore, a diverse mitigation radiological consequences analysis would show that the doses for the diverse ATWT scenario would be less than those reported for the non-LOCA DBAs and doses for the diverse core cooling scenario would be much less than for the design basis LOCA. The diverse mitigation analyses would not have to meet the Target 4 BSL for frequent faults and would meet the Target 4 BSL for infrequent faults.

9.1.2.5 As Low as Reasonably Practicable Assessment

The ALARP discussion for this event is the same as for Inadvertent Opening of a Steam Generator Relief or Safety Valve event, as described in Section 9.1.4.5.

9.1.2.6 Conclusions

The results of the analysis show that the minimum DNBR encountered for an excessive feedwater addition at power is above the design limit value. The DNBR design basis is described in Section 22.7.1.1.

Additionally, the reactivity insertion rate that occurs at no-load conditions following excessive feedwater addition is less than the maximum value considered in the analysis of the rod withdrawal from subcritical condition analysis (see Section 9.4.1).

This event has also been adequately assessed with respect to ATWT considerations. This event was not explicitly analysed for the change in the current design reference point in the UK as described in Reference 9.1-9. However, the evaluation conducted to closeout FS-03 demonstrated with a subset of events (Reference 9.1-10) that there is little impact on the key analysis trends, results, and margin to the applicable acceptance criteria. Therefore, the subset of events confirmed the change in design reference point would not invalidate the conclusions presented for this event.

Diverse core cooling capabilities have been demonstrated.

DBA radiological consequences are within the Target 4 BSL for frequent faults (1 mSv offsite and 20 mSv onsite). Thus, the identification of necessary Class 1 SSCs is adequate to meet DB requirements.

It has been shown that the AP1000 plant design includes adequate systems for the protection of this fault, which limit the radiological consequences such that they are compliant with the SAPs targets and the risks have been reduced to be ALARP.

9.1.3 Excessive Increase in Secondary Steam Flow (Fault 1.15.18)

9.1.3.1 Identification of Causes and Accident Description

An excessive increase in secondary system steam flow (excessive load increase incident) results in a power mismatch between the reactor core power and the steam generator load demand. The plant control system is designed to accommodate a 10-percent step load increase or a 5-percent-per-minute ramp load increase in the range of 25- to 100-percent full power. Any loading rate in excess of these values may cause a reactor trip actuated by the protection and safety monitoring system. Steam flow increases greater than 10 percent are analysed in Sections 9.1.4, 9.1.5 and 9.1.6.

This accident could result from either an administrative violation such as excessive loading by the operator or an equipment malfunction in the steam dump control or turbine speed control.

During power operation, turbine bypass to the condenser is controlled by reactor coolant condition signals. A high reactor coolant temperature indicates a need for turbine bypass. A single controller malfunction does not cause turbine bypass. An interlock blocks the opening of the valves unless a large turbine load decrease or a turbine trip has occurred.

Protection against an excessive load increase accident is provided by the following protection and safety monitoring system signals:

- Overpower ΔT
- Overtemperature ΔT
- Power range high positive flux rate
- Power range high neutron flux

The possible consequence of this accident (assuming no protective functions) is a departure from nucleate boiling with subsequent fuel damage. The accident is typically characterized by an approach of parameter values to the protection setpoints without the setpoints actually being reached. However, the reactor trip setpoints (high neutron flux, overpower ΔT, and overtemperature ΔT) could be reached during the analysis of the excessive load increase event.

These protection functions are defeated in the analysis to preclude reactor trip, ensure the most severe DNB condition is reached, and demonstrate that the plant reaches a new equilibrium condition at a higher power level corresponding to the increase in steam flow.

Determination of the effects produced by a possible consequential loss of offsite power during the excessive load increase event is not applicable to this event. As discussed in Section 9.0.12, the loss of offsite power need be considered only as a direct consequence of a turbine trip occurring while the plant is operating at power. For the four excessive load increase cases presented, reactor and turbine trips are not predicted to occur. However, even if a reactor trip were to occur, a consequential loss of ac power would not adversely affect the analysis results. This conclusion is based on a review of the time sequence of events associated with a consequential loss of ac power in comparison to the reactor shutdown time for the event. The primary effect of the loss of ac power is the coastdown of the RCPs. The PMS includes a five-second minimum delay between the reactor trip and the turbine trip. In addition, a three-second delay between the turbine trip and the loss of offsite ac power is assumed, consistent with Section 9.0.12. Considering these delays between the time of the reactor trip and RCP coastdown due to the loss of ac power, it is clear that the plant shutdown sequence will have passed the critical point and the control rods will have been completely inserted before the RCPs begin to coast down. Therefore, the consequential loss of ac power does not adversely affect this analysis because the plant will be shut down well before the RCPs begin to coast down.

9.1.3.2 Design Basis Mitigation

Analysis is performed to demonstrate the adequacy of the PMS to detect and mitigate the fault and show that the safety analysis criteria are satisfied including:

- No fuel failures (confirmed using minimum DNBR and fuel melt criteria),
- The RCS pressure criterion is met,
- The MSS pressure criterion is met, and
- The pressuriser does not fill (which could result in a LOCA).

With respect to the peak RCS and MSS pressure criteria, this event is bounded by the Turbine Trip DB analysis in Section 9.2.3 and is not explicitly verified. Also, pressuriser fill criterion is not challenged for this event, and is not explicitly verified.

9.1.3.2.1 DBA Method of Analysis

This accident is primarily analysed using the LOFTRAN computer code (Reference 9.1-1). LOFTRAN simulates the neutron kinetics, reactor coolant system, pressuriser, pressuriser safety valves, pressuriser spray, steam generator, steam generator safety valves, and feedwater system. The code computes pertinent plant variables including temperatures, pressures, and power level.

Four cases are analysed to demonstrate plant behaviour following a 10-percent step load increase from rated load. These cases are as follows:

- Reactor control in manual with minimum moderator reactivity feedback
- Reactor control in manual with maximum moderator reactivity feedback
- Reactor control in automatic with minimum moderator reactivity feedback
- Reactor control in automatic with maximum moderator reactivity feedback

For the minimum moderator feedback cases, the core has the least negative moderator temperature coefficient of reactivity; therefore, reductions in coolant temperature have the least impact on core power. For the maximum moderator feedback cases, the moderator temperature coefficient of reactivity has its highest absolute value. This results in the largest amount of reactivity feedback

due to changes in coolant temperature. For all the cases analysed both with and without automatic rod control, no credit is taken for ΔT trips on overtemperature or overpower in order to demonstrate the inherent transient capability of the plant. Under actual operating conditions, such a trip may occur, after which the plant quickly stabilizes.

A 10-percent step increase in steam demand is assumed, and each case is analysed without credit being taken for pressuriser heaters. At initial reactor power, reactor coolant system pressure and temperature are assumed to be at their full power values. Uncertainties in initial conditions are included in the limit DNBR as described in WCAP-11397-P-A (Reference 9.1-2). Plant characteristics and initial conditions are further discussed in Section 9.0.2.

Normal reactor control systems and engineered safety systems are not required to function.

9.1.3.2.2 DBA Credited SSCs

For the DB, all of the claimed SSCs are Class 1. The claimed Class 1 SSCs are listed in Table 9.0-10. The presented DBA does not generate a reactor trip; however, essential safety functions for the long term safe shutdown analysis (Appendix 9C) bound safe shutdown response for this event. The primary core cooling is provided by the PRHR and passive containment cooling. Other SSCs include the CMTs, containment isolation, pressuriser SVs and steam generator SVs. The PMS provides the following:

- No RT credited
- PRHR actuation on Low-2 SG NR level coincident with Low-2 SFW flow
- CMTs and containment isolation on Low-2 CL temperature
- PCS on High-2 containment pressure

9.1.3.2.3 DBA Results

Figures 9.1.3-1 through 9.1.3-10 show the transient with the reactor in the manual control mode and no reactor trip signals occur. At the beginning of the minimum moderator feedback case, there is a slight power increase and the average core temperature shows a large decrease. This results in a DNBR that increases above its initial value. At the beginning of the maximum moderator feedback manually controlled case, there is a much faster increase in reactor power due to the moderator feedback. A reduction in the DNBR occurs, but the DNBR remains above the design limit (see Section 22.7.1.1).

Figures 9.1.3-11 through 9.1.3-20 show the transient assuming the reactor is in the automatic control mode. At the beginning of the maximum moderator feedback case, the core power increases and the coolant average temperature and pressuriser pressure decrease slowly. For this case, no reactor trip signal is generated. For the minimum moderator feedback case, a reactor trip signal setpoint is reached, but conservatively, reactor trip is not credited. At the beginning of the minimum moderator feedback case, the core power increases, but the coolant average temperature and pressuriser pressure decrease rapidly. For this case, the transients oscillate and eventually stabilize. For both of these cases, the minimum DNBR remains above the design limit (see Section 22.7.1.1).

The excessive load increase incident is an overpower transient for which the fuel temperature rises. Reactor trip is not credited in any of the cases analysed, and the plant reaches a new equilibrium condition at a higher power level corresponding to the increase in steam flow.

Because DNB does not occur during the excessive load increase transients, the capability of the primary coolant to remove heat from the fuel rod is not reduced. Thus, the fuel cladding temperature does not rise significantly above its initial value during the transient.

The calculated sequence of events for the excessive load increase cases with no reactor trip are shown in Table 9.1.2-1.

Appendix 9C provides discussion and analysis of long term safe shutdown for non-LOCA events.

9.1.3.3 Diverse Mitigation

Diverse mitigation capabilities are the same as for the loss of normal feedwater fault, as described in Section 9.2.7.3.

9.1.3.3.1 Diverse Mitigation for ATWT

For the primary DBA safety case, the excessive load increases were limited to 10% flow increase and were divided into two types of cases: an excessive load increase due to an administrative violation (such as an excessive loading by the operator), and an excessive load increase due to an equipment malfunction. Larger excessive load increases are bounded by the hot full power steamline break event. For the ATWT diversity analysis, an investigation of the expected frequency of occurrence of various secondary-side steam load increases was performed (Reference 9.1-10).

The ATWT diversity cases studied cover three distinct initiating faults: a fault that results in an increase in turbine load, an inadvertent opening of a secondary-side valve, and a secondary-side line break. Since the maximum steam load capacity of the AP1000 turbine is less than 110% of nominal full-power steam flow, no further consideration is given in this study to this fault, as it is already covered by the DBA. As such, the excessive steam load increase scenarios to be considered are those initiated by the opening of one or more secondary-side valves, or by a break in a secondary-side line.

9.1.3.3.1.1 Diverse ATWT Method of Analysis

The ATWT investigation considered various failures, including steam breaks up to approximately 0.037 m^2 (0.4 ft^2), the opening of up to two steam generator power-operated relief or safety valves, or the opening of all six turbine bypass valves. These ATWT scenarios would conservatively bound (i.e., lower expected frequency) the frequent fault limit.

ATWT cases can generally be divided into symmetric cooldown cases (those where the fault affects steam flow for both secondary loops) and asymmetric cooldown cases (those where the fault affects steam flow for one of the secondary loops). For the ATWT diversity cases, all reactor trip safety functions were disabled. Otherwise, the DBA transient analysis methodology described in Section 9.1.3 is followed for the symmetric cases and the DBA case transient analysis methodology of Section 9.1.6 is followed for the asymmetric cases.

The following ATWT acceptance criteria are applicable to this event:

- A coolable geometry for reactor core is maintained
- The reactor coolant pressure boundary integrity is maintained
- The containment vessel integrity is maintained

For the ATWT excessive load diversity cases, the primary acceptance criterion is maintaining a coolable geometry. During the event, the reactor coolant pressure decreases due to the large cooldown; therefore, the reactor coolant pressure boundary integrity is not challenged. The containment vessel integrity is maintained by diverse actuation of the containment cooling system via a high containment temperature DAS setpoint, if the incident were to involve a steam line rupture inside containment.

Five potential fuel failure criteria were considered to confirm that a coolable geometry is maintained: DNB, fuel melt, rod internal pressure, transient clad stress, and clad corrosion. The assessments of these five potential fuel failure mechanisms were performed for an expected maximum duration of [ ] ; appropriate operator action to terminate the transient would be expected within this timeframe.

The minimum DNBR for each case considered was calculated using the VIPRE-01 code. Due to the relatively low power levels reached and the decrease in RCS temperature, the DNBR limits were not challenged for these cases.

The fuel melt, rod internal pressure, transient clad stress and clad corrosion criteria were all confirmed using detailed core design and fuel rod design codes. These calculations were performed without the uncertainties typically applied to frequent fault calculations. The calculations showed that fuel melt is precluded. They also showed that rod internal pressure, transient clad stress and clad corrosion were all within the applicable frequent fault limits.

9.1.3.3.1.2 Diverse ATWT Credited SSCs

For all ATWT excessive load cases, no claimed SSCs (PMS or DAS functions) are credited to initiate passive safety features. Instead, the plant will reach an equilibrium power condition and ATWT criteria would be met for sustained operation at power for at least 30 minutes. Ultimately, manual operator action would be required to shut down the plant.

9.1.3.3.1.3 Diverse ATWT Results

The limiting cases are a 40% steam load increase caused by the opening of all six turbine bypass valves that results in a symmetric cooldown, and a 0.045 m^2 (0.48 ft^2) rupture of the steam line that results in an asymmetric cooldown. As stated previously, all acceptance criteria required to maintain a coolable geometry, including minimum DNBR, fuel centerline melt, rod internal pressure, transient clad stress, and clad corrosion, were met.

The sequence of events for these ATWT cases is presented in Table 9.1.3-1. Transient plots for the symmetric case are presented in Figures 9.1.3-21 through 9.1.3-25. Transient plots for the asymmetric case are presented in Figures 9.1.3-26 through 9.1.3-30.

9.1.3.3.2 Diverse Mitigation for Core Cooling

The loss of normal feedwater diverse core cooling, as analysed in Section 9.2.7.3.2, was determined to be bounding of all non-LOCA events.

9.1.3.4 Radiological Consequences

Design Basis

In the case where offsite power remains available, there is no release of activity to the environment and the Target 4 BSOs (0.01 mSv offsite and 0.1 mSv onsite) are met.

In the DBA case where offsite power is lost, a small release of activity may occur as a result of steam dump to the atmosphere due to unavailability of the condensers. With no fuel damage and primary and secondary circuits intact, the initiating event has no impact on the doses. The doses are a consequence of the assumed loss of offsite power. Therefore, the loss of offsite power doses from Section 9.2.6.4 are presented. The calculated maximum doses for all relevant pathways (inhalation, cloudshine, and groundshine) are as follows:

- Offsite dose: 0.05 mSv Worker dose: 1.5 mSv

These doses are within the Target 4 BSL for frequent faults (1 mSv offsite and 20 mSv onsite).

Diverse Mitigation

Both the ATWT and the diverse core cooling scenarios demonstrate that the RCS does not overpressurise and there is no significant fuel damage. For a diverse mitigation radiological consequences analysis better estimate assumptions would be credited. This would include reactor coolant system activity levels significantly lower than those modelled for the DBA and better activity retention in containment and in the steam generators. In addition better estimate atmospheric dispersion factors would be used. Therefore, a diverse mitigation radiological consequences analysis would show that the doses for the diverse ATWT scenario would be less than those reported for the non-LOCA DBAs and doses for the diverse core cooling scenario would be much less than for the design basis LOCA. The diverse mitigation analyses would not have to meet the Target 4 BSL for frequent faults and would meet the Target 4 BSL for infrequent faults.

9.1.3.5 As Low As Reasonably Practicable Assessment

The ALARP discussion for this event is the same as for Inadvertent Opening of a Steam Generator Relief or Safety Valve event, as described in Section 9.1.4.5.

9.1.3.6 Conclusions

The DB analysis presented in this section demonstrates that for a 10-percent step load increase, the DNBR remains above the design limit. The design basis for DNB is described in Section 22.7.1.1. The plant rapidly reaches a stabilized condition following the load increase.

This event has also been adequately assessed with respect to ATWT considerations and all credible cases meet ATWT criteria.

Diverse core cooling capabilities have been demonstrated.

DBA radiological consequences are within the Target 4 BSL for frequent faults (1 mSv offsite and 20 mSv onsite). Thus, the identification of necessary Class 1 SSCs is adequate to meet DB requirements.

It has been shown that the AP1000 plant design includes adequate systems for the protection of this fault, which limit the radiological consequences such that they are compliant with the SAPs targets and the risks have been reduced to be ALARP.

9.1.4 Inadvertent Opening of a Steam Generator Relief or Safety Valve (Fault 1.22.1)

9.1.4.1 Identification of Causes and Accident Description

The most severe core conditions resulting from an accidental depressurisation of the main steam system are associated with an inadvertent opening of a single steam dump, relief, or safety valve. The analyses performed assuming a rupture of a main steam line are given in Sections 9.1.5 and 9.1.6.

The steam release, as a consequence of this accident, results in an initial increase in steam flow which decreases during the accident as the steam pressure falls. The energy removal from the reactor coolant system causes a reduction of coolant temperature and pressure. In the presence of a negative moderator temperature coefficient, the cooldown results in an insertion of positive reactivity.

The objective of the DB analysis is to demonstrate that the DNBR criterion is met.

Assuming the most reactive stuck RCCA, with offsite power available, and assuming a single failure in the engineered safety features system, there will be no consequential damage to the fuel or reactor coolant system after reactor trip for a steam release equivalent to the spurious opening, with failure to close, of the largest of any single steam dump, relief, or safety valve. This criterion is met by showing the DNB design basis is not exceeded.

9.1.4.2 Design Basis Mitigation

Analysis is performed to demonstrate the adequacy of the PMS to detect and mitigate the fault and show that the safety analysis criteria are satisfied including:

- No fuel failures (confirmed using minimum DNBR and fuel melt criteria),
- The RCS pressure criterion is met,
- The MSS pressure criterion is met, and
- The pressuriser does not fill (which could result in a LOCA).

With respect to the peak RCS and MSS pressure criteria, this event is bounded by the Turbine Trip DB analysis in Section 9.2.3 and is not explicitly verified. Also, pressuriser fill criterion is not challenged for this event, and is not explicitly verified.

9.1.4.2.1 DBA Method of Analysis

The analysis of a secondary system steam release is performed to determine the following:

- The core heat flux and reactor coolant system temperature and pressure resulting from the cooldown, due to the steam release. The LOFTRAN code (References 9.1-1 and 9.1-6) is used to model the system transient.

- The thermal-hydraulic behaviour of the core due to the steam release. A detailed thermal-hydraulic digital computer code, VIPRE-01 (Reference 9.1-7), is used to determine if DNB occurs for the core transient conditions computed by the LOFTRAN code.

The following conditions are assumed to exist at the time of a secondary system steam release:

- End-of-life shutdown margin at no-load, equilibrium xenon conditions, and with the most reactive RCCA stuck in its fully withdrawn position. Operation of RCCA mechanical shim

and axial offset banks during core burnup is restricted by the insertion limits so that shutdown margin requirements are satisfied.

- A most negative moderator temperature coefficient corresponding to the end-of-life rodded core with the most reactive RCCA in the fully withdrawn position. The variation of the coefficient with temperature is included. The k_{eff} (considering moderator temperature and density effects) versus temperature corresponding to the negative moderator temperature coefficient used is shown in Figure 9.1.4-1. The core power is calculated as a function of core mass flow, core boron concentration, and core inlet temperature.

- Minimum capability for injection of boric acid solution corresponding to the most restrictive single failure in the passive core cooling system. There are no single failures that prevent core makeup tank injection; however, the analysis models the failure of one core makeup tank discharge valve. Low-concentration boric acid must be swept from the core makeup tank lines downstream of isolation valves before delivery of boric acid (3400 ppm) to the reactor coolant loops. This effect has been accounted for in the analysis.

- The case analysed models a flow area of 0.02 m^2 (0.2 ft^2), which is based on a steam flow of 235.9 kg/sec (520 lbm/s) at 8.274 MPa abs (1200 psia) with offsite power available. This conservatively bounds the maximum capacity of any single steam dump, relief, or safety valve.

- Initial hot shutdown conditions at time zero are assumed because this represents the most conservative initial conditions. Should the reactor be just critical or operating at power at the time of a steam release, the reactor is tripped by the normal overpower protection when power level reaches a trip point. Following a trip at power, the reactor coolant system contains more stored energy than at no-load. This is because the average coolant temperature is higher than at no-load, and there is appreciable energy stored in the fuel. The additional stored energy is removed via the cooldown caused by the steam release before the no-load conditions of the reactor coolant system temperature and shutdown margin assumed in the analyses are reached. After the additional stored energy is removed, the cooldown and reactivity insertions proceed in the same manner as in the analysis that assumes no-load condition at time zero. However, because the initial steam generator water inventory is greatest at no-load, the magnitude and duration of the reactor coolant system cooldown are less for a steam line release occurring at power:

- In computing the steam flow, the Moody Curve (Reference 9.1-3) for f(L/D) = 0 is used.

- Perfect moisture separation occurs in the steam generator.

- Offsite power is available, because this maximises the cooldown.

- Maximum cold startup feedwater flow is assumed.

- Four reactor coolant pumps are initially operating.

- Manual actuation of the PRHR system at time zero is conservatively assumed to maximise the cooldown.

9.1.4.2.2 DBA Credited SSCs

For the DB, all claimed SSCs are Class 1. The available Class 1 SSCs are listed in Table 9.0-10. The presented DBA ends shortly after CMT boron injection ends the return-to-power transient

(core subcritical); however, essential safety functions for the long term safe shutdown analysis (Appendix 9C) bound safe shutdown response for this event. Other SSCs include the feedwater isolation valves, steamline isolation valves, CMTs, containment isolation, pressuriser SVs and steam generator SVs. The PMS provides the following:

- RT is available, but not credited; rods already inserted for limiting case
- PRHR actuation on Low-2 SG NR level coincident with Low-2 SFW flow
- CMTs and containment isolation on Low-2 CL temperature
- PCS on High-2 containment pressure

9.1.4.2.3 DBA Results

The calculated sequence of events for the analysed case is shown in Table 9.1.2-1. The results presented conservatively bound the events that would occur assuming a secondary system steam release because it is postulated that the conditions described in Section 9.1.4.2.1 exist simultaneously.

Figures 9.1.4-2 through 9.1.4-12 show the transient results for the event.

Core makeup tank injection and the associated tripping of the reactor coolant pumps are initiated automatically by the Low-2 T_{cold} "S" signal. Boron solution at 3400 ppm enters the reactor coolant system, providing enough negative reactivity to prevent a significant return to power and core damage. Later in the transient, as the reactor coolant pressure continues to fall, the accumulators actuate and inject boron solution at 2600 ppm.

Appendix 9C provides discussion and analysis of long term safe shutdown for non-LOCA events**.**

The analysis demonstrates that the DNB design basis, as described in Section 22.7.1.1, is met for the inadvertent opening of a steam generator relief or safety valve. As shown in Figure 9.1.4-2, no significant return to power occurs and, therefore, DNB does not occur. The minimum DNBR is conservatively calculated and is above the 95/95 limit.

9.1.4.3 Diverse Mitigation

Diverse mitigation capabilities are the same as for the loss of normal feedwater fault, as described in Section 9.2.7.3.

9.1.4.3.1 Diverse Mitigation for ATWT

The inadvertent opening of a SG PORV or safety valve will not increase power to the point at which a reactor trip is needed. Therefore, diverse mitigation for ATWT for the inadvertent opening of a steam generator relief or safety valve is not addressed further.

9.1.4.3.2 Diverse Mitigation for Core Cooling

The loss of normal feedwater diverse core cooling, as analysed in Section 9.2.7.3.2, was determined to be bounding of all non-LOCA events.

9.1.4.4 Radiological Consequences

Design Basis

Since there is no fuel damage and the primary circuit remains intact, only secondary coolant and any primary coolant that leaks into the secondary circuit during the event will be released through the stuck-open SG valve. Therefore, the radiological consequences are limited and no dose calculations have been obtained specifically for this case. However, doses have been calculated for the SGTR accident discussed in Section 9.6.3. An SG relief valve is also assumed to stick open during the SGTR accident, but in the SGTR there is a direct pathway for the release of primary coolant to the environment via the ruptured tube and the stuck valve. Therefore, the dose associated with the SGTR accident bounds the dose that arises from the stuck-open SG relief valve event. The SGTR doses from Section 9.6.3 are presented. The calculated maximum doses for all relevant pathways (inhalation, cloudshine, and groundshine) are as follows:

- Offsite dose: 0.91 mSv Worker dose: 4.8 mSv

These doses for the SGTR accident, which significantly bound the doses associated with the stuck-open SG relief or safety valve event, are within the Target 4 BSL for frequent faults (1 mSv offsite and 20 mSv onsite).

Diverse Mitigation

ATWT is not applicable to this event. The diverse core cooling scenarios demonstrate that the RCS does not overpressurise and there is no significant fuel damage. For a diverse mitigation radiological consequences analysis better estimate assumptions would be credited. This would include reactor coolant system activity levels significantly lower than those modelled for the DBA and better activity retention in containment and in the steam generators. In addition better estimate atmospheric dispersion factors would be used. Therefore, a diverse mitigation radiological consequences analysis would show that the doses for the diverse ATWT scenario would be less than those reported for the non-LOCA DBAs and doses for the diverse core cooling scenario would be much less than for the design basis LOCA. The diverse mitigation analyses would not have to meet the Target 4 BSL for frequent faults and would meet the Target 4 BSL for infrequent faults.

9.1.4.5 As Low as Reasonably Practicable Assessment

For this event, the identification of the primary safety functions as Class 1 SSCs has been shown to be adequate to meet DB requirements.

The diverse mitigation functions, including other Class 1 safety functions and the DAS function, which is Class 2, is also shown by analysis to meet the corresponding requirements for this event. See Reference 9.1-12 for additional discussions on these diverse mitigation features.

Additionally, the AP1000 plant design has a third level of redundancy/diversity which is provided by Class 2 defence in depth (DiD) systems. The applicable DiD functions include:

- CVS boration for long-term reactivity control
- CVS make-up for RCS inventory control
- SFW with steam dump for short–term decay heat removal
- RNS cooling of the RCS for long-term decay heat removal. The RNS requires support from the component cooling water system (CCS) and service water system (SWS) cooling water systems.

- Control by the PLS C&I

The characteristics of the above features were compared to improvements that were evaluated for the RNS for its mitigation of cliff edge small LOCAs. First it should be recognized that in this situation the RNS provides the second level of defence for this event and is therefore more important than the above DiD features which provide a 3rd level of defence. The RNS improvements included making the RNS alignment / start automatic, increasing the RNS pump head, and adding a RNS suction supply tank that is separate from the Class 1 system. None of these potential improvements were found to be ALARP (Reference 9.1-11). However, the SFW and CVS already include characteristics similar to these proposed improvements. Another improvement that could be made to these DiD systems is to upgrade them to Class 1. This would be very expensive especially and would have wide reaching impacts to the design of SSCs; notable would be the impact on component and building design to address hazards including seismic and storm winds/missiles. Such a change would not be ALARP because the cost would be grossly disproportional to its benefit.

As discussed in Chapter 9.0.15, the AP1000 has incorporated ALARP thinking throughout its development. In addition, the current risk of a large radioactivity release is significantly less than the SAP Target 9 BSO (1E-7 pa). Considering the ALARP thinking that went into the AP1000 development, its low risk profile and the additional level of defence discussed above (including their performance characteristics), improving the Class 2 DiD to better remove decay heat or shutdown the reactor would be grossly disproportional to the risk reduction that might be achieved. As a result, the current design is considered ALARP.

9.1.4.6 Conclusions

The analysis shows that the key fuel failure criterion is satisfied. For an inadvertent opening of any single steam dump or a steam generator relief or safety valve, the DNB design basis is met.

This event has also been adequately assessed with respect to ATWT considerations.

Diverse core cooling capabilities have been demonstrated.

DBA radiological consequences for the SGTR accident, which significantly bound those associated with the stuck-open SG relief or safety valve event, are within the Target 4 BSL for frequent faults (1 mSv offsite and 20 mSv onsite). Thus, the identification of necessary Class 1 SSCs is adequate to meet DB requirements.

It has been shown that the AP1000 plant design includes adequate systems for the protection of this fault, which limit the radiological consequences such that they are compliant with the SAPs targets and the risks have been reduced to be ALARP.

9.1.5 Steam System Piping Failure at Hot Zero Power (Fault 1.21.1a)

9.1.5.1 Identification of Causes and Accident Description

The steam release arising from a rupture of a main steam line results in an initial increase in steam flow, which decreases during the accident as the steam pressure falls. The energy removal from the reactor coolant system causes a reduction of coolant temperature and pressure. In the presence of a negative moderator temperature coefficient, the cooldown results in an insertion of positive reactivity.

A fast-acting main steam isolation valve is provided in each steam line. These valves are modelled to fully close within 10 seconds of actuation following a large break in the steam line. For breaks

downstream of the main steam line isolation valves, closure of the isolation valves will terminate the blowdown. For any break in any location, no more than one steam generator would experience an uncontrolled blowdown even if one of the main steam line isolation valves fails to close.

Flow restrictors are installed in the steam generator outlet nozzle, as an integral part of the steam generator. The effective throat area of the nozzles is 0.13 m^2 (1.4 ft^2), which is considerably less than the main steam pipe area; thus, the flow restrictors serve to limit the maximum steam flow for a break at any location.

If the most reactive RCCA is assumed stuck in its fully withdrawn position after reactor trip, there is an increased possibility that the core will become critical and return to power. A return to power following a steam line rupture is a potential problem mainly because of the existing high-power peaking factors, assuming the most reactive RCCA to be stuck in its fully withdrawn position. The core is ultimately shut down by the boric acid solution delivered by the passive core cooling system.

Assuming the most reactive stuck RCCA with or without offsite power and assuming a single failure in the engineered safety features system, the core cooling capability is maintained. As shown in Section 9.1.5.4, radiological consequences are within the guidelines.

Effects of minor secondary system pipe breaks are bounded by the analysis presented in this section.

The steam line rupture at full-power conditions is explicitly analysed and discussed in Section 9.1.6.

9.1.5.2 Design Basis Mitigation

Analysis is performed to demonstrate the adequacy of the PMS to detect and mitigate the fault and show that the safety analysis criteria are satisfied including:

- No fuel failures (confirmed using minimum DNBR and fuel melt criteria),
- The RCS pressure criterion is met,
- The MSS pressure criterion is met, and
- The pressuriser does not fill (which could result in a LOCA).

With respect to the peak RCS and MSS pressure criteria, this event is bounded by the Turbine Trip DB analysis in Section 9.2.3 and is not explicitly verified. Also, pressuriser fill criterion is not challenged for this event, and is not explicitly verified. It is noted that DNB and possible cladding perforation following a steam pipe rupture are not necessarily unacceptable. However, the DB analysis shows that the DNB design basis is not exceeded for any steam line rupture, assuming the most reactive RCCA is stuck in its fully withdrawn position.

9.1.5.2.1 DBA Method of Analysis

The major rupture of a steam line is the most limiting cooldown transient and is analysed at zero power with no decay heat. Decay heat retards the cooldown and thereby reduces the likelihood that the reactor returns to power. A detailed analysis of this transient with the most limiting break size, a double-ended rupture, is presented here. Certain assumptions used in this analysis are discussed in WCAP-9226-P-A (Reference 9.1-4). WCAP-9226-P-A also contains a discussion of the spectrum of break sizes and power levels analysed.

The analysis of the steam pipe rupture is performed to determine the following:

- The core heat flux and reactor coolant system temperature and pressure resulting from the cooldown following the steam line break. The LOFTRAN code (References 9.1-1 and 9.1-6) is used to model the system transient.

- The thermal-hydraulic behaviour of the core following a steam line break. A detailed thermal-hydraulic digital computer code, VIPRE-01 (Reference 9.1-7), is used to determine if DNB occurs for the core transient conditions computed by the LOFTRAN code.

The following conditions are assumed to exist at the time of a main steam line break accident:

- End-of-cycle shutdown margin at no-load, equilibrium xenon conditions, and the most reactive RCCA stuck in its fully withdrawn position. Operation of RCCA mechanical shim and axial offset banks during core burnup is restricted by the insertion limits so that shutdown margin requirements are satisfied.

- A most negative moderator temperature coefficient corresponding to the end-of-life rodded core with the most reactive RCCA in the fully withdrawn position. The variation of the coefficient with temperature is included. The k_{eff} (considering moderator temperature and density effects) versus temperature corresponding to the negative moderator temperature coefficient used is shown in Figure 9.1.4-1. The core power is calculated as a function of core mass flow, core boron concentration, and core inlet temperature.

  The moderator properties used in the LOFTRAN code for feedback calculations are generated by combining those in the sector nearest the affected steam generator with those associated with the remaining sector. The resultant properties reflect a combination process that accounts for inlet plenum fluid mixing and a conservative weighting of the fluid properties from the coldest core sector.

  In verifying the conservatism of this method, the power predictions of the LOFTRAN modelling are confirmed by comparison with detailed core analysis for the limiting conditions of the cases considered. This core analysis conservatively models the hypothetical core configuration (that is, stuck RCCA, non-uniform inlet temperatures, pressure, flow, and boron concentration) and directly evaluates the total reactivity feedback including power, boron, and density redistribution in an integral fashion. The effect of void formation is also included.

  Comparison of the results from the detailed core analysis with the LOFTRAN predictions verifies the overall conservatism of the methodology. That is, the specific power, temperature, and flow conditions used to perform the DNB analysis are conservative.

- Minimum capability for injection of boric acid solution corresponding to the most restrictive single failure in the passive core cooling system. The core makeup tanks and the accumulators are the portions of the passive core cooling system used in mitigating a steam line rupture. There are no single failures that prevent core makeup tank injection; however, the analysis models the failure of one core makeup tank discharge valve. Low-concentration boric acid must be swept from the core makeup tank lines downstream of the isolation valves before delivery of boric acid (3400 ppm) to the reactor coolant loops. This effect has been accounted for in the analysis.

- The maximum overall fuel-to-coolant heat transfer coefficient is used to maximise the rate of cooldown.

- Because the steam generators are provided with integral flow restrictors with a 0.13 m^2 (1.4 ft^2) throat area, any rupture in a steam line with a break area greater than 0.13 m^2

(1.4 ft^2), regardless of location, has the same effect on the primary plant as the 0.13 m^2 (1.4-ft^2) double-ended rupture. The limiting case considered in determining the core power and reactor coolant system transient is the complete severance of a pipe, with the plant initially at no-load conditions and full reactor coolant flow with offsite power available. The results of this case bound the loss of offsite power case for the following reasons:

- Loss of offsite power results in an immediate reactor coolant pump coastdown at the initiation of the transient. This reduces the severity of the reactor coolant system cooldown by reducing primary-to-secondary heat transfer. The lessening of the cooldown, in turn, reduces the magnitude of the return to power.

- Following its actuation, the core makeup tank provides borated water that injects into the reactor coolant system. Flow from the core makeup tank increases if the reactor coolant pumps have coasted down. Therefore, the analysis performed with offsite power and continued reactor coolant pump operation reduces the rate of boron injection into the core and is conservative.

- The protection system automatically provides a safety-related signal that initiates the coastdown of the reactor coolant pumps in parallel with core makeup tank actuation. Because this reactor coolant pump trip function is actuated early during the steam line break event (right after core makeup tank actuation), there is very little difference in the predicted DNBR between cases with and without offsite power.

- Because of the passive nature of the safety injection system, the loss of offsite power does not delay the actuation of the safety injection system.

- Power peaking factors corresponding to one stuck RCCA are determined at the end of core life. The coldest core inlet temperatures are assumed to occur in the sector with the stuck rod. The power peaking factors account for the effect of the local void in the region of the stuck RCCA during the return to power phase following the steam line break. This void in conjunction with the large negative moderator coefficient partially offsets the effect of the stuck RCCA. The power peaking factors depend upon the core power, temperature, pressure, and flow and, therefore, may differ for each case studied.

- The analysis assumes initial hot standby conditions at time zero in order to present a representative case which will yield limiting post-trip DNBR results for this transient. If the reactor is just critical or operating at power at the time of a steam line break, the reactor is tripped by the overpower protection system when power level reaches a trip point.

  Following a trip at power, the reactor coolant system contains more stored energy than at no-load because the average coolant temperature is higher than at no-load, and there is energy stored in the fuel. The additional stored energy reduces the cooldown caused by the steam line break before the no-load conditions of reactor coolant system temperature and shutdown margin assumed in the analyses are reached. After the additional stored energy has been removed, the cooldown and reactivity insertions proceed in the same manner as in the analysis that assumes a no-load condition at time zero. However, because the initial steam generator water inventory is greatest at no-load, the magnitude and duration of the reactor coolant system cooldown are less for a steam line break occurring at power.

- In computing the steam flow during a steam line break, the Moody Curve (Reference 9.1-3) for f(L/D) = 0 is used.

- Perfect moisture separation occurs in the steam generator.
- Maximum cold startup feedwater flow plus nominal 100 percent main feedwater flow is assumed.
- Four reactor coolant pumps are initially operating.
- Manual actuation of the PRHR system at time zero is conservatively assumed in order to maximise the cooldown.

9.1.5.2.2 DBA Credited SSCs

For the DB, all claimed SSCs are Class 1. The available Class 1 SSCs are listed in Table 9.0-10. The presented DBA ends after CMT boron injection turns around the return-to-power transient; however, essential safety functions for the long term safe shutdown analysis (Appendix 9C) bound safe shutdown response for this event. Other SSCs include the CMTs, containment isolation, steam line isolation valves and SG flow restrictors. The PMS provides the following:

- RT is available, but not credited; rods already inserted at start of analysis
- PRHR actuation on Low-2 SG WR Level, but is assumed to actuate at start of transient (maximizes cooldown)
- CMTs and containment isolation on Low-2 steam line pressure
- PCS on High-2 containment pressure

9.1.5.2.3 DBA Results

The calculated sequence of events for the analysed case is shown in Table 9.1.2-1. The results presented conservatively indicate the events that would occur assuming a steam line rupture because it is postulated that the conditions described in Section 9.1.5.2.1 exist simultaneously.

Figures 9.1.5-1 through 9.1.5-13 show the transient results following a main steam line rupture (complete severance of a pipe) at initial no-load condition.

Offsite power is assumed available so that, initially, full reactor coolant flow exists. During the course of the event, the reactor protection system initiates a trip of the reactor coolant pumps in conjunction with actuation of the core makeup tanks. The transient shown assumes an uncontrolled steam release from only one steam generator. Steam release from more than one steam generator is prevented by automatic trip of the main steam isolation valves in the steam lines by Low-2 steam line pressure signals. Even with the failure of one valve, release is limited to approximately 10 seconds for the other steam generator while the one generator blows down. The main steam isolation valves fully close in less than 10 seconds from receipt of a closure signal.

As shown in Figure 9.1.5-1, the core attains criticality with the RCCAs inserted (with the design shutdown assuming the most reactive RCCA stuck) before boron solution at 3400 ppm (from core makeup tanks) or 2600 ppm (from accumulators) enters the reactor coolant system. A peak core power significantly lower than the nominal full-power value is attained.

The calculation assumes that the boric acid is mixed with and diluted by the water flowing in the reactor coolant system before entering the reactor core. The concentration after mixing depends upon the relative flow rates in the reactor coolant system and from the core makeup tanks or

accumulators (or both). The variation of mass flow rate in the reactor coolant system due to water density changes is included in the calculation. The variation of flow rate from the core makeup tanks or accumulators (or both) due to changes in the reactor coolant system pressure and temperature and the pressuriser level is also included. The reactor coolant system and passive injection flow calculations include line losses.

At no time during the analysed steam line break event does the core makeup tank level approach the setpoint for actuation of the automatic depressurisation system. During non-LOCA events, the core makeup tanks remain filled with water. The volume of injection flow leaving the core makeup tank is offset by an equal volume of recirculation flow that enters the core makeup tanks via the reactor coolant system cold leg balance lines.

The PRHR system provides a passive, long-term means of removing the core decay and stored heat by transferring the energy via the PRHR heat exchanger to the IRWST. The PRHR heat exchanger is normally actuated automatically when the steam generator level falls below the Low-2 wide-range level. For the main steam line rupture case analysed, the PRHR exchanger is conservatively actuated at time zero to maximise the cooldown.

The case analysed conservatively models the expected behaviour of the plant during a steam system piping failure. This includes the tripping of the reactor coolant pumps coincident with core makeup tank actuation. A DNB analysis was performed using limiting assumptions that bound those of Section 9.1.5.2.1.

Under the low flow (natural circulation) conditions present in the transient, the return to power is severely limited by the large negative feedback due to flow and power. The minimum DNBR is conservatively calculated and remains above the 95/95 limit.

Appendix 9C provides discussion and analysis of long term safe shutdown for non-LOCA events.

9.1.5.3 Diverse Mitigation

As this is an infrequent fault (DB1), a diverse mitigation assessment is not required.

9.1.5.4 Radiological Consequences

Design Basis

The evaluation of the radiological consequences of a postulated main steam line break outside containment assumes that the reactor has been operating with a limited number of fuel rods containing cladding defects and that leaking steam generator tubes have resulted in a buildup of activity in the secondary coolant.

Following the rupture, startup feedwater to the faulted loop is isolated and the steam generator is allowed to steam dry, releasing all activity initially present. Any radionuclides carried from the primary coolant into the faulted steam generator via leaking tubes are assumed to be released directly to the environment. It is assumed that the intact loop is isolated from the faulted loop via the MSIV, and that the passive systems are removing decay heat, thus the intact SG is not modelled in the dose analysis.

Assumptions are chosen to bound both hot zero power and full power scenarios.

9.1.5.4.1 Source Term

There is no fuel damage as a result of the accident. Therefore, the most significant radionuclide releases from the MSLB are the noble gases, alkali metals, and iodines that are present in the primary and secondary coolants, become airborne, and are released to the environment as a result of the accident.

The methodology assesses two different reactor coolant iodine source terms, both of which consider the iodine-spiking phenomenon. In one case, the initial iodine concentrations are assumed to be those associated with the equilibrium operating limit for primary coolant iodine activity. The iodine spike is assumed to be initiated by the accident, with the spike causing an increasing level of iodine in the reactor coolant.

The second case assumes that the iodine spike occurs prior to the accident and that the maximum resulting reactor coolant iodine concentration exists at the time the accident occurs.

The secondary coolant iodine and alkali metal concentrations are assumed to be 10 percent of the primary concentrations. Noble gases are not assumed to accumulate in the secondary coolant

9.1.5.4.2 Release Pathways

There are two components to the accident releases.

- The secondary coolant in the steam generator of the faulted loop is assumed to be released out the break as steam. Any iodine and alkali metal activity contained in the coolant is assumed to be released.

- The reactor coolant leaking into the steam generator of the faulted loop is assumed to be released to the environment without any credit for partitioning or plateout onto the interior of the steam generator.

9.1.5.4.3 Dose Calculation Models

The models used to calculate doses are provided in Appendix 9A.

9.1.5.4.4 Analytical Assumptions and Parameters

The assumptions and parameters used in the analysis are listed in Table 9.1.5-1.

9.1.5.4.5 Doses

Design Basis

The highest doses are found to be for the accident-initiated iodine spike. The calculated maximum doses for all relevant pathways (inhalation, cloudshine, and groundshine) are as follows:

- Offsite dose: 9.3 mSv Worker dose: 78 mSv

These doses are within the Target 4 BSL for infrequent faults (10 mSv offsite and 200 mSv onsite).

The limiting conditions for operation of the Technical Specifications used in the dose assessment are provided in Table 9.1.5-2. The Table 9.1.5-2 values ensure the Target 4 BSLs are met.

9.1.5.5 As Low As Reasonably Practicable Assessment

For this event, the identification of the primary safety functions as Class 1 SSCs has been shown to be adequate to meet DB requirements.

Diverse mitigation functions are only required for more probable events including smaller pipe breaks and stuck open valves. The plant is able to ride out these small load increases as shown in reference 9.1-12, such that diverse mitigation is not required. However, diverse mitigation functions are available for this event (see Table 9.1.5-3). These features include other Class 1 safety functions and the DAS function, which is Class 2. See Reference 9.1-12 for additional discussions on these diverse mitigation features.

Additionally, the AP1000 plant design has a third level of redundancy/diversity that is provided by the DiD systems for these smaller break sizes. The applicable DiD functions include:

- CVS boration for long-term reactivity control
- CVS make-up for RCS inventory control
- SFW with steam dump for short-term decay heat removal
- RNS cooling of the RCS for long-term decay heat removal. The RNS requires support from the CCS and SWS cooling water systems.
- Control by the PLS C&I

The characteristics of the above features were compared to improvements that were evaluated for the RNS for its mitigation of cliff edge small LOCAs. First it should be recognized that in this situation the RNS provides the second level of defence for this event and is therefore more important than the above DiD features which provide a 3rd level of defence. The RNS improvements included making the RNS alignment / start automatic, increasing the RNS pump head, and adding a RNS suction supply tank that is separate from the Class 1 system. None of these potential improvements were found to be ALARP (Reference 9.1-11). However, the SFW and CVS already include characteristics similar to these proposed improvements. Another improvement that could be made to these DiD systems is to upgrade them to Class 1. This would be very expensive especially and would have wide reaching impacts to the design of SSCs; notable would be the impact on component and building design to address hazards including seismic and storm winds/missiles. Such a change would not be ALARP because the cost would be grossly disproportional to its benefit.

Potential operator actions are listed in Table 9.1.5-4. As discussed in Chapter 9.0.15, the AP1000 has incorporated ALARP thinking throughout its development. In addition, the current risk of a large radioactivity release is significantly less than the SAP Target 9 BSO (1E-7 pa). Considering the ALARP thinking that went into the AP1000 development, its low risk profile and the additional level of defence discussed above (including their performance characteristics), improving the Class 2 DiD to better remove decay heat or shutdown the reactor would be grossly disproportional to the risk reduction that might be achieved. As a result, the current design is considered ALARP.

9.1.5.6 Conclusions

DNB and possible cladding perforation are not unacceptable consequences following a steam pipe rupture based on the applicable acceptance criteria. Nevertheless, the preceding analysis shows that no DNB, and therefore, no cladding perforation occurs for the main steam line rupture assuming the most reactive RCCA stuck in its fully withdrawn position.

DBA radiological consequences for the steam system piping failure are within the Target 4 BSL for infrequent faults (10 mSv offsite and 200 mSv onsite). Thus, the identification of necessary Class 1 SSCs is adequate to meet DB requirements.

It has been shown that the AP1000 plant design includes adequate systems for the protection of this fault, which limit the radiological consequences such that they are compliant with the SAPs targets and the risks have been reduced to be ALARP.

9.1.6 Steam System Piping Failure at Full Power (Fault 1.21.1)

9.1.6.1 Identification of Causes and Accident Description

A rupture in the main steam system piping from an at-power condition creates an increased steam load, which extracts an increased amount of heat from the reactor coolant system via the steam generators. This results in a reduction in reactor coolant system temperature and pressure. In the presence of a strong negative moderator temperature coefficient, typical of end-of-life conditions, the colder core inlet coolant temperature causes the core power to increase from its initial level due to the positive reactivity insertion. The power approaches a level equal to the total steam flow.

Depending upon the break size, the reactor may be tripped on any of the following trip signals to provide the necessary protection against the rupture of a main steam line:

- Overpower ΔT
- Low pressuriser pressure
- Safeguards (“S”) actuation signal
  - Low steam line pressure
  - Low cold leg temperature

The steam system piping failure accident analysis described in Section 9.1.5 is performed assuming a hot zero-power initial condition with the control rods inserted in the core, except for the most reactive rod in the fully withdrawn position out of the core. That condition could occur while the reactor is at hot shutdown at the minimum required shutdown margin or after the plant has been tripped manually or by the reactor protection system following a steam line break from an at-power condition. For an at-power break, the analysis in Section 9.1.5 represents the limiting condition with respect to core protection for the time following reactor trip. This section describes the analysis of a steam system piping failure occurring from an at-power initial condition to demonstrate that core protection is maintained before and immediately following reactor trip. The analysis initiated from hot full power does not extend into the portion of the transient where the PRHR or core makeup tanks are actuated.

9.1.6.2 Design Basis Mitigation

Analysis is performed to demonstrate the adequacy of the PMS to detect and mitigate the fault and show that the safety analysis criteria are satisfied including:

- No fuel failures (confirmed using minimum DNBR and fuel melt criteria),
- The RCS pressure criterion is met,
- The MSS pressure criterion is met, and
- The pressuriser does not fill (which could result in a LOCA).

With respect to the peak RCS and MSS pressure criteria, this event is bounded by the Turbine Trip DB analysis in Section 9.2.3 and is not explicitly verified. Also, pressuriser fill criterion is not challenged for this event, and is not explicitly verified.

9.1.6.2.1 DBA Method of Analysis

The analysis of the steam line rupture is performed in the following stages:

- The LOFTRAN code (References 9.1-1 and 9.1-6) is used to calculate the nuclear power, core heat flux, and reactor coolant system temperature and pressure transients resulting from the cooldown following the steam line break.

- The core radial and axial peaking factors are determined using the thermal-hydraulic conditions from LOFTRAN as input to the nuclear core models. A detailed thermal-hydraulic code, VIPRE-01 (Reference 9.1-7), is then used to calculate the DNBR for the limiting time during the transient.

This accident is analysed with the RTDP as described in WCAP-11397-P-A (Reference 9.1-2).

The following assumptions are made in the transient analysis:

- Initial conditions – RTDP DNB methodology was used; therefore, the uncertainties in the initial conditions are included in the DNBR limits. Thus, nominal full-power values are used in LOFTRAN. The reactor coolant system minimum measured flow is used.

- Break size – A spectrum of break sizes was analysed. Small breaks do not result in a reactor trip. Intermediate breaks result in a reactor trip on overpower ΔT. Larger break sizes result in a reactor trip on low steam line pressure safeguards actuation.

- Break flow – In computing the steam flow during a steam line break, the Moody curve (Reference 9.1-3) for $fL/D = 0$ is used.

- Reactivity coefficients – The analysis assumes maximum moderator reactivity feedback and minimum Doppler power feedback to maximise the power increase following the break.

- Protection system – The protection system features that mitigate the effects of a steam line beak are described in Section 9.1.5. This analysis considers only the initial phase of the transient initiated from an at-power condition. Protection in this phase of the transient is provided by reactor trip, if necessary (specifically overpower ΔT and low steam line pressure safeguards actuation).

- Control systems – Control systems are not credited in the accident analysis unless their function would result in more severe consequences. The only control system that is assumed to function during the hot full-power steam line break event is the main feedwater system. For this event, the feedwater flow is assumed to match the steam flow.

Anticipated operational occurrences and postulated accidents are analysed assuming a loss of offsite ac power. The loss of offsite power is not considered as a single failure, and the analysis is performed without changing the event category. In the analyses, the loss of offsite ac power is considered to be a potential consequence of an event due to disruption of the grid following a turbine trip during the event.

For those events where offsite ac power is lost, an appropriate time delay between turbine trip and the postulated loss of offsite ac power is assumed in the analyses. A time delay of 3 seconds is used. This time delay is based on the inherent stability of the offsite power grid. Following the time delay, the effect of the loss of offsite ac power on plant auxiliary equipment – such as reactor coolant pumps, main feedwater pumps, condenser, startup feedwater pumps, and RCCAs – is

considered in the analyses. Turbine trip occurs 5 seconds following a reactor trip condition being reached. This delay is part of the reactor trip system and was chosen to allow the reactor to be tripped and have the rods inserted to the bottom of the core before a turbine trip signal. As a result, reactor coolant pump coastdown would be delayed an additional 5 seconds, the control rods would be fully inserted, and there would be no adverse DNB impact from the resulting core flow reduction. Thus, there is no need for an explicit analysis of this event with loss of offsite ac power.

9.1.6.2.2 DBA Credited SSCs

For the DB, no claim is placed on systems that are not Class 1. For this fault, the available Class 1 systems are listed in Table 9.0-10. The presented DBA ends shortly after reactor trip; however, essential safety functions for the long term safe shutdown analysis (Appendix 9C) bound safe shutdown response for this event. Other SSCs include the CMTs, containment isolation, steam line isolation valves and SG flow restrictors. The PMS provides the following:

- RT on (dependent on break size):
  - Overpower ΔT
  - Low-2 steam line pressure
- PRHR actuation on Low-2 SG NR level coincident with Low-2 SFW flow
- CMTs and containment isolation on Low-2 CL temperature
- PCS on High-2 containment pressure

9.1.6.2.3 DBA Results

A spectrum of steam line break sizes was analysed from 0.01 m^2 (0.1 ft^2) to 0.13 m^2 (1.4 ft^2). The results show that for small break sizes up to and including 0.03 m^2 (0.35 ft^2), a reactor trip is not generated. In this case, the event is similar to an excessive load increase event; the core reaches a new equilibrium condition at a higher power equivalent to the increased steam release. For break sizes from 0.03 m^2 (0.36 ft^2) up to and including 0.08 m^2 (0.87 ft^2), the reactor trips on overpower ΔT. For break sizes from 0.08 m^2 (0.88 ft^2) to 0.13 m^2 (1.4 ft^2), the reactor trips on the low steam line pressure safeguards actuation signal.

The limiting case for demonstrating DNB and kW/ft (kW/m) protection is the 0.08 m^2 (0.87 ft^2) break, the largest break size that results in a trip on overpower ΔT. The time sequence of events for this case is shown on Table 9.1.6-1. Figures 9.1.6-1 through 9.1.6-7 show the transient response.

Appendix 9C provides discussion and analysis of long term safe shutdown for non-LOCA events.

9.1.6.3 Diverse Mitigation

Diverse mitigation for this event is not required as it is an infrequent fault classified as DB1. The diversity analyses for large excessive load increase events which are classified as frequent faults are presented in Section 9.1.3.3.

9.1.6.4 Radiological Consequences

The main steamline break doses presented in Section 9.1.5.4 are based on assumptions chosen to bound both hot zero power and full power scenarios. Therefore, the main steamline break doses from Section 9.1.5.4 are presented. The calculated maximum doses for all relevant pathways (inhalation, cloudshine, and groundshine) are as follows:

- Offsite dose: 9.3 mSv Worker dose: 78 mSv

These doses are within the Target 4 BSL for infrequent faults (10 mSv offsite and 200 mSv onsite).

Thus, the identified Class 1 SSCs are adequate to meet DB requirements for this fault.

9.1.6.5 As Low as Reasonably Practicable Assessment

The ALARP discussion for this event is the same as for the main steamline break at hot zero power, as described in Section 9.1.5.5.

9.1.6.6 Conclusions

The analysis shows that the DNB and fuel centreline melt (kW/ft (kW/m)) design bases are met for the limiting DB case. Although DNB and possible cladding perforation following a steam pipe rupture are not necessarily precluded by the criteria, the above analysis shows that the minimum DNBR remains above the limit value for any rupture occurring from an at-power condition before and immediately following a reactor trip.

Radiological consequences for the steam system piping failure are within the Target 4 BSL for infrequent faults (10 mSv offsite and 200 mSv onsite). Thus, the identification of necessary Class 1 SSCs is adequate to meet DB requirements.

It has been shown that the AP1000 plant design includes adequate systems for the protection of this fault, which limit the radiological consequences such that they are compliant with the SAPs targets and the risks have been reduced to be ALARP.

9.1.7 Inadvertent Operation of the PRHR Heat Exchanger (Fault 1.15.15)

9.1.7.1 Identification of Causes and Accident Description

The inadvertent actuation of the PRHR heat exchanger causes an injection of relatively cold water into the reactor coolant system. This produces a reactivity insertion in the presence of a negative moderator temperature coefficient. To prevent this reactivity increase from causing reactor power increase, a reactor trip is initiated when either PRHR discharge valve comes off of its fully shut seat.

The inadvertent actuation of the PRHR heat exchanger could be caused by operator error or a false actuation signal, or by malfunction of a discharge valve. Actuation of the PRHR heat exchanger involves opening one of the isolation valves, which establishes a flow path from one reactor coolant system hot leg, through the PRHR heat exchanger, and back into its associated steam generator cold leg plenum.

The PRHR heat exchanger is located above the core to promote natural circulation flow when the reactor coolant pumps are not operating. With the reactor coolant pumps in operation, flow through the PRHR heat exchanger is enhanced. The heat sink for the PRHR heat exchanger is provided by the IRWST, in which the PRHR heat exchanger is submerged. Because the fluid in the heat exchanger is in thermal equilibrium with water in the tank, the initial flow out of the PRHR heat exchanger is significantly colder than the reactor coolant system fluid. Following this initial insurge, the reduction in cold leg temperature is limited by the cooling capability of the PRHR heat exchanger. Because the PRHR heat exchanger is connected to only one reactor coolant system loop, the cooldown resulting from its actuation is asymmetric with respect to the core.

The response of the plant to an inadvertent PRHR heat exchanger actuation with the plant at no-load conditions is bounded by the analyses performed for the inadvertent opening of a steam generator relief or safety valve event (Section 9.1.4) and the steam system piping failure event (Section 9.1.5). Both of these events are conservatively analysed assuming PRHR heat exchanger actuation coincident with the steam line depressurisation. Therefore, only the response of the plant to an inadvertent PRHR initiation with the core at power is considered.

The effects of a possible consequential loss of ac power during an inadvertent PRHR heat exchanger actuation event have been evaluated to not adversely impact the analysis results. This conclusion is based on a review of the time sequence associated with a consequential loss of ac power in comparison to the reactor shutdown time for an inadvertent PRHR heat exchanger actuation event. The primary effect of the loss of ac power is to cause the RCPs to coast down. The protection and safety monitoring system includes a 5-second minimum delay between the reactor trip and the turbine trip. In addition, a 3-second delay between the turbine trip and the loss of offsite ac power is assumed, consistent with Section 9.0.12. Considering these delays between the time of the reactor trip and RCP coastdown due to the loss of ac power, it is clear that the plant shutdown sequence will have passed the critical point and the control rods will have been completely inserted before the RCPs begin to coast down. Therefore, the consequential loss of ac power does not adversely impact this inadvertent PRHR heat exchanger actuation analysis because the plant will be shut down well before the RCPs begin to coast down.

Plant systems and equipment available to mitigate the effects of the accident are discussed in Section 9.0.4 and listed in Table 9.0-10. Due to the potential consequences as a result of the reactivity excursion, a reactor trip has been designed so that upon an inadvertent PRHR actuation, a reactor trip will occur. This reactor trip is generated when either of the discharge valves is not closed. This ensures that the reactor will be tripped prior to a power increase due to the cold water injection.

9.1.7.2 Design Basis Mitigation

Since a reactor trip is initiated as soon as the PRHR discharge valves are not fully closed, this event is essentially a reactor trip from the initial condition and requires no separate transient analysis. Table 9.1.2-1 shows the sequence of events for the inadvertent PRHR heat exchanger actuation.

9.1.7.3 Diverse Mitigation

Diverse mitigation capabilities are the same as for the loss of normal feedwater fault, as described in Section 9.2.7.3.

9.1.7.3.1 Diverse Mitigation for ATWT

A reactor trip has been designed so that upon an inadvertent PRHR actuation, a reactor trip will occur. Failure of this reactor trip would allow a power increase due to the cold water injection.

A number of cases were considered to address different potential CCFs that can affect the PMS and its ability to insert RCCAs. The inadvertent operation of the PRHR analysis documented in this section is performed to bound the following events:

- Inadvertent operation of the PRHR with a PMS CCF – The CCF prevents all PMS reactor trips signals and engineered safeguards features signals. The DAS is assumed to be completely operable. Offsite power and turbine bypass are also assumed available.

- Inadvertent operation of the PRHR with a PMS reactor trip breaker CCF - This failure prevents the PMS from inserting the rods; however, PMS logic continues to function, and all engineered safeguards features signals are operable. DAS is completely operable, including its capability to drop rods. Offsite power and turbine bypass are also assumed to be available.

- Inadvertent operation of the PRHR with a RCCA mechanical CCF - The PMS, DAS, and control systems are assumed to be operable except that RCCAs do not insert into the core on a trip signal.

This analysis is performed to demonstrate the adequacy of the operable portions of the PMS (considering the impact of the CCF) as well as the DAS to detect and actuate mechanical SSCs to mitigate the fault. The following ATWT acceptance criteria are applicable to this event:

- The RCS does not overpressurise due to reactor coolant heatup. The ATWT pressure limit is 22.06 MPa-rel (3200 psig).

- There is no significant fuel damage.

- The rate and duration of energy release to containment is much less than for the design basis LOCA. This demonstrates that the containment does not overpressurise due to the energy release to the containment.

9.1.7.3.1.1 Diverse ATWT Method of Analysis

For the inadvertent operation of the PRHR with a PMS CCF a short-term analysis of the out surge of cold water from the PRHR heat exchanger was performed. All PMS reactor trip and engineered safeguards automatic functions are assumed inoperable in this scenario.

For the mechanical failure of control rods to drop scenario, two outcomes are possible, depending on whether a PMS reactor trip setpoint is exceeded or not. If no PMS reactor trip setpoints are reached, the plant will reach an equilibrium power level equal to the combined heat removal rates of the PRHR and the turbine load. The results will be the same as the analyses results for an inadvertent operation of the PRHR with a PMS failure. If a PMS reactor trip setpoint is reached, the turbine will trip and the RCCAs are assumed not to insert due to the postulated mechanical CCF. Following the turbine trip, the event will be similar to the turbine trip events discussed in Section 9.2.3.5, where feedwater flow is assumed to be available. The turbine trips analyses show

that maximum reactor coolant pressure is limited to less than 110 percent of reactor coolant design pressure.

For the reactor trip breaker CCF scenario, the PMS is assumed to be operable. However, when a reactor trip signal is generated, all trip breakers are assumed to fail to open such that the control rods do not insert. All DAS functions (including reactor trip by tripping of the M-G sets) are operable. The response for this scenario is similar to that discussed for the case with a mechanical CCF, except that the operator may trip the rods using the DAS.

9.1.7.3.1.2 Diverse ATWT Credited SSCs

For the PMS CCF ATWT cases presented, no available SSCs (PMS or DAS functions) are credited to initiate passive safety features. Instead, the plant will reach a stable steady-state power condition and ATWT criteria would be met for sustained operation at the stabilized power. Ultimately, manual operator action using PMS or DAS would be required to shut down the plant. The SSCs modelled as available for this analysis are listed in Table 9.0-14.

9.1.7.3.1.3 Diverse ATWT Results

Results from this analysis with a PMS CCF are shown in Figures 9.1.7-1 to 9.1.7-4 and a sequence of events is provided in Table 9.1.7-1. Figure 9.1.7-1 shows the short term nuclear power transient following activation of the PRHR from full-power conditions. Due to the initial cold water at containment temperature, there is a rapid nuclear power increase to about 119 percent. Once the initial water in the PRHR is purged, the temperature of the water exiting from the PRHR is limited by the cooling capacity of the PRHR and the fluid temperature entering the PRHR from the hot leg (see Figure 9.1.7-3). Core power then decreases until it reaches an equilibrium power equal to the steam generator load plus the PRHR heat removal capacity (see Figure 9.1.7-2).

The maximum core average heat flux obtained for this case was 118.7 percent. The power level remained low enough that the local linear power did not result in fuel melting. The minimum DNBR was above the limit value. Thus the ATWT acceptance criteria are met for the short-term period of an inadvertent PRHR.

Eventually, equilibrium conditions will be reached with the core at approximately 110 percent power, reactor coolant pressure near the nominal value and temperature in the PRHR loop slightly lower than the normal operating value.

During the transient, the pressuriser safety valves are not opened, and no challenge to the pressure integrity of the reactor coolant boundary occurs. Once diagnosed by the operator, the operator uses the DAS to trip and recover the plant.

9.1.7.3.2 Diverse Mitigation for Core Cooling

The loss of normal feedwater diverse core cooling, as analysed in Section 9.2.7.3.2, was determined to be bounding of all non-LOCA events.

9.1.7.4 Radiological Consequence

Design Basis

In the case where offsite power remains available, there is no release of activity to the environment and the Target 4 BSOs (0.01 mSv offsite and 0.1 mSv onsite) are met.

In the case where offsite power is lost, a small release of activity may occur as a result of steam dump to the atmosphere due to unavailability of the condensers. With no fuel damage and primary and secondary circuits intact, the initiating event has no impact on the doses. Therefore, the radiological consequences are limited and no dose calculations have been obtained specifically for this case. However, the doses have been calculated for the loss of offsite power in Section 9.2.6.4. Operation of the PRHR at the start of the event would reduce the steam generator releases. Therefore, the dose associated with the loss of offsite power bounds the dose associated with the inadvertent opening of the PRHR. The loss of offsite power doses from Section 9.2.6.4 are presented. The calculated maximum doses for all relevant pathways (inhalation, cloudshine, and groundshine) are as follows:

- Offsite dose: 0.05 mSv Worker dose: 1.5 mSv

These doses are within the Target 4 BSL for frequent faults (1 mSv offsite and 20 mSv onsite).

Thus, the identified Class 1 SSCs are adequate to meet DB requirements for this fault.

Diverse Mitigation

Both the diverse ATWT and diverse core cooling scenarios demonstrate that the RCS does not overpressurise and there is no significant fuel damage. For a diverse mitigation radiological consequences analysis better estimate assumptions would be credited. This would include reactor coolant system activity levels significantly lower than those modelled for the DBA and better activity retention in containment and in the steam generators. In addition better estimate atmospheric dispersion factors would be used. Therefore, a diverse mitigation radiological consequences analysis would show that the doses for the diverse ATWT scenario would be less than those reported for the non-LOCA DBAs and doses for the diverse core cooling scenario would be much less than for the design basis LOCA. The diverse mitigation analyses would not have to meet the Target 4 BSL for frequent faults and would meet the Target 4 BSL for infrequent faults.

9.1.7.5 As Low As Reasonably Practicable Assessment

The ALARP discussion for this event is the same as for Inadvertent Opening of a Steam Generator Relief or Safety Valve event, as described in Section 9.1.4.5.

9.1.7.6 Conclusions

Inadvertent actuation of the PRHR does not result in violation of the core thermal design limits (DNB and linear power generation) or RCS overpressure.

This event has also been adequately assessed with respect to ATWT considerations. This event was not explicitly analysed for the change in the current design reference point in the UK as described in Reference 9.1-9. However, the evaluation conducted to closeout FS-03 demonstrated with a subset of events (Reference 9.1-10) that there is little impact on the key analysis trends, results, and margin to the applicable acceptance criteria. Therefore, the subset of events confirmed the change in design reference point would not invalidate the conclusions presented for this event.

Diverse core cooling capabilities have been demonstrated.

DBA radiological consequences are within the Target 4 BSL for frequent faults (1 mSv offsite and 20 mSv onsite).

Thus, the identified Class 1 SSCs are adequate to meet DB requirements for this fault.

It has been shown that the AP1000 plant design includes adequate systems for the protection of this fault, which limit the radiological consequences such that they are compliant with the SAPs targets and the risks have been reduced to be ALARP.

9.1.8 References

9.1-1 Westinghouse Documents WCAP-7907-P-A, Rev. 0 (Proprietary), and WCAP-7907-A, Rev. 0 (Non-Proprietary), "LOFTRAN Code Description," April 1984.

9.1-2 Westinghouse Documents WCAP-11397-P-A (Proprietary) and WCAP-11397-A (Non-Proprietary), "Revised Thermal Design Procedure," April 1989.

9.1-3 Moody, F. S., "Transactions of the ASME, Journal of Heat Transfer," Figure 3, page 134, February 1965.

9.1-4 Westinghouse Documents WCAP-9226-P-A, Rev. 1 (Proprietary) and WCAP-9227-A, Rev. 1 (Non-Proprietary), "Reactor Core Response to Excessive Secondary Steam Releases," February 1998.

9.1-5 Westinghouse Report UKP-GW-GLR-016, Rev. B, "Evaluation of ATWS Events for UK AP1000™ Pressurized Water Reactor," October 2010.

9.1-6 Westinghouse Documents WCAP-15644-P, Rev. 2 (Proprietary) and WCAP-15644-NP, Rev. 2 (Non-Proprietary), "AP1000 Code Applicability Report," March 2004.

9.1-7 Westinghouse Documents WCAP-14565-P-A, Rev. 0 (Proprietary) and WCAP-15306-NP-A, Rev. 0 (Non-Proprietary), "VIPRE-01 Modeling and Qualification for Pressurized Water Reactor Non-LOCA Thermal-Hydraulic Safety Analysis," October 1999.

9.1-8 Westinghouse Report UKP-GW-GL-067, Rev. 1, "AP1000 Assessment of Diverse Mitigation of Frequent Faults for the UK," December 2011.

9.1-9 Westinghouse Report UKP-SSAR-GLR-001, Revision 0, "UK Fault Studies Analysis Basis," August 2016.

9.1-10 Westinghouse Report UKP-SSAR-GLR-002, Revision 0, "UK AP1000® Plant: Summary Report Supporting the Closure of Fault Studies Issue 03," May 2016.

9.1-11 Westinghouse Report UKP-GW-GL-797, Revision 1, "AP1000 ALARP Assessment of Diverse Mitigation of 'Frequent Fault' Small Break LOCAs," July 2016.

9.1-12 Westinghouse Report UKP-GW-GL-083, Revision 0, "AP1000 Flux Protection and Diversity for Frequent Faults," June 2016.

Table 9.1.2-1 (Sheet 1 of 2). DBA Time Sequence Of Events For Incidents That Result In An Increase In Heat Removal From The Primary System

Accident	Event	Time (seconds)
Excessive increase in secondary steam flow		
– Manual reactor control (minimum moderator feedback)	10-percent step load increase	0.0
	Equilibrium conditions reached (approximate time only)	200.0
– Manual reactor control (maximum moderator feedback)	10-percent step load increase	0.0
	Equilibrium conditions reached (approximate time only)	170.0
– Automatic reactor control (minimum moderator feedback)	10-percent step load increase	0.0
	Equilibrium conditions reached (approximate time only)	400.0[(a)]
– Automatic reactor control (maximum moderator feedback)	10-percent step load increase	0.0
	Equilibrium conditions reached (approximate time only)	70.0
Feedwater system malfunctions that result in an increase in feedwater flow	Both main feedwater control valves fail fully open	0.0
	Minimum DNBR occurs	103.9
	Turbine trip/feedwater isolation and reactor trip on high steam generator level	230.7
	Rod motion begins	232.7
Inadvertent operation of the PRHR	PRHR discharge valves go fully open	0.0
	Reactor trip setpoint reached	0.0
	Rod motion begins	1.25
	Rods fully inserted	3.95

Note:
a. Although oscillation in the transients occurs, the nuclear power and DNBR stabilize after 400 seconds.

Table 9.1.2-1 (Sheet 2 of 2). DBA Time Sequence Of Events For Incidents That Result In An Increase In Heat Removal From The Primary System

Accident	Event	Time (seconds)
Inadvertent opening of a steam generator relief or safety valve	Inadvertent opening of one main steam safety or relief valve	0.0
	"S" actuation signal on safeguards Low-2 T_{cold}	119.0
	Core makeup tank actuation	136.0
	Boron reaches core	156.2
Steam system piping failure at hot zero power	Steam line ruptures	0.0
	"S" actuation signal on safeguards Low-2 steam line pressure	1.4
	Criticality attained	55.2
	Boron reaches core	30.6
	Pressuriser and surge line empty	50.4

Table 9.1.3-1. ATWT Time Sequence of Events Time Sequence Of Events For Incidents That Result In An Excessive Increase in Secondary Steam Flow

Accident	Event	Time (seconds)
Excessive increase in secondary steam flow diversity case		
– Common cause failure of all 6 turbine bypass valves with common cause failure of the PMS	Increase in steam demand begins	0.0
	Maximum core heat flux occurs	102.4
	Core heat flux reaches steady state	~160
– 0.045 m^2 (0.48 ft^2) break with a common cause failure of the PMS	Steam line rupture occurs	0.0
	Core heat flux exceeds 118% RTP	34.3
	Maximum core heat flux occurs	~1197.5

Table 9.1.4-1. Not Used

Table 9.1.4-2. Not Used

Table 9.1.5-1. DBA Parameters Used In Evaluating The Radiological Consequences Of A Main Steam Line Break

Reactor coolant iodine activity	
– Accident-initiated spike	Initial activity equal to the operating limit for reactor coolant activity of 9.25E6 Bq/kg (0.25 µCi/g) dose equivalent I-131 (see Table 9A-1) with an assumed iodine spike that increases the rate of iodine release from fuel into the coolant (see Table 9A-2) by a factor of 335. Duration of spike is 8 hours.
– Pre-accident spike	Equal to the abnormal operating limit for reactor coolant activity of 5.55E8 Bq/kg (15 µCi/g) dose equivalent I-131 (a factor of 60 times the iodine values in Table 9A-1)
Reactor coolant noble gas activity	Equal to the operating limit for reactor coolant activity of 2.6E9 Bq/kg (70 µCi/g) dose equivalent Xe-133 (see Table 9A-1)
Reactor coolant alkali metal activity	Design basis activity (see Table 9A-1)
Secondary coolant initial iodine and alkali metal activity	10% of design basis reactor coolant concentrations at maximum equilibrium conditions
Duration of accident	24 hr
Reactor coolant mass	1.684E5 kg (3.713E5 lbm)
Steam generator in faulted loop	
– Initial water mass	1.37E5 kg (3.017E5 lbm)
– Primary to secondary leak rate	3.95E-01[(a)] kg/min (0.871 lbm/min)
Offsite atmospheric dispersion factors	See Table 9A-5
Control room modelling	See Appendix 9A

Note:

a. Equivalent to 0.57 m^3 (150 gal) per day per SG cooled liquid at 1000 kg/m^3 (62.4 lbm/ft^3).

Table 9.1.5-2. DBA Main Steamline Break Technical Specifications Used In Dose Analysis

Limit or Condition	Tech Spec Identification and Notes
Primary-to-secondary leakage rate	3.4.7 leak rate to be < 0.57 m^3 (150 gal) per day for any one SG
Primary coolant specific activity	3.4.10 dose equivalent specific activity to be < 9.25E6 Bq/kg (0.25 µCi/g) for I-131 and < 2.6E9 Bq/kg (70 µCi/g) for Xe-133 3.4.10 dose equivalent specific activity to be < 5.55E8 Bq/kg (15 µCi/g) for I-131 short term abnormal operation only
Secondary coolant specific activity	3.7.4 dose equivalent I-131 specific activity to be < 9.25E5 Bq/kg (0.025 µCi/g)

Table 9.1.5-3. Main Steamline Break Mitigation Features

Category A Safety Function	Provision	SSCs	Classification
Short-term reactivity control	Primary means	Reactor trip Breakers (PMS)	1
	Diverse means	Motor-generator set field breakers (DAS)	2
Long-term reactivity control	Primary means	CMT Recirculation	1
	Diverse means	Passive feed and bleed	1
Decay heat removal	Primary means	PRHR HX	1
	Diverse means	Passive feed and bleed	1
RCS pressure control	Primary means	Not required – Transient does not challenge this function	
	Diverse means		
RCS inventory control	Primary means	CMTs	1
	Diverse means	Passive feed and bleed	1
Containment cooling	Primary means	PCS AOVs	1
	Diverse means	PCS MOVs	1

Table 9.1.5-4. Main Steamline Break Potential Operator Actions

Operator Action	Class
On failure of automatic shutdown, initiate shutdown manually using DAS.	1
On failure of shutdown rods to insert, initiate RCP trip and actuation of CMTs to achieve shutdown by boration of the primary circuit.	1
If PRHR fails, activate ADS to allow automatic actuation of recirculation residual heat removal (RHR) via the IRWST.	1

Table 9.1.6-1. DBA Time Sequence Of Events For Steam System Piping Failure At Full Power – 0.08 m^2 (0.87 ft^2) Break Size

Event	Time (seconds)
Steam line rupture	0.0
OPΔT reactor trip setpoint reached	12.9
Rods begin to drop	13.9
Minimum DNBR occurs	14.9
Maximum core heat flux occurs	14.9

Table 9.1.7-1. ATWT Time Sequence of Events for Inadvertent PRHR with a PMS CCF

Event	Time (Sec)
PRHR initiated	10.0
High neutron flux trip setpoint reached. PMS trip blocked	15.7
Initial fluid in PRHR purged	~16.2
maximum core heat flux percent reached	22.8
maximum RCS pressure reached	34.8
Core power matches turbine load and PRHR heat removal	~75

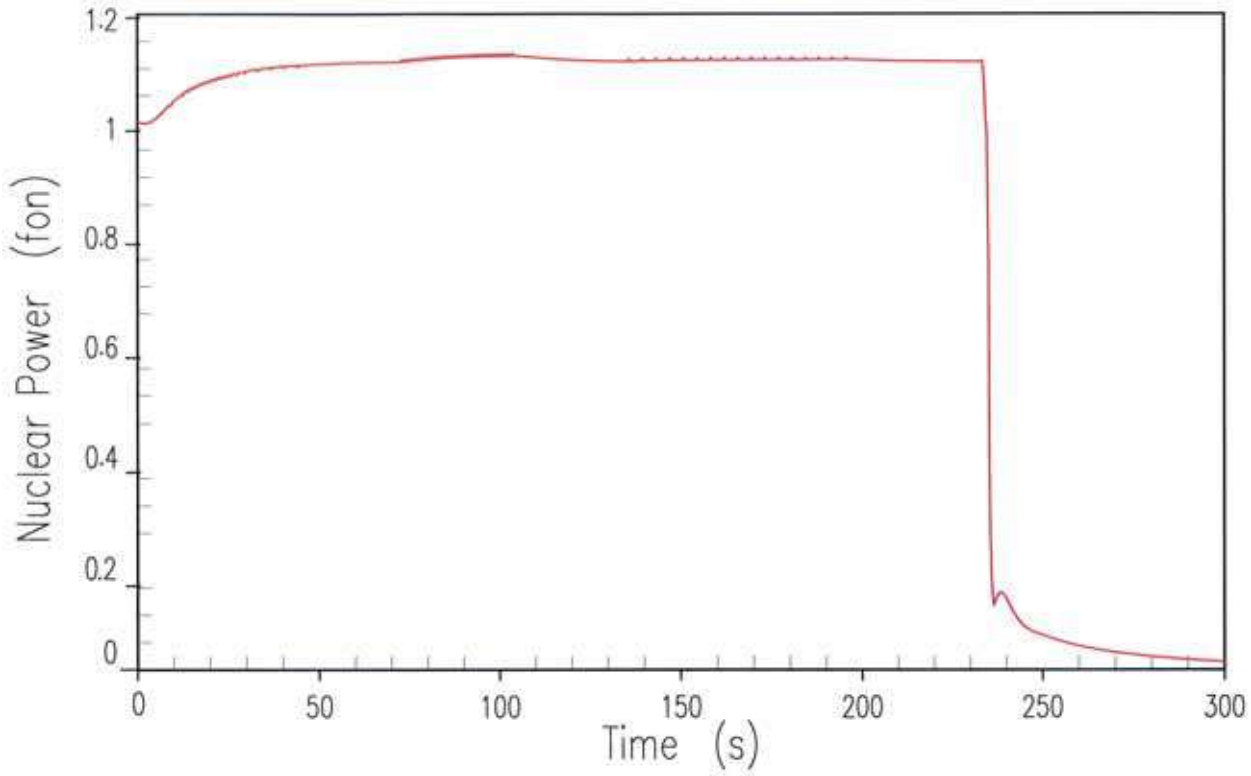


Figure 9.1.2-1. DBA Feedwater Control Valve Malfunction Nuclear Power

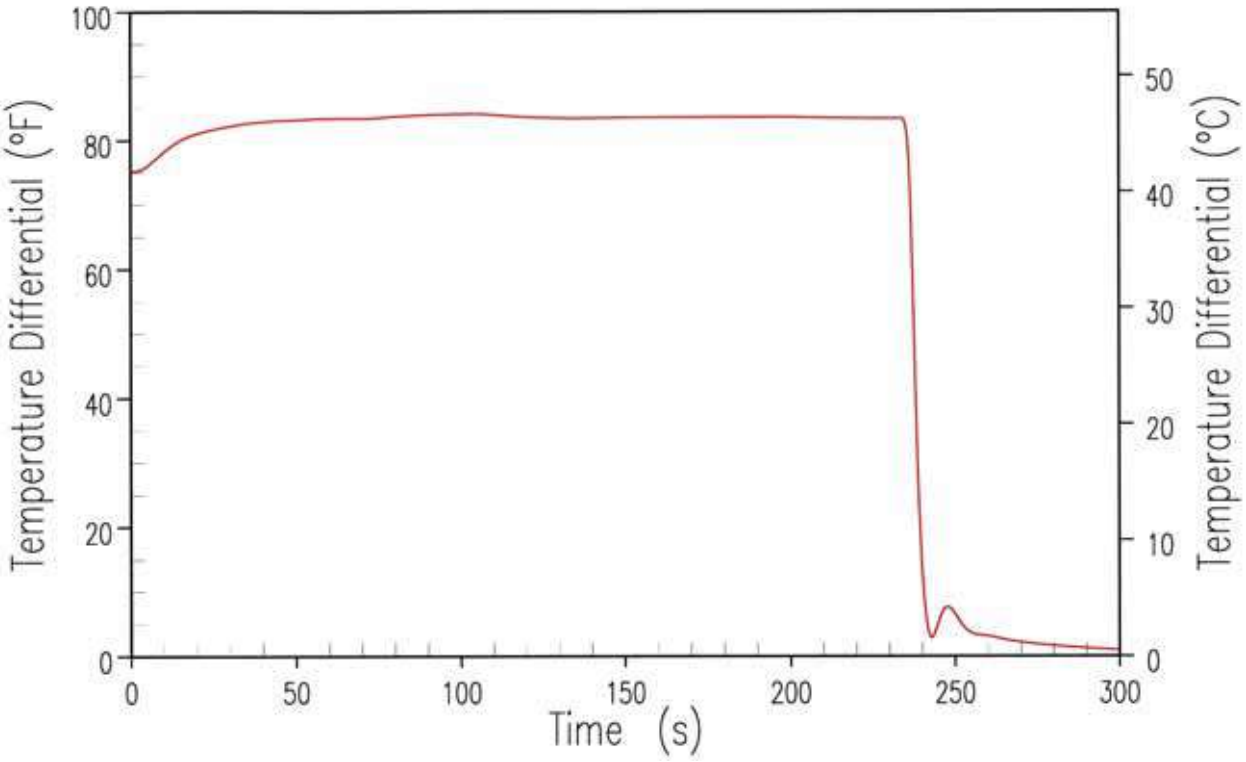


Figure 9.1.2-2. DBA Feedwater Control Valve Malfunction Loop ΔT

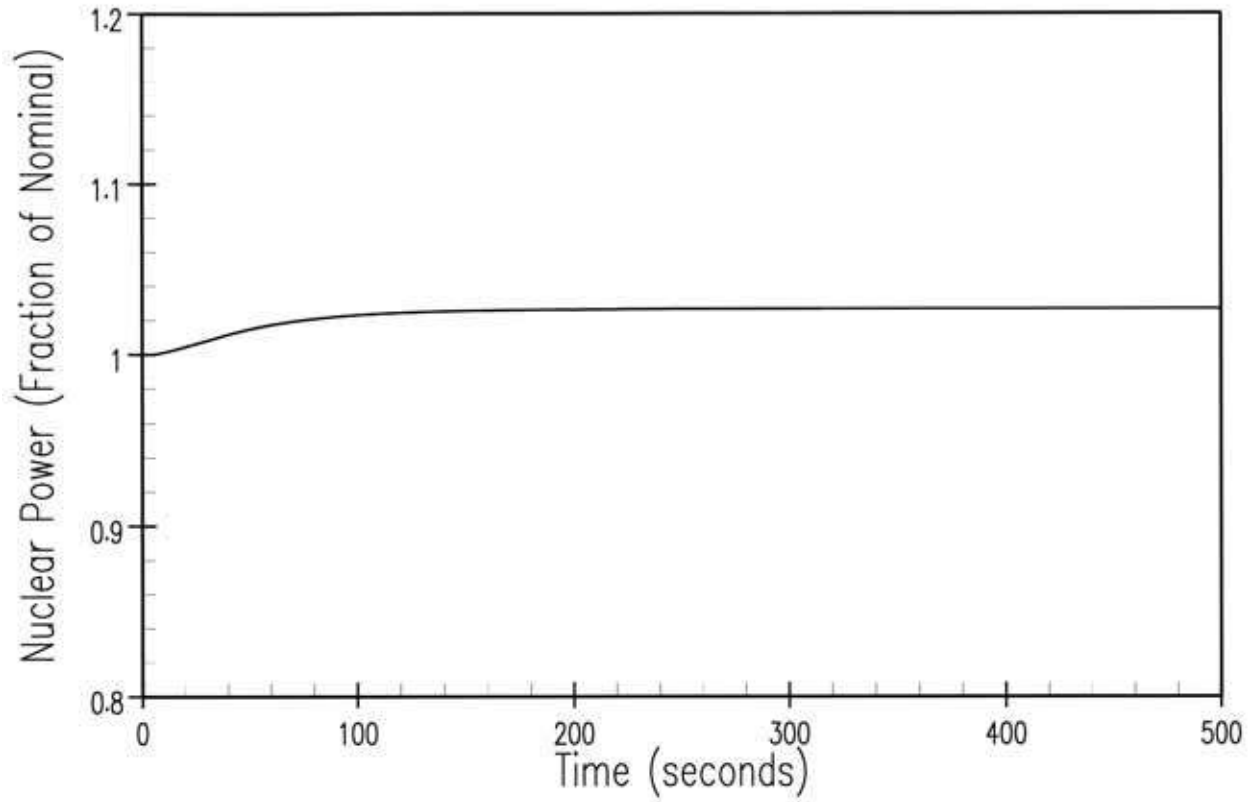


Figure 9.1.3-1. DBA Nuclear Power Versus Time for 10-percent Step Load Increase, Manual Control and Minimum Moderator Feedback

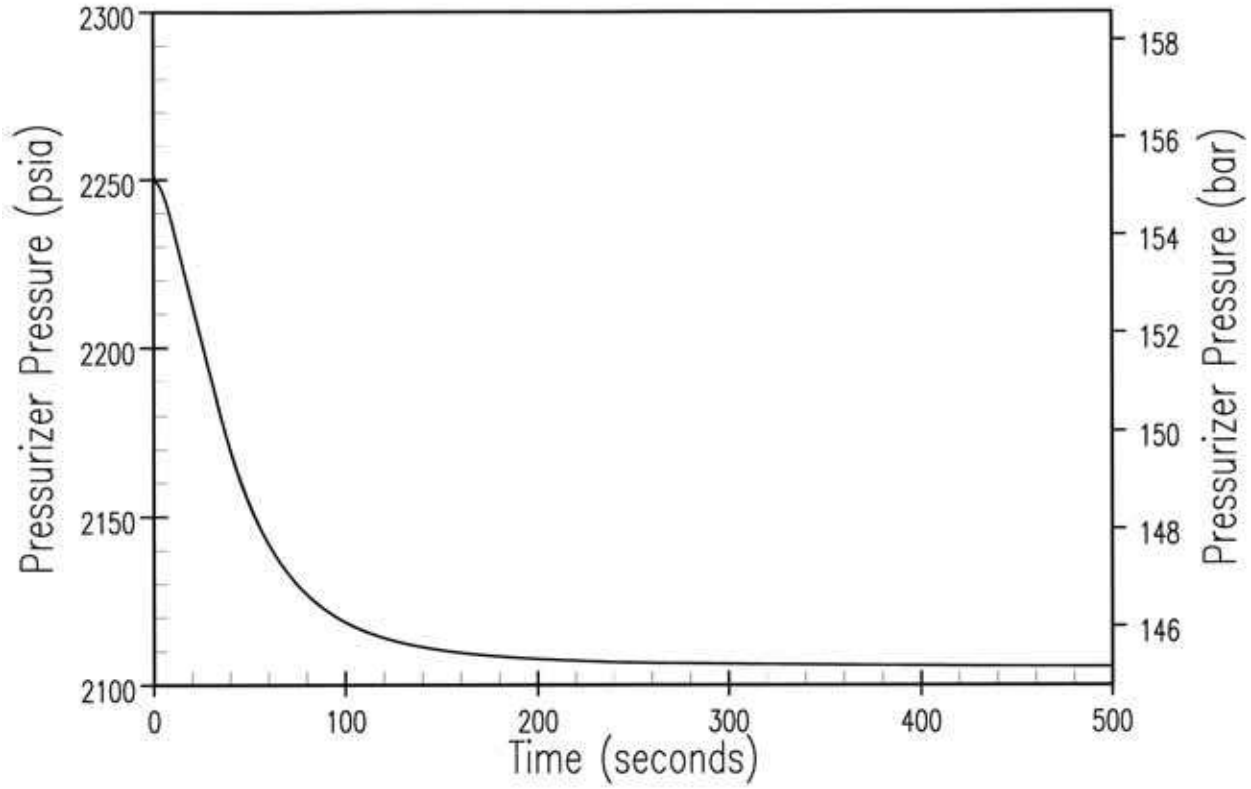


Figure 9.1.3-2. DBA Pressuriser Pressure Versus Time for 10-percent Step Load Increase, Manual Control and Minimum Moderator Feedback

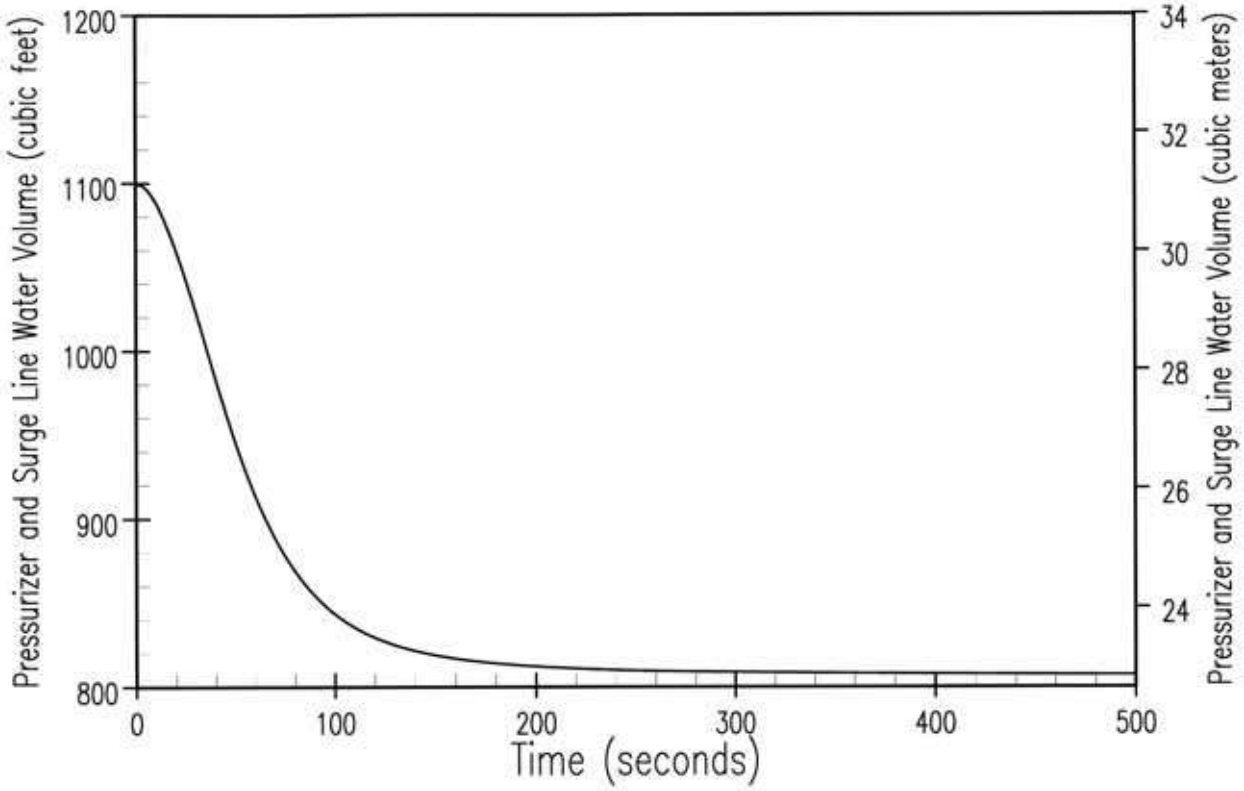


Figure 9.1.3-3. Pressuriser Water Volume Versus Time for 10-percent Step Load Increase, Manual Control and Minimum Moderator Feedback

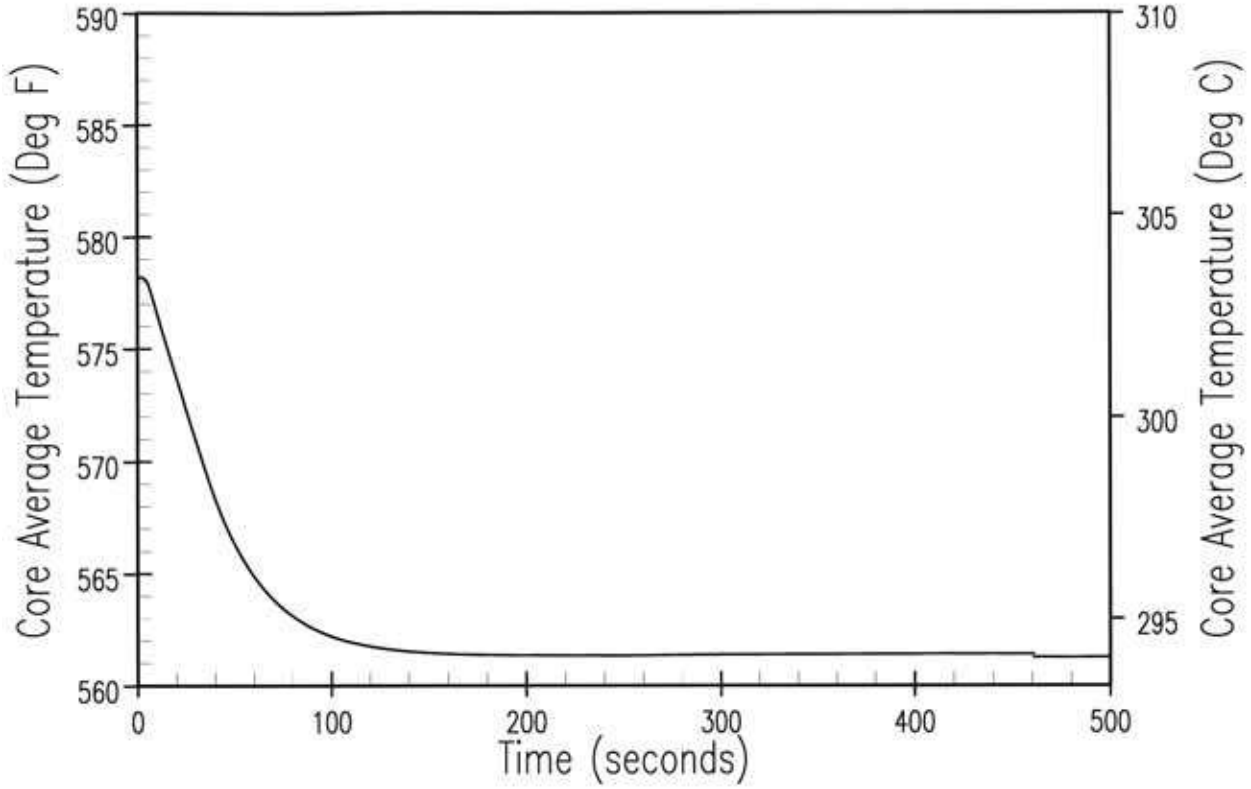


Figure 9.1.3-4. DBA Core Average Temperature Versus Time for 10-percent Step Load Increase, Manual Control and Minimum Moderator Feedback

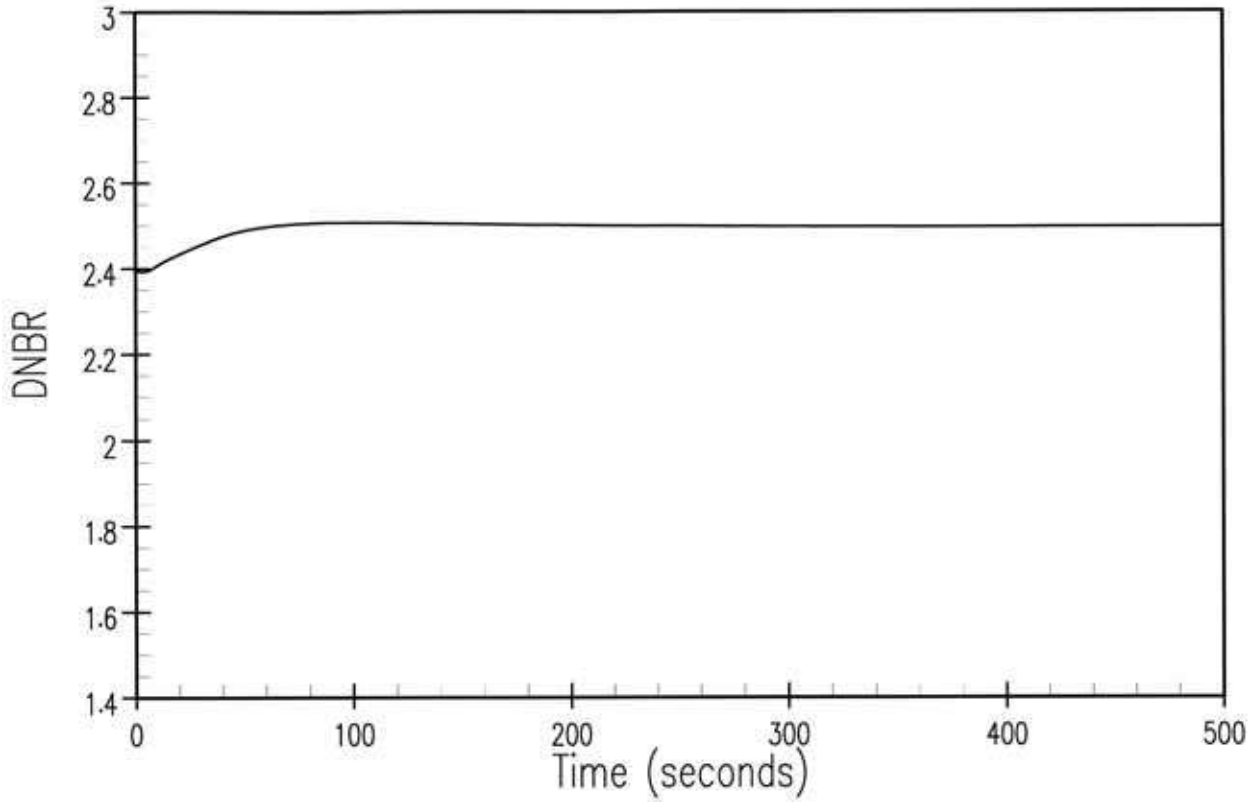


Figure 9.1.3-5. DBA DNBR Versus Time for 10-percent Step Load Increase, Manual Control and Minimum Moderator Feedback

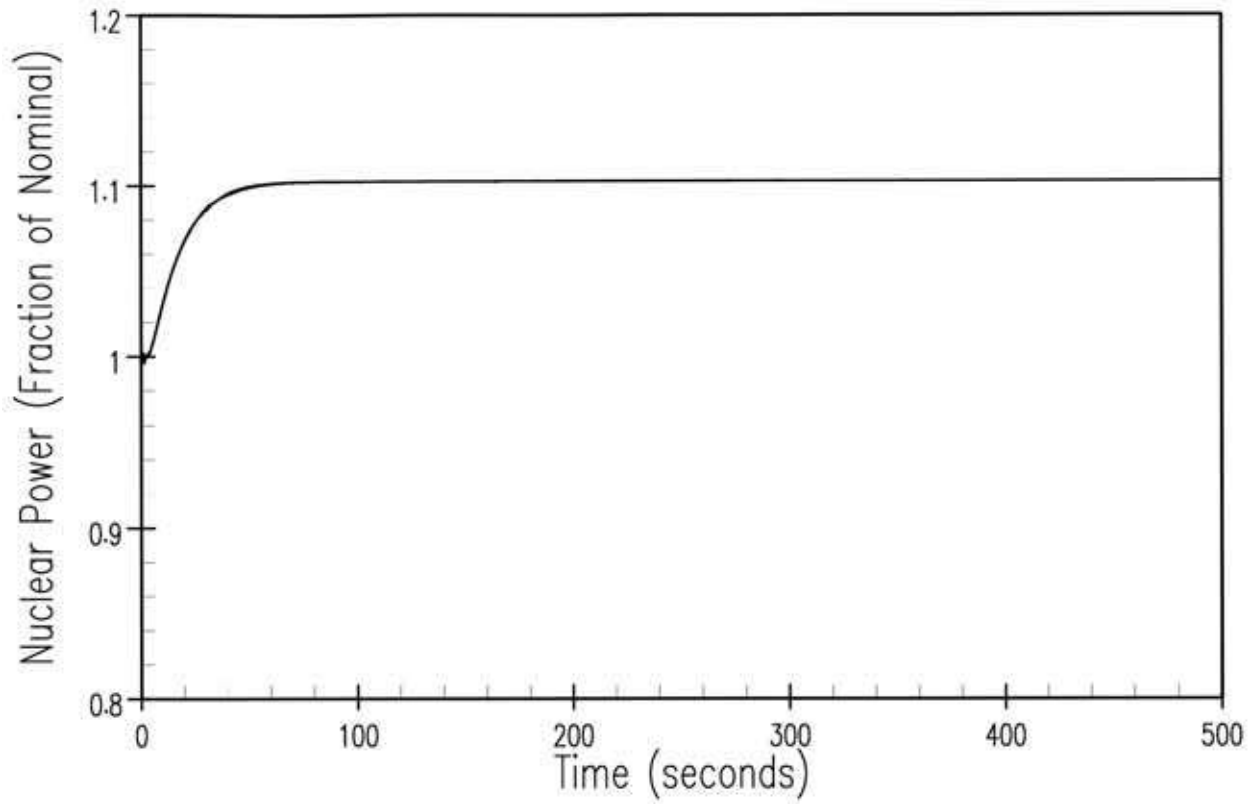


Figure 9.1.3-6. DBA Nuclear Power Versus Time for 10-percent Step Load Increase, Manual Control and Maximum Moderator Feedback

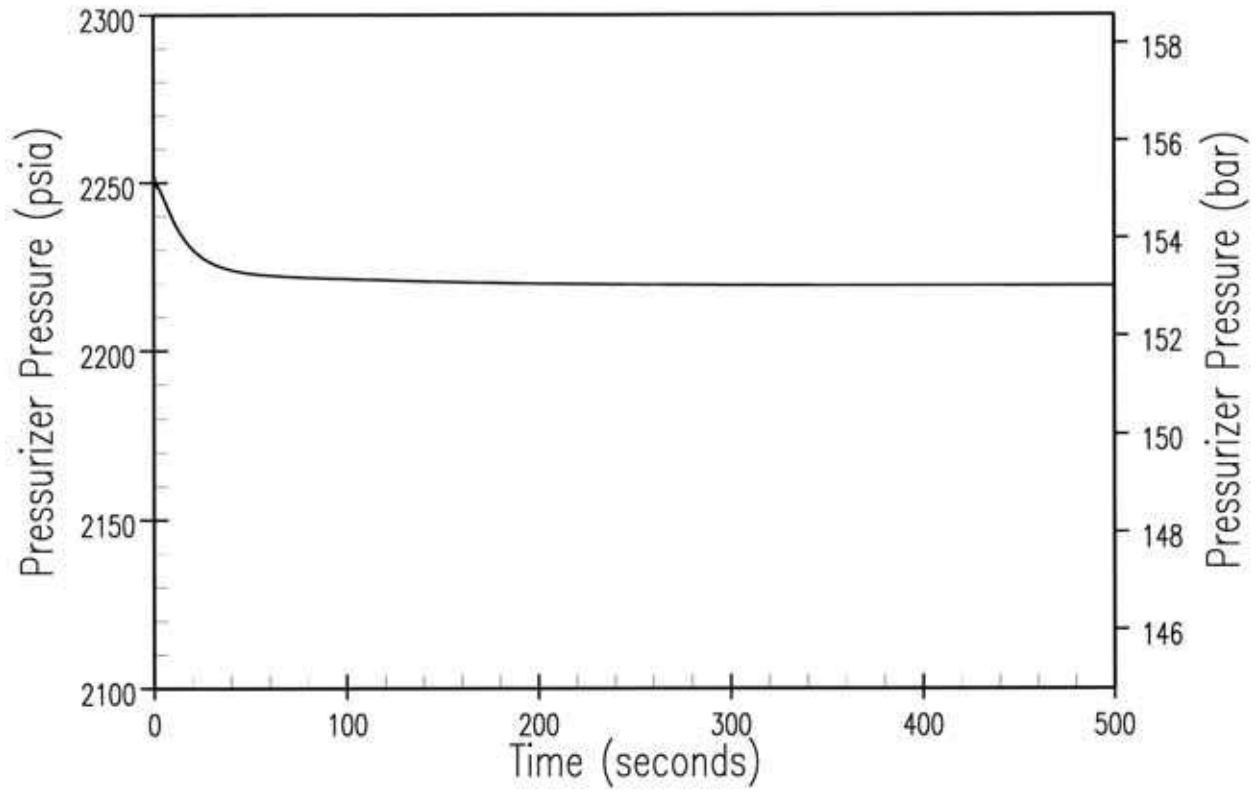


Figure 9.1.3-7. DBA Pressuriser Pressure Versus Time for 10-percent Step Load Increase, Manual Control and Maximum Moderator Feedback

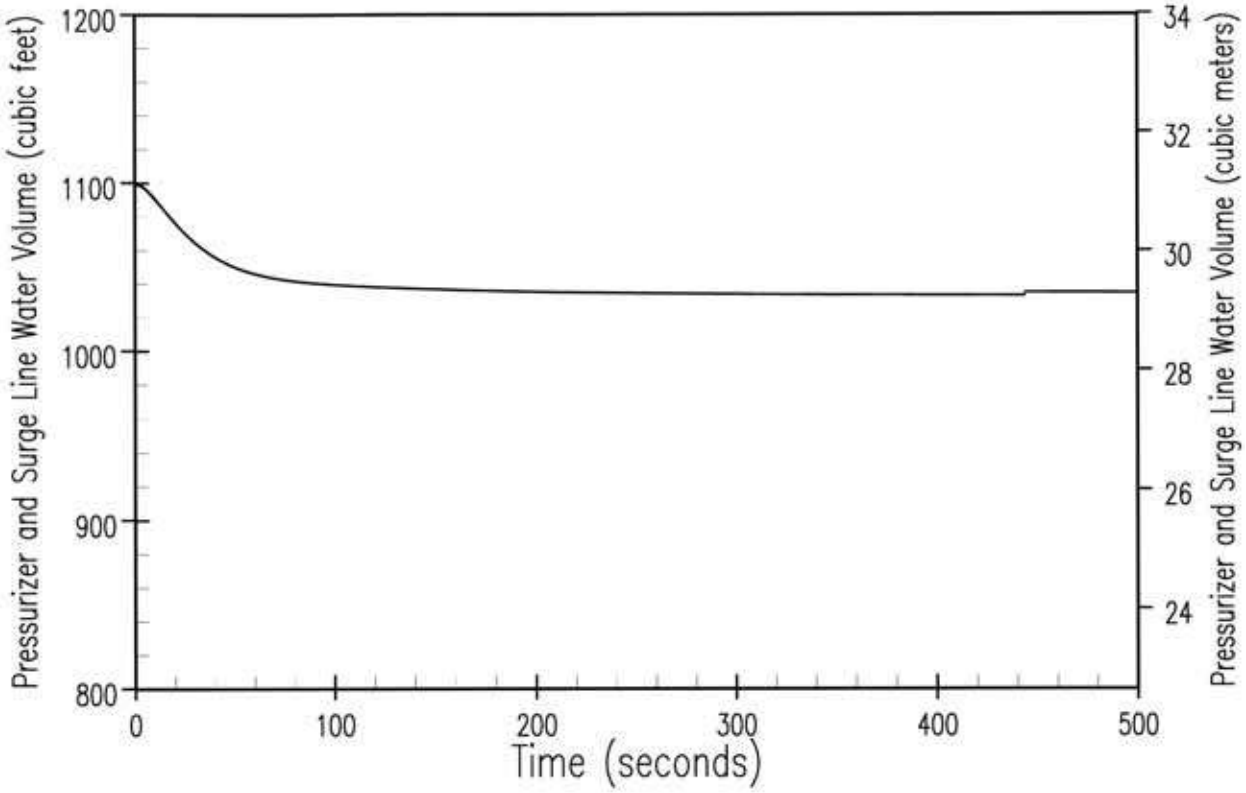


Figure 9.1.3-8. Pressuriser Water Volume Versus Time for 10-percent Step Load Increase, Manual Control and Maximum Moderator Feedback

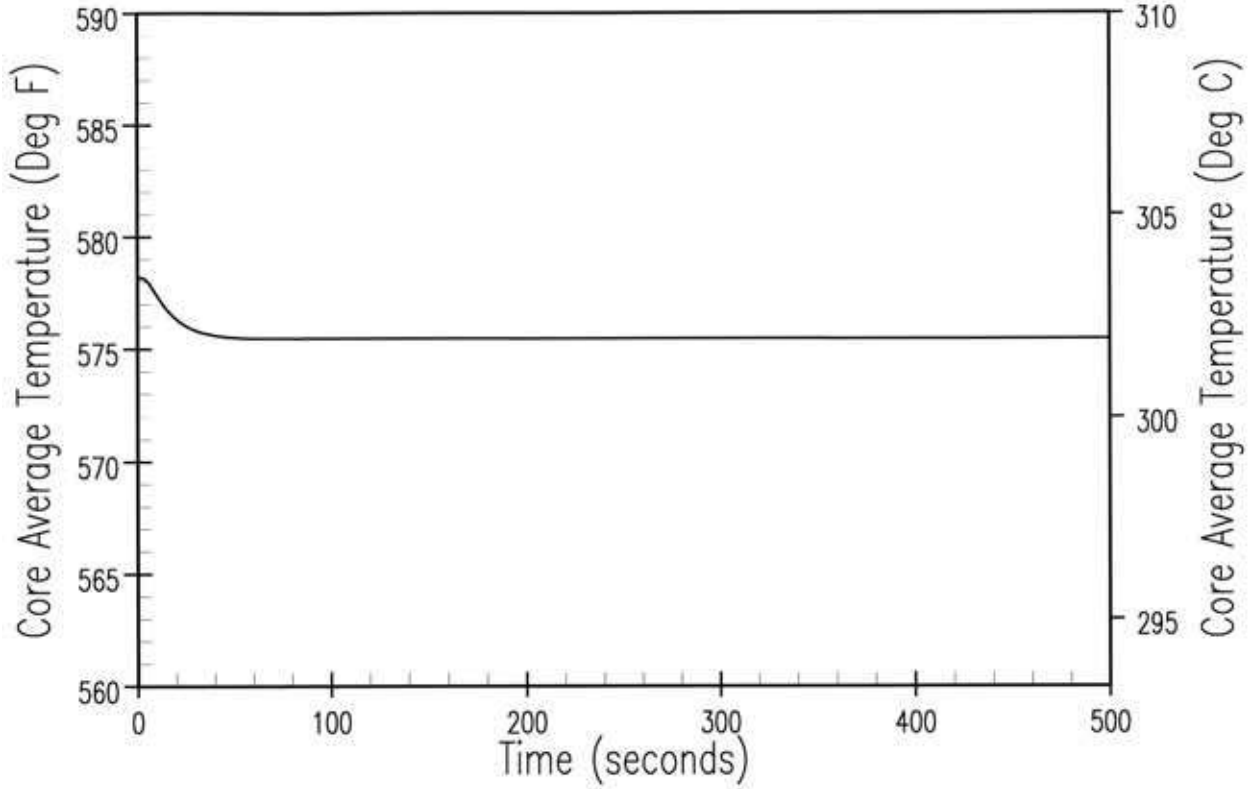


Figure 9.1.3-9. DBA Core Average Temperature Versus Time for 10-percent Step Load Increase, Manual Control and Maximum Moderator Feedback

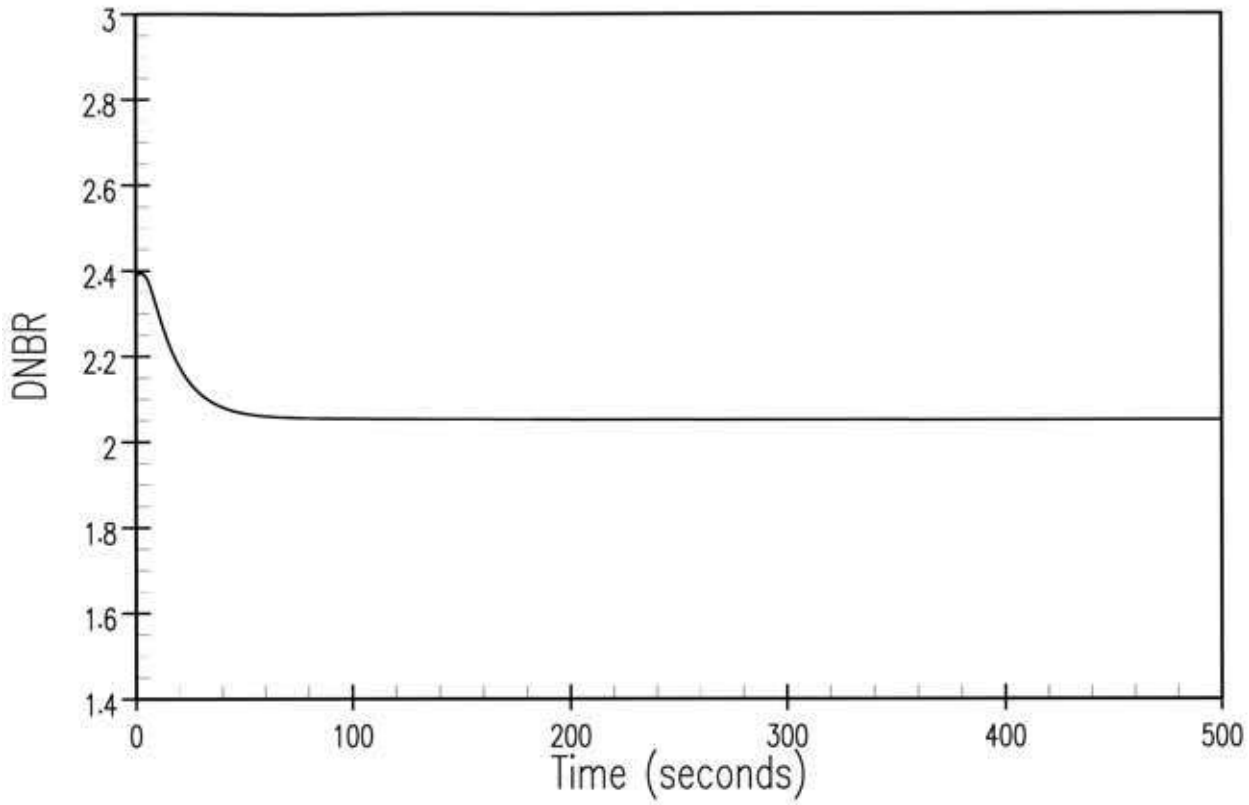


Figure 9.1.3-10. DBA DNBR Versus Time for 10-percent Step Load Increase, Manual Control and Maximum Moderator Feedback

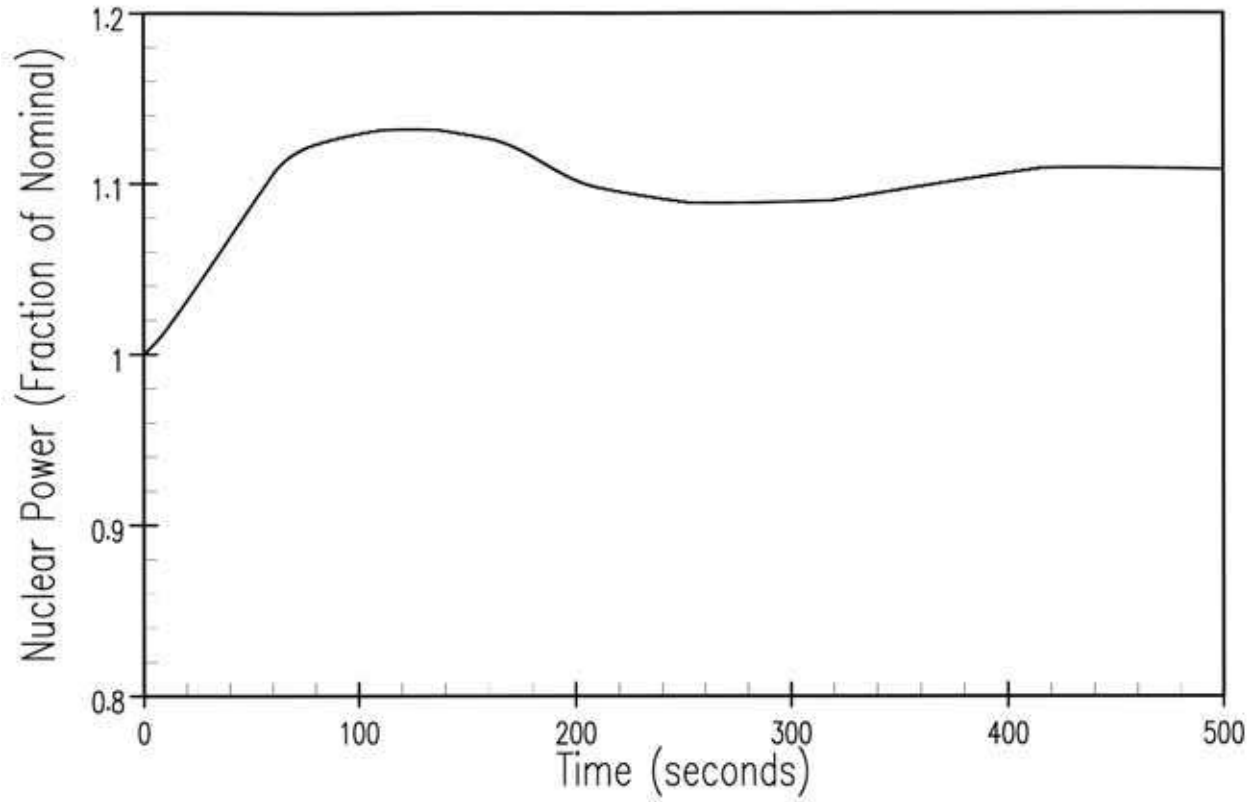


Figure 9.1.3-11. DBA Nuclear Power Versus Time for 10-percent Step Load Increase, Automatic Control and Minimum Moderator Feedback

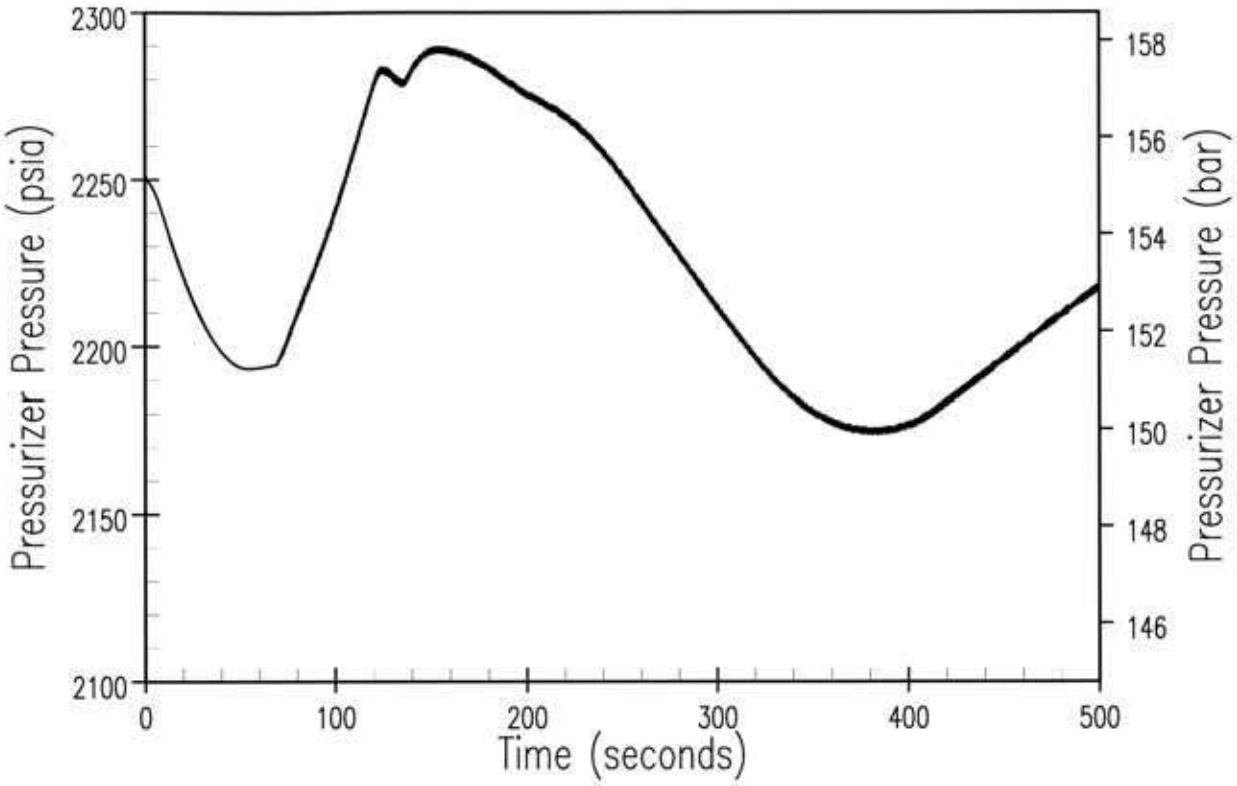


Figure 9.1.3-12. DBA Pressuriser Pressure Versus Time for 10-percent Step Load Increase, Automatic Control and Minimum Moderator Feedback

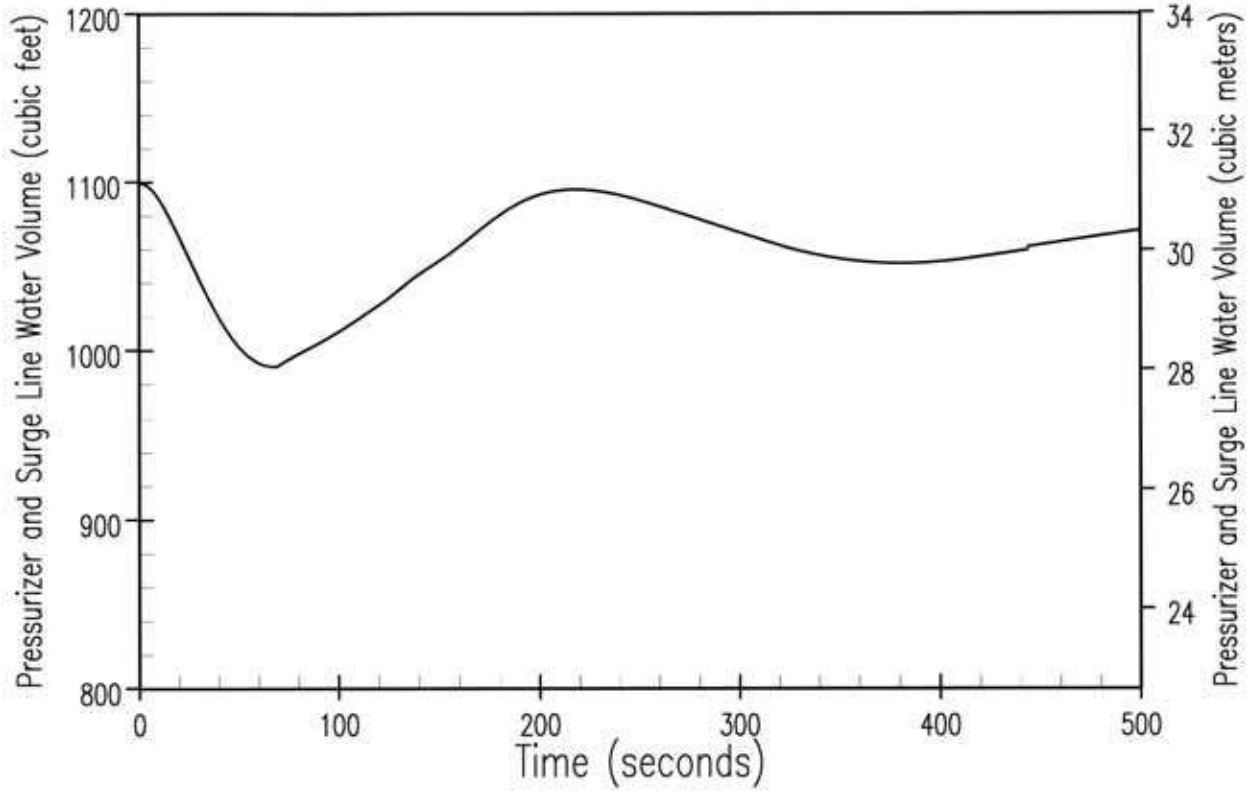


Figure 9.1.3-13. Pressuriser Water Volume Versus Time for 10-percent Step Load Increase, Automatic Control and Minimum Moderator Feedback

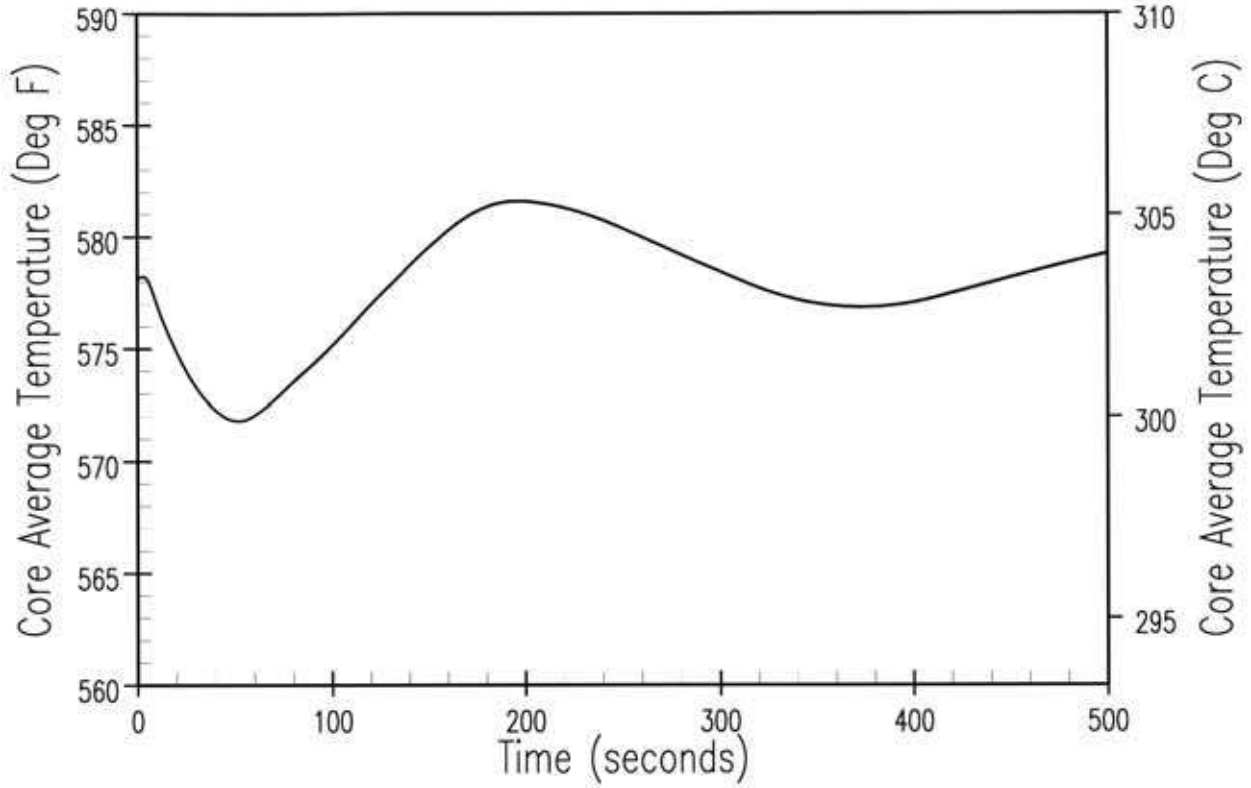


Figure 9.1.3-14. DBA Core Average Temperature Versus Time for 10-percent Step Load Increase, Automatic Control and Minimum Moderator Feedback

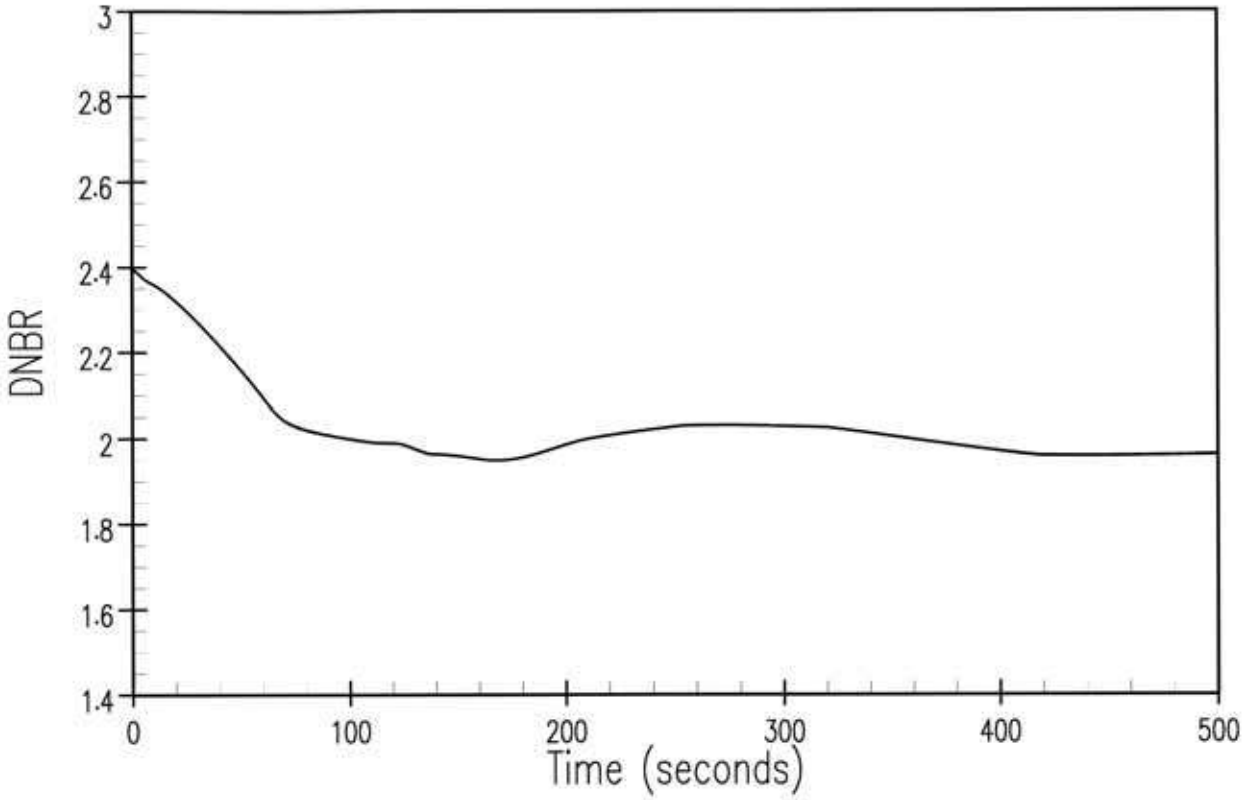


Figure 9.1.3-15. DBA DNBR Versus Time for 10-percent Step Load Increase, Automatic Control and Minimum Moderator Feedback

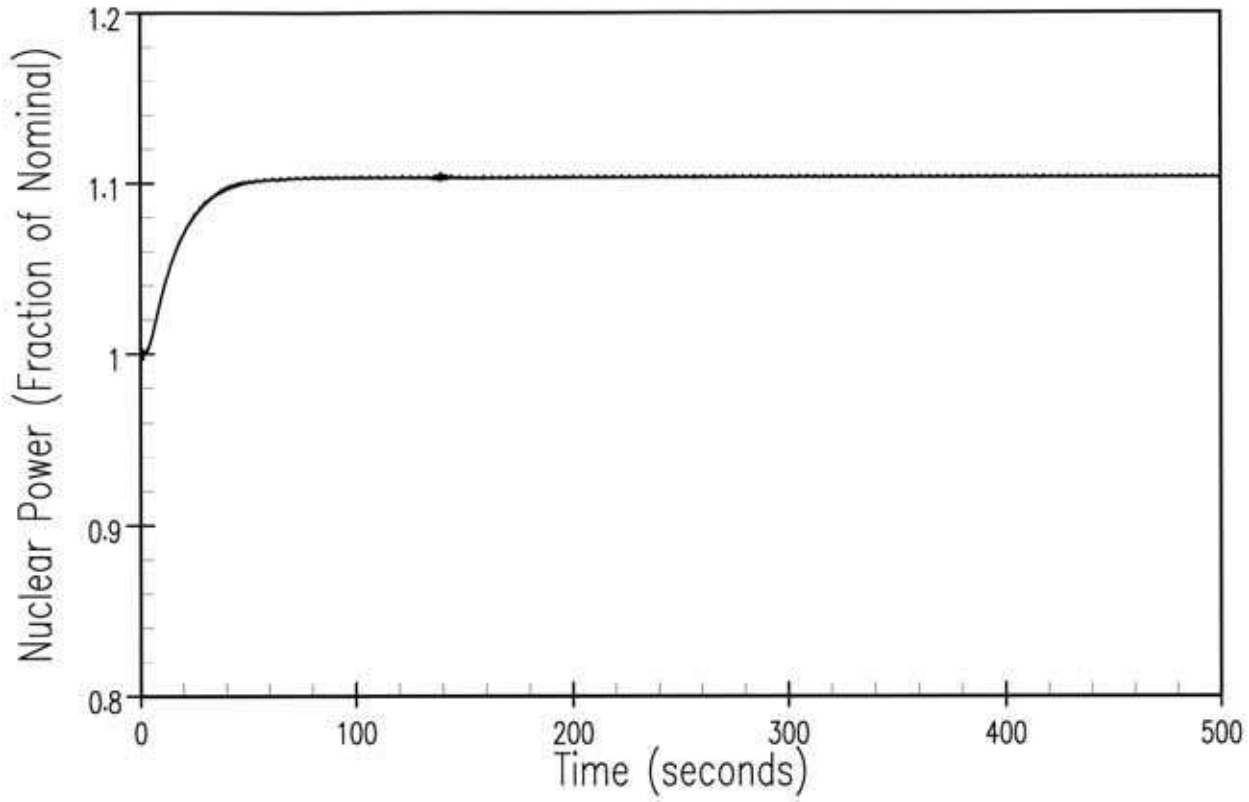


Figure 9.1.3-16. DBA Nuclear Power Versus Time for 10-percent Step Load Increase, Automatic Control and Maximum Moderator Feedback

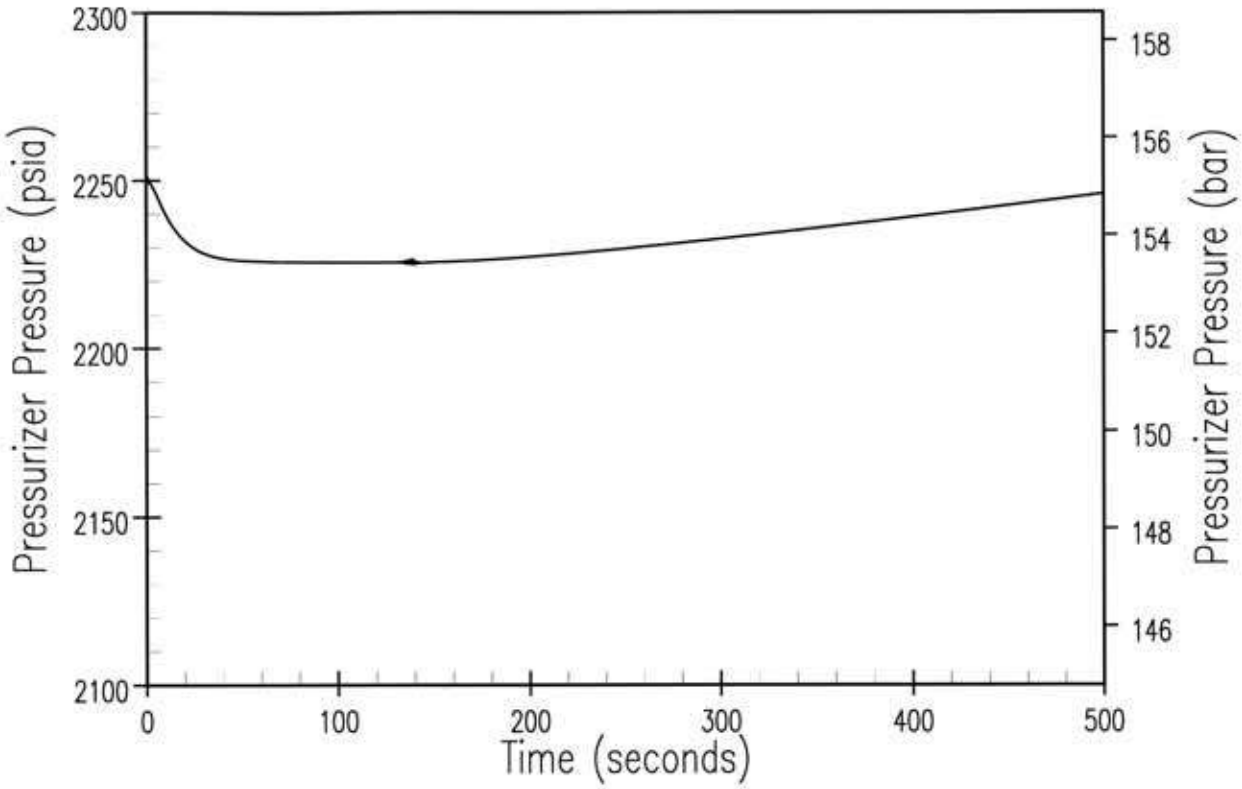


Figure 9.1.3-17. DBA Pressuriser Pressure Versus Time for 10-percent Step Load Increase, Automatic Control and Maximum Moderator Feedback

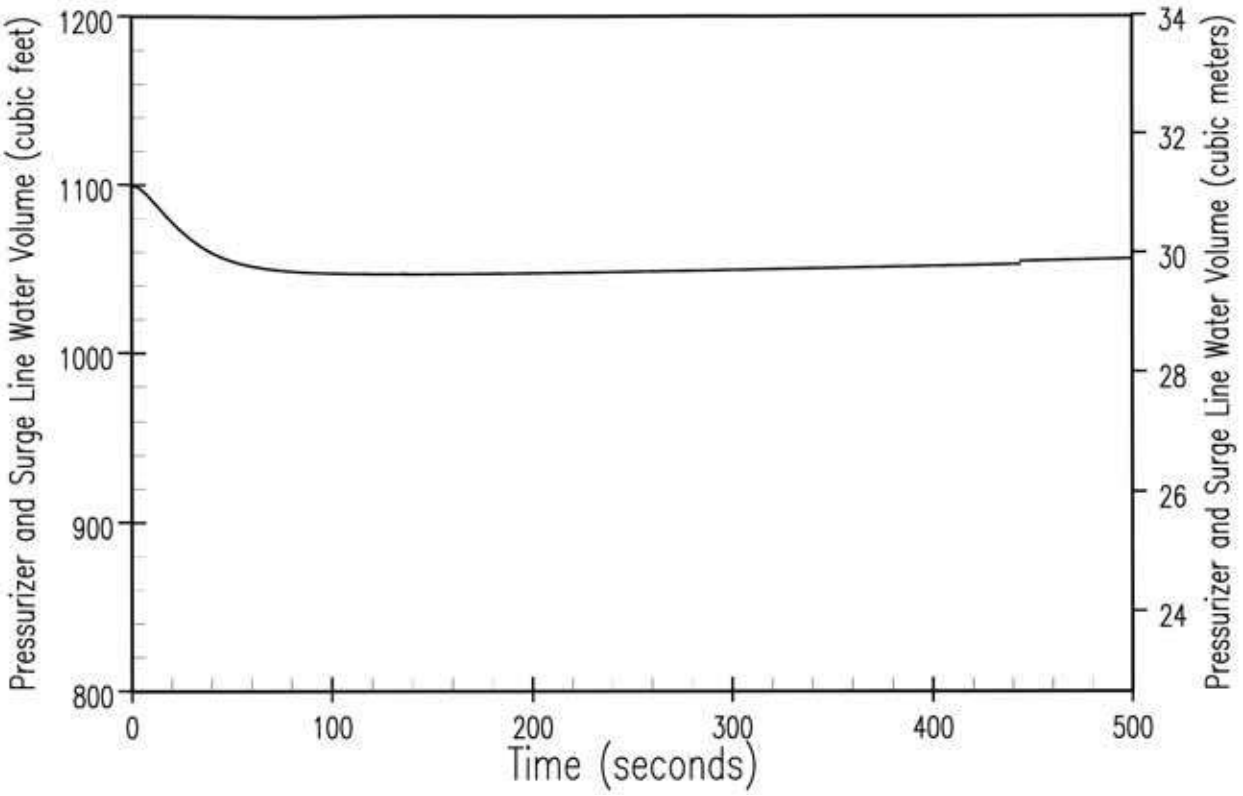


Figure 9.1.3-18. Pressuriser Water Volume Versus Time for 10-percent Step Load Increase, Automatic Control and Maximum Moderator Feedback

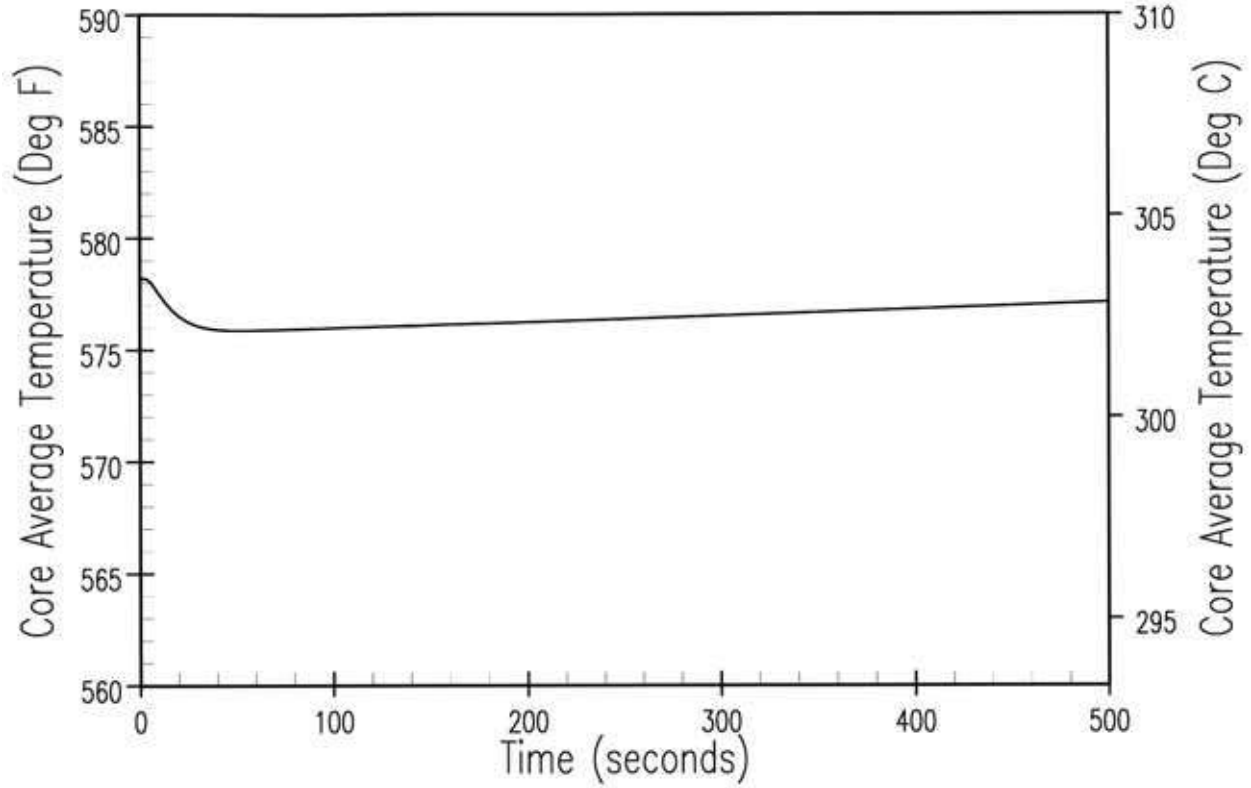


Figure 9.1.3-19. DBA Core Average Temperature Versus Time for 10-percent Step Load Increase, Automatic Control and Maximum Moderator Feedback

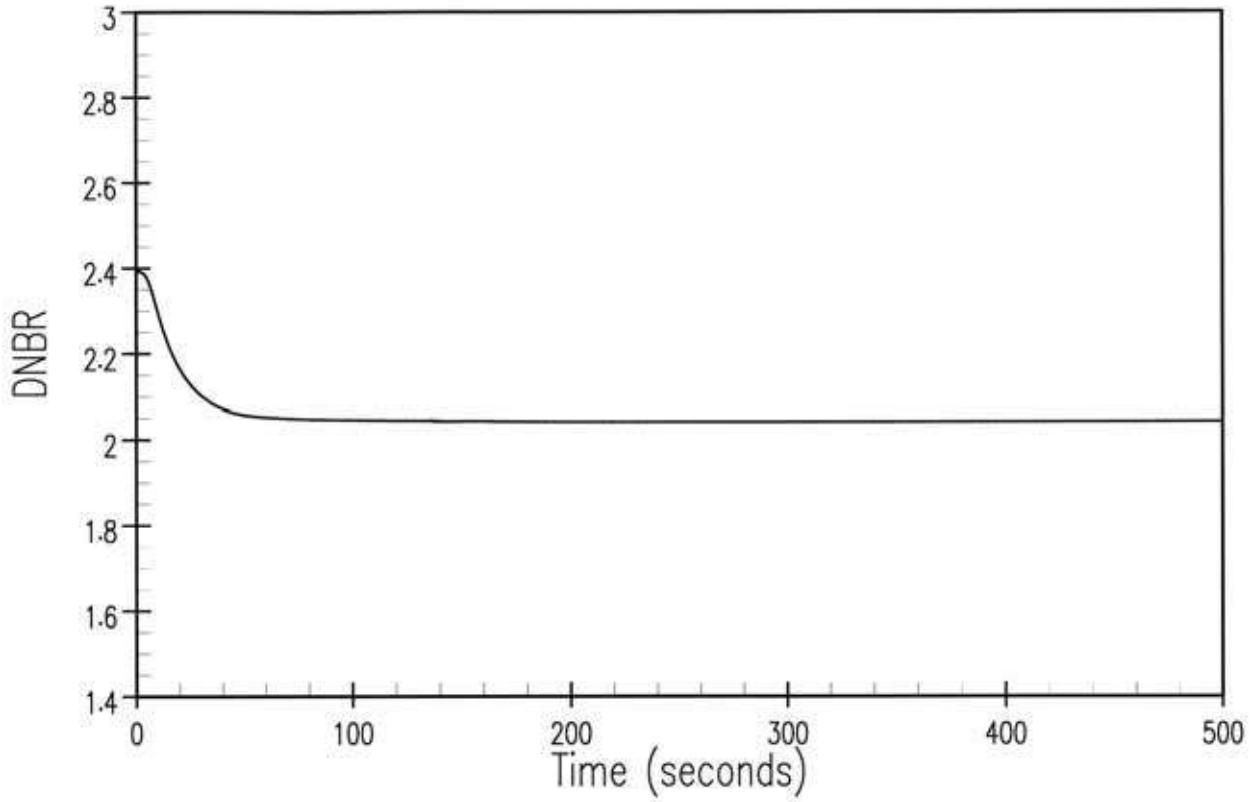


Figure 9.1.3-20. DBA DNBR Versus Time for 10-percent Step Load Increase, Automatic Control and Maximum Moderator Feedback

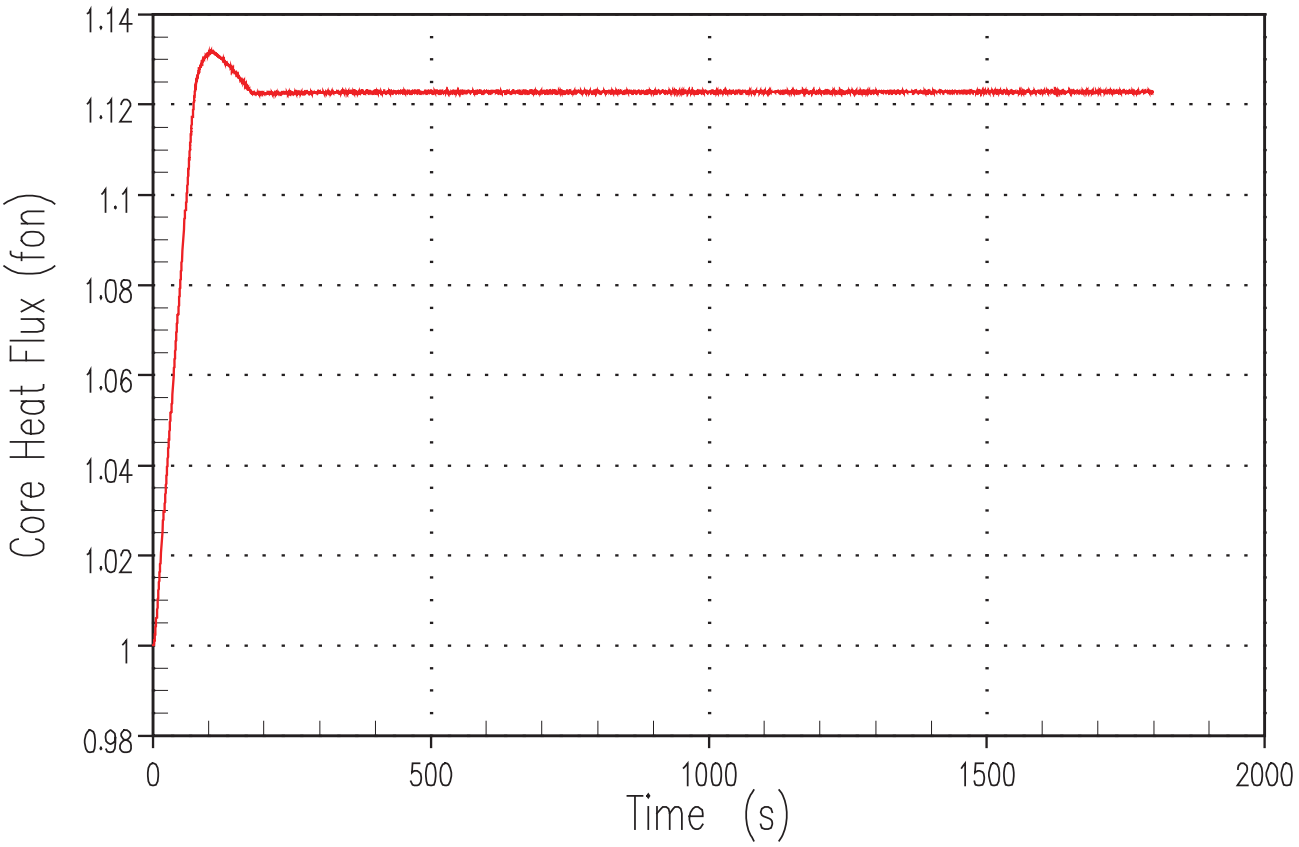


Figure 9.1.3-21. ATWT Core Heat Flux versus Time for an Inadvertent Opening of all Turbine Bypass Valves at Power with a PMS Common Cause Failure

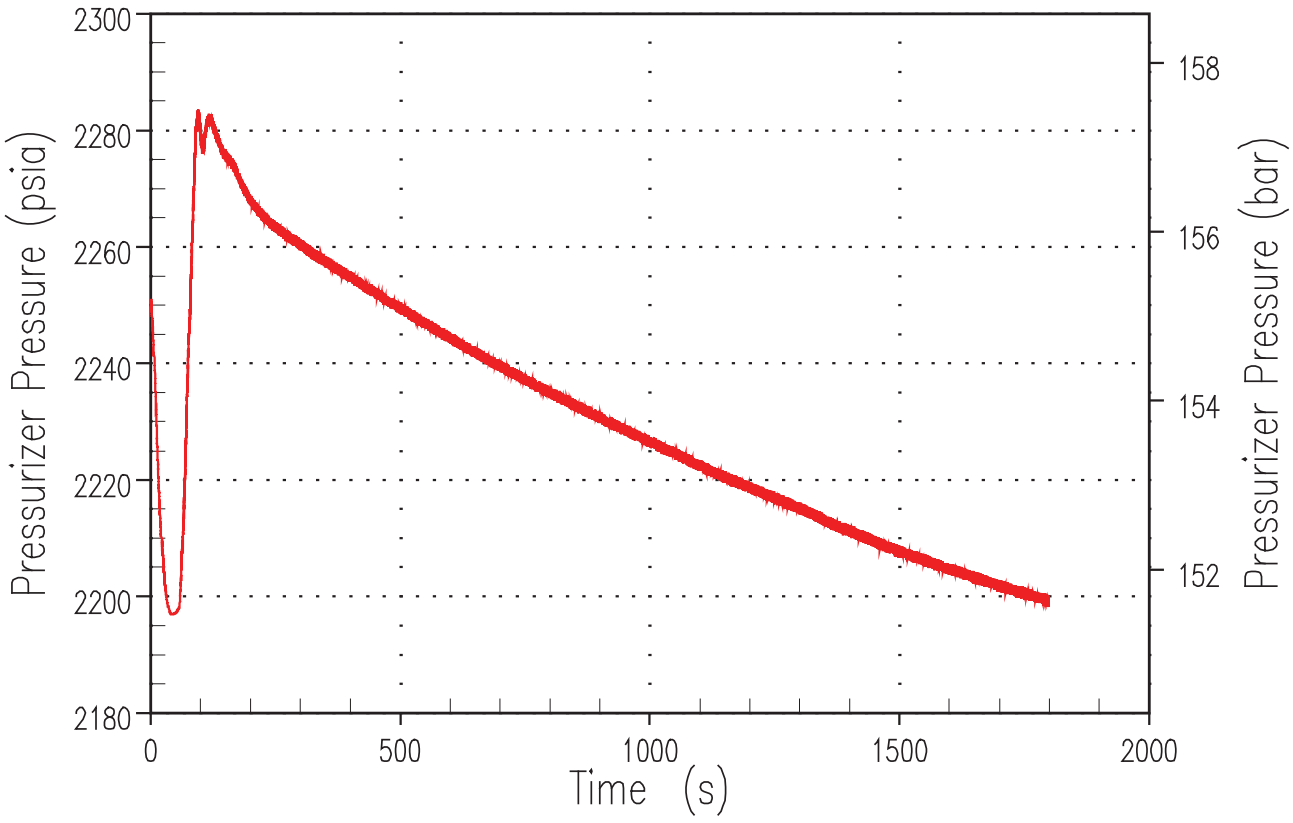


Figure 9.1.3-22. ATWT Pressuriser Pressure versus Time for an Inadvertent Opening of all Turbine Bypass Valves at Power with a PMS Common Cause Failure

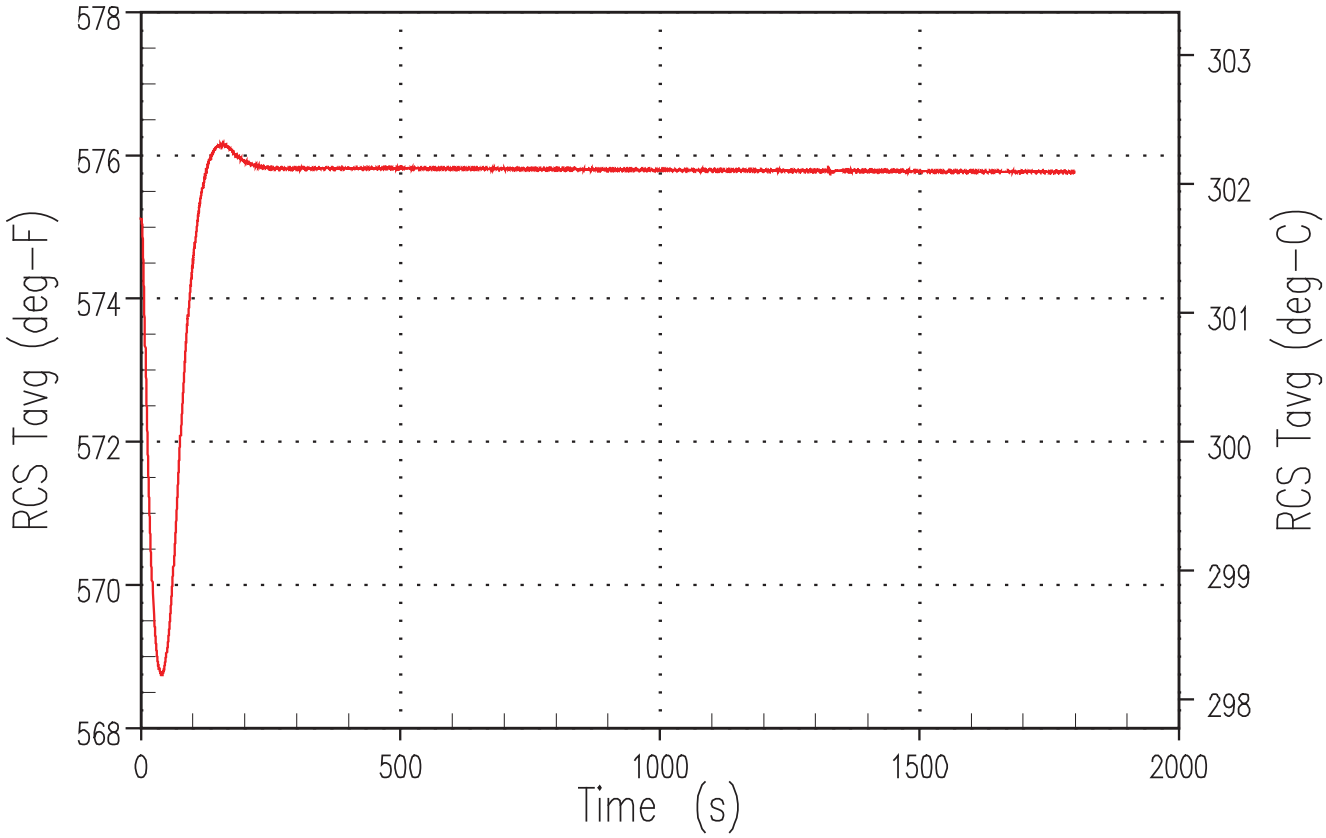


Figure 9.1.3-23. ATWT RCS Average Temperature versus Time for an Inadvertent Opening of all Turbine Bypass Valves at Power with a PMS Common Cause Failure

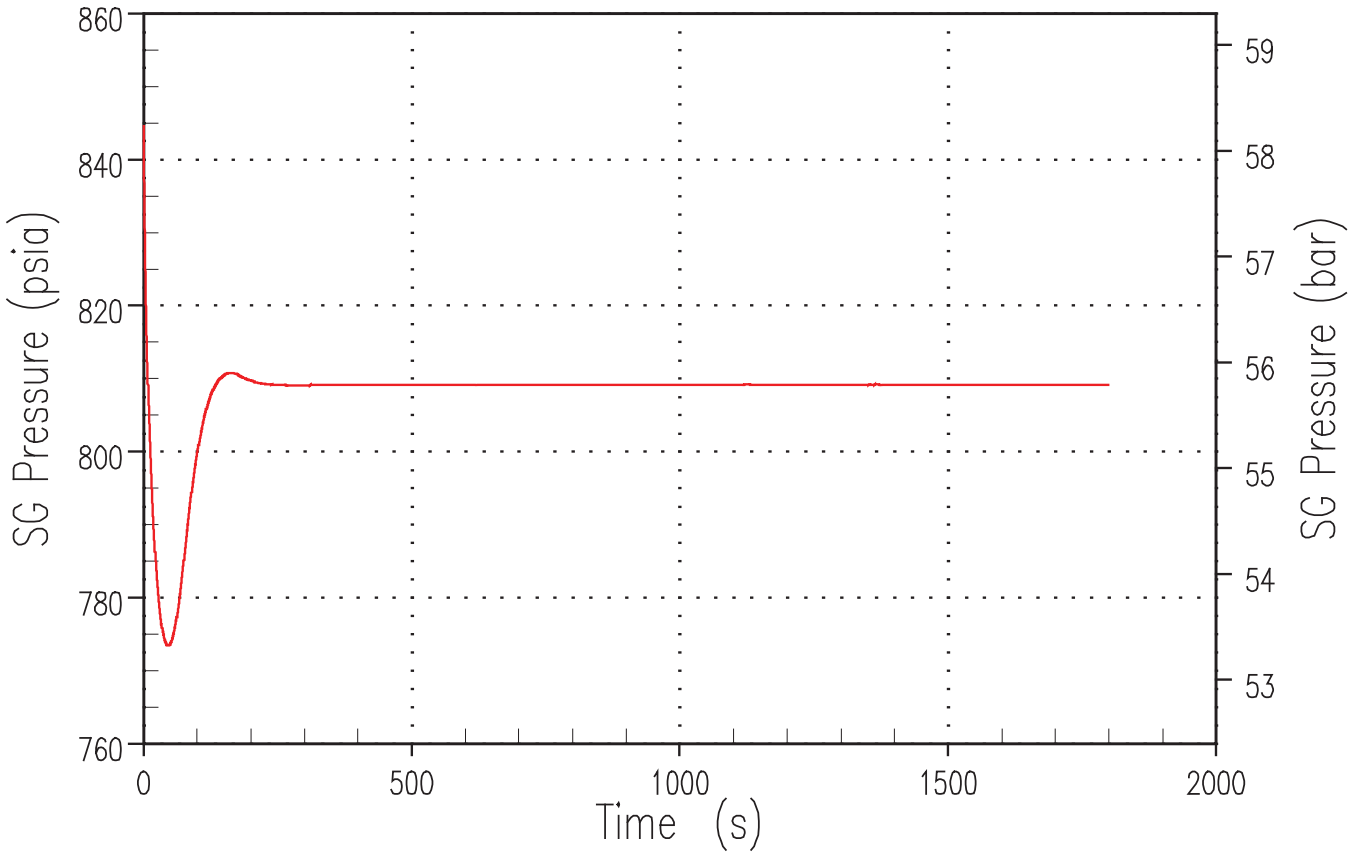


Figure 9.1.3-24. ATWT Steam Generator Pressure versus Time for an Inadvertent Opening of all Turbine Bypass Valves at Power with a PMS Common Cause Failure

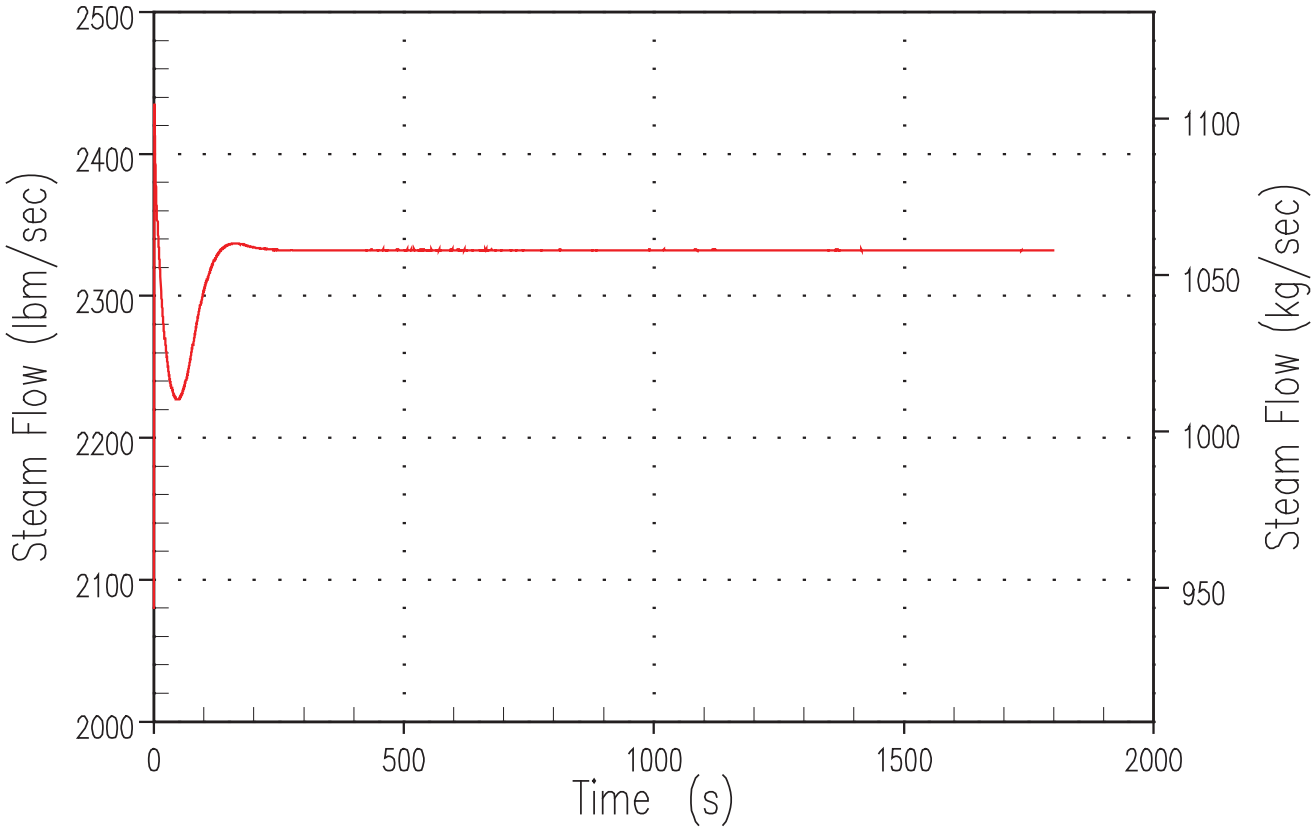


Figure 9.1.3-25. ATWT Steam Flow versus Time for an Inadvertent Opening of all Turbine Bypass Valves at Power with a PMS Common Cause Failure

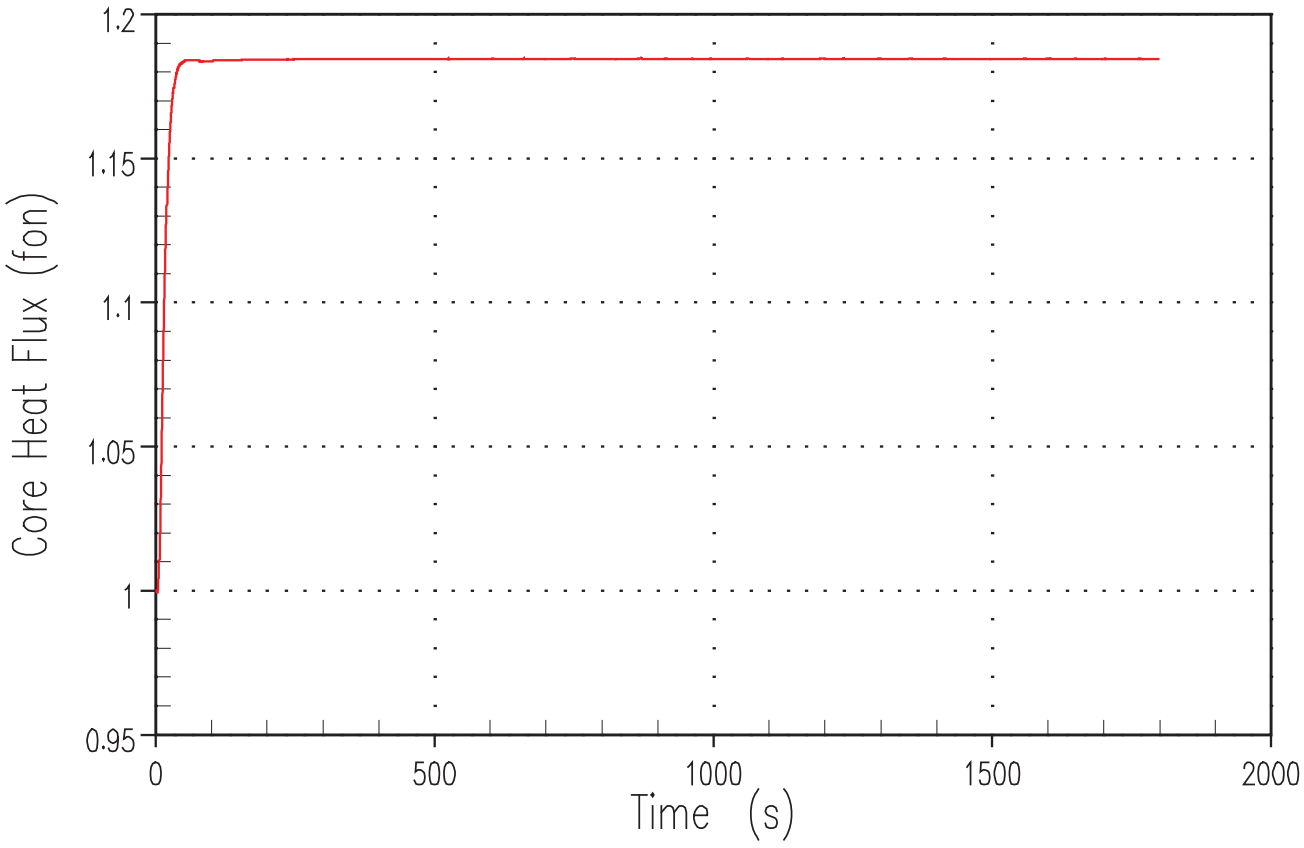


Figure 9.1.3-26. ATWT Core Heat Flux versus Time for a 0.045 m² Steam Line Break at Power with a PMS Common Cause Failure

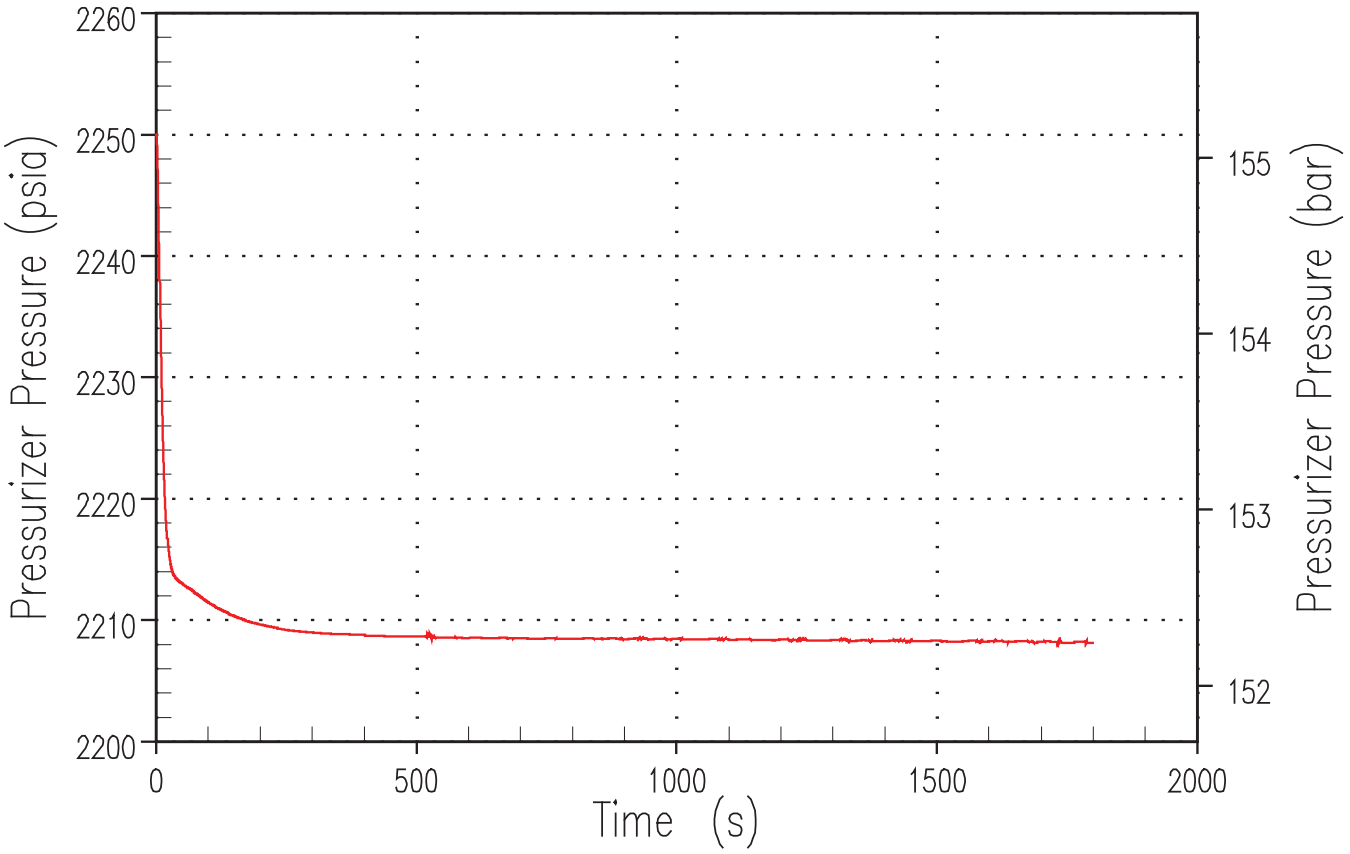


Figure 9.1.3-27. ATWT Pressuriser Pressure versus Time for a 0.045 m² Steam Line Break at Power with a PMS Common Cause Failure

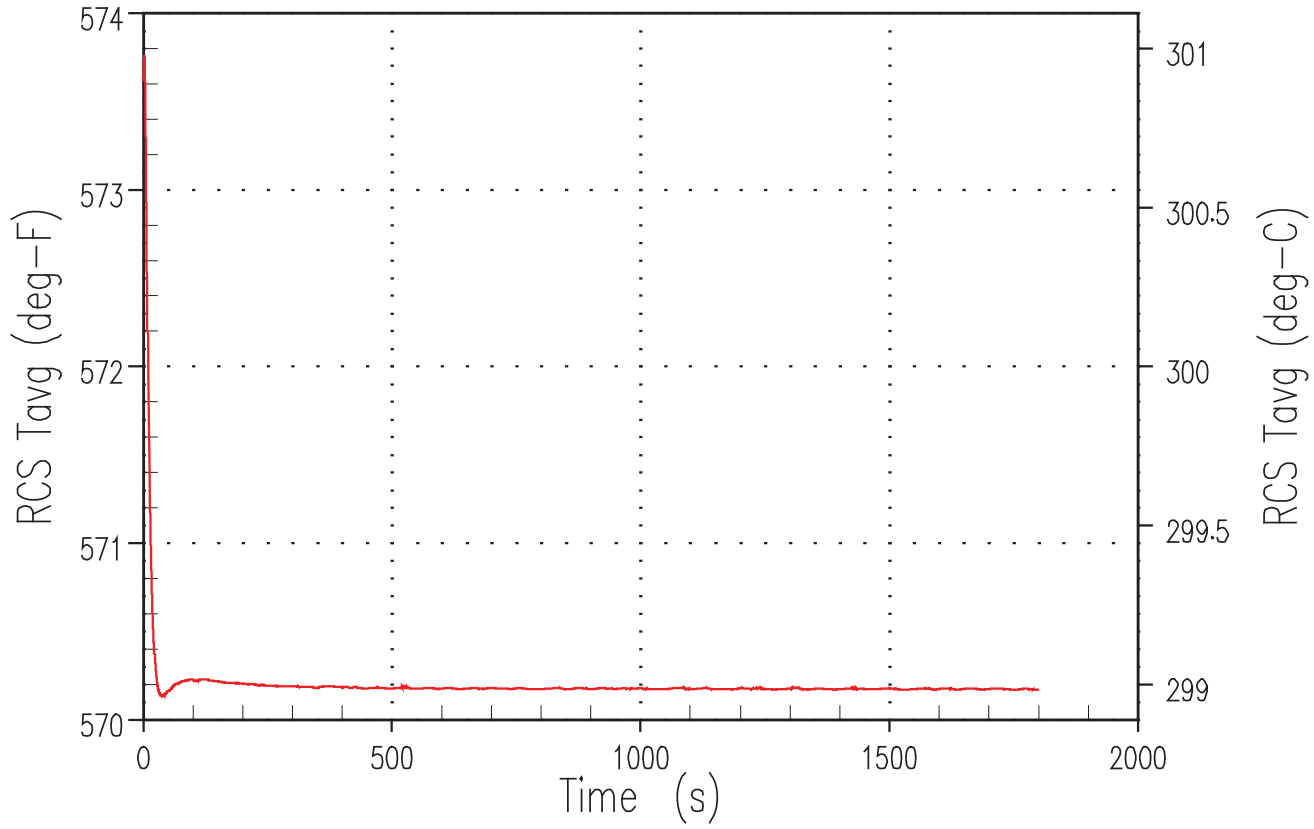


Figure 9.1.3-28. ATWT RCS Average Temperature versus Time for a 0.045 m² Steam Line Break at Power with a PMS Common Cause Failure

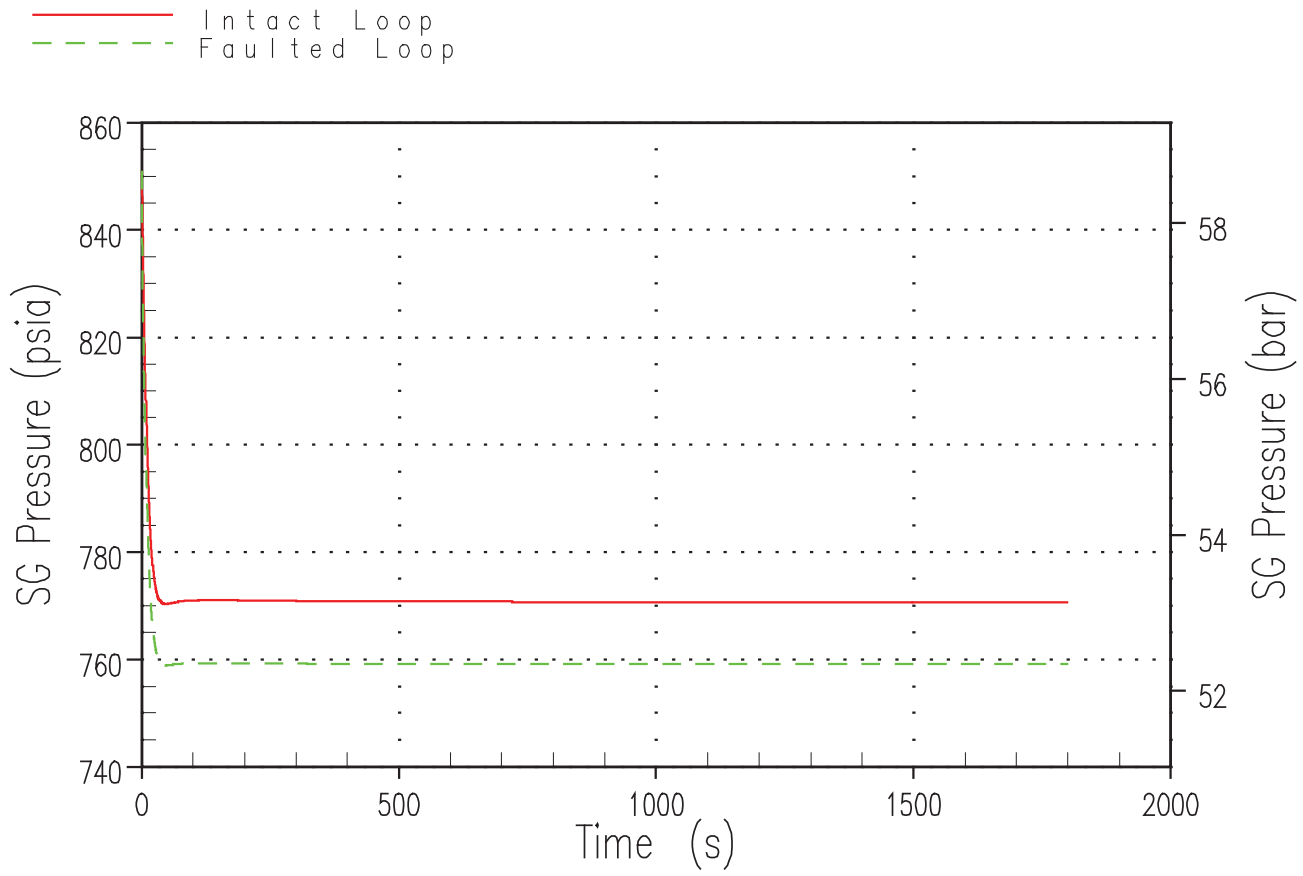


Figure 9.1.3-29. ATWT Steam Generator Pressure versus Time for a 0.045 m² Steam Line Break at Power with a PMS Common Cause Failure

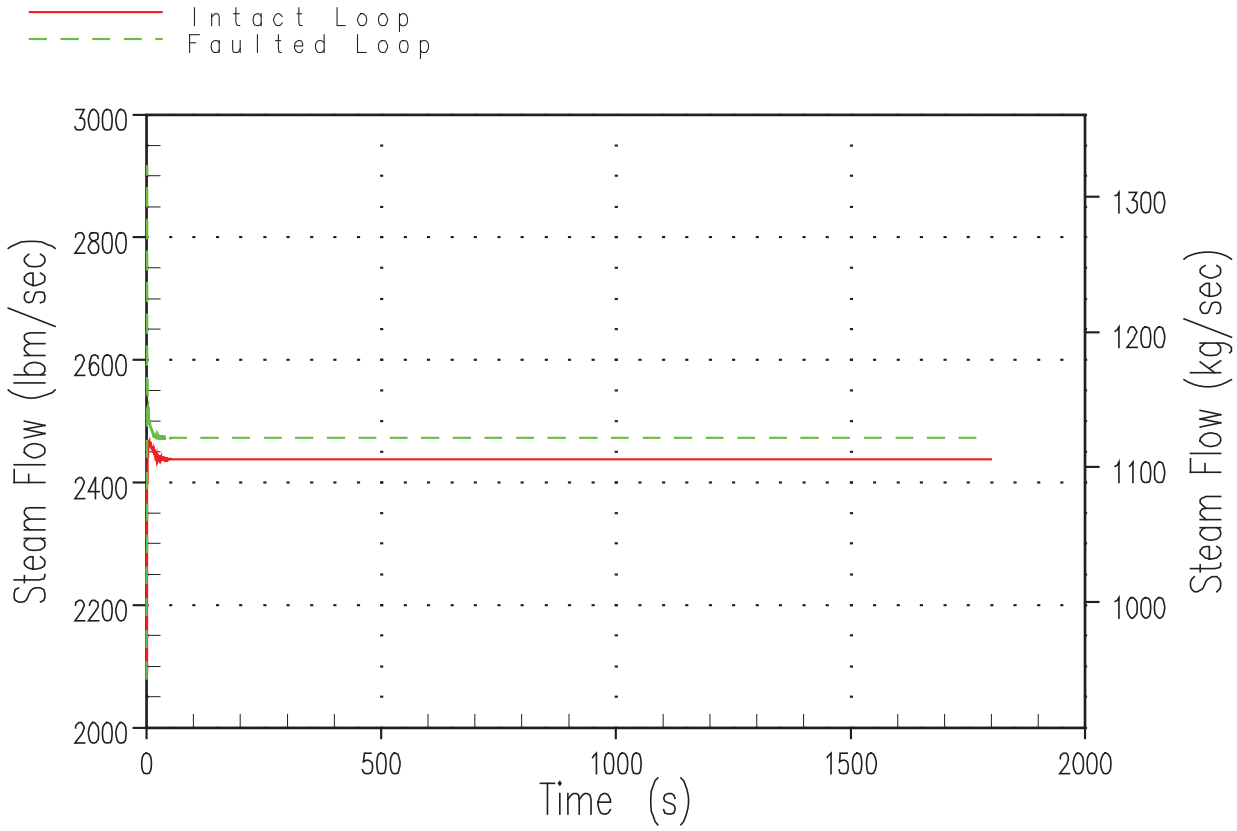


Figure 9.1.3-30. ATWT Steam Flow versus Time for a 0.045 m² Steam Line Break at Power with a PMS Common Cause Failure

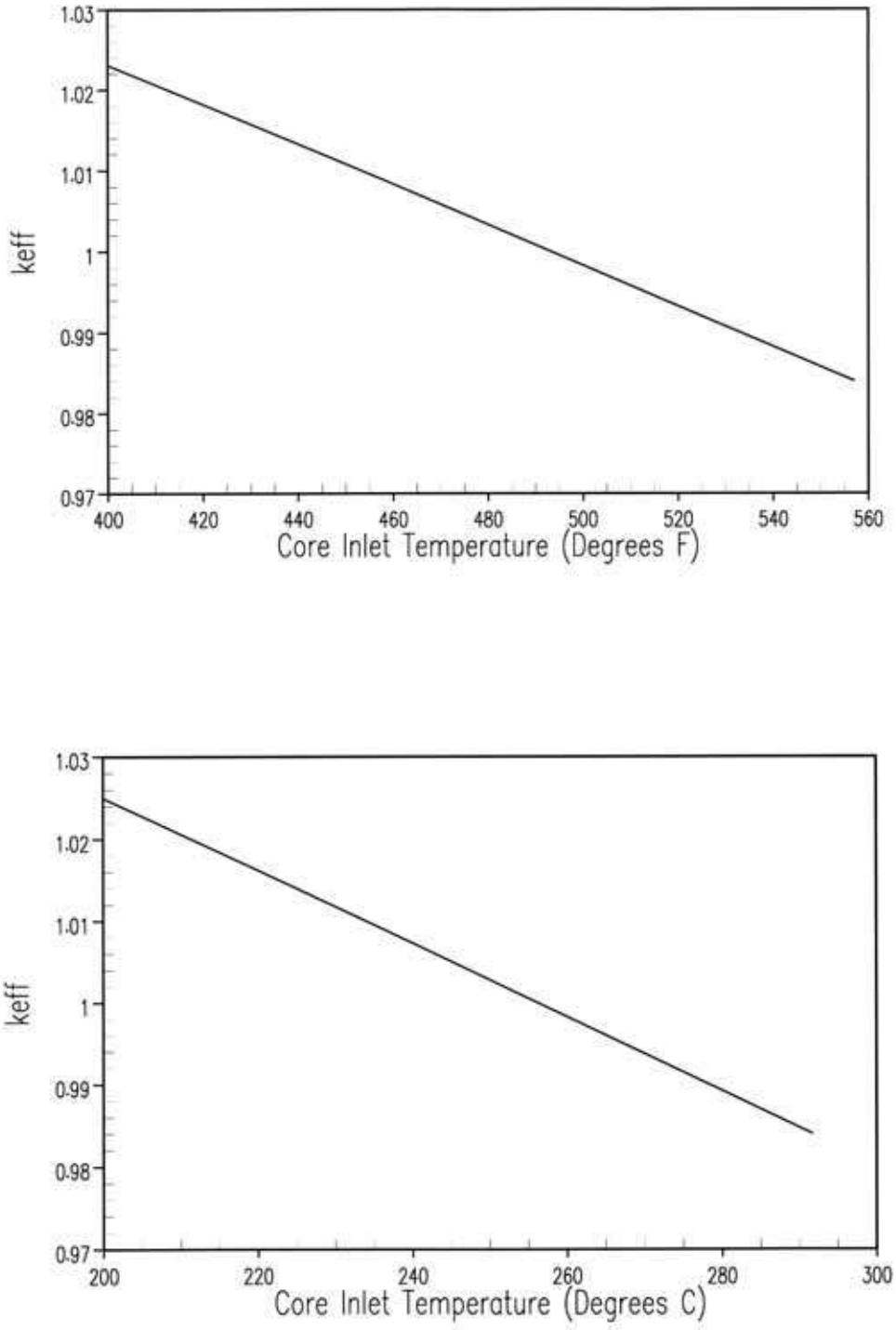


Figure 9.1.4-1. DBA K_{eff} Versus Core Inlet Temperature Steam Line Break Events

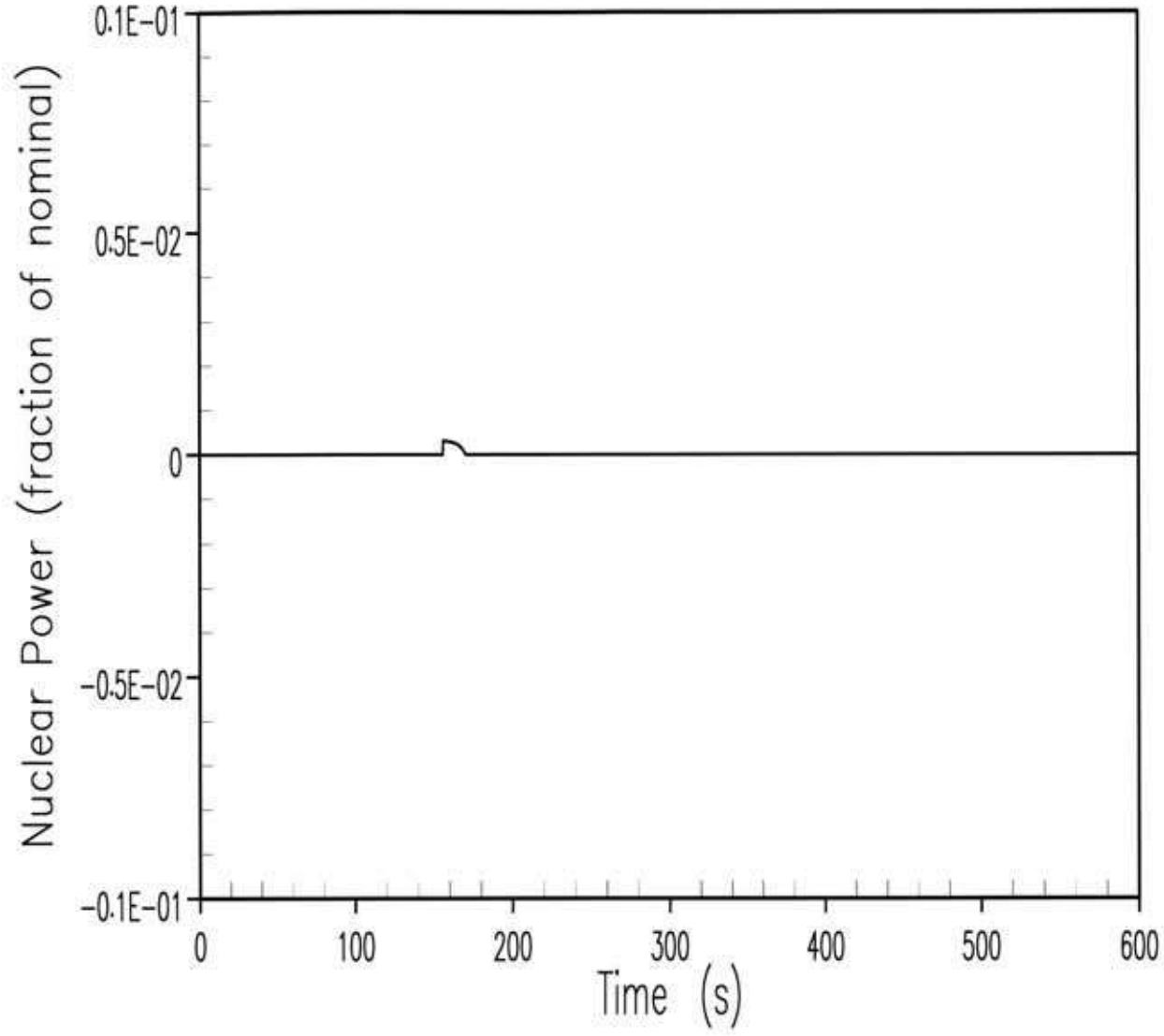


Figure 9.1.4-2. DBA Nuclear Power Transient Inadvertent Opening of a Steam Generator Relief or Safety Valve

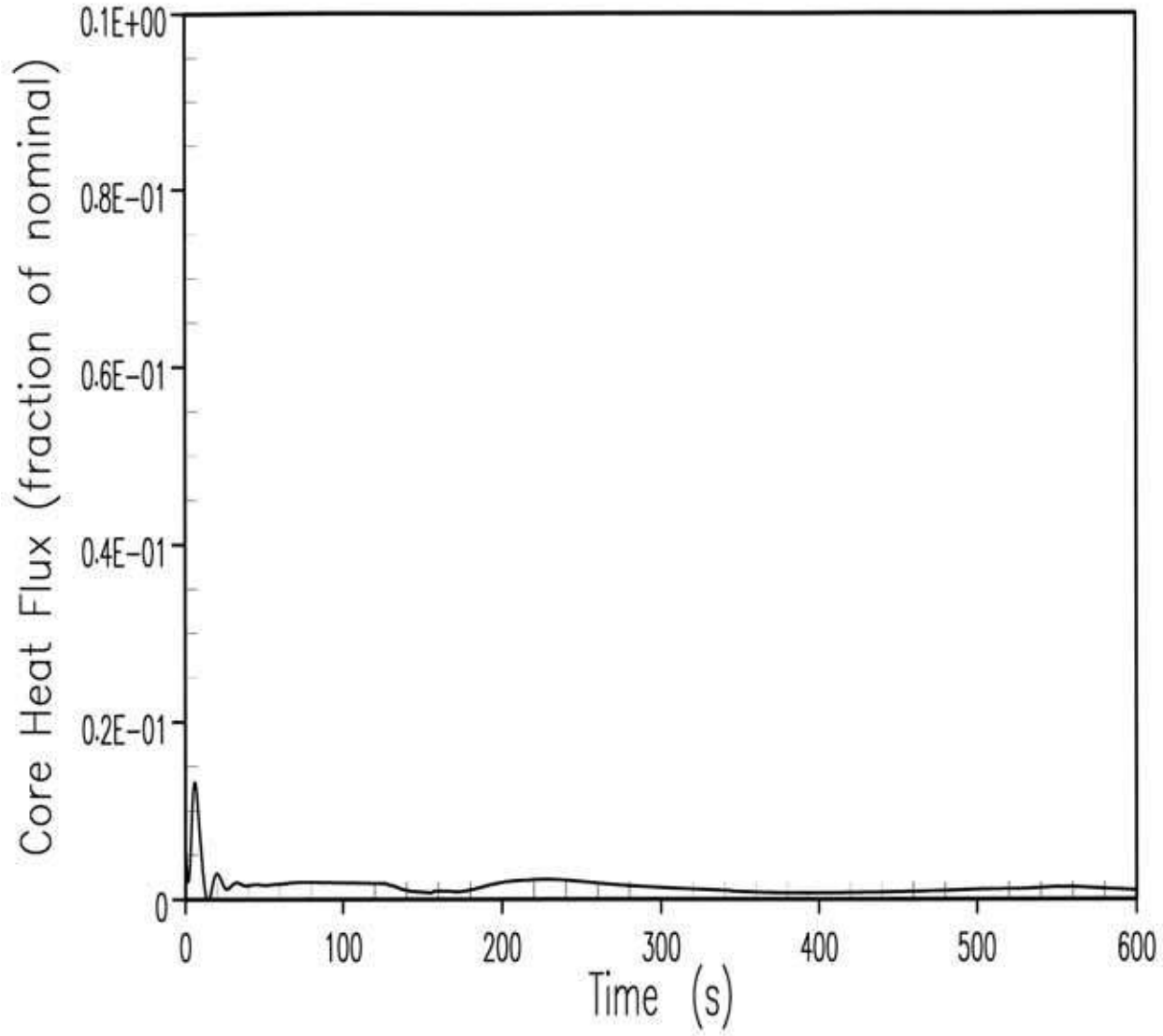


Figure 9.1.4-3. DBA Core Heat Flux Transient Inadvertent Opening of a Steam Generator Relief or Safety Valve

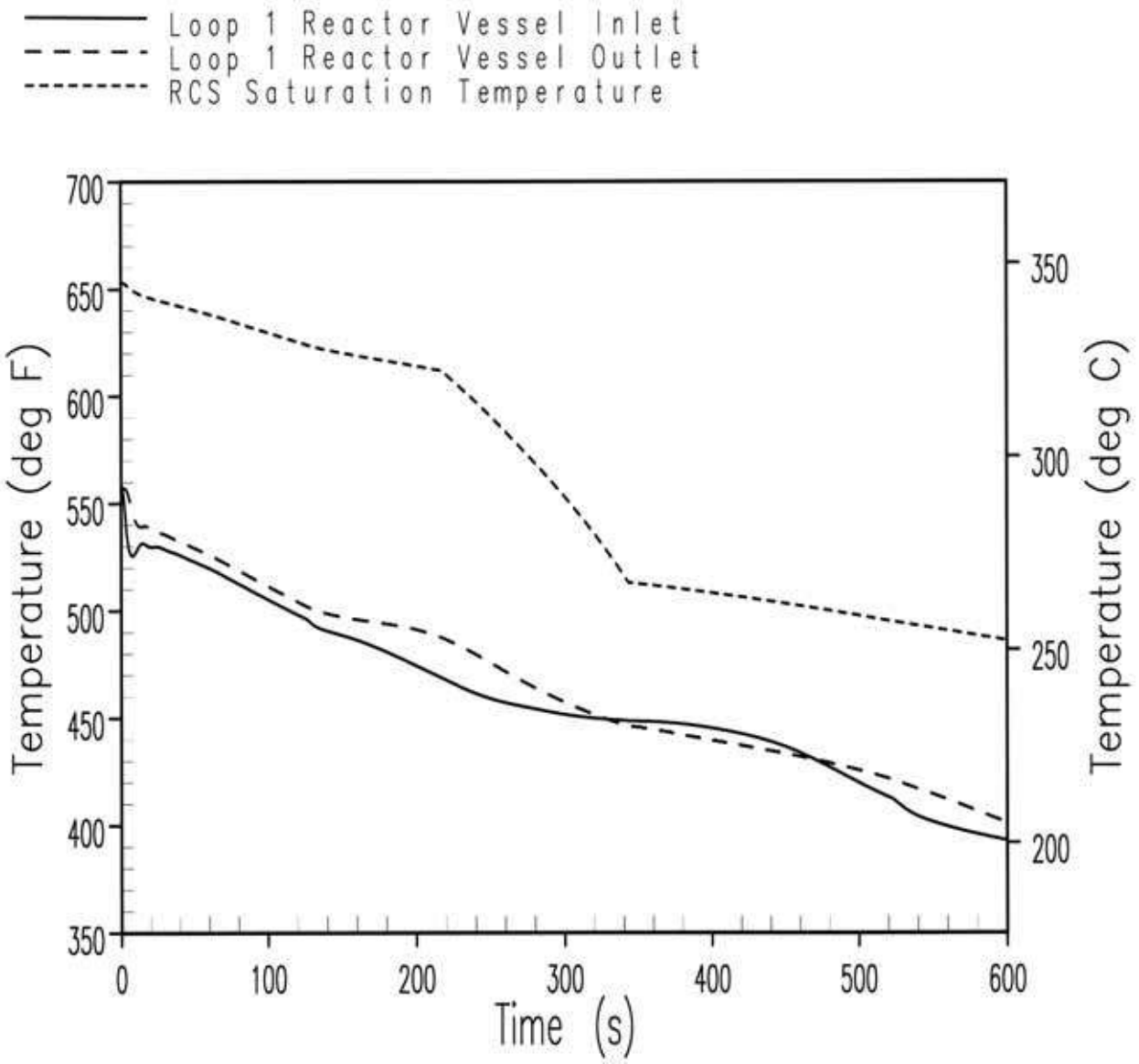


Figure 9.1.4-4. DBA Loop 1 Reactor Coolant Temperatures Inadvertent Opening of a Steam Generator Relief or Safety Valve

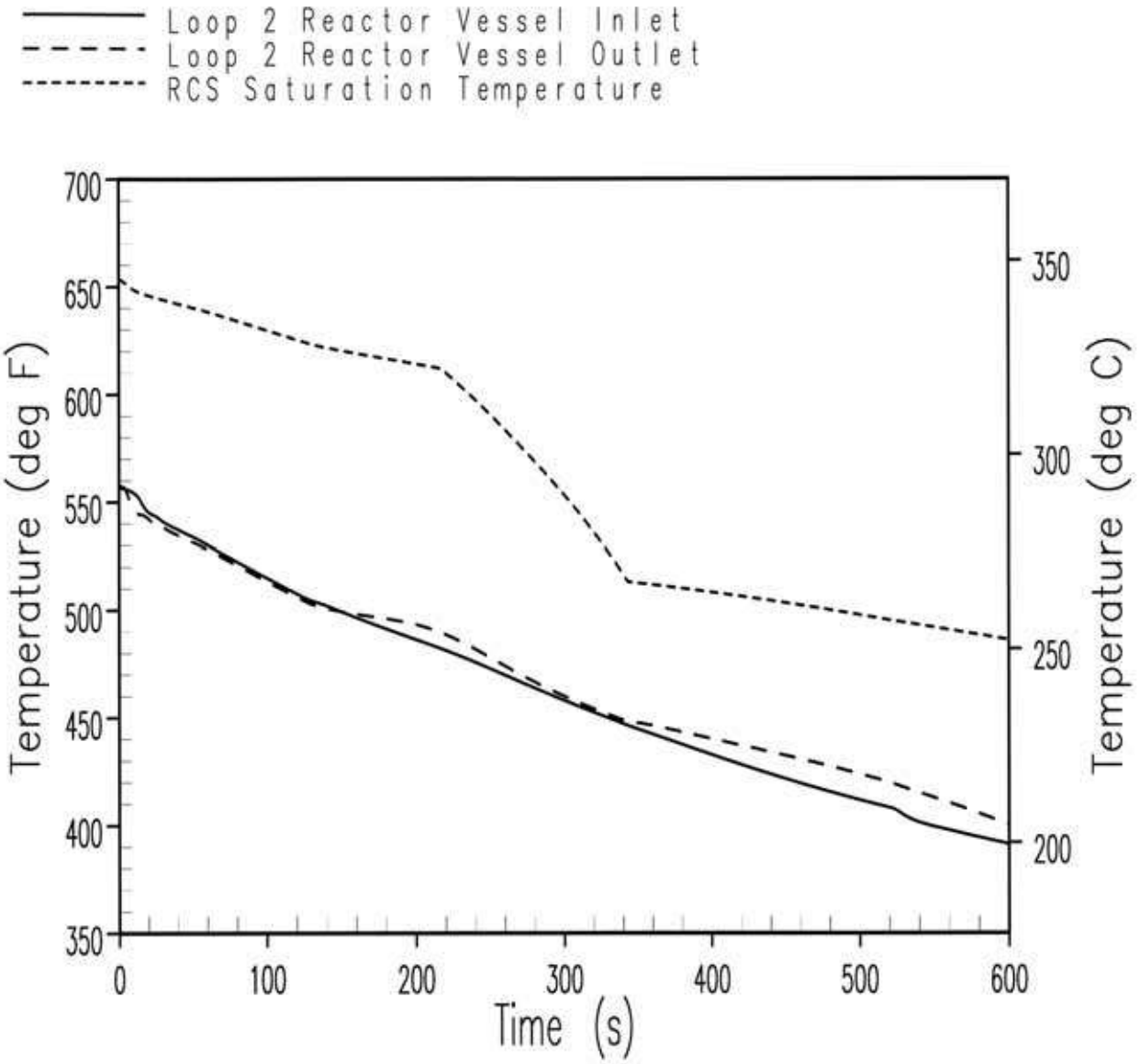


Figure 9.1.4-5. DBA Loop 2 (Faulted Loop) Reactor Coolant Temperatures Inadvertent Opening of a Steam Generator Relief or Safety Valve

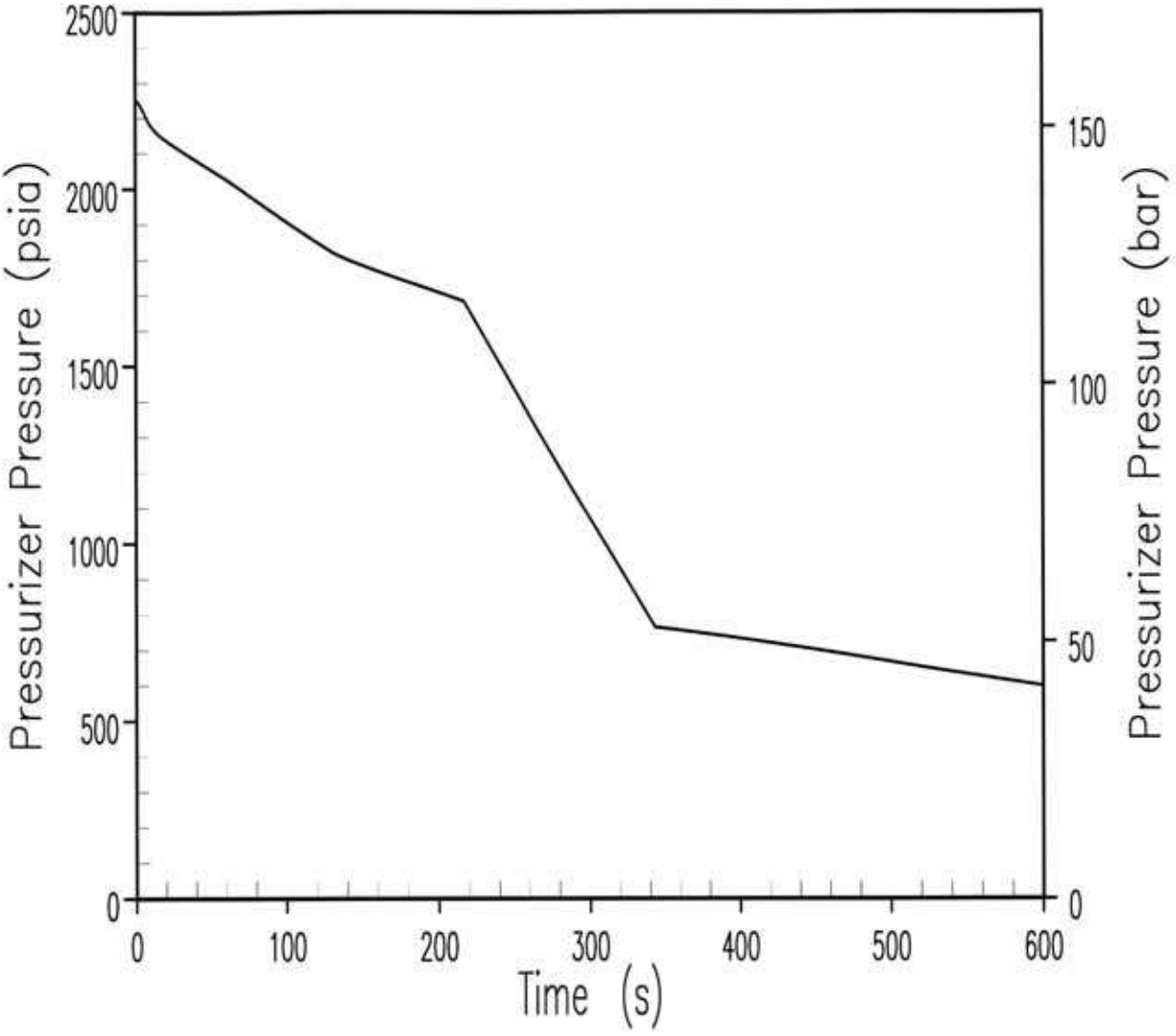


Figure 9.1.4-6. DBA Pressuriser Pressure Transient Inadvertent Opening of a Steam Generator Relief or Safety Valve

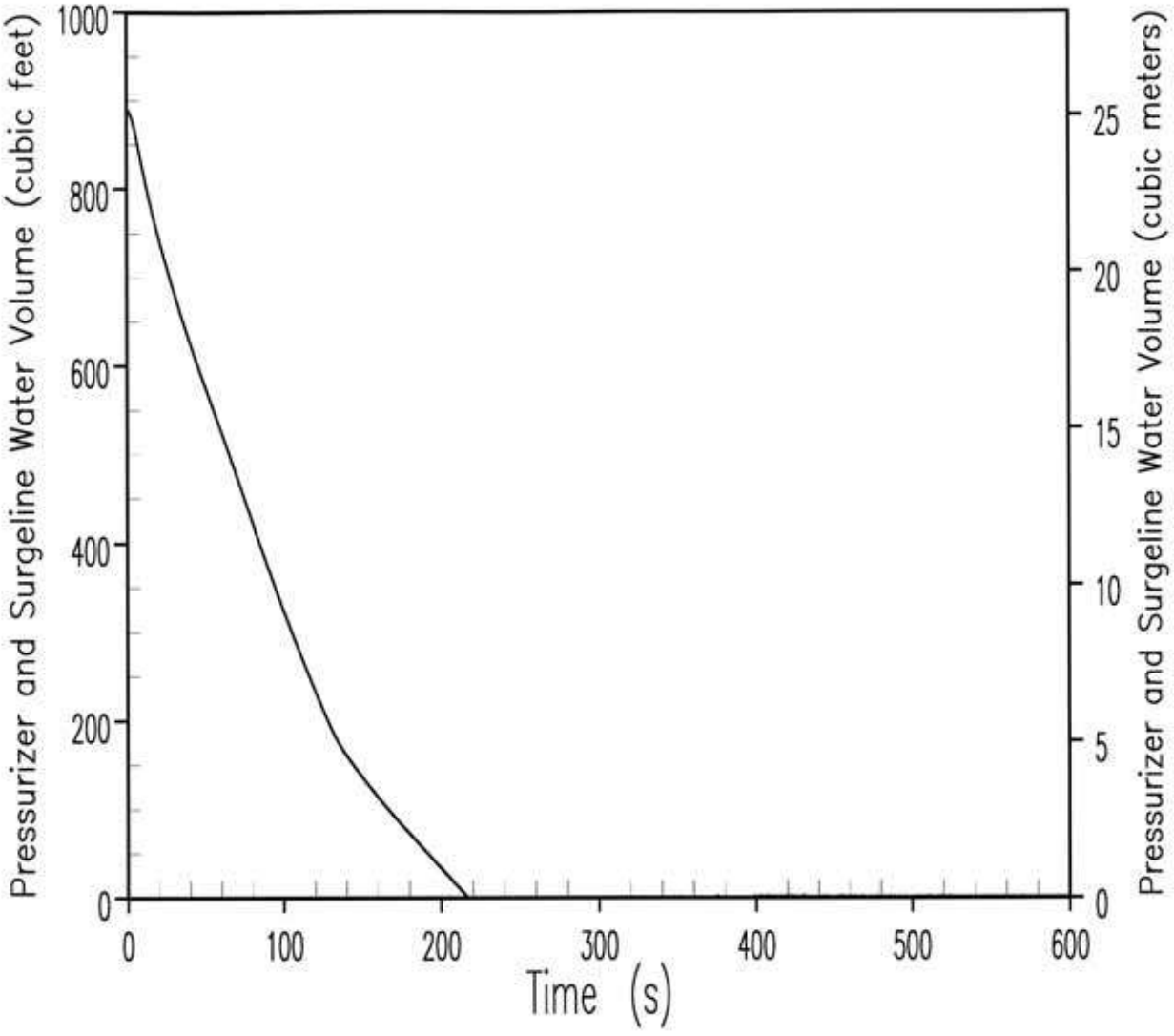


Figure 9.1.4-7. DBA Pressuriser and Surgeline Water Volume Transient Inadvertent Opening of a Steam Generator Relief or Safety Valve

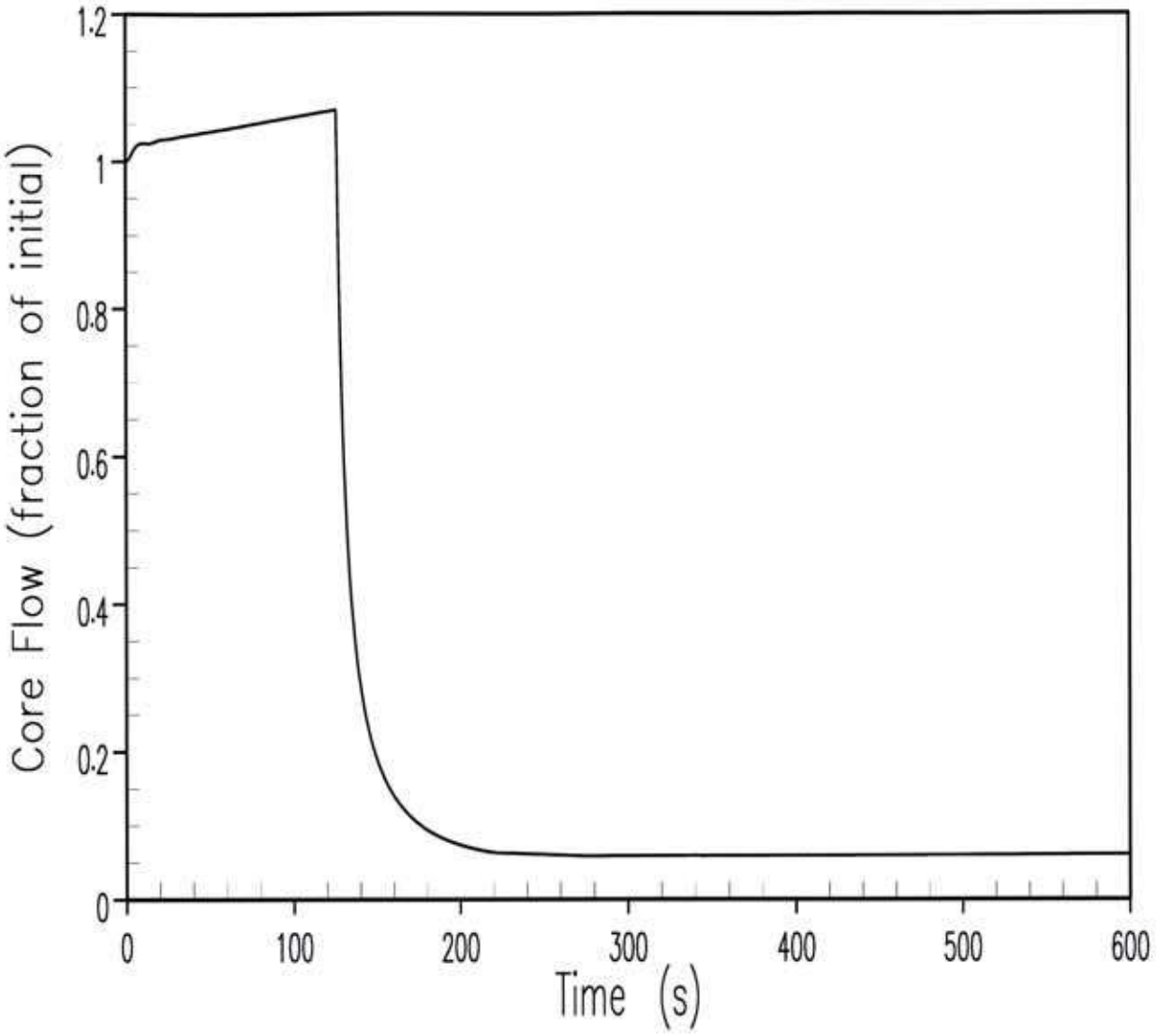


Figure 9.1.4-8. DBA Core Flow Transient Inadvertent Opening of a Steam Generator Relief or Safety Valve

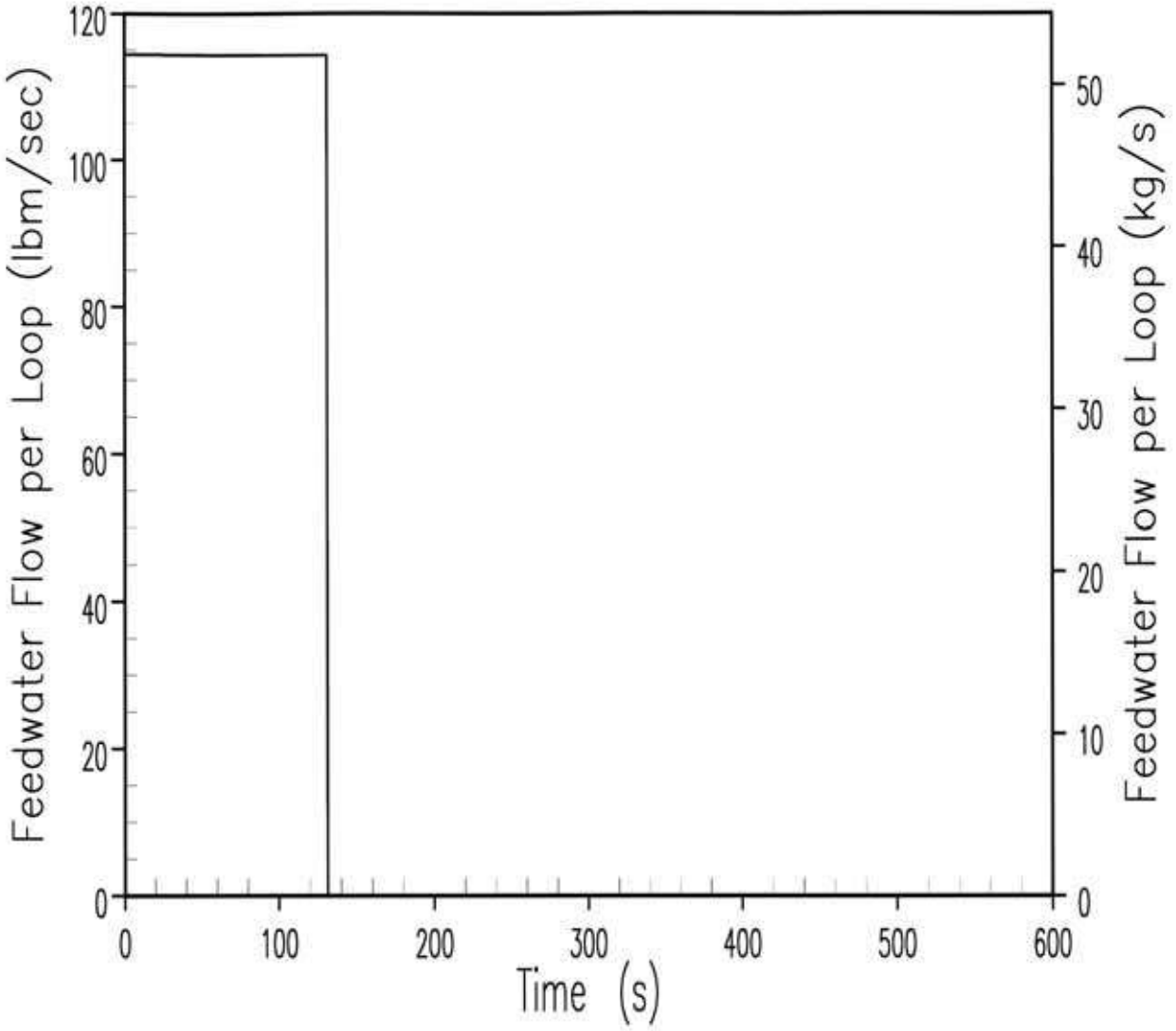


Figure 9.1.4-9. DBA Feedwater Flow Transient
Inadvertent Opening of a Steam Generator Relief or Safety Valve

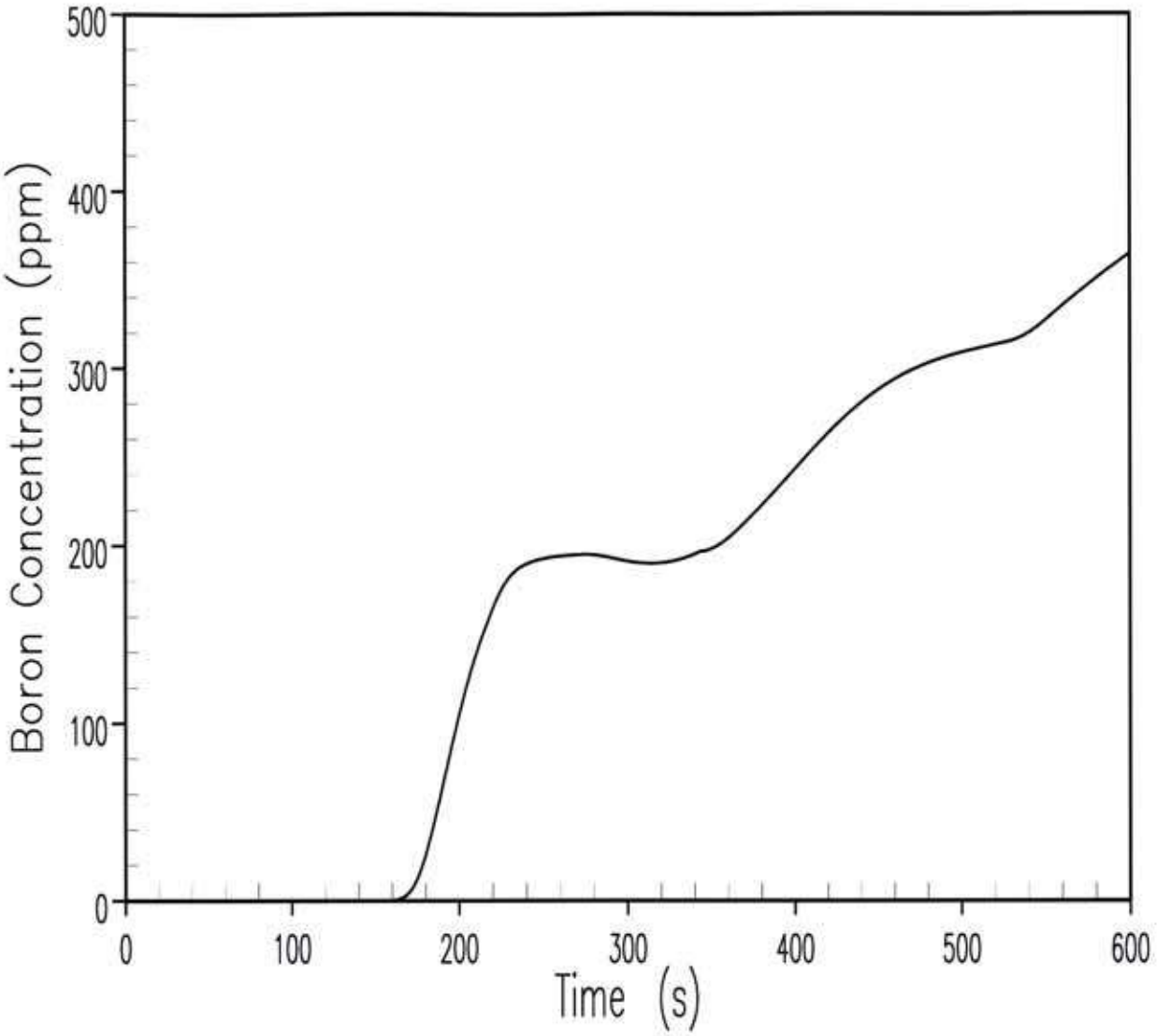


Figure 9.1.4-10. DBA Core Boron Concentration Transient Inadvertent Opening of a Steam Generator Relief or Safety Valve

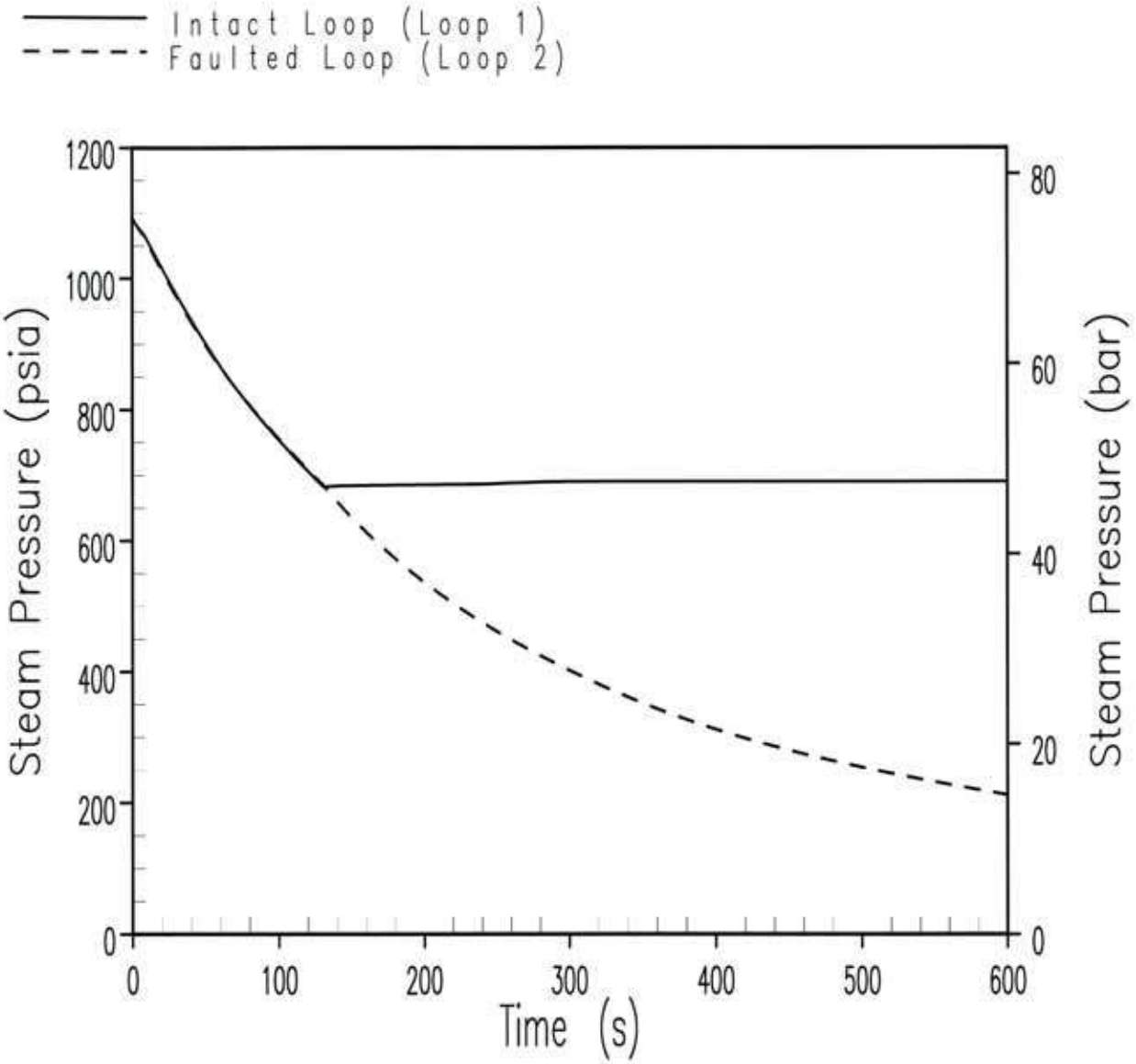


Figure 9.1.4-11. DBA Steam Pressure Transient Inadvertent Opening of a Steam Generator Relief or Safety Valve

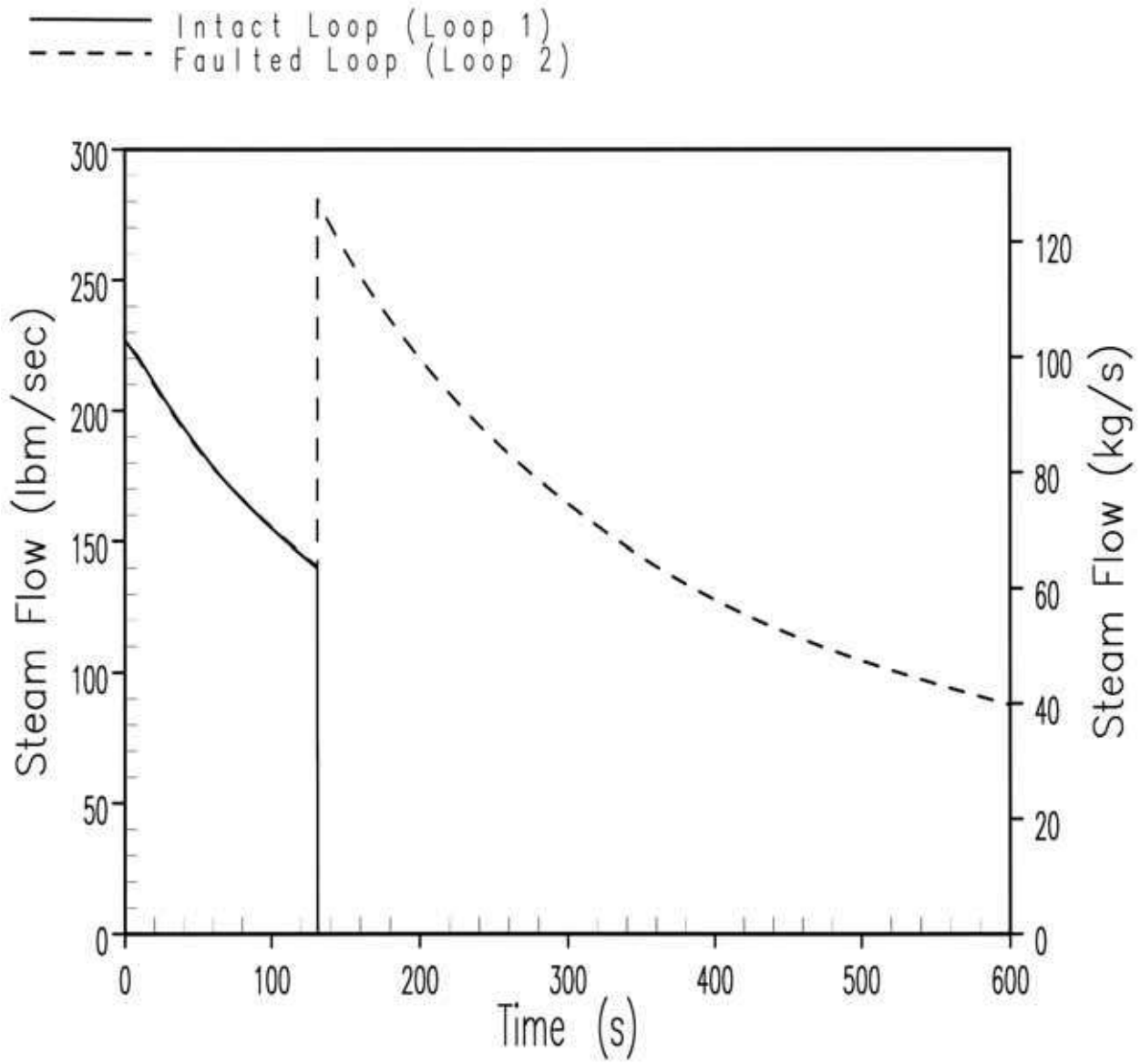


Figure 9.1.4-12. DBA Steam Flow Transient Inadvertent Opening of a Steam Generator Relief or Safety Valve

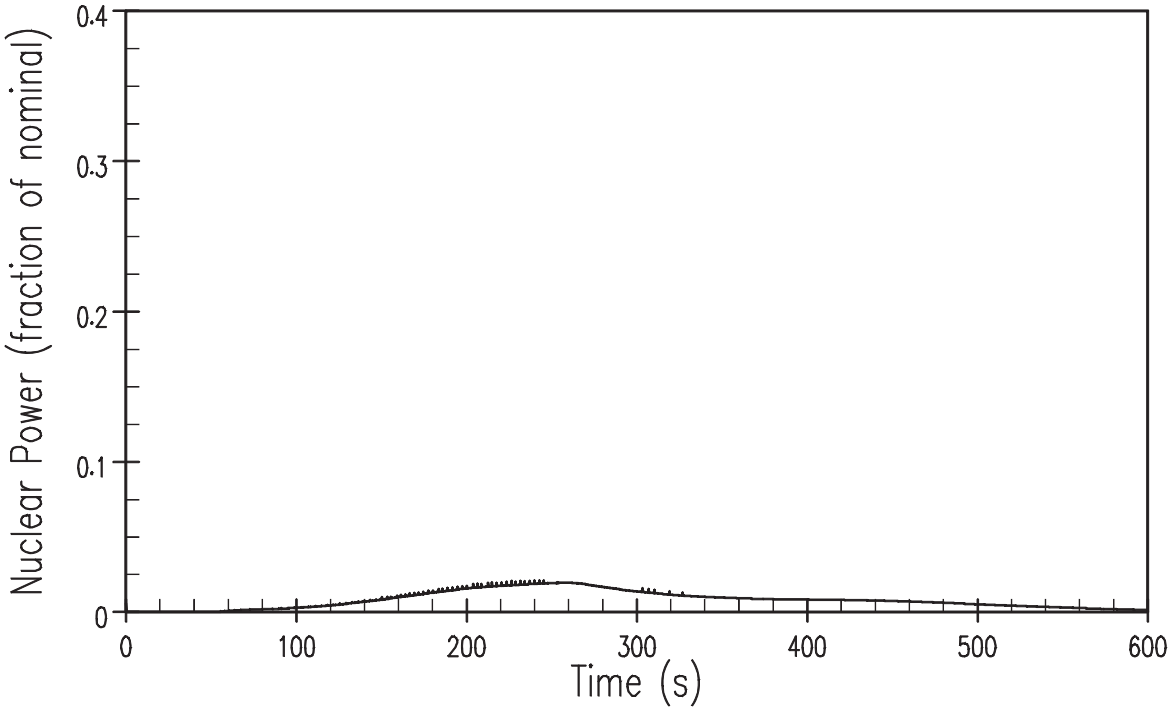


Figure 9.1.5-1. DBA Nuclear Power Transient Steam System Piping Failure at Hot Zero Power

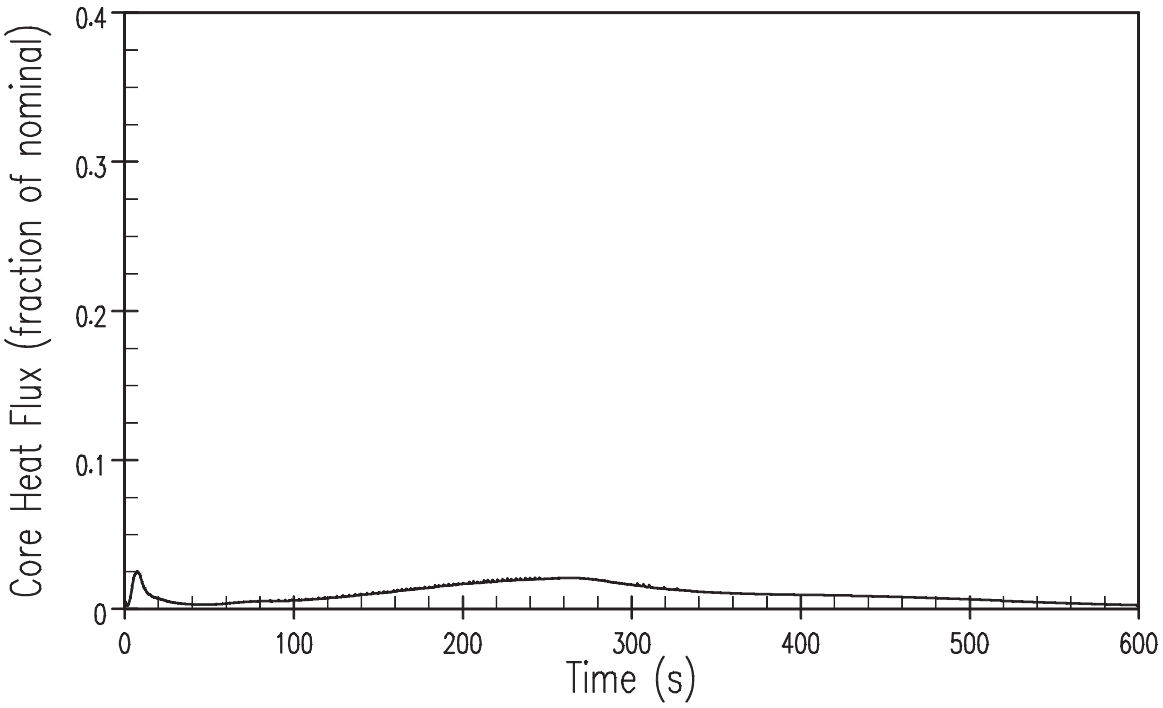


Figure 9.1.5-2. DBA Core Heat Flux Transient Steam System Piping Failure at Zero Power

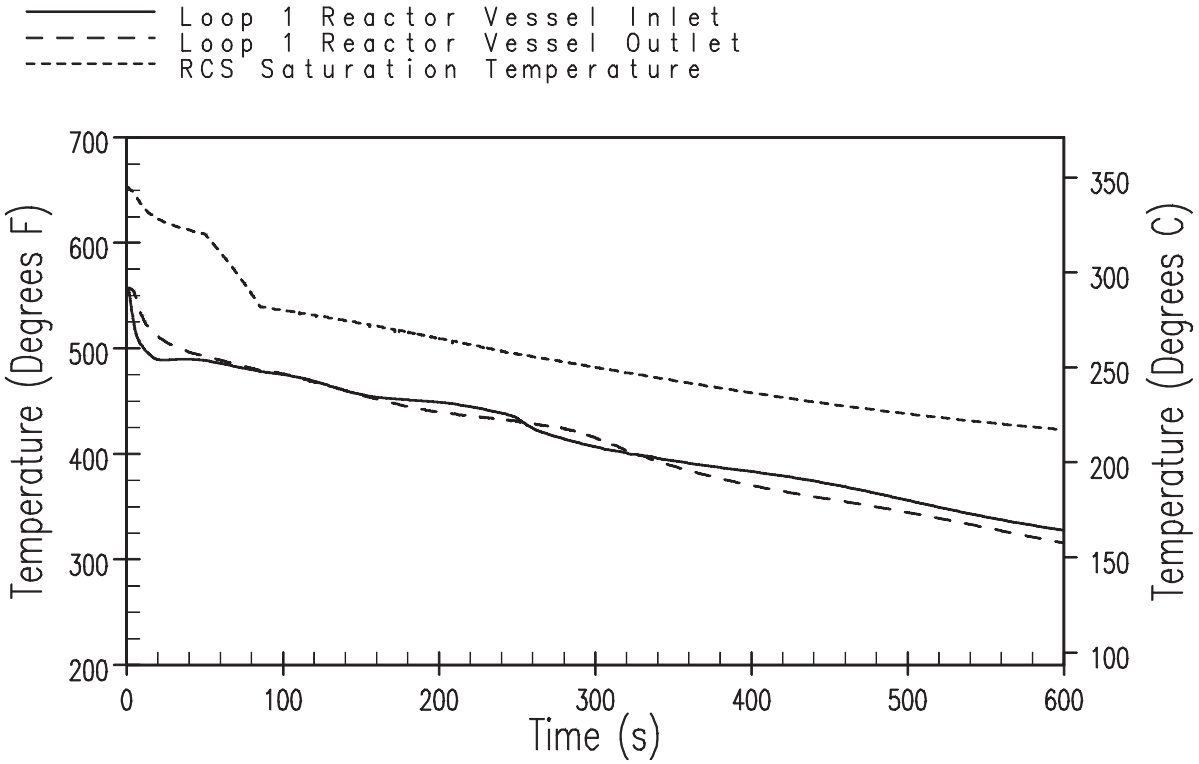


Figure 9.1.5-3. DBA Loop 1 Reactor Coolant Temperatures Steam System Piping Failure at Zero Power

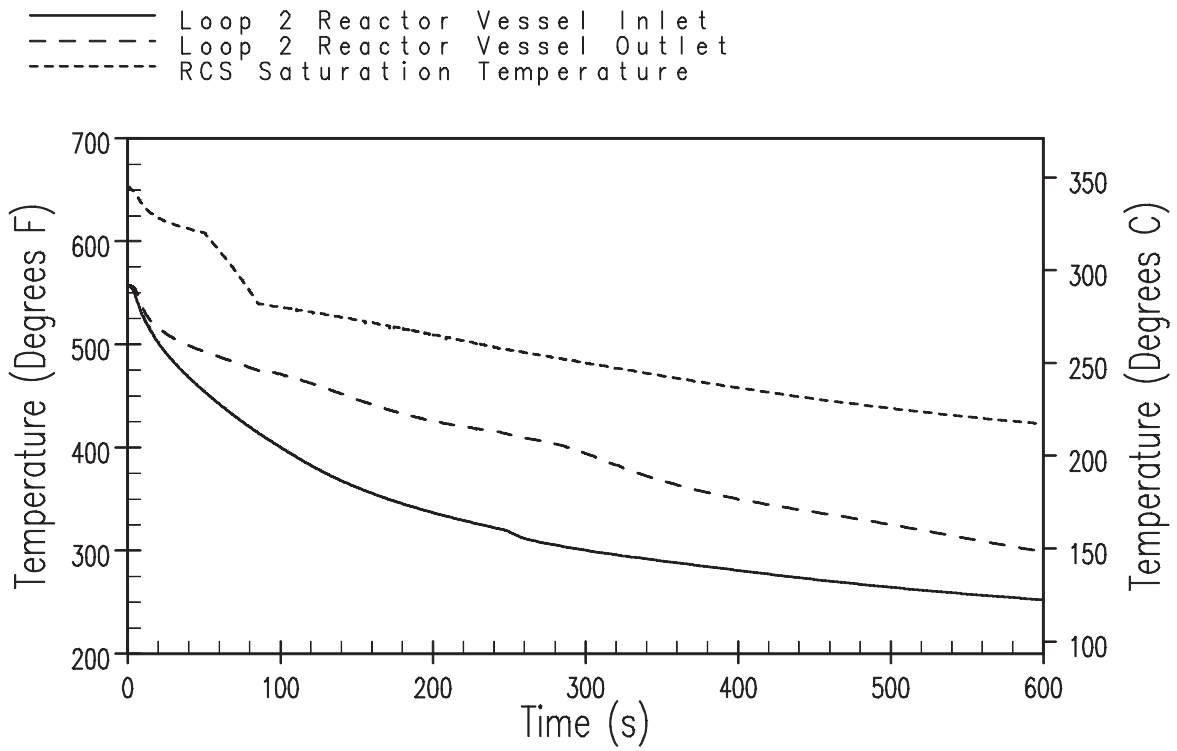


Figure 9.1.5-4. DBA Loop 2 Reactor Coolant Temperatures Steam System Piping Failure at Zero Power

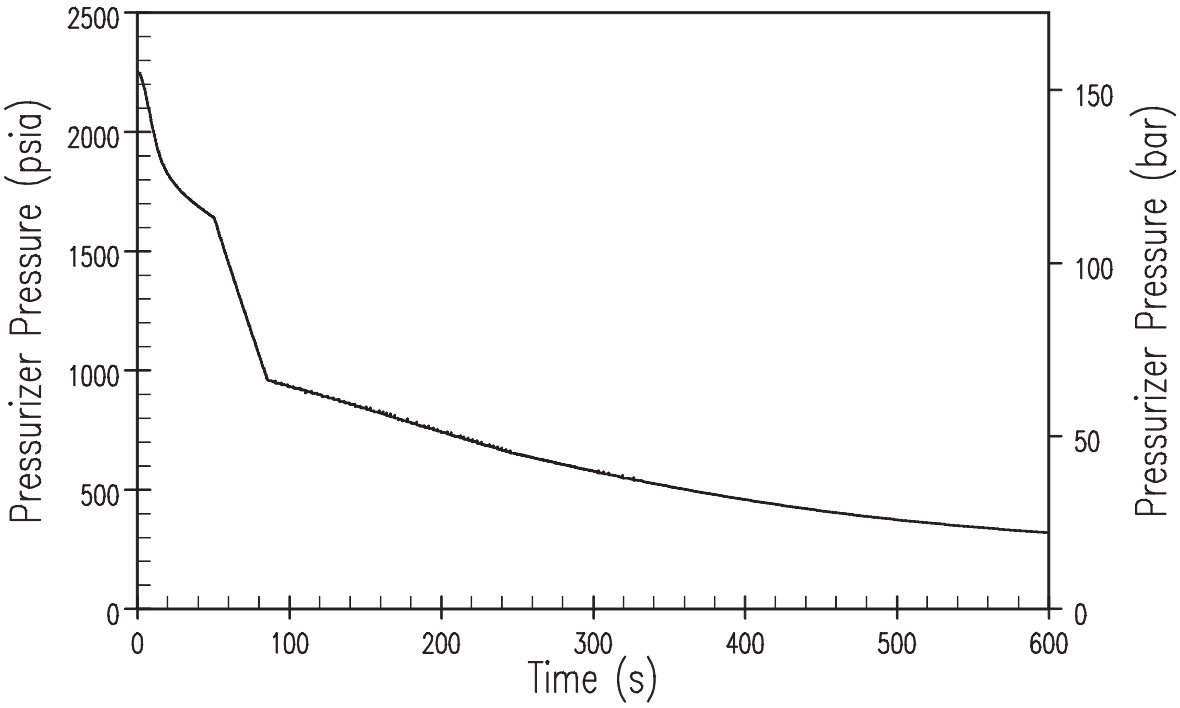


Figure 9.1.5-5. DBA Pressuriser Pressure Transient Steam System Piping Failure at Zero Power

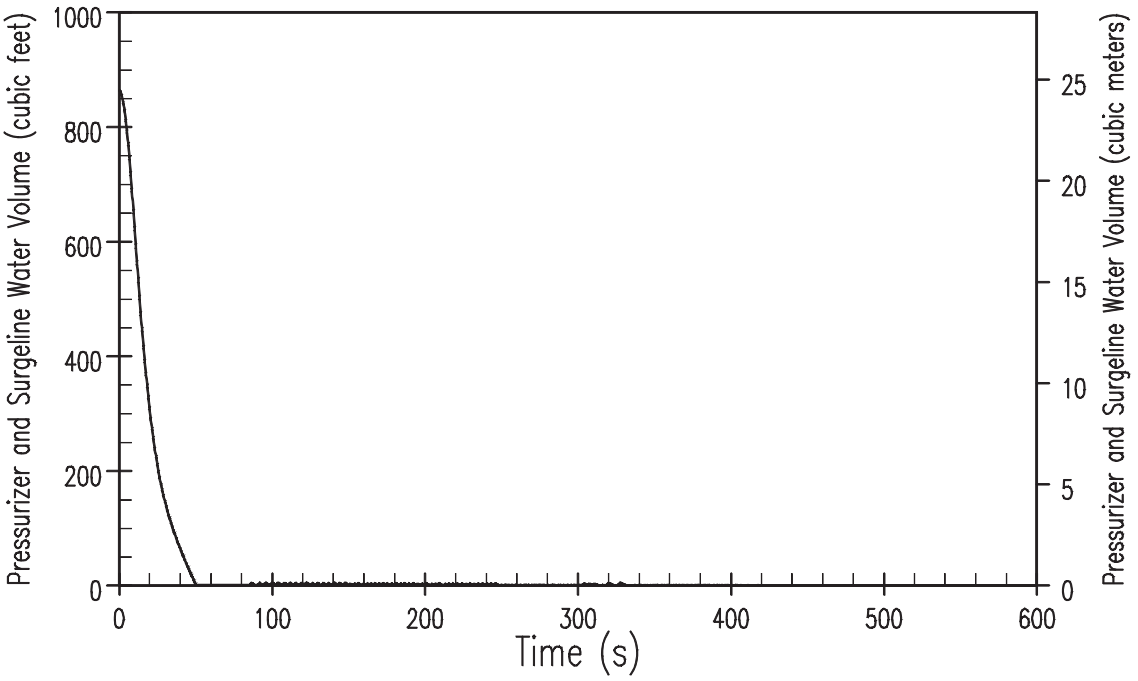


Figure 9.1.5-6. DBA Pressuriser and Surgeline Water Volume Transient Steam System Piping Failure at Zero Power

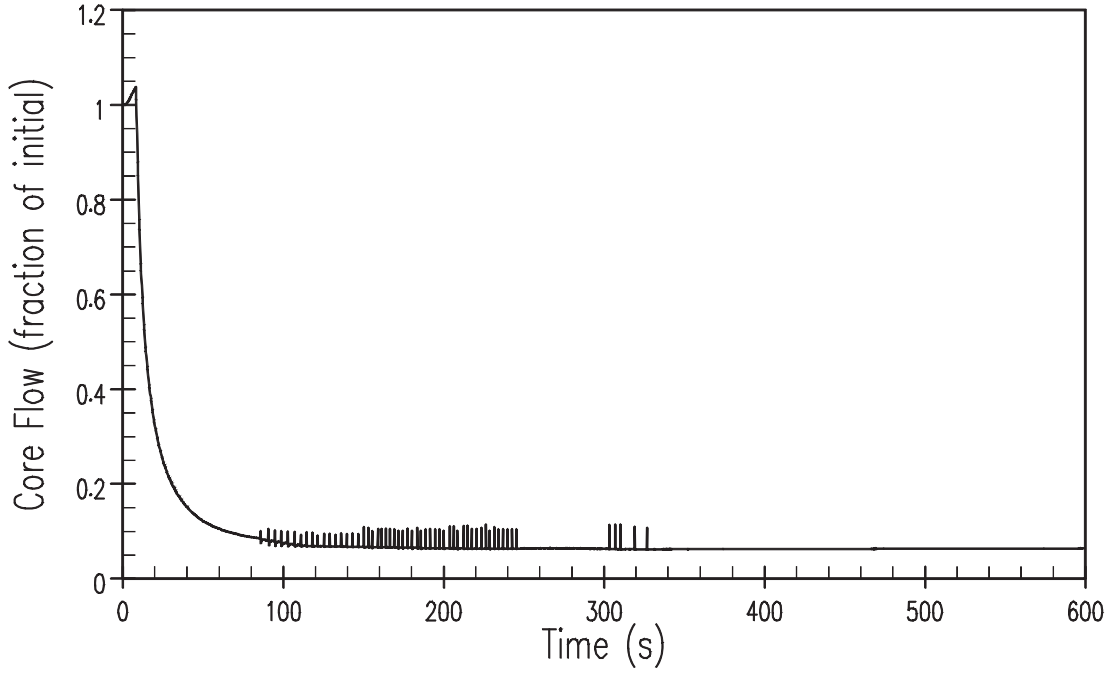


Figure 9.1.5-7. DBA Core Flow Transient Steam System Piping Failure at Zero Power

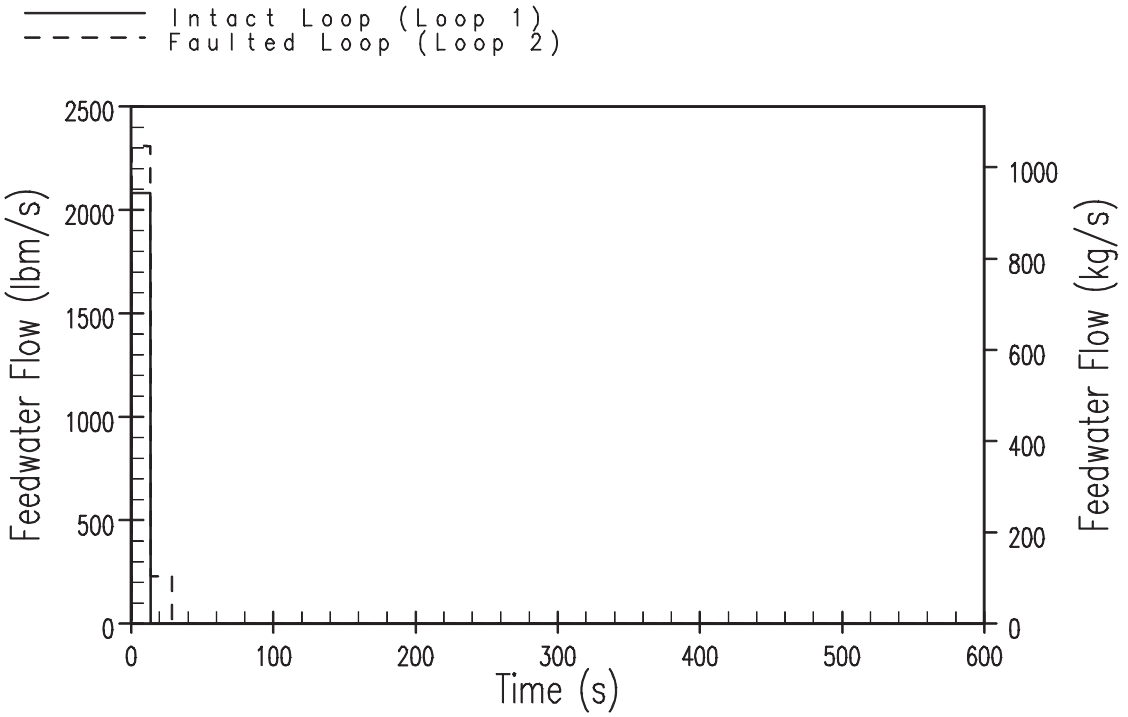


Figure 9.1.5-8. DBA Feedwater Flow Transient Steam System Piping Failure at Zero Power

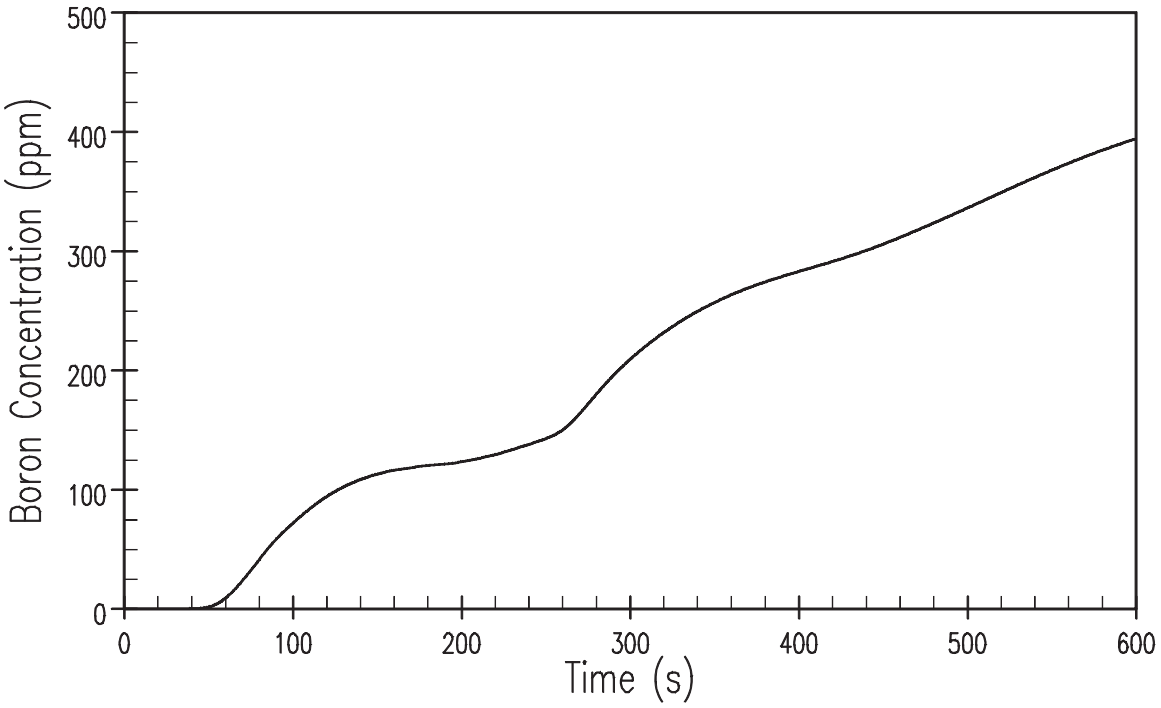


Figure 9.1.5-9. DBA Core Boron Concentration Transient Steam System Piping Failure at Zero Power

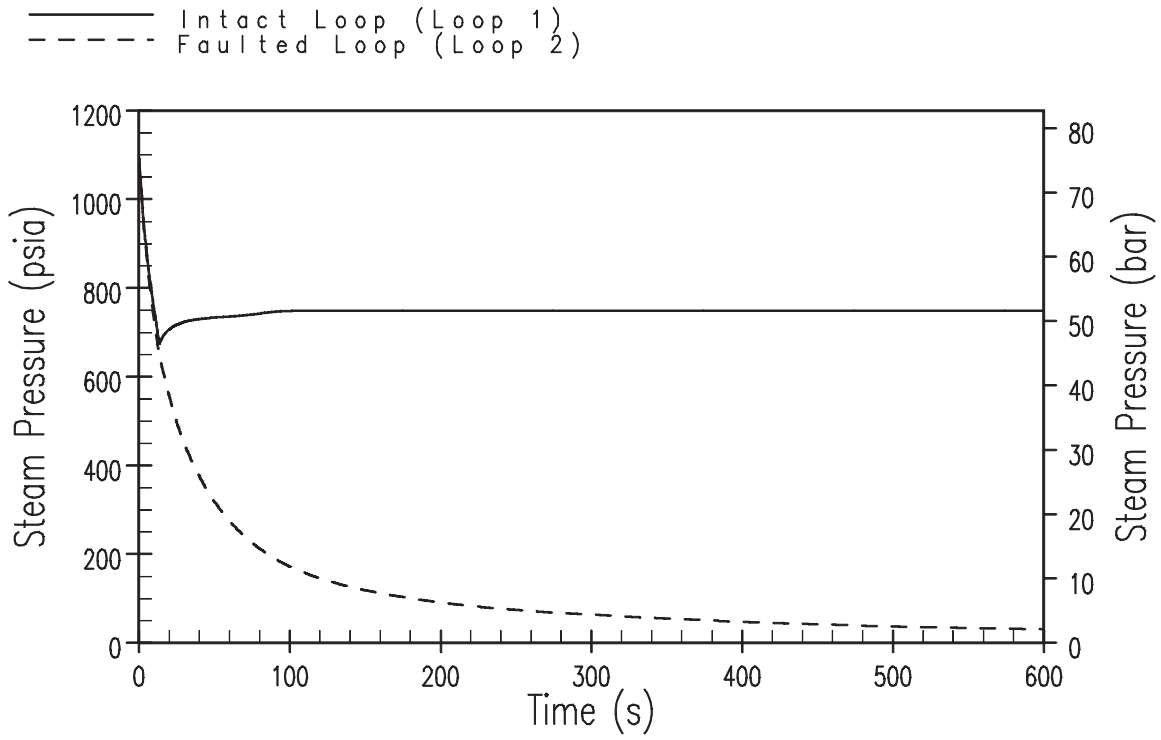


Figure 9.1.5-10. DBA Steam Pressure Transient Steam System Piping Failure at Zero Power

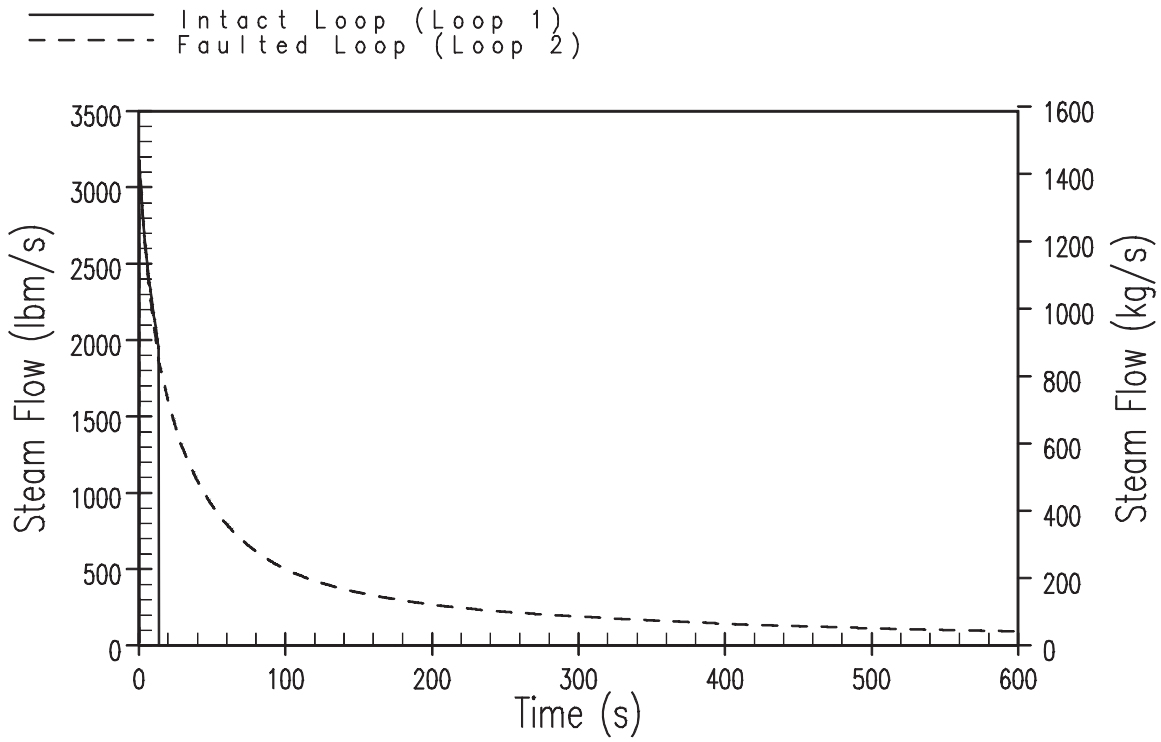


Figure 9.1.5-11. DBA Steam Flow Transient Steam System Piping Failure at Zero Power

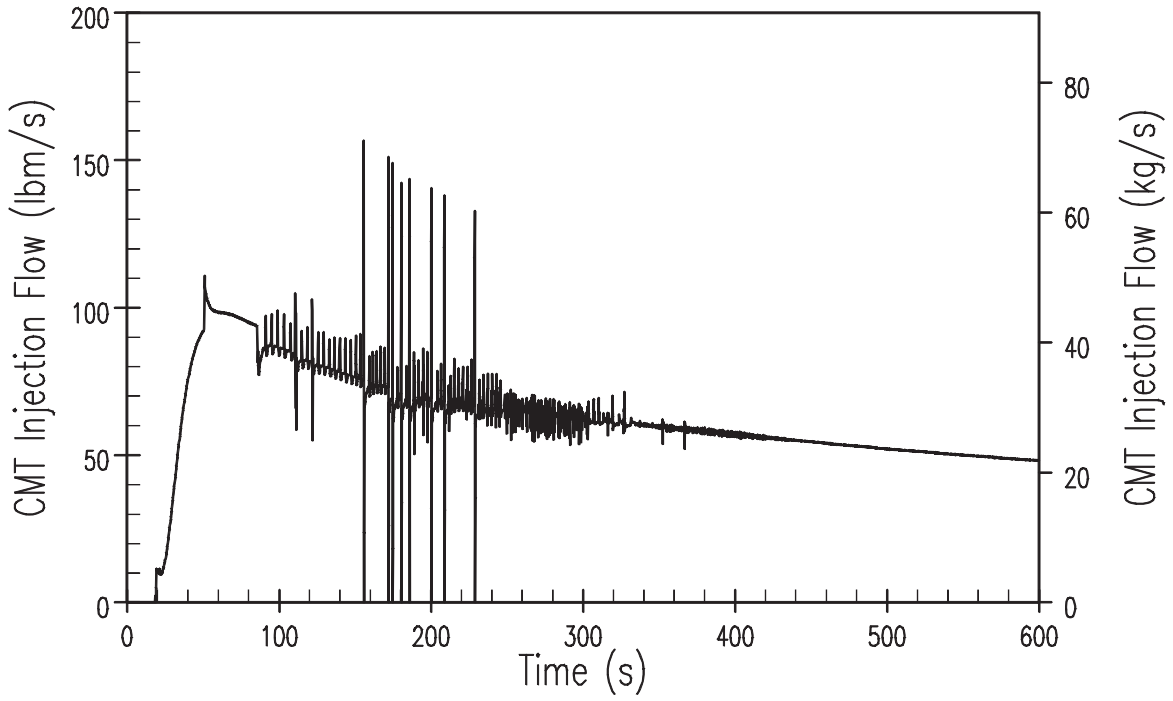


Figure 9.1.5-12. DBA Core Makeup Tank Injection Flow Steam System Piping Failure at Zero Power

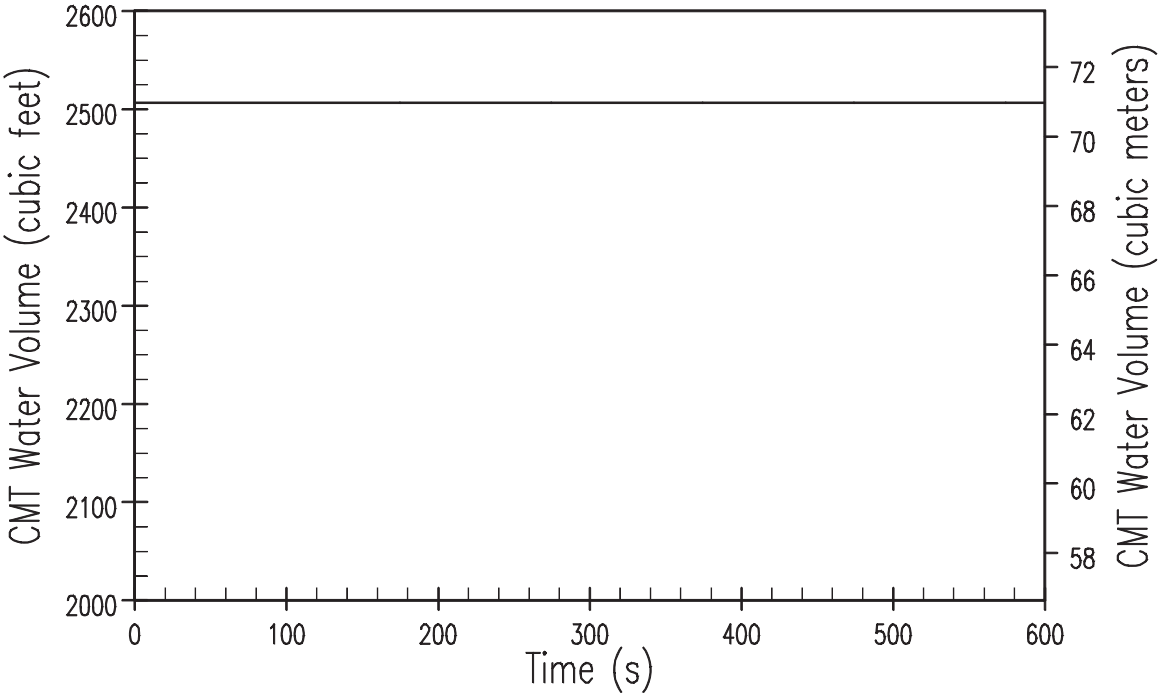


Figure 9.1.5-13. DBA Core Makeup Tank Water Volume Steam System Piping Failure at Zero Power

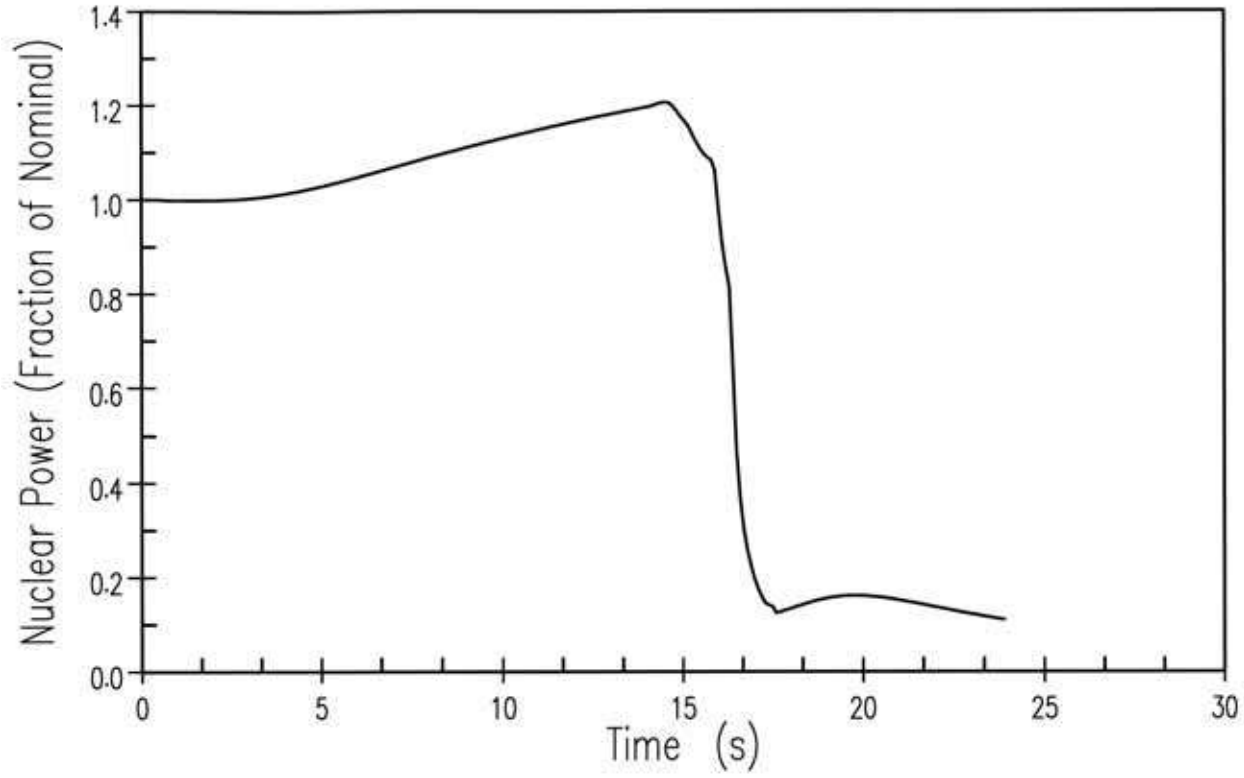


Figure 9.1.6-1. DBA Nuclear Power Transient Steam System Piping Failure at Full Power – 0.08 m^2 (0.87 ft^2) Break Size

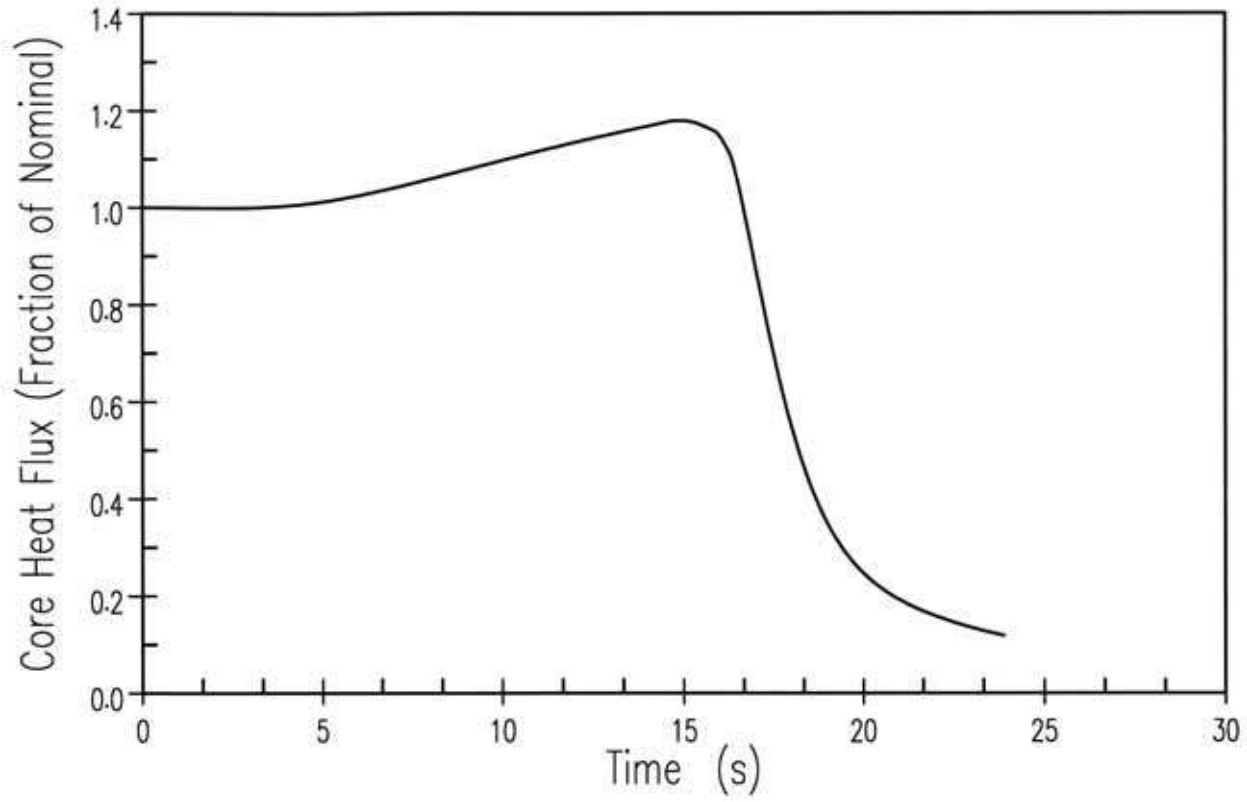


Figure 9.1.6-2. DBA Core Heat Flux Transient Steam System Piping Failure at Full Power – 0.08 m^2 (0.87 ft^2) Break Size

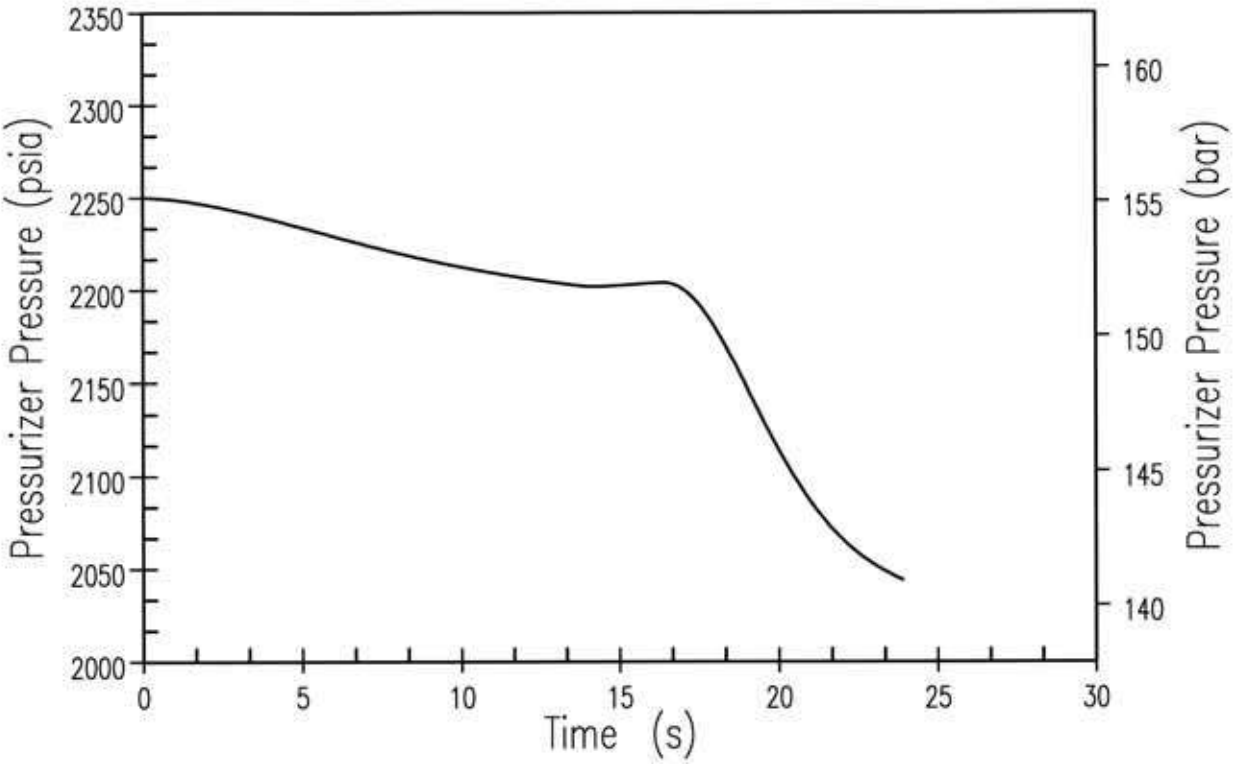


Figure 9.1.6-3. DBA Pressuriser Pressure Transient Steam System Piping Failure at Full Power – 0.08 m^2 (0.87 ft^2) Break Size

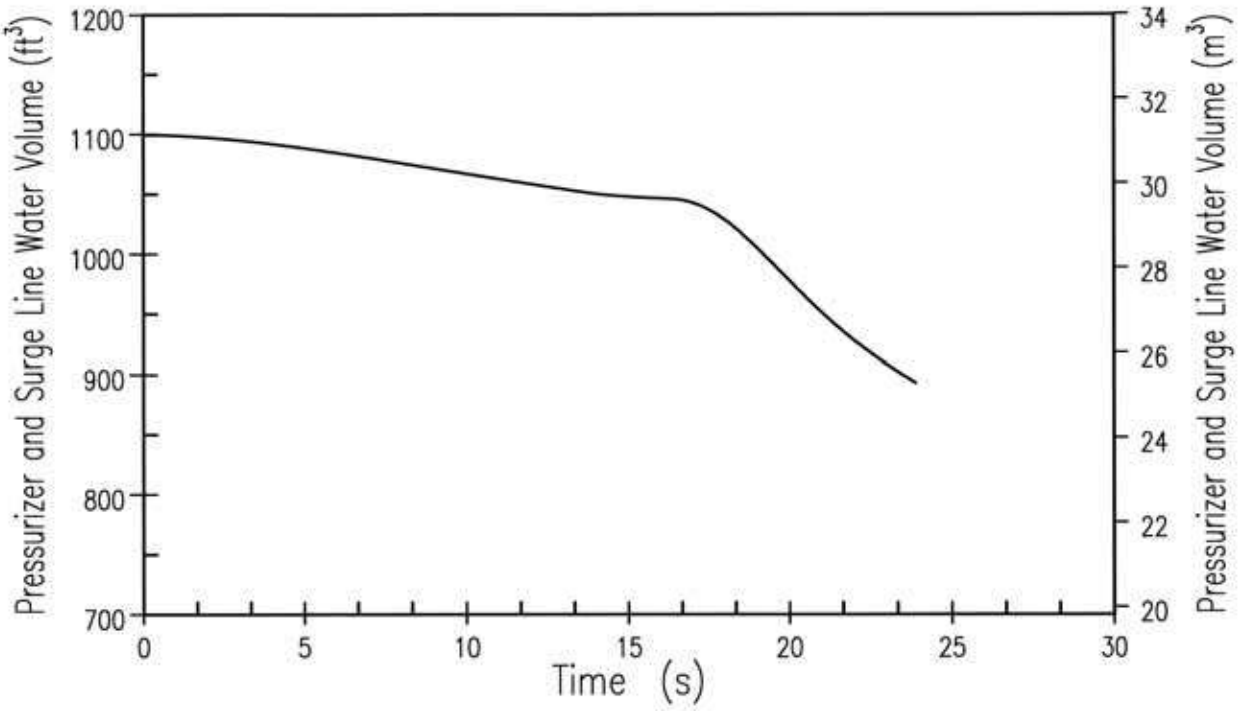


Figure 9.1.6-4. DBA Pressuriser Water Volume Transient
Steam System Piping Failure at Full Power – 0.08 m^2 (0.87 ft^2) Break Size

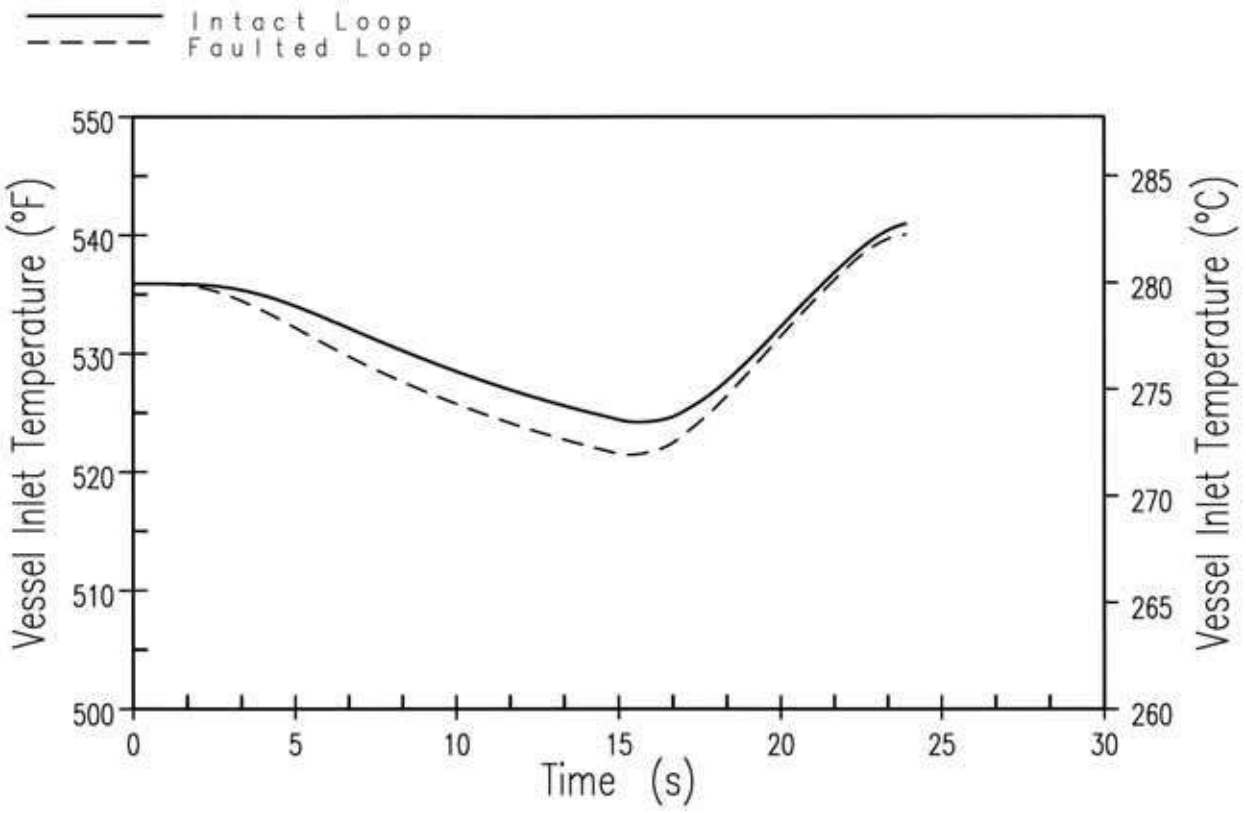


Figure 9.1.6-5. DBA Vessel Inlet Temperature Transient (Intact and Faulted Loops) Steam System Piping Failure at Full Power – 0.08 m^2 (0.87 ft^2) Break Size

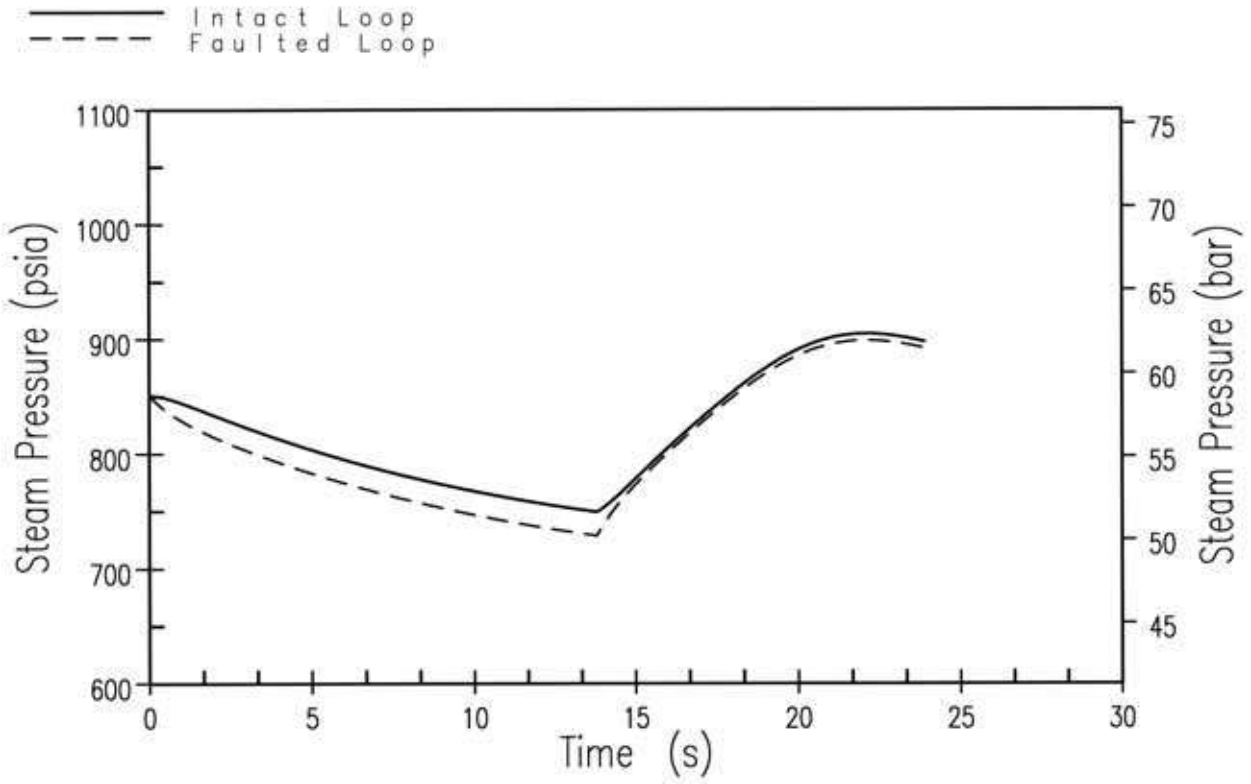


Figure 9.1.6-6. DBA Steam Generator Pressure Transient (Intact and Faulted Loops) Steam System Piping Failure at Full Power – 0.08 m^2 (0.87 ft^2) Break Size

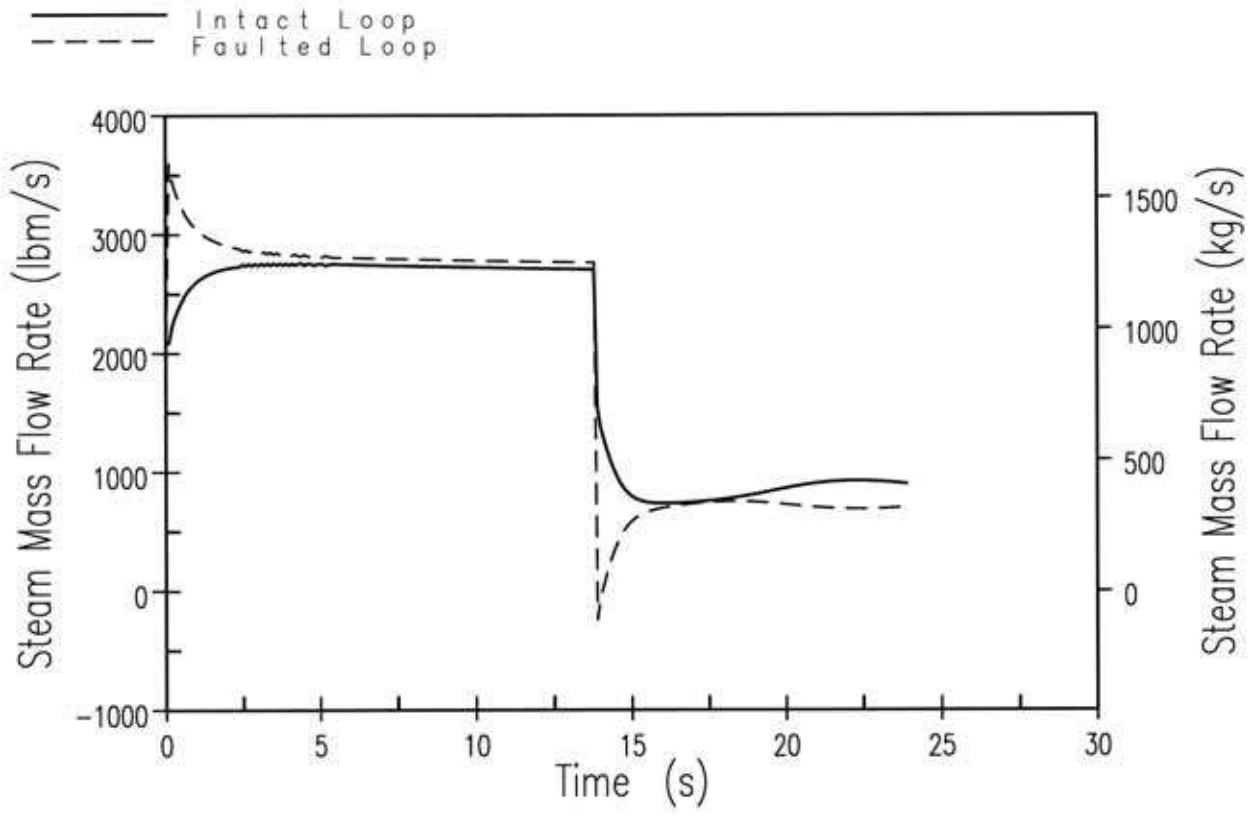


Figure 9.1.6-7. DBA Steam Flow Transient (Intact and Faulted Loops) Steam System Piping Failure at Full Power – 0.08 m^2 (0.87 ft^2) Break Size

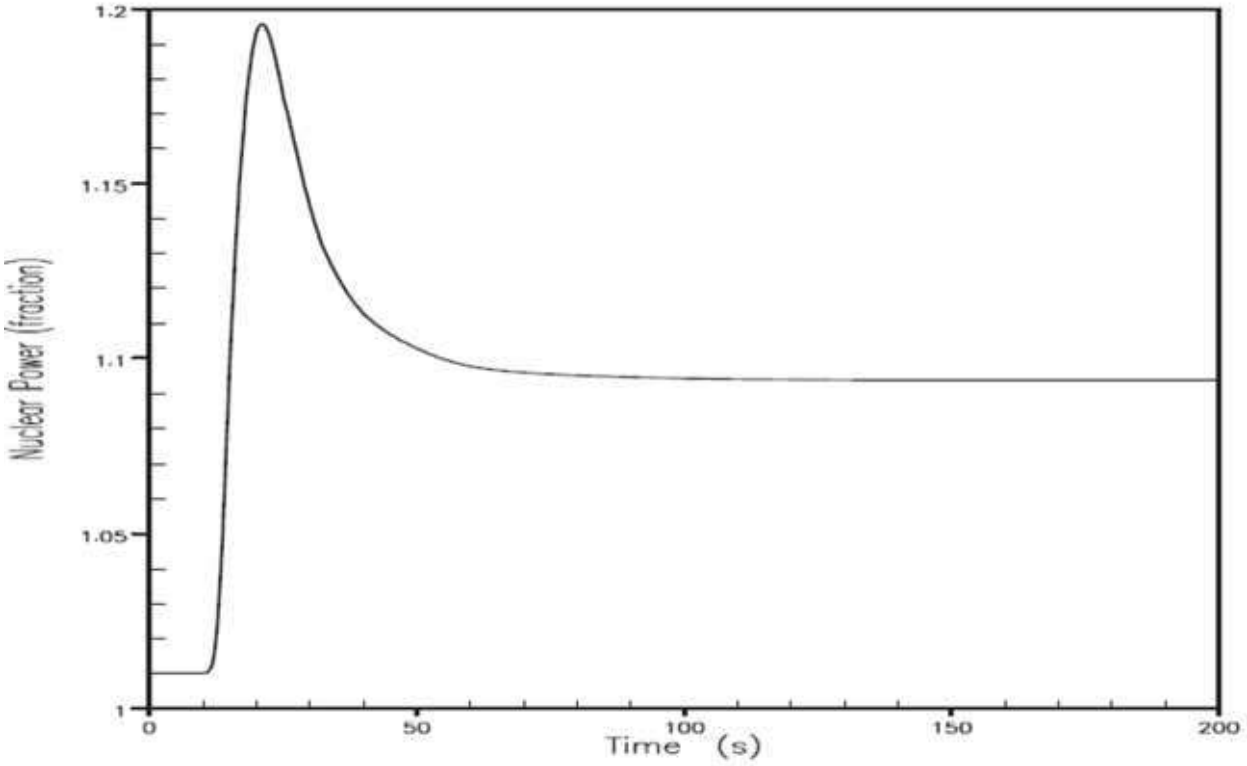


Figure 9.1.7-1. ATWT Inadvertent PRHR with a PMS CCF – Nuclear Power

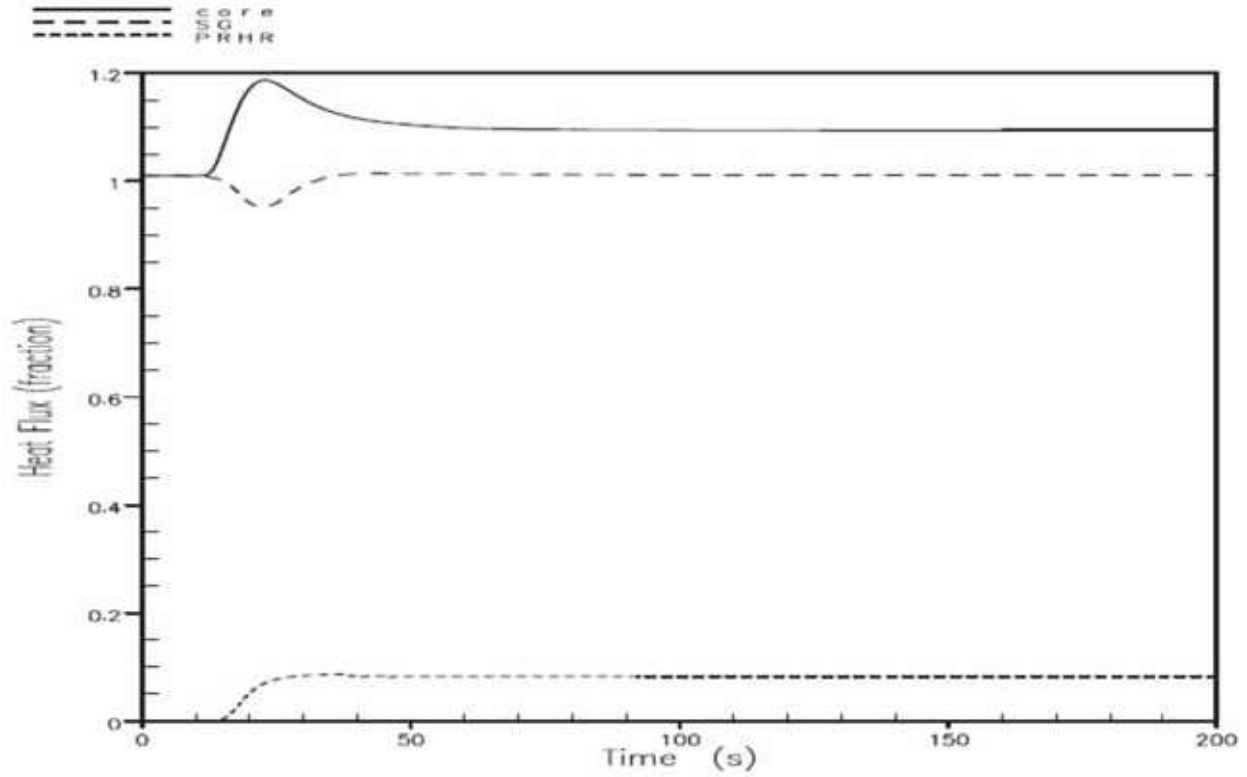


Figure 9.1.7-2. ATWT Inadvertent PRHR with a PMS CCF – Heat Flux (Core, SG, and PRHR)

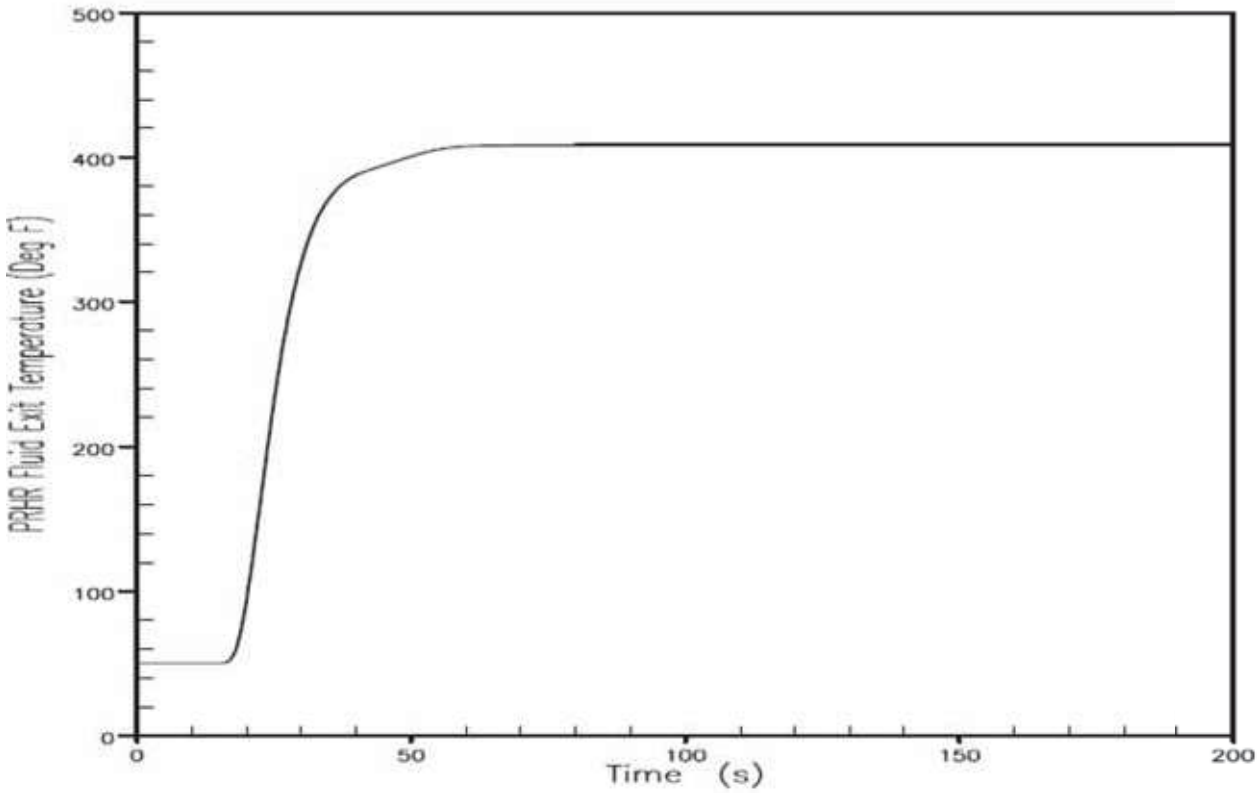


Figure 9.1.7-3. ATWT Inadvertent PRHR with a PMS CCF – PRHR Fluid Exit Temperature

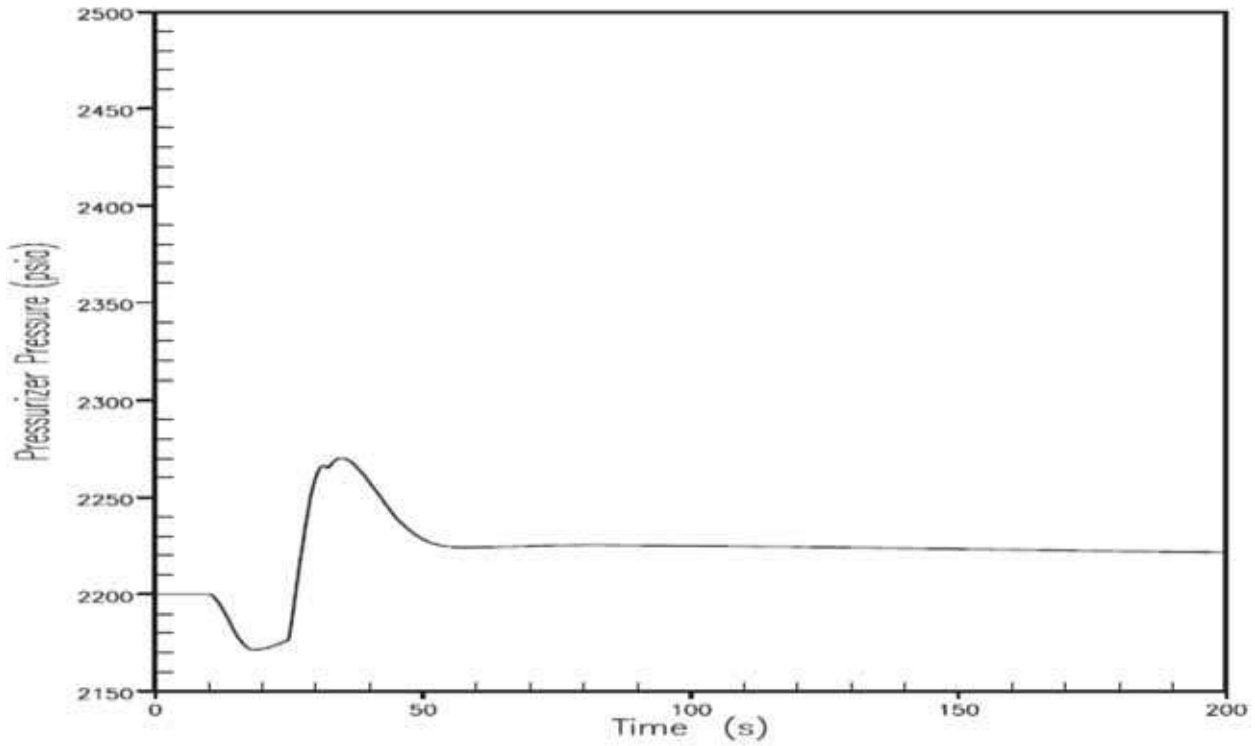


Figure 9.1.7-4. Inadvertent PRHR with a PMS CCF – Pressuriser Pressure

9.2 Decrease in Heat Removal by the Secondary System

A number of faults that could result in a decrease in heat removal by the secondary system are postulated. The events are discussed in this section. Detailed analyses are presented for the most limiting of the primary system heat removal decrease events.

9.2.0 Introduction and Overview of Faults

Decrease in heat removal from the secondary side can be caused by a number of initiating faults, represented by loss of main feedwater, all of which have similar behaviours.

A loss of normal feedwater (from pump failures, valve malfunctions, loss of ac power sources, or a break in the feedwater line) results in a reduction in the capability of the secondary system to remove the heat generated in the reactor core.

The normal response of the plant to this fault is to trip the reactor and provide SG feed from the SFW system. However, the most limiting fault occurs if the loss of feed results from a double-ended rupture of the feedwater line, so that no main feedwater (MFW) or SFW is delivered to the faulted SG. In the longer term, decay heat removal is via the RNS.

If SFW is not available, the Class 1 passive residual heat removal heat exchanger (PRHR HX) is actuated automatically by the PMS on either a low SG water level (narrow range) coincidentally with a low SFW flow rate signal or a low SG water level (wide range) signal. The PRHR HX transfers the core decay heat and sensible heat to the IRWST, so that core heat removal is uninterrupted following a loss of normal feedwater and SFW.

For this report the faults are split into two parts:

- Feedwater line break accident
  - Main feed line break upstream of main feedwater isolation valves (MFWIVs)
  - Main feed line break downstream of MFWIVs
- All other loss of MFW events
  - Loss of main feedwater to one SG
  - Loss of main feedwater to both SGs
  - Loss of condenser
  - Loss of compressed air
  - Loss of offsite power

The feedwater line break accident is considered separately, as it differs significantly from the other loss of MFW events because:

- Secondary inventory is lost though the break.
- As noted above, SFW cannot be delivered to the faulted SG.
- The transient is strongly asymmetric.

Each fault is first described; the initial event frequency and the design basis class are provided and the bounding fault or faults are identified (if needed). The analysed faults are presented individually in Table 8A-2.

The analysed fault(s) are then described in additional detail in the subsequent sections to complete the safety case for each fault, including:

- Identification of Causes and Accident Description
- Design Basis Analysis of Effects and Consequences
- Assessment of the Radiological Consequences for the DBA
- Diverse Mitigation and ATWT for Frequent Faults
- ALARP Assessment
- Conclusions

ATWT analyses presented herein are based on Reference 9.2-11.

9.2.0.1 Decrease in Heat Removal Faults (excluding Feedline Break)

Description

A number of transients and accidents could result in a reduction of the capacity of the secondary system to remove heat generated in the RCS. These faults are as follows (Appendix 8A):

- Steam pressure regulator malfunction or failure that results in decreasing steam flow
- Loss of external electrical load (Fault 1.12.8)
- Turbine trip (Fault 1.12.8)
- Inadvertent closure of main steam isolation valves (MSIVs) (Fault 1.16.7)
- Loss of condenser vacuum and other events resulting in turbine trip (Fault 1.18.1)
- Loss of offsite ac power to the station auxiliaries (Fault 1.19.1)
- Loss of normal feedwater flow (Fault 1.16.1)

Spurious reactor trip is also included here, as this initiator leads to a turbine trip after a short delay, and therefore is bounded by the turbine trip fault.

Possible causes of a loss of normal feedwater to one SG (Fault 1.17.1) are:

- Instabilities in flow as a result of operator error
- Instabilities in flow as a result of mechanical causes
- Feed heater blockage

The feedwater line break accident, which also leads to a loss of feedwater, is considered separately and is discussed in the next section.

Other faults that could cause a decrease in heat removal are:

- Loss of circulating water (Fault 1.18.1)
- Condenser leakage (Fault 1.18.1)
- Loss of compressed air (Fault 1.20.1)
- Loss of ultimate heat sink (Fault 1.18.1)

In practice, there are no steam pressure regulators in the AP1000 plant for which failure or malfunction would cause a steam flow transient with loss of external load, inadvertent closure of the MSIVs, and loss of condenser vacuum, all leading to a turbine trip event.

Initiating Event Frequency[1]

The AP1000 design PSA gives the IEF for loss of MFW to both SGs as 8.9E-2/yr and the loss of feed to one SG as 1.92E-1/yr (Table 8A-2). There are also other faults that could result in a reduction of the capacity of the secondary system to remove heat generated in the RCS and are considered in this section along with the loss of MFW, and therefore this is classified as a frequent fault.

Design Basis Class

The unmitigated consequences of these faults are assumed to be greater than the Target 4 BSL for frequent faults (1 mSv offsite and 20 mSv onsite). Given the IEF above, the event is in the DB2 class.

9.2.0.2 Feedwater Line Break Fault

Description

This fault is a break in an SG feedwater line (Fault 1.16.8).

A feedwater line rupture reduces the ability to remove heat generated by the core from the RCS for the following reasons:

- Feedwater flow to the SGs is reduced, causing the reactor coolant temperatures to increase prior to reactor trip.
- Fluid in the SG may be discharged through the break and not be available for decay heat removal after trip.
- The break may be large enough to prevent the addition of MFW or SFW after trip.

Depending upon the size of the break and the plant operating conditions at the time of the break, the break could cause either an RCS cooldown (by excessive energy discharge through the break) or an RCS heatup. Potential RCS cooldown resulting from a secondary pipe rupture is essentially the same as the MSLB fault (see Section 9.1.5) and is not considered further here. Therefore, only the RCS heatup effects are evaluated for a feedwater line rupture in this section.

The severity of the feedwater line rupture transient depends on a number of system parameters, including the break size, initial reactor power, and the functioning of various control and safety systems. Sensitivity studies (Reference 9.2-4) have shown that the most limiting feedwater line rupture is a double-ended rupture of the largest feedwater line. At the beginning of the transient, the MFW control system is assumed to malfunction because of an adverse environment. Interactions between the break and the MFW control system result in no feedwater flow being injected or lost through the SG feedwater nozzles. This assumption causes the water levels in both SGs to decrease equally until the low SG level (narrow range) reactor trip setpoint is reached.

[1] As discussed in Chapter 8, the frequency for initiating events from the PSA is used in both Chapters 8 and 9 with the sole purpose of supporting the categorisation of the fault to a specific DB category. As noted in Chapter 8, these probabilities should not be considered to be representative of actual frequency of the events, and for several events they can be significantly conservative. Detailed PSA results and their basis are discussed in Chapter 10 of this PCSR.

After reactor trip, a full double-ended rupture of the feedwater line is assumed, such that the faulted SG blows down through the break and no MFW is delivered to the intact SG. These assumptions conservatively bound the most limiting feedwater line rupture that can occur.

Initiating Event Frequency

An examination of the AP1000 design PSA provides reasonable assurance that the revised PSA will yield a full double-ended rupture feedwater line break probability of no greater than 6.6E-4/yr (Table 8A-2), which makes the event an infrequent fault.

Design Basis Class

The unmitigated consequences of a feedwater line break are assumed to be greater than the Target 4 BSL for frequent faults (1 mSv offsite and 20 mSv onsite). Given the IEF above, the event is in the DBL class.

9.2.1 Not Used

9.2.2 Loss of External Electrical Load (Fault 1.12.8)

9.2.2.1 Identification of Causes and Accident Description

A major load loss on the plant can result from a loss of electrical load due to an electrical system disturbance. The ac power remains available to operate plant components such as the reactor coolant pumps; as a result, the standby onsite diesel generators do not function for this event. Following the loss of generator load, an immediate fast closure of the turbine control valves occurs. The automatic turbine bypass system accommodates the excess steam generation. Reactor coolant temperatures and pressure do not significantly increase if the turbine bypass system and pressuriser pressure control system function properly. If the condenser is not available, the excess steam generation is relieved to the atmosphere. Additionally, main feedwater flow is lost if the condenser is not available. For this transient, feedwater flow is maintained by the startup feedwater system.

For a loss of electrical load without subsequent turbine trip, no direct reactor trip signal is generated. The plant trips from the PMS if a safety limit is approached. A continued steam load of approximately 5 percent exists after total loss of external electrical load because of the steam demand of plant auxiliaries.

If a safety limit is approached, protection is provided by High-2 pressuriser pressure, high pressuriser water level, and overtemperature ΔT trips. Voltage and frequency relays associated with the reactor coolant pump provide no additional safety function for this event. Following a complete loss of external electrical load, the maximum turbine overspeed is not expected to affect the voltage and frequency sensors. Any increased frequency to the reactor coolant pump motors results in a slightly increased flow rate and subsequent additional margin to safety limits. For postulated loss of load and subsequent turbine-generator overspeed, an overfrequency condition is not seen by the PMS equipment or other safety-related loads. Safety-related loads and the PMS equipment are supplied from the 120-Vac instrument power supply system, which in turn is supplied from the inverters. The inverters are supplied from a dc bus energised from batteries or by a regulated ac voltage.

If the steam dump valves fail to open following a large loss of load, the steam generator safety valves may lift and the reactor may be tripped by the High-2 pressuriser pressure signal, the high pressuriser water level signal, or the overtemperature ΔT signal. This would cause steam generator

shell side pressure and reactor coolant temperature to increase rapidly. However, the pressuriser safety valves and steam generator safety valves are sized to protect the reactor coolant system and steam generator against overpressure for load losses, without assuming the operation of the turbine bypass system, pressuriser spray, or automatic rod cluster control assembly control.

The steam generator safety valve capacity is sized to remove the steam flow at the nuclear steam supply system thermal rating from the steam generator, without exceeding 110 percent of the steam system design pressure. The pressuriser safety valve capacity is sized to accommodate a complete loss of heat sink with the plant initially operating at the maximum turbine load. The pressuriser safety valves can then relieve sufficient steam to maintain the reactor coolant system pressure within 110 percent of the reactor coolant system design pressure.

A discussion of overpressure protection can be found in WCAP-7769, Revision 1 (Reference 9.2-1) and WCAP-16779 (Reference 9.2-9).

A loss-of-external-load event results in a plant transient that is bounded by the turbine trip event analysed in Section 9.2.3. Therefore, a detailed transient analysis is not presented for the loss-of-external-load event.

The primary side transient is caused by a decrease in heat transfer capability, from primary to secondary, due to a rapid termination of steam flow to the turbine, accompanied by an automatic reduction of feedwater flow (should feedwater flow not be reduced, a larger heat sink is available and the transient is less severe). Reduction of steam flow to the turbine following a loss-of-external load event occurs due to automatic fast closure of the turbine control valves. Following a turbine trip event, termination of steam flow occurs via turbine stop valve closure, which occurs in approximately 0.15 seconds. The transient in primary pressure, temperature, and water volume is less severe for the loss-of-external-load event than for the turbine trip due to a slightly slower loss of heat transfer capability.

Appendix 9C provides discussion and analysis of long term safe shutdown for non-LOCA events.

9.2.2.2 Design Basis Mitigation

Refer to Section 9.2.3.2 for the method used to analyse the limiting transient (turbine trip) in this set of events. The results of the turbine trip event analysis bound those expected for the loss-of-external-load event, as discussed in Section 9.2.2.1.

Plant systems and equipment that may be required to function in order to mitigate the effects of a complete loss of load are discussed in Section 9.0.4 and listed in Table 9.0-10.

The PMS may be required to terminate core heat input and to prevent DNB. Depending on the magnitude of the load loss, pressuriser safety valves and/or steam generator safety valves may open to maintain system pressures below allowable limits. No single active failure prevents operation of any system required to function. Normal plant control systems and engineered safety systems are not required to function. The PRHR system may be automatically actuated following a loss of main feedwater, further mitigating the effects of the transient.

9.2.2.3 Diverse Mitigation

Diverse mitigation capabilities are the same as for the loss of normal feedwater fault, as described in Section 9.2.7.3.

9.2.2.3.1 Diverse Mitigation for ATWT

A decrease in heat removal by the secondary system can result from a loss of electrical load due to an electrical system disturbance. In this situation, the ac power remains available to operate plant auxiliaries such as reactor coolant pumps and feedwater to the steam generators. If the main electrical generator is disconnected from the grid and a turbine trip does not occur, the main turbine control system will reduce steam flow to the turbine to match the electrical power demand to station auxiliaries.

Normally, for large step change load reductions, steam is bypassed directly to the condenser via the turbine bypass system. If the turbine bypass system is not available or not sufficient, steam may be vented to the atmosphere via the power-operated atmospheric relief valves and the main steam safety valves.

The sudden reduction in steam flow due to the turbine trip will cause the RCS to heat up. This may result in a reactor trip on high pressuriser pressure and opening of pressuriser safety valves. Like the inadvertent turbine trip event, the loss of external electrical load is a type of load rejection incident. Therefore, the results and conclusions of the turbine trip analysis can be applied to bound the loss of external electrical load event.

The turbine trip event, as analysed in Section 9.2.3.3.1, was determined to be bounding of this event.

9.2.2.3.2 Diverse Mitigation for Core Cooling

The loss of normal feedwater diverse core cooling, as analysed in Section 9.2.7.3.2, was determined to be bounding of all non-LOCA events.

9.2.2.4 Radiological Consequences

Refer to Section 9.2.3.4 for the design basis radiological consequences for the limiting transient (turbine trip) in this set of events. The results of the turbine trip event analysis bound those expected for the loss-of-external-load event, as discussed in Section 9.2.2.1.

9.2.2.5 As Low As Reasonably Practicable Assessment

The ALARP discussion for this event is the same as for the loss of normal feedwater fault event, as described in Section 9.2.7.5.

9.2.2.6 Conclusions

Based on results obtained for the turbine trip event and considerations described in Section 9.2.2.1, the evaluation criteria for a loss-of-external-load event are met (see Section 9.2.3).

This event has also been adequately assessed with respect to ATWT considerations.

It has been shown that the AP1000 plant design includes adequate systems for the protection of this fault, which limit the radiological consequences such that they are compliant with the SAPs targets and the risks have been reduced to be ALARP.

9.2.3 Turbine Trip (Fault 1.12.8)

9.2.3.1 Identification of Causes and Accident Description

The turbine stop valves close rapidly (about 0.15 seconds) on loss of trip fluid pressure actuated by one of a number of possible turbine trip signals. Turbine trip initiation signals include:

- Generator trip
- Low condenser vacuum
- Loss of lubricating oil
- Turbine thrust bearing failure
- Turbine overspeed
- Manual trip
- Reactor trip

Upon stop valve closure due to a turbine trip, steam flow to the turbine stops abruptly. Sensors for the Turbine First Stage Pressure detect the loss in steam flow and initiate turbine bypass. The loss of steam flow results in a rapid increase in secondary system temperature and pressure, with a resultant primary system transient, described in Section 9.2.2.1, for the loss-of-external-load event. A slightly more severe transient occurs for the turbine trip event due to the rapid loss of steam flow caused by the abrupt valve closure.

The automatic turbine bypass system accommodates up to 40 percent of rated steam flow. Reactor coolant temperatures and pressure do not increase significantly if the turbine bypass system and pressuriser pressure control system are functioning properly. If the condenser is not available, the excess steam generation is relieved to the atmosphere and main feedwater flow is lost. For this situation, feedwater flow is maintained by the startup feedwater system to provide adequate residual and decay heat removal capability. Should the turbine bypass system fail to operate, the steam generator safety valves may lift to provide pressure control. See Section 9.2.2.1 for a further discussion of the transient.

A turbine trip is a more limiting than a loss-of-external-load event, loss of condenser vacuum, and other events which result in a turbine trip. As such, this event is analysed and presented in Section 9.2.3.2.

Appendix 9C provides discussion and analysis of long term safe shutdown for non-LOCA events.

9.2.3.2 Design Basis Mitigation

Analysis is performed to demonstrate the adequacy of the PMS to detect and mitigate the fault and show that the safety analysis criteria are satisfied including:

- No fuel failures (confirmed using minimum DNBR and fuel melt criteria),
- The RCS pressure criterion is met,
- The MSS pressure criterion is met, and
- The pressuriser does not fill (which could result in a LOCA)

9.2.3.2.1 DBA Method of Analysis

In this analysis, the behaviour of the unit is evaluated for a complete loss of steam load from 100 percent of full power, without rapid power reduction, primarily to show the adequacy of the pressure-relieving devices, and to demonstrate core protection margins. The turbine is assumed to

trip without actuating the rapid power reduction system. This assumption delays reactor trip until conditions in the reactor coolant system result in a trip due to other signals. Thus, the analysis assumes a bounding transient. In addition, no credit is taken for the turbine bypass system. Main feedwater flow is terminated at the time of turbine trip, with no credit taken for startup feedwater or the PRHR heat exchanger (except for long-term recovery) to mitigate the consequences of the transient.

Analyses are performed to evaluate the effects produced by a possible consequential loss of offsite power during a complete loss of steam load. As discussed in Section 9.0.12, the loss of offsite power is considered as a direct consequence of a turbine trip occurring while the plant is operating at power. The primary effect of the loss of offsite power is to cause the reactor coolant pumps to coast down.

The turbine trip transients are analysed by using a modified version of the LOFTRAN code (Reference 9.2-2) as described in Reference 9.2-6. The program simulates the neutron kinetics, reactor coolant system, pressuriser, pressuriser safety valves, pressuriser spray, steam generator, and steam generator safety valves. The program computes pertinent plant variables, including temperatures, pressures, and power level.

In the turbine trip analyses, which include a primary coolant flow coastdown caused by a consequential loss of offsite power, a combination of three computer codes is used to perform the DNBR analyses. First, the LOFTRAN code (References 9.2-2 and 9.2-6) is used to calculate the plant system transient. The FACTRAN code (Reference 9.2-7) or the VIPRE-01 fuel rod model (Reference 9.2-8), which is equivalent to FACTRAN, is then used to calculate the core heat flux based on nuclear power and reactor coolant flow from LOFTRAN. Finally, the VIPRE-01 code is used to calculate the DNBR using heat flux from FACTRAN (or the VIPRE-01 fuel rod model) and flow from LOFTRAN.

The major assumptions used in the analysis are summarised below.

Initial Operating Conditions

Two sets of initial operating conditions are used. Cases performed to evaluate the minimum DNBR obtained are analysed using the revised thermal design procedure. Initial core power, reactor coolant temperature, and pressure are assumed to be at their nominal values consistent with steady-state full-power operation. Uncertainties in initial conditions are included in the DNBR limit as described in WCAP-11397-P-A (Reference 9.2-5). Instrument bias on the RCS temperature signal is also considered to ensure it is reflected in either the modelled initial conditions or the safety analysis DNBR limit value.

Cases performed to evaluate the maximum calculated RCS pressure include uncertainties on the initial conditions. Initial core power, reactor coolant temperature, and pressure are assumed to be at the nominal full-power values plus or minus uncertainties. The direction of the uncertainties is chosen to maximise the RCS pressure.

Reactivity Coefficients

Two cases are analysed:

- Minimum reactivity feedback – A least-negative moderator temperature coefficient and a least-negative Doppler-only power coefficient are assumed (see Figure 9.0-3).

- Maximum reactivity feedback – A conservatively large negative moderator temperature coefficient and a most-negative Doppler-only power coefficient are assumed (see Figure 9.0-3).

Rod Control

From the standpoint of the maximum RCS pressure and minimum DNBR attained, it is conservative to assume that the reactor is in manual rod control. If the reactor is in automatic rod control, the control rod banks move prior to trip and reduce the severity of the transient.

Steam Release

No credit is taken for the operation of the turbine bypass system or steam generator power-operated relief valves. The steam generator pressure rises to the safety valve setpoint where steam release through safety valves limits secondary steam pressure at the setpoint value.

Pressuriser Spray

Two cases for both the minimum and maximum reactivity feedback cases are analysed:

- Full credit is taken for the effect of pressuriser spray in reducing or limiting the coolant pressure. Safety valves are also available. These cases are analysed primarily to address DNBR concerns.

- No credit is taken for the effect of pressuriser spray in reducing or limiting the coolant pressure. Safety valves are operable. These cases are analysed to address RCS overpressure concerns.

Feedwater Flow

Main feedwater flow to the steam generators is assumed to be lost at the time of turbine trip. No credit is taken for startup feedwater flow or the PRHR heat exchanger, because a stabilized plant condition is reached before initiation of the startup feedwater or the PRHR heat exchanger is normally assumed to occur. The startup feedwater flow or PRHR heat exchanger removes core decay heat following plant stabilization.

Reactor Trip

Reactor trip is actuated by the first reactor trip setpoint reached, with no credit taken for the rapid power reduction on the turbine trip. Trip signals are expected due to High-2 pressuriser pressure, overtemperature ΔT, Low-2 RCP speed, high pressuriser water level, or low steam generator water level.

Plant characteristics and initial conditions are further discussed in Section 9.0.2. Plant systems and equipment that may be required to function in order to mitigate the effects of a turbine trip event are discussed in Section 9.0.4 and listed in Table 9.0-10.

The PMS may be required to function following a turbine trip. Pressuriser safety valves and/or steam generator safety valves may be required to open to maintain system pressures below allowable limits. No single active failure prevents operation of systems required to function. Cases are analysed, both with and without the operation of pressuriser spray, to determine the worst case for presentation.

Availability of Offsite Power

Each case is analysed with and without offsite power available. As discussed in Section 9.0.12, the loss of offsite power is considered to be a consequence of an event due to disruption of the electrical grid following a turbine trip during the event. The grid is assumed to remain stable for 3 seconds following the turbine trip. In the analysis for the complete loss of steam load, the event is initiated by a turbine trip. Therefore, offsite power is assumed to be lost 3 seconds after the start of the event. For the loss of steam load analysis, the primary impact of the loss of offsite power is a coastdown of the reactor coolant pumps.

Main Steam System Pressure

Additional cases are performed to evaluate the maximum MSS pressure, with initial condition uncertainties chosen to maximize MSS pressure. The additional cases include cases with and without offsite power available for minimum and maximum reactivity feedback.

9.2.3.2.2 DBA Credited SSCs

For the DB, all of the claimed SSCs are Class 1. The claimed Class 1 SSCs are listed in Table 9.0-10. The presented DBA ends shortly after reactor trip; however, essential safety functions for the long term safe shutdown analysis (Appendix 9C) bound safe shutdown response for this event. The primary core cooling is provided by the PRHR and passive containment cooling. Other SSCs include the CMTs, containment isolation, pressuriser SVs and steam generator SVs. The PMS provides the following:

- RT on one of the following (scenario dependent):
  - High-2 pressuriser pressure
  - Overtemperature ΔT
  - Low-2 RCP speed
- PRHR actuation on Low-2 SG NR level coincident with Low-2 SFW flow
- CMTs and containment isolation on Low-2 CL temperature
- PCS on High-2 containment pressure

9.2.3.2.3 DBA Results

The transient responses for a turbine trip from 100 percent of full-power operation are shown for eight cases. The eight analysis cases are performed assuming minimum and maximum reactivity feedback, with and without credit for pressuriser spray, and with and without offsite power available. The results of the analyses are shown in Figures 9.2.3-1 through 9.2.3-26. The calculated sequence of events for the accident is shown in Table 9.2-1. Additional cases performed to address maximum MSS pressure concerns confirm that the steam generator safety valves provide sufficient pressure relief to prevent overpressurisation of the MSS.

Minimum Reactivity Feedback, With Pressuriser Spray, With and Without Offsite Power Available

Figures 9.2.3-1 through 9.2.3-7 show the transient responses for two cases analysed for DNBR concerns with and without offsite power available. In the case with offsite power available, the reactor is tripped by the overtemperature ΔT trip function. The transient DNBR is shown in

Figure 9.2.3-6; the minimum DNBR remains above the safety analysis DNBR limit value at all times. Based on this, the DNB design basis defined in Section 22.7.1.1 is met.

The case without offsite power is tripped by the low reactor coolant pump speed trip function. The minimum DNBR remains above the safety analysis DNBR limit value at all times, as shown in Figure 9.2.3-6; therefore, the DNBR design basis defined in Section 22.7.1.1 is met. This case is the limiting case with respect to the DNBR margin of the turbine trip cases.

Maximum Reactivity Feedback, With Pressuriser Spray, With and Without Offsite Power Available

Figures 9.2.3-8 through 9.2.3-14 show the transient responses for the other two cases analysed for DNBR concerns, with and without offsite power available. In the case with offsite power available, the reactor is tripped by the overtemperature ΔT trip function. The transient DNBR is shown in Figure 9.2.3-13; the minimum DNBR remains above the safety analysis DNBR limit value at all times. Based on this, the DNBR design basis defined in Section 22.7.1.1 is met for this case.

The case without offsite power is tripped by the low reactor coolant pump speed trip function. The DNBR transient is similar to, and bounded by, the minimum feedback case with pressuriser spray and without offsite power discussed above. The minimum DNBR remains above the safety analysis DNBR limit value at all times, as shown in Figure 9.2.3-13; therefore, the DNBR design basis defined in Section 22.7.1.1 is met.

Minimum Reactivity Feedback, Without Pressuriser Spray, With and Without Offsite Power Available

Figures 9.2.3-15 through 9.2.3-20 show the transient responses for two cases analysed to address RCS overpressure concerns, with and without offsite power available. In the case with offsite power available, the reactor is tripped by the high pressuriser pressure trip function. The case without offsite power is tripped by the low reactor coolant pump speed reactor trip function. The pressuriser safety valves actuate in both of these cases and maintain the reactor coolant system pressure below 110 percent of the design value. RCS pressure for these cases is shown in Figure 9.2.3-16. Note that with and without offsite power cases have different assumptions regarding initial pressure. The initial pressure assumptions were based upon sensitivities that were run. With respect to maximum reactor coolant system pressure, the case with offsite power available is the most limiting for turbine trip cases.

Maximum Reactivity Feedback, Without Pressuriser Spray, With and Without Offsite Power Available

Figures 9.2.3-21 through 9.2.3-26 show the transient responses for the two other cases analysed to address RCS pressure concerns, with and without offsite power available. In the case with offsite power available, the reactor is tripped by the High-2 pressuriser pressure function. The case without offsite power is tripped by the low reactor coolant pump speed trip function. The pressuriser safety valves actuate in both of these cases and maintain the reactor coolant system pressure below 110 percent of the design value. RCS pressure for both cases is shown in Figure 9.2.3-22. Note that with and without power cases have different assumptions regarding initial pressure. The initial pressure assumptions were based upon sensitivities that were run.

9.2.3.3 Diverse Mitigation

Diverse mitigation capabilities are the same as for the loss of normal feedwater fault, as described in Section 9.2.7.3.

9.2.3.3.1 Diverse Mitigation for ATWT

Turbine trip events are characterised by a reduction in steam flow from the steam generator. The reduction in steam flow causes the RCS and secondary system to heat up. The turbine trip event produces a transient that is similar to a loss of generator electrical load, the closure of the main steam isolation valves, and a loss of the condenser. In general, these events produce a turbine trip and a sudden reduction of steam flow from the steam generators.

The turbine trip analyses documented in this section are performed to bound the following events:

- As discussed in Section 9.2.2.4, the loss of generator electrical load can result in the turbine control system tripping the turbine. AC power for plant auxiliary loads is then supplied by offsite power. The condenser would be expected to be available in this case. With the condenser available, turbine bypass and the feedwater system would also be operable.

- The closure of the main steam isolation valves (Section 9.2.4) results in termination of the steam flow from the steam generators, similar to a turbine trip. Closure of the main steam isolation valves also isolates the turbine bypass system from the steam generators.

- The loss of condenser event (Section 9.2.5) results in an immediate turbine trip. If the condenser is unavailable, then turbine bypass which exhausts to the condenser will also be unavailable. Without exhaust steam from the turbine or the turbine bypass system to the condenser, the inventory for the feedwater system will be depleted after some time.

The scenarios with turbine trip and simultaneous loss of feedwater are analysed in Section 9.2.7.

A number of cases were considered to address different potential CCFs that can affect the PMS and its ability to insert RCCAs. The turbine trip analysis documented in this section is performed to bound the following events:

- Turbine trip with a PMS CCF – The CCF prevents all PMS reactor trips signals and engineered safeguards features signals. The DAS is assumed to be completely operable. Offsite power and turbine bypass are also assumed available.

- Turbine trip with a PMS reactor trip breaker CCF - This failure prevents the PMS from inserting the rods; however, PMS logic continues to function, and all engineered safeguards features signals are operable. DAS is completely operable, including its capability to drop rods. Offsite power and turbine bypass are also assumed to be available.

- Turbine trip with a RCCA mechanical CCF - The PMS, DAS, and control systems are assumed to be operable except that RCCAs do not insert into the core on a trip signal.

This analysis is performed to demonstrate the adequacy of the operable portions of the PMS (considering the impact of the CCF) as well as the DAS to detect and actuate mechanical SSCs to mitigate the fault. The following ATWT acceptance criteria are applicable to this event:

- The RCS does not overpressurise due to reactor coolant heatup. The ATWT pressure limit is 22.06 MPa-rel (3200 psig).
- There is no significant fuel damage.
- The rate and duration of energy release to containment is much less than for the design basis LOCA. This demonstrates that the containment does not overpressurise due to the energy release to the containment.

9.2.3.3.1.1 Diverse ATWT Method of Analysis

The analysis uses the methods outlined for the DBA, with revised assumptions. The assumptions used for the limiting ATWT turbine trip, a common cause failure of the PMS, are discussed below.

- Plant initial conditions are at the nominal full power values.
- No measurement/instrumentation errors are assumed.
- Core kinetics parameters and initial boron concentration are both assumed to be at beginning of cycle (BOC) values.
- Moderator temperature coefficient (MTC) is modelled as discussed in Reference 9.2-11.
- Pressuriser pressure and level control systems are not credited in the analyses.
- SG power operated relief valves are assumed to be operable for all cases.
- The turbine bypass system is assumed to be operable. It is noted that the assumption of turbine bypass operability is conservative, [ ] The RCS temperature reduction will increase core reactivity.

9.2.3.3.1.2 Diverse ATWT Credited SSCs

As noted in 9.2.3.3.1.3, no available SSCs (PMS or DAS functions) are credited to initiate passive safety features for this limiting ATWT. Instead, the plant will reach an equilibrium power condition and ATWT criteria would be met. Ultimately, manual operator action would be required to shut down the plant. Section 9.2.7.3.1 considers the turbine trip and simultaneous loss of feedwater ATWT, which bounds this event.

9.2.3.3.1.3 Diverse ATWT Results

Turbine Trip with PMS CCF

This section describes a turbine trip with a CCF of the PMS. The CCF prevents all PMS reactor trips signals and engineered safeguards features signals. The DAS is assumed to be completely operable. Offsite power, turbine bypass, and feedwater are also assumed available. It is noted that turbine trip with simultaneous loss of normal feedwater (LONF) with a PMS CCF is addressed in the Section 9.2.7.3.1.

Table 9.2.3-1 shows the sequence of events for the fault. The transient response of the event is shown in Figures 9.2.3-27 to 9.2.3-31.

At the start of the event, the turbine is tripped and all steam flow from the steam generators is terminated. The feedwater system and main coolant pumps are assumed to continue operating normally. The feedwater control system maintains SG level. The loss of secondary side steam flow causes the secondary and primary systems to heatup.

The turbine bypass system control logic block in the PLS is cleared due to the turbine trip detection and the turbine bypass system starts to open in average temperature (T_{avg}) mode. Several seconds after the turbine trip, the turbine bypass valves are fully open. However, the turbine bypass system is unable to remove all of the energy transferred to the secondary side, and secondary side pressure increases until the SG PORVs are opened.

The RCS heatup causes fluid expansion and an increase in pressuriser water level and is accompanied by an increase in pressure until the pressuriser safety valves open for a short period. PMS reactor trip high pressuriser pressure and level setpoints are reached, but no PMS action occurs due to the PMS mode failure. There are no parameters monitored by DAS which would cause DAS system intervention. As the reactor coolant temperature increases, core power decreases due to moderator feedback. Core power decreases to an equilibrium value that is equal to the energy removal rate of the turbine bypass system and the steam generator relief valves.

Without turbine steam flow, extraction steam for feedwater heaters will be lost, and feedwater temperature will decrease toward the condenser hot well temperature, thus increasing the amount of energy the turbine bypass can remove from the nuclear steam supply system (NSSS). Atmospheric relief would carry off any excess steam generation. If this steam is not replenished, the SG liquid inventory will eventually decrease to the point at which heat transfer from the primary is diminished. This would cause further heating of the RCS and reduction of core power. If feedwater is lost entirely, the event becomes a LONF from a reduced power and is bounded by the analyses in Section 9.2.7.3.1. Otherwise, the stable power would continue until terminated by manual action.

To shut down the reactor from these stable conditions, operator action will be necessary.

This fault is less limiting for RCS overpressure than the loss of feedwater ATWT event as analysed in Section 9.2.7.3, less limiting for core damage than the complete loss of RCS flow ATWT event as analysed in Section 9.3.2.3, and does not involve substantial energy release to containment. Therefore, since those events are shown to meet the ATWT acceptance criteria, the AP1000 design meets the ATWT acceptance criteria for the turbine trip event.

9.2.3.3.2 Diverse Mitigation for Core Cooling

The loss of normal feedwater diverse core cooling, as analysed in Section 9.2.7.3.2, was determined to be bounding of all non-LOCA events.

9.2.3.4 Radiological Consequences

Design Basis

In the case where offsite power remains available, there is no release of activity to the environment and the Target 4 BSOs (0.01 mSv offsite and 0.1 mSv onsite) are met.

In the case where offsite power is lost, a small release of activity may occur as a result of steam dump to the atmosphere due to unavailability of the condensers. With no fuel damage and primary and secondary circuits intact, the initiating event has no impact on the doses. The doses are a consequence of the assumed loss of offsite power. Therefore, the loss of offsite power doses from Section 9.2.6.4 are presented. The calculated maximum doses for all relevant pathways (inhalation, cloudshine, and groundshine) are as follows:

- Offsite dose: 0.05 mSv Worker dose: 1.5 mSv

These doses are within the Target 4 BSL for frequent faults (1 mSv offsite and 20 mSv onsite).

Diverse Mitigation

Both the diverse ATWT and diverse core cooling scenarios (bounded by the loss of normal feedwater diverse core cooling, as analysed in Section 9.2.7.3.2) demonstrate that the RCS does not overpressurise and there is no significant fuel damage. For a diverse mitigation radiological consequences analysis better estimate assumptions would be credited. This would include reactor coolant system activity levels significantly lower than those modelled for the DBA and better activity retention in containment and in the steam generators. In addition better estimate atmospheric dispersion factors would be used. Therefore, a diverse mitigation radiological consequences analysis would show that the doses for the diverse ATWT scenario would be less than those reported for the non-LOCA DBAs and doses for the diverse core cooling scenario would be much less than for the design basis LOCA. The diverse mitigation analyses would not have to meet the Target 4 BSL for frequent faults and would meet the Target 4 BSL for infrequent faults.

9.2.3.5 As Low As Reasonably Practicable Assessment

The ALARP discussion for this event is the same as for the loss of normal feedwater fault event, as described in Section 9.2.7.5.

9.2.3.6 Conclusions

Results of the DB analyses show that a turbine trip presents no challenge to the integrity of the reactor coolant system or the main steam system. Pressure-relieving devices incorporated in the two systems are adequate to limit the maximum pressures to within the design limits.

The DB analyses show that the predicted DNBR is greater than the safety analysis DNBR limit value at any time during the transient. Thus, the departure from nucleate boiling design basis, as described in Section 22.7.1.1, is met.

The ATWT acceptance criteria are met. This event was explicitly analysed for the change in the current design reference point in the UK as described in Reference 9.2-13. The evaluation conducted to closeout FS-03 (Reference 9.2-14) demonstrated that there is little impact on the key analysis trends, results, and margin to the applicable acceptance criteria. Therefore, the change in design reference point would not invalidate the conclusions presented for this event.

Diverse core cooling capabilities have been demonstrated.

DBA radiological consequences are within the Target 4 BSL for frequent faults (1 mSv offsite and 20 mSv onsite). Thus, the identification of necessary Class 1 SSCs is adequate to meet DB requirements.

It has been shown that the AP1000 plant design includes adequate systems for the protection of this fault, which limit the radiological consequences such that they are compliant with the SAPs targets and the risks have been reduced to be ALARP.

9.2.4 Inadvertent Closure of Main Steam Isolation Valves (Fault 1.16.7)

Inadvertent closure of the main steam isolation valves results in a turbine trip with no credit taken for the turbine bypass system. Turbine trips are discussed in Section 9.2.3.

The inadvertent closure of the main steam isolation valves ATWT event is bounded by the analysis of the turbine trip ATWT event discussed in Section 9.2.3.5. There are two justifications for this assertion: one is related to the physical difference between valve stroke times, and the other is related to conservatisms in modelling.

The turbine admission valves can close in tenths of a second. In contrast, the main steam isolation valves require several seconds to close. Therefore, if other parameters are equal, the faster closing valve will cause the more severe pressure increase.

In reality, the other parameters are not equal. There is considerable steam piping volume between the isolation valves and the turbine, which will attenuate the pressure increase. However, it is Westinghouse practice to assume zero steam piping volume for simplicity and conservatism. That practice is continued on these ATWT analyses. Thus, instantaneous closure of the isolation valves is identical to instantaneous closure of the turbine admission valves (with no turbine bypass).

For these reasons, an inadvertent closure of main steam isolation valves ATWT event is bounded by the analysis of the turbine trip ATWT event in Section 9.2.3.5.

9.2.5 Loss of Condenser Vacuum and Other Events Resulting in Turbine Trip (Fault 1.18.1)

Loss of condenser vacuum is one of the events that can cause a turbine trip. Turbine trip initiating events are described in Section 9.2.3. A loss of condenser vacuum prevents the use of steam dump to the condenser. Because steam dump is assumed to be unavailable in the turbine trip analysis, no additional adverse effects result if the turbine trip is caused by loss of condenser vacuum. Therefore, the analysis results and conclusions contained in Section 9.2.3 apply to the loss of the condenser vacuum. In addition, analyses for the other possible causes of a turbine trip, listed in Section 9.2.3.1, are covered by Section 9.2.3. Possible overfrequency effects, due to a turbine overspeed condition, are discussed in Section 9.2.2.1 and are not a concern for this type of event.

Loss of condenser will result in an immediate reactor trip. The difference from other ATWT turbine trips (Section 9.2.3.3.1) is that turbine bypass is not available. If SG steam release is necessary, unavailability of turbine bypass would cause atmospheric steam release at a slightly higher steam pressure. The higher steam pressure would cause a slightly higher RCS cold-leg and core inlet temperature, which is beneficial for RCS overpressure. The increased core inlet temperature would also provide better reactivity feedback and would reduce the equilibrium core power, which is beneficial for DNB. Therefore, a separate assessment of this event is not necessary.

9.2.6 Loss of ac Power to the Plant Auxiliaries (Fault 1.19.1)

9.2.6.1 Identification of Causes and Accident Description

The loss of power to the plant auxiliaries is caused by a complete loss of the offsite grid accompanied by a turbine-generator trip. The onsite standby ac power system remains available but is not credited to mitigate the accident.

From the decay heat removal point of view, in the long term this transient is more severe than the turbine trip event analysed in Section 9.2.3 because, for this case, the decrease in heat removal by the secondary system is accompanied by a reactor coolant flow coastdown, which further reduces the capacity of the primary coolant to remove heat from the core. The reactor will trip:

- Upon reaching one of the trip setpoints in the primary or secondary systems as a result of the flow coastdown and decrease in secondary heat removal.

- Due to the loss of power to the control rod drive mechanisms as a result of the loss of power to the plant.

Following a loss of ac power with turbine and reactor trips, the sequence described below occurs:

- Plant vital instruments are supplied from the Class 1E and uninterruptable power supply.

- As the steam system pressure rises following the trip, the steam generator power-operated relief valves may be automatically opened to the atmosphere. The condenser is assumed not to be available for turbine bypass. If the steam flow path through the power-operated relief valves is not available, the steam generator safety valves may lift to dissipate the sensible heat of the fuel and coolant plus the residual decay heat produced in the reactor.

- The onsite standby power system, if available, supplies ac power to the selected plant non-safety loads.

- As the no-load temperature is approached, the steam generator power-operated relief valves (or safety valves, if the power-operated relief valves are not available) are used to dissipate the residual decay heat and to maintain the plant at the hot shutdown condition if the startup feedwater is available to supply water to the steam generators.

- If startup feedwater is not available, the PRHR heat exchanger is actuated.

During a plant transient, core decay heat removal is normally accomplished by the startup feedwater system if available, which is started automatically when low levels occur in either steam generator. If that system is not available, emergency core decay heat removal is provided by the PRHR heat exchanger. The PRHR heat exchanger is a C-tube heat exchanger connected, through inlet and outlet headers, to the reactor coolant system. The inlet to the heat exchanger is from the reactor coolant system hot leg, and the return is to the steam generator outlet plenum. The heat exchanger is located above the core to provide natural circulation flow when the reactor coolant pumps are not operating. The IRWST provides the heat sink for the heat exchanger. The PRHR heat exchanger, in conjunction with the passive containment cooling system, keeps the reactor coolant subcooled for greater than 14 days. After the IRWST water reaches saturation, steam starts to vent to the containment atmosphere. The condensation that collects on the containment steel shell (cooled by the passive containment cooling system) returns to the IRWST, maintaining fluid level for the PRHR heat exchanger heat sink. The analysis shows that the natural circulation flow

in the reactor coolant system following a loss of ac power event is sufficient to remove residual heat from the core.

Upon the loss of power to the reactor coolant pumps, coolant flow necessary for core cooling and the removal of residual heat is maintained by natural circulation in the reactor coolant and PRHR loops.

This event is more limiting with respect to long-term heat removal than the turbine trip initiated decrease in secondary heat removal without loss of ac power, which is discussed in Section 9.2.3. A loss of offsite power to the plant auxiliaries will also result in a loss of normal feedwater.

Appendix 9C provides discussion and analysis of long term safe shutdown for non-LOCA events.

9.2.6.2 Design Basis Mitigation

Analysis is performed to demonstrate the adequacy of the PMS to detect and mitigate the fault. It also demonstrates the capability of the PRHR heat exchanger to sufficient decay heat following a loss of normal feedwater. Those systems show that the safety criteria are satisfied including:

- No fuel failures (confirmed using minimum DNBR and fuel melt criteria),
- The RCS pressure criterion is met,
- The MSS pressure criterion is met, and
- The pressuriser does not fill (which could result in a LOCA)

It is noted that this event is bounded by the Section 9.2.3 analysis with respect to fuel damage and RCS/MSS pressure criteria, therefore, these limits are not explicitly confirmed for this event. Accordingly, Pressuriser filling is the primary criterion for this analysis.

9.2.6.2.1 DBA Method of Analysis

A modified version of the LOFTRAN code (Reference 9.2-2), described in WCAP-15644 (Reference 9.2-6), is used to simulate the system transient following a plant loss of offsite power. The simulation describes the plant neutron kinetics and reactor coolant system, including the natural circulation, pressuriser, and steam generator system responses. The digital program computes pertinent variables, including the steam generator level, pressuriser water level, and reactor coolant average temperature.

The assumptions used in this analysis minimize the energy removal capability of the PRHR heat exchanger and maximise the coolant system expansion.

The assumptions used in the analysis are as follows:

- The plant is initially operating at 101 percent of the design power rating with initial reactor coolant temperature 4.4°C (8°F) below the nominal value and the pressuriser pressure 0.345 MPa (50 psi) above the nominal value.

- Core residual heat generation is based on ANSI/ANS 5.1-1979 (Reference 9.2-3). ANSI 5.1 is a conservative representation of the decay energy release rates.

- Reactor trip occurs on RCP speed-low.

- A heat transfer coefficient is assumed in the steam generator associated with reactor coolant system natural circulation flow conditions following the reactor coolant pump coastdown.

- The PRHR heat exchanger is actuated by the Low-2 steam generator water level (narrow range coincident with Low-2 start up feed water flow).

- For the loss of ac power to the station auxiliaries and following reactor trip, the main safety function required is core decay heat removal. That is accomplished by the secondary steam relief through the steam generator safety valves and by the PRHR heat exchanger. One of two parallel valves in the PRHR outlet line is assumed to fail to open. This is the worst single failure.

- The pressuriser safety valves are assumed to function.

Plant characteristics and initial conditions are further discussed in Section 9.0.2.

Plant systems and equipment necessary to mitigate the effects of a loss of ac power to the station auxiliaries are discussed in Section 9.0.4 and listed in Table 9.0-10. Normal reactor control systems are not required to function. The PMS is required to function following a loss of ac power. The PRHR heat exchanger is required to function with an overall minimum capability to extract heat from the reactor coolant system. No single active failure prevents operation of any system required to function.

Parameters used in the analysis are selected to maximise the pressuriser water volume. Input parameters are not selected to maximise the transient primary side and secondary side pressure. Transient primary side and secondary side pressures during a loss of ac power to station auxiliaries are bounded by those calculated for the turbine trip analyses described in Section 9.2.3.

With respect to DNB concerns, the loss of ac power to station auxiliaries event is bounded by the loss of ac power case analysed for the turbine trip event described in Section 9.2.3.

9.2.6.2.2 DBA Credited SSCs

For the DB, all of the claimed SSCs are Class 1. The claimed Class 1 SSCs are listed in Table 9.0-10. The presented DBA ends before CMT actuation; however, the long term safe shutdown analysis (Appendix 9C) bounds safe shutdown response for this event. The primary core cooling is provided by the PRHR and passive containment cooling. Other SSCs include the CMTs, containment isolation, pressuriser SVs and steam generator SVs. The PMS provides the following:

- RT on Low-2 RCP speed

- PRHR actuation on Low-2 SG NR level coincident with Low-2 SFW flow

- CMTs and containment isolation on Low-2 CL temperature

- PCS on High-2 containment pressure

9.2.6.2.3 DBA Results

The transient response of the reactor coolant system following a loss of ac power to the plant auxiliaries is shown in Figures 9.2.6-1 through 9.2.6-12. The calculated sequence of events for this event is listed in Table 9.2-1.

The loss of ac power event results in a pressuriser water volume increase until the actuation of the steam generator safety valves. Actuation of the steam generator safety valves attenuates the

pressuriser water volume until actuation of the PRHR, which turns around the pressuriser water volume increase. PRHR heat extraction and steam generator safety valve relief results in a consequential decrease in the pressuriser water volume until the safety valve relief stops. After the steam generator safety valve flow stops, the pressuriser water volume begins a slight increase until the PRHR heat extraction matches and then exceeds the decay heat addition resulting in a reduction in the pressuriser water volume.

9.2.6.3 Diverse Mitigation

Diverse mitigation capabilities are the same as for the loss of normal feedwater fault, as described in Section 9.2.7.3.

9.2.6.3.1 Diverse Mitigation for ATWT

Loss of ac power to the station auxiliaries will cause loss of RCS flow, loss of main feedwater and immediate turbine trip, and loss of power to the rod control system (causing immediate reactor trip regardless of whether any PMS or DAS signal exists). This would become an ATWT event only if a control rod mechanical failure is postulated that prevents control rod insertion. In the event of postulated failure of the control rods to insert, this event becomes similar to a loss of feedwater with turbine trip, addressed in Section 9.2.7.3.1, with the only difference being that a loss of ac power would result in a trip of RCPs at the beginning of the transient. An immediate trip of RCPs is beneficial for RCS overpressure and does not cause DNB (as shown in Section 9.3.2.5). Therefore, no separate assessment of this event is required to demonstrate that the AP1000 design meets the ATWT acceptance criteria.

9.2.6.3.2 Diverse Mitigation for Core Cooling

The loss of normal feedwater diverse core cooling, as analysed in Section 9.2.7.3.2, was determined to be bounding of all non-LOCA events.

9.2.6.4 Radiological Consequences

Design Basis

The DBA evaluation of the radiological consequences of a postulated loss of offsite power assumes that the reactor has been operating with a limited number of fuel rods containing cladding defects and that leaking steam generator tubes have resulted in a build-up of activity in the secondary coolant.

It is determined that no fuel rods are damaged as a result of the accident such that the activity contained in the fuel-cladding gap is released to the reactor coolant.

Two separate accident scenarios are addressed. In the first scenario, it is assumed that the non-safety grade SFW system is not available to provide feedwater to the steam generators. In this event, the water level in the steam generators drops, resulting in PRHR actuation. The period of steaming is terminated when the capacity of the PRHR system exceeds the decay heat generation rate.

In the second scenario, it is assumed that SFW is available to maintain water level in the steam generators such that PRHR is not actuated, resulting in a longer period of steaming releases. The period of steaming is terminated when RNS is in service and its capacity exceeds the decay heat generation rate.

Diverse Mitigation

Both the diverse ATWT and diverse core cooling scenarios demonstrate that the RCS does not overpressurise and there is no significant fuel damage. For a diverse mitigation radiological consequences analysis better estimate assumptions would be credited. This would include reactor coolant system activity levels significantly lower than those modelled for the DBA and better activity retention in containment and in the steam generators. In addition better estimate atmospheric dispersion factors would be used. Therefore, a diverse mitigation radiological consequences analysis would show that the doses for the diverse ATWT scenario would be less than those reported for the non-LOCA DBAs and doses for the diverse core cooling scenario would be much less than for the design basis LOCA. The diverse mitigation analyses would not have to meet the Target 4 BSL for frequent faults and would meet the Target 4 BSL for infrequent faults.

9.2.6.4.1 DBA Source Term

There is no fuel damage as a result of the accident. Therefore, the most significant radionuclide releases are the noble gases, alkali metals, and iodines that are present in the primary and secondary coolants, become airborne, and are released to the environment as a result of the accident.

The initial reactor coolant system iodine concentrations are assumed to be those associated with the equilibrium operating limit for primary coolant iodine activity. An iodine spike is assumed to be initiated by the accident, with the spike causing an increasing level of iodine in the reactor coolant.

The secondary coolant iodine and alkali metal concentrations are assumed to be 10 percent of the primary concentrations. Noble gases are not assumed to accumulate in the secondary coolant

9.2.6.4.2 DBA Release Pathways

The reactor coolant leaking into the steam generators is assumed to mix with the secondary coolant. As steam is released, a portion of the iodine and alkali metal activity in the coolant is released. The fraction of activity released is defined by the reducing conditions within the steam generator. Volatile (elemental) iodines are treated as a direct release from the RCS to the environment. Non-volatile (particulate) iodines and alkali metals are assumed to enter the secondary coolant. Release from the secondary coolant is limited by the assumed moisture carryover. The noble gas activity entering the secondary side is released to the environment. These releases are terminated when the steam releases stop.

9.2.6.4.3 DBA Dose Calculation Models

The models used to calculate offsite and control room doses are provided in Appendix 9A.

9.2.6.4.4 DBA Analytical Assumptions and Parameters

The assumptions and parameters used in the analysis are listed in Table 9.2.6-1.

9.2.6.4.5 DBA Doses

The highest doses are found to be for the case with SFW available. The calculated maximum doses for all relevant pathways (inhalation, cloudshine, and groundshine) are as follows:

- Offsite dose: 0.05 mSv Worker dose: 1.5 mSv

These doses are within the Target 4 BSL for frequent faults (1 mSv offsite and 20 mSv onsite).

The limiting conditions for operation of the Technical Specifications used in the dose assessment are provided in Table 9.2.6-2. The Table 9.2.6-2 values ensure the Target 4 BSLs are met.

9.2.6.5 As Low As Reasonably Practicable Assessment

The ALARP discussion for this event is the same as for the loss of normal feedwater fault event, as described in Section 9.2.7.5.

9.2.6.6 Conclusions

Results of the DB analysis show that for the loss of ac power to plant auxiliaries event, all safety criteria are met. The heat extraction provided by the steam relief capacity of the steam generator safety valves and the operation of the PRHR is sufficient to prevent water relief through the pressuriser safety valves.

The DB analysis demonstrates that sufficient long-term reactor coolant system heat removal capability exists, via the steam generator safety valves, natural circulation, and the PRHR heat exchanger, following reactor coolant pump coastdown to prevent fuel or cladding damage and reactor coolant system overpressure.

This event has also been adequately assessed with respect to ATWT considerations.

Diverse core cooling capabilities have been demonstrated.

DBA radiological consequences are within the Target 4 BSL for frequent faults (1 mSv offsite and 20 mSv onsite). Thus, the identification of necessary Class 1 SSCs is adequate to meet DB requirements.

It has been shown that the AP1000 plant design includes adequate systems for the protection of this fault, which limit the radiological consequences such that they are compliant with the SAPs targets and the risks have been reduced to be ALARP.

9.2.7 Loss of Normal Feedwater Flow (Fault 1.16.1)

9.2.7.1 Identification of Causes and Accident Description

A loss of normal feedwater (from pump failures or valve malfunctions) results in a reduction in the capability of the secondary system to remove the heat generated in the reactor core. If startup feedwater is not available, the Class 1 PRHR heat exchanger is automatically aligned by the PMS to remove decay heat.

A small secondary system break can affect normal feedwater flow control, causing low steam generator levels prior to protective actions for the break. This scenario is addressed by the assumptions made for the feedwater system pipe break (see Section 9.2.8).

The following occurs upon loss of normal feedwater (assuming main feedwater pump fails or valve malfunctions):

- The steam generator water inventory decreases as a consequence of the continuous steam supply to the turbine. The mismatch between the steam flow to the turbine and the feedwater flow leads to the reactor trip on a low steam generator water level signal. The same signal also actuates the startup feedwater system (see Section 9.2.6.1).

- As the steam system pressure rises following the trip, the steam generator power-operated relief valves are automatically opened to the atmosphere. The condenser is assumed to be unavailable for turbine bypass. If the steam flow path through the power-operated relief valves is not available, the steam generator safety valves may lift to dissipate the sensible heat of the fuel and coolant plus the residual decay heat produced in the reactor.

- As the no-load temperature is approached, the steam generator power-operated relief valves (or safety valves, if the power-operated relief valves are not available) are used to dissipate the decay heat and to maintain the plant at the hot shutdown condition, if the startup feedwater is used to supply water to the steam generator.

- If startup feedwater is not available, the PRHR heat exchanger is actuated on either a Low -2 steam generator water level (narrow range) coincident with a low startup feedwater flow rate signal or a low steam generator water level (wide range) signal.

- The PRHR heat exchanger extracts heat from the reactor coolant system causing a temperature reduction and an "S" signal on a Low Tcold signal. This actuates the core makeup tanks and trips the RCPs. Both core makeup tanks inject mass into the reactor coolant system. For some time the pressuriser level continues to decrease as the combined cooling from the PRHR and the CMTs (with them injecting colder water) continues. As the CMT water heats up, its cooling effect decreases and the RCS begins to heat up. The RCS heatup causes a pressuriser level increase transient. The operators will be alerted that a potential filling event is occurring by the High-2 pressuriser level signal. The operator action assumed in the analysis is to open the reactor vessel head vent following receipt of the High-3 pressuriser level signal; this action is at least 30 minutes after the operator has been alerted by the High-2 pressuriser level signal. When the head vent is opened, the pressuriser level increase slows and ultimately the level begins to decrease.

- Later in the transient, the PRHR heat transfer matches decay heat the RCS heatup is stopped and the RCS temperature begins to decrease.

Appendix 9C provides discussion and analysis of long term safe shutdown for non-LOCA events.

9.2.7.2 Design Basis Mitigation

Analysis is performed to demonstrate the adequacy of the PMS to detect and mitigate the fault. It also demonstrates the capability of the PRHR heat exchanger to remove sufficient decay heat following a loss of normal feedwater. Those systems in conjunction with the operator action to open the reactor head vent show that the safety criteria are satisfied including::

- No fuel failures (confirmed using minimum DNBR and fuel melt criteria),
- The RCS pressure criterion is met,
- The MSS pressure criterion is met, and
- The pressuriser does not fill (which could result in a LOCA)

It is noted that this event is bounded by the Section 9.2.3 analysis with respect to RCS/MSS pressure criteria, therefore, these limits are not explicitly confirmed for this event.

9.2.7.2.1 DBA Method of Analysis

An analysis using a modified version of the LOFTRAN code (Reference 9.2-2), described in WCAP-15644 (Reference 9.2-6), is performed to obtain the plant transient following a loss of normal feedwater. The simulation describes the neutron kinetics, reactor coolant system (including the natural circulation), pressuriser, and steam generators. The program computes pertinent variables, including the steam generator level, pressuriser water level, and reactor coolant average temperature.

Two cases are analysed. One case assumes a consequential loss of ac power to the plant auxiliaries resulting from the turbine trip after reactor trip. The loss of ac power results in a coastdown of the reactor coolant pumps. A second case does not assume the consequential loss of ac power, which maintains the reactor coolant pumps at normal speed until automatically tripped when the core makeup tanks are actuated.

The assumptions used in the analysis are as follows:

- The plant is initially operating at 101 percent of the design power rating.
- Reactor trip occurs on steam generator Low-2 (narrow range) level.
- The principal safety function required after reactor trip is the core decay heat removal. That function is carried out by the PRHR heat exchanger. The worst single failure is assumed to occur in the PRHR heat exchanger. The actuation of the PRHR heat exchanger requires the opening of one of the two fail-open valves arranged in parallel at the PRHR heat exchanger discharge. Because no single failure can be assumed that impairs the opening of both valves, the failure of a single valve is assumed.

  The PRHR heat exchanger is actuated by the Low-2 steam generator water level narrow range signal coincident with Low-2 startup feedwater flow, or by the Low-2 steam generator water level wide range signal.
- Plant cooldown with the PRHR heat exchanger may cause a reduction in the low cold leg temperature such that the Safeguards setpoint is reached, which will actuate the core makeup tanks. The additional borated fluid added by the core makeup tanks may cause excessive pressuriser water volume. Prevention of pressuriser filling is accomplished by an operator action to open the reactor head vent.
- Secondary system steam relief is achieved through the steam generator safety valves.
- The initial reactor coolant average temperature is 4.4°C (8°F) lower than the nominal value, and initial pressuriser pressure is 0.345 MPa (50 psi) lower than nominal.

The loss of normal feedwater analyses are performed to demonstrate the adequacy of the PMS and the PRHR heat exchanger in removing long-term decay heat. Such decay heat removal prevents excessive heatup of the reactor coolant system with possible resultant reactor coolant system overpressurisation or loss of reactor coolant system water. The assumptions used in this analysis minimize the energy removal capability of the system, and maximise the coolant system expansion.

With respect to the overpressure evaluation, the loss of normal feedwater transient with and without ac power available events are bounded by the turbine trip event presented in Section 9.2.3.

Plant characteristics and initial conditions are further discussed in Section 9.0.2.

Plant systems and equipment necessary to mitigate the effects of a loss of normal feedwater accident are discussed in Section 9.0.4 and listed in Table 9.0-10. Normal reactor control systems are not required to function. The PMS is required to function following a loss of normal feedwater. The PRHR heat exchanger is required to function with an overall minimum capability to extract heat from the reactor coolant system. No single active failure prevents operation of any system to perform its required function.

9.2.7.2.2 DBA Credited SSCs

For the DB, all of the claimed SSCs are Class 1. The claimed Class 1 SSCs are listed in Table 9.0-10. The primary core cooling is provided by the PRHR and passive containment cooling. Other SSCs include the CMTs, containment isolation, pressuriser SVs, and reactor vessel head vent valves. The PMS provides the following:

- RT on Low-2 SG narrow-range water level in either SG
- Manual head vent valve operation on High-2 pressuriser level
- PRHR actuation on Low-2 SG NR level coincident with Low-2 SFW flow
- CMTs and containment isolation on Low-2 CL temperature
- PCS on High-2 containment pressure

9.2.7.2.3 DBA Results

The transient responses for a loss of main feedwater flow are shown for cases without and with a consequential loss of ac power.

Loss of Normal Feedwater flow with ac power available

The calculated sequence of events for this accident is listed in Table 9.2-1. Figures 9.2.7-1 through 9.2.7-13 show the significant plant parameters following a loss of normal feedwater.

The loss of main feedwater results in an increase in the pressuriser water volume until reactor trip on low steam generator water level (narrow range). The pressuriser water volume then decreases briefly due to the reactor trip. However, due to loss of secondary heat removal capacity and injection from the CVS, the pressuriser water volume begins to increase. The pressuriser water volume then increases until the PRHR actuates.

The capacity of the PRHR heat exchanger, when the reactor coolant pumps are operating, is much larger than the decay heat, and in the first part of the transient, the reactor coolant system is cooled down. The cooldown continues until the reactor coolant temperature reaches the low T_{cold} setpoint. When the low T_{cold} setpoint is reached, the reactor coolant pumps are tripped, CVS is isolated, and the core makeup tanks are actuated.

The pressuriser water volume then increases due to the cold borated water injected by the core makeup tanks and the reduced PRHR efficiency due to the loss of forced flow resulting from the reactor coolant pump trip. Pressuriser water volume increases during this period. The operators are alerted to the pressuriser level increase when the level exceeds the High-2 pressuriser level

setpoint. The operator action assumed in this analysis is to open the reactor vessel head vent following receipt of the High-3 pressuriser level signal; this action is at least 30 minutes after the operator has been alerted by the High-2 pressuriser level signal. After that point, the pressuriser water volume begins to decrease. The operator action to open the reactor vessel head vent and the capacity of the PRHR heat exchanger is sufficient to avoid water relief through the pressuriser safety valves.

The DNBR transient for the loss of normal feedwater event is shown in Figure 9.2.7-12.

Loss of Normal Feedwater flow with a consequential loss of ac power

The calculated sequence of events for this accident is listed in Table 9.2-1. Figures 9.2.7-14 through 9.2.7-26 show the significant plant parameters following a loss of normal feedwater with a consequential loss of ac power to plant auxiliaries.

The first increase in pressuriser water volume is turned around by the heat extraction provided by the steam generator safety valves. Due to the steam generator safety valve relief, the pressuriser water volume decreases until the heat extraction provided by the steam generator safety valves relief stops once the steam pressure decreases below the steam generator safety valve setpoints. With no steam generator safety valve relief, the pressuriser water volume begins to increase until the PRHR heat extraction approaches the magnitude of the decay heat addition. Once this occurs, pressuriser water volume decreases for the remainder of the transient.

9.2.7.3 Diverse Mitigation

In addition to the Class 1 passive systems credited in the DBA, the plant also provides diverse mitigation capability that is able to supply the Category A safety functions for frequent faults. The diverse features are also Class 1 except for the diverse C&I, which is Class 2.

Two different diverse mitigation analyses are provided in the following subsections. One demonstrates the reactor can be shut down when a CCF prevents control rod insertion. Such an event is defined as an ATWT event. The other demonstrates that adequate core cooling can be provided when a CCF affects the core cooling credited in the DBA. In the diverse core cooling case rod insertion is assumed to occur.

The diverse core cooling is provided by passive feed and bleed using PXS injection and ADS venting (Class 1). The DAS provides diverse reactor trip and safety system actuation (Class 2).

In these diverse mitigation analyses, the containment function is provided by the fuel cladding and by the RCS, neither of which is threatened in the DBA. The containment building provides diverse containment and is identified as a Class 1 system on that basis for this fault.

Table's 9.2.7-3 and Table 9.2.7-4 summarize the SSCs credited in these diverse fault assessments. The information provided in Table 9.2.7-3 is from Reference 9.2-10, which documents the diversity for the frequent faults and provides additional information on the diverse mitigation functions.

9.2.7.3.1 Diverse Mitigation for ATWT

The loss of main feedwater produces a large imbalance in the heat source/sink relationship. When feedwater flow to the steam generators is terminated, the secondary subcooled feed system can no longer remove all the heat that is generated in the reactor core. This excess primary system heat causes the RCS temperature and pressure to rise and the pressuriser water level to increase, due to

the insurge of expanding reactor coolant. Water levels in the steam generators drop as the remaining water in the secondary system is boiled off. When the steam generator water level falls to the point where the steam generator tubes are uncovered, primary to secondary heat transfer is reduced, causing the reactor coolant temperature and pressure to increase at a greater rate. This rate of primary system temperature and pressure increase is maintained as the pressuriser fills and discharges water through the safety valves. Reactivity feedback effects, due to the higher primary system temperature, reduce core power. Eventually, the balance between the heat source and sink is re-established, system temperature and pressure decreases, and a steam bubble is formed in the pressuriser again.

A number of cases were considered to address different potential CCFs that can affect the PMS and its ability to insert RCCAs. The LONF analysis documented in this section is performed to bound the following events:

- Complete or Partial LONF with a PMS CCF – The CCF prevents all PMS reactor trips signals and engineered safeguards features signals. The DAS is assumed to be completely operable. Offsite power and turbine bypass are also assumed available.

- Complete or Partial LONF with a PMS reactor trip breaker CCF - This failure prevents the PMS from inserting the rods; however, PMS logic continues to function, and all engineered safeguards features signals are operable. DAS is completely operable, including its capability to drop rods. Offsite power and turbine bypass are also assumed to be available.

- Complete or Partial LONF with a RCCA mechanical CCF - The PMS, DAS, and control systems are assumed to be operable except that RCCAs do not insert into the core on a trip signal.

This analysis is performed to demonstrate the adequacy of the operable portions of the PMS (considering the impact of the CCF) as well as the DAS to detect and actuate mechanical SSCs to mitigate the fault. The following ATWT acceptance criteria are applicable to this event:

- The RCS does not overpressurise due to reactor coolant heatup. The ATWT pressure limit is 22.06 MPa-rel (3200 psig).

- There is no significant fuel damage.

- The rate and duration of energy release to containment is much less than for the design basis LOCA. This demonstrates that the containment does not overpressurise due to the energy release to the containment.

9.2.7.3.1.1 Diverse ATWT Method of Analysis

The analysis uses the methods outlined for the DBA, with revised assumptions. The assumptions used for the limiting ATWT LONF, a complete LONF with a RCCA mechanical CCF, are discussed below. No measurement/instrumentation errors are assumed.

- Plant initial conditions are at the nominal full power values

- Core kinetics parameters and initial boron concentration are both assumed to be at BOC values.

- MTC is modelled as discussed in Reference 9.2-11.

- Pressuriser spray is assumed to be available because it results in a slightly higher peak pressure.

- Turbine trip on reactor trip function is assumed to be operable. Not tripping the turbine would cause worse ATWT consequences, since it would draw more steam from the SG and more heat would be removed from the primary system early in the transient. As a consequence, core power level would stay relatively high during the period when SG heat transfer degrades. This would result in higher pressuriser insurge and peak pressure. For this reason, diverse actuation of the turbine trip following loss of heat sink (i.e., low SG water level) is required on all Westinghouse PWRs.

  Turbine trip is assumed after the reactor trip setpoint is reached. A scenario with turbine trip at the beginning of the event would be almost the same. The only difference is that the switch of turbine bypass to pressure mode would happen sooner.

- Startup Feedwater system is not credited in the analyses.

- PMS and DAS automatic actions are available for this event except that rod insertion fails due to the RCCA CCF.

- ac power is assumed to be available since it is more likely and produces worse results.

9.2.7.3.1.2 Diverse ATWT Credited SSCs

For the diverse ATWT all of the claimed SSCs are Class 1 except for the DAS. The claimed Class 1 SSCs are listed in Table 9.0-14. For the limiting ATWT case, the PMS and DAS provide the following:

- PMS PRHR actuation on Low-2 SG NR level coincident with Low-2 SFW flow

- PMS PCS and containment isolation on High-2 containment pressure

- DAS PRHR[2] and CMT actuation on Low-2 SG wide range (WR) level

9.2.7.3.1.3 Diverse ATWT Results

Complete LONF with a RCCA CCF (limiting case)

Table 9.2.7-1 shows the event progression for the limiting ATWT diversity LONF case. Transient response of this event is shown in Figures 9.2.7-27 to 9.2.7-32.

At the start of the event, all main feedwater is terminated completely. SG water is boiled off in a higher rate because of the loss of subcooled feedwater. The turbine control system throttles turbine valves to maintain nominal load and secondary pressure increases slowly. The decreased load demand causes the primary temperature to increase resulting in a slow power decrease due to moderator feedback. SG water level decreases continually but SG heat transfer is still maintained. Eventually, SG water level decreases and reaches narrow range low SG level PMS reactor trip

2 As analysed, the DAS actuation occurs simultaneously as the PMS actuation; as such, both are presented.

setpoint value. As the result of reactor trip signal, the turbine is tripped and turbine bypass control switches to pressure mode.

Several seconds after the turbine trip, the turbine bypass valves open fully (in steam pressure control mode). The turbine bypass system is unable to remove all of the energy transferred to the secondary side and the secondary pressure increases until SG PORV and then safety valves are opened. As the reactor coolant temperature increases, core power decreases due to moderator feedback. The heatup of the reactor coolant causes fluid expansion which increases the pressuriser level and pressure until the pressuriser safety valves open.

Eventually, core power decreases to a value that is equal to the energy removal rate of the turbine bypass system and the steam generator relief and safety valves. This reduced core power is approximately 70 percent of RTP when the liquid inventory in the steam generators has been depleted to the point where full heat transfer through the tube bundle cannot be maintained. At this point, heat transfer through the tube bundle continues to degrade as the remaining liquid in the steam generators is boiled off.

The reduction in steam generator heat transfer causes the primary side temperatures to begin rising again. As reactor coolant temperature increases, core power again decreases due to moderator feedback. When the steam generator level reaches wide range low level setpoint in both steam generators, the PMS and DAS actuate PRHR, the DAS actuates the CMT, and the RCPs are tripped.

The heatup caused by the reduction of heat transfer in the SG causes the pressuriser level to increase until the pressuriser fills. Liquid relief from the pressuriser safety valves occurs at this time and RCS pressure increases to a peak value. Reactor coolant pressure then begins to decrease as core power is reduced due to moderator feedback. The PRHR cycle is established, and it transfers core power to the IRWST. The SG heat transfer ceases. Eventually, the hot-leg temperatures in both loops approach saturation while the cold-leg temperature in loop 2 reaches saturation. However, since the PRHR is connected to the loop 1 SG plenum, the inlet loop 1 cold leg temperature remains subcooled. Core power is reduced by moderator temperature feedback, and it eventually reaches equilibrium with the PRHR heat removal rate. Reactor coolant pressure continues to decrease and the pressuriser safety valves close. Eventually, the CMT-induced boration of the RCS will bring the reactor to subcritical conditions.

The peak RCS pressure is less than the limit of 22.06 MPa-rel (3200 psig).

There is no significant core damage, as evidenced by the bounding analysis for a loss of flow ATWT in Section 9.3.

The rate and duration of energy release to containment is much less than for the design basis loss of coolant accident.

9.2.7.3.2 Diverse Mitigation for Core Cooling

Analysis is performed considering several different CCFs that can affect the SSCs used to provide core cooling to demonstrate the adequacy of the SSCs not affected by the CCF. The same safety criteria as those for the ATWT are applicable to this event:

- The RCS does not overpressurise due to reactor coolant heatup. The ATWT pressure limit is 22.06 MPa-rel (3200 psig).

- There is no significant fuel damage. The fuel peak clad temperature is less than 1204°C (2200°F)

- The rate and duration of energy release to containment is much less than for the design basis LOCA. This demonstrates that the containment does not overpressurise due to the energy release to the containment.

9.2.7.3.2.1 Diverse Core Cooling Method of Analysis

An analysis using a RELAP 5 Mod 3.3 code (Reference 9.2-12), is performed to obtain the plant transient following a loss of normal feedwater. The simulation describes the neutron kinetics, reactor coolant system (including the natural circulation), pressuriser, and steam generators. The program computes pertinent variables, including the steam generator level, pressuriser water level, and reactor coolant average temperature.

A conservative bounding case is analysed with multiple CCFs. Multiple CCFs are assumed such that only one additional diverse analysis case is required to demonstrate diverse core cooling. Table 9.2.7-4 compares the SSCs credited in the DBA case (Section 9.2.7.2.1) with this bounding diverse core cooling case.

The general assumptions used in this analysis are the same as those used in the diverse ATWT LONF (Section 9.2.7.3.1) case except for the differences in the SSCs credited.

At the start of this event, all main feedwater is terminated. As a result, the SG water level decreases rapidly. Since PMS is assumed to be unavailable (due to a CCF) the SG level drops to the low SG WR DAS setpoint before the RT occurs. Due to the initiating event and the delayed RT, the SG heat removal stops early in the transient. At this point the reactor decay heat causes the RCS temperature to increase to the saturation point at the pressuriser safety valve setpoint. Due to the heatup of the reactor coolant, the pressuriser fills and the pressuriser SVs discharge water. Pressuriser SV discharge continues until ADS stage 1 valves are manually opened via DAS.

Once the ADS valves are opened the RCS pressure decreases and accumulator injection occurs. As the RCS pressure decreases further, the IRWST also provides injection; DAS manual is used to open these valves.

9.2.7.3.2.2 Diverse Core Cooling Credited SSCs

Table 9.2.7-4 lists the major SSCs credited in this analysis. Since the PMS is assumed to have suffered a CCF it is not credited for any actuation. Other SSCs include the accumulators, containment isolation, and pressuriser SVs. The DAS provides the following:

- RT motor-generator (MG) set field breakers on Low SG WR level

- PCS and containment isolation (CI) on high containment temperature

- Manual actuations of ADS 1- 4, IRWST injection, and containment recirculation

In addition, self-actuation of the accumulators is also credited.

9.2.7.3.2.3 Diverse Core Cooling Results

Table 9.2.7-2 shows the event progression. Transient response to this event is shown in Figures 9.2.7-33 to 9.2.7-38. Due to the CCF of the PMS, operator actions are credited in this analysis. The timing of these actions has an important impact on the results. Typically 30 minute action times are considered reasonable, especially for events like this that are very low probability (requiring multiple CCFs). In this case the operator action has been delayed for an additional 10 minutes (40 minutes total) to add additional margin.

At the start of this event, all main feedwater is terminated. As a result, the SG water level decreases rapidly. Since PMS is assumed to be unavailable (due to a CCF) the SG level drops to the low SG WR DAS setpoint before the RT. Due to the initiating event and the delayed RT, the SG heat removal stops early in the transient. At this point the reactor decay heat causes the RCS temperature to increase to the saturation point at the pressuriser SV setpoint. Due to the heatup of the reactor coolant the pressuriser fills and the pressuriser SVs then discharge water. Pressuriser SV discharge continues until ADS stage 1 valves are manually opened via DAS at 40 minutes.

Once the ADS valves are opened the RCS pressure decreases and accumulator injection occurs. As the RCS pressure decreases further, the IRWST also provides injection; DAS manual is used to open these valves.

Due to the loss of reactor coolant out the pressuriser SVs, there is some fuel uncovery and heatup. The peak clad temperature is reached at about the time that accumulator injection starts (about 2600 seconds). Accumulator injection quickly decreases the clad temperature. There is a small second clad temperature rise that occurs between the time the accumulators empty and the IRWST injection starts. After this time the fuel clad temperature remains stable.

Note that this case actually assumes three separate CCF; one each for PMS, PRHR and CMTs even though ONR guidance only requires that one be assumed. This approach is taken so that fewer analysis cases are required. The following discusses the impact of assuming fewer failures.

- PMS failure only – DAS would automatically trip the reactor and start PRHR. Manual actions and use of passive feed and bleed would not be required.

- PRHR failure only – PMS would automatically actuate CMTs. The CMTs would feed the reactor when heated up after the boil off of the SG inventory. When the CMT levels decreased ADS would be automatically actuated. Not operator action would be required and core uncover would not be expected.

- PMS and PRHR failures only – In this case the CMTs would be automatically actuated by DAS. Their availability would delay SG dry out by about 1000 seconds. In addition, they would provide additional water injection during the RCS depressurization. Operator action would still be required but more time would be available, on the order of 1 hour total.

The peak RCS pressure is 17.8 MPa abs (2582 psia) which is well below the acceptance criteria.

The peak clad temperature is of 847°C (1556°F) which is well below the acceptance criteria.

The mass energy input to the containment will be much less than that for a large break LOCA.

9.2.7.4 Radiological Consequences

Design Basis

In the case where offsite power remains available, there is no release of activity to the environment and the Target 4 BSOs (0.01 mSv offsite and 0.1 mSv onsite) are met.

In the case where offsite power is lost, a small release of activity may occur as a result of steam dump to the atmosphere due to unavailability of the condensers. With no fuel damage and primary and secondary circuits intact, the initiating event has no impact on the doses. The doses are a consequence of the assumed loss of offsite power. Therefore, the loss of offsite power doses from Section 9.2.6.4 are presented. The calculated maximum doses for all relevant pathways (inhalation, cloudshine, and groundshine) are as follows:

- Offsite dose: 0.05 mSv Worker dose: 1.5 mSv

These doses are within the Target 4 BSL for frequent faults (1 mSv offsite and 20 mSv onsite).

Diverse Mitigation

Both the diverse ATWT and diverse core cooling scenarios demonstrate that the RCS does not overpressurise and there is no significant fuel damage. For a diverse mitigation radiological consequences analysis better estimate assumptions would be credited. This would include reactor coolant system activity levels significantly lower than those modelled for the DBA and better activity retention in containment and in the steam generators. In addition better estimate atmospheric dispersion factors would be used. Therefore, a diverse mitigation radiological consequences analysis would show that the doses for the diverse ATWT scenario would be less than those reported for the non-LOCA DBAs and doses for the diverse core cooling scenario would be much less than for the design basis LOCA. The diverse mitigation analyses would not have to meet the Target 4 BSL for frequent faults and would meet the Target 4 BSL for infrequent faults.

9.2.7.5 As Low As Reasonably Practicable Assessment

For this event, the identification of the primary safety functions as Class 1 SSCs has been shown to be adequate to meet DB requirements.

The diverse mitigation functions, including other Class 1 safety functions and the DAS function, which is Class 2, is also shown by analysis to meet the corresponding requirements for this event. See Reference 9.2-10 for additional discussions on these diverse mitigation features.

Additionally, the AP1000 plant design has a third level of redundancy provided by the DiD systems. The applicable DiD functions include:

- CVS boration for long-term reactivity control
- CVS make-up for RCS inventory control
- SFW with steam dump for decay heat removal
- Pressuriser spray and auxiliary spray for RCS pressure control
- RNS cooling of the RCS for long-term decay heat removal. The RNS requires support from the CCS and SWS cooling systems.
- Control by the PLS C&I

The characteristics of the above features were compared to improvements that were evaluated for the RNS for its mitigation of cliff edge small LOCAs. First it should be recognized that in this situation the RNS provides the second level of defence for this event and is therefore more important than the above DiD features which provide a 3rd level of defence. The RNS improvements included making the RNS alignment and actuation automatic, increasing the RNS pump head, and adding a RNS suction supply tank that is separate from the Class 1 system. None of these potential improvements were found to be ALARP (See Section 9.1.4.5). However, the SFW and CVS already include characteristics similar to these proposed improvements. Another improvement that could be made to these DiD systems is to upgrade them to Class 1. This would be very expensive especially and would have wide reaching impacts to the design of SSCs; notable would be the impact on component and building design to address hazards including seismic and storm winds/missiles. Such a change would not be ALARP because the cost would be grossly disproportional to its benefit.

As discussed in Chapter 9.0.15, the AP1000 has incorporated ALARP thinking throughout its development. In addition, the current risk of a large radioactivity release is significantly less than the SAP Target 9 BSO (1E-7 pa). Considering the ALARP thinking that went into the AP1000 development, its low risk profile and the additional level of defence discussed above (including their performance characteristics), improving the Class 2 DiD to better remove decay heat or shutdown the reactor would be grossly disproportional to the risk reduction that might be achieved. As a result, the current design is considered ALARP.

9.2.7.6 Conclusions

Results of the DB analyses show that a loss of normal feedwater or a loss of normal feedwater with a consequential loss of ac power to the plant auxiliaries does not adversely affect the core, the reactor coolant system, or the steam system. The heat removal capacity of the PRHR heat exchanger, the steam generator safety valves, and the fluid relief capacity of the reactor vessel head vent is such that reactor coolant water is not relieved from the pressuriser safety valves and the pressuriser does not fill. DNBR always remains above the design limit values, and RCS and MSS pressures remain below 110 percent of their design values.

The ATWT acceptance criteria are met for this event. This event was explicitly analysed for the change in the current design reference point in the UK as described in Reference 9.2-13. The evaluation conducted to closeout FS-03 (Reference 9.2-14) demonstrated that there is little impact on the key analysis trends, results, and margin to the applicable acceptance criteria. Therefore, the change in design reference point would not invalidate the conclusions presented for this event.

Diverse core cooling capabilities have been demonstrated.

DBA radiological consequences are within the Target 4 BSL for frequent faults (1 mSv offsite and 20 mSv onsite). Thus, the identification of necessary Class 1 SSCs is adequate to meet DB requirements.

It has been shown that the AP1000 plant design includes adequate systems for the protection of this fault, which limit the radiological consequences such that they are compliant with the SAPs targets and the risks have been reduced to be ALARP.

9.2.8 Feedwater System Pipe Break (Fault 1.16.8)

9.2.8.1 Identification of Causes and Accident Description

A major feedwater line rupture is a break in a feedwater line large enough to prevent the addition of sufficient feedwater to the steam generators in order to maintain shell-side fluid inventory in the steam generators. If the break is postulated in a feedwater line between the check valve and the steam generator, fluid from the steam generator may also be discharged through the break. (A break upstream of the feedwater line check valve would affect the plant only as a loss of feedwater. This case is covered by the evaluation in Section 9.2.7.)

Depending upon the size of the break and the plant operating conditions at the time of the break, the break could cause either a reactor coolant system cooldown (by excessive energy discharge through the break) or a reactor coolant system heatup. Potential reactor coolant system cooldown resulting from a secondary pipe rupture is evaluated in Section 9.1.5. Therefore, only the reactor coolant system heatup effects are evaluated for a feedwater line rupture in this section.

The feedwater line rupture reduces the ability to remove heat generated by the core from the reactor coolant system for the following reasons:

- Feedwater flow to the steam generators is reduced. Because feedwater is subcooled, its loss may cause reactor coolant temperatures to increase prior to reactor trip.

- Fluid in the steam generator may be discharged through the break and would not be available for decay heat removal after trip.

- The break may be large enough to prevent the addition of main feedwater after trip.

The severity of the feedwater line rupture transient depends on a number of system parameters, including the break size, initial reactor power, and the functioning of various control and safety-related systems. Sensitivity studies presented in WCAP-9230 (Reference 9.2-4) illustrate that the most limiting feedwater line rupture is a double-ended rupture of the largest feedwater line. At the beginning of the transient, the main feedwater control system is assumed to malfunction due to an adverse environment. Interactions between the break and the main feedwater control system result in no feedwater flow being injected or lost through the steam generator feedwater nozzles. This assumption causes the water levels in both steam generators to decrease equally until the Low-2 steam generator level (narrow range) reactor trip setpoint is reached. After reactor trip, a full double-ended rupture of the feedwater line is assumed such that the faulted steam generator blows down through the break and no main feedwater is delivered to the intact steam generator. These assumptions conservatively bound the most limiting feedwater line rupture that can occur. Analysis is performed at full power assuming the loss of offsite power at the time of the reactor trip. This is more conservative than the case where power is lost at the initiation of the event. The case with offsite power available is not explicitly examined because, due to the fast generation of "S" signal (generated by the Low-2 steam line pressure), the reactor coolant pumps would be tripped by the PMS shortly after the reactor trip. The only difference between the cases with and without offsite power available would be a small difference in when the reactor coolant pumps are tripped.

9.2.8.2 Design Basis Mitigation

Analysis is performed to demonstrate the adequacy of the PMS to detect and mitigate the fault and show that the safety criteria are satisfied including:

- The reactor coolant system pressure criterion is met (demonstrating the adequacy of these systems in preventing excessive heatup.)
- Subcooling is maintained in the RCS (demonstrating core cooling capability is maintained).

Some fuel damage may occur as a consequence of infrequent faults, such as the feedwater line break accident. In practice, the results of the DB analysis presented below show that no fuel damage is expected to occur since DNB does not occur.

9.2.8.2.1 DBA Method of Analysis

An analysis using a modified version, described in WCAP-15644 (Reference 9.2-6), of the LOFTRAN code (Reference 9.2-2) is performed to determine the plant transient following a feedwater line rupture. The code describes the reactor thermal kinetics, reactor coolant system (including natural circulation), pressuriser, steam generators, and feedwater system responses and computes pertinent variables, including the pressuriser pressure, pressuriser water level, and reactor coolant average temperature.

The case analysed assumes a double-ended rupture of the largest feedwater pipe at full power. Major assumptions used in the analysis are as follows:

- The plant is initially operating at 101 percent of the design plant rating. The main feedwater flow measurement supports a 1-percent power uncertainty.

- Initial reactor coolant average temperature is 4.4°C (8°F) above the nominal value, and the initial pressuriser pressure is 0.345 MPa (50 psi) below its nominal value.

- The pressuriser spray is turned on.

- Initial pressuriser level is at a conservative maximum value and a conservative initial steam generator water level is assumed in both steam generators.

- At the start of the transient, interaction between the break in the feedline and the main feedwater control system is assumed to result in a complete loss of feedwater flow to both steam generators. No feedwater flow is delivered to or lost through the steam generator nozzles.

- Reactor trip is assumed to be initiated by the Low-2 steam generator water level (narrow range) signal on the ruptured steam generator. A two second delay is assumed following the low level setpoint being reached to allow for the system response times.

- After reactor trip, the faulted steam generator blows down through a double-ended break area of 0.10 m^2 (1.117 ft^2). A saturated liquid discharge is assumed until all the water inventory is discharged from the faulted steam generator. This minimizes the heat removal capability of the faulted steam generator and maximises the resultant heatup of the reactor coolant. The PRHR heat exchanger is assumed to be actuated by the Low-2 steam generator water level

(wide range) signal. A 17-second delay is assumed following the low level setpoint being reached to allow for the system response times and the valve stroke time.

- Credit is taken for heat energy deposited in reactor coolant system metal during the reactor coolant system heatup.
- No credit is taken for charging or letdown.
- Pressuriser safety valve setpoint is assumed to be at its minimum value.
- Steam generator heat transfer area is assumed to decrease as the shell-side liquid inventory decreases. The heat transfer remains approximately 100 percent in the faulted steam generator until the liquid mass reaches about 11 percent. The heat transfer is then reduced to 0 percent with the liquid inventory.
- Conservative core residual heat generation is assumed based upon long-term operation at the initial power level preceding the trip (Reference 9.2-3).
- No credit is taken for the following four PMS reactor trip signals to mitigate the consequences of the accident:
  - High-2 pressuriser pressure
  - Overtemperature ΔT
  - High pressuriser water level
  - High containment pressure

The PRHR heat exchanger is initiated once the steam generator water level drops to the Low-2 steam generator level (wide range). Similarly, receipt of a Low-2 steam line pressure signal in at least one steam line initiates a steam line isolation signal that closes all main steam line and feed line isolation valves. This signal also gives an "S" signal that initiates flow of cold borated water from the core makeup tanks to the reactor coolant system.

Plant characteristics and initial conditions are further discussed in Section 9.0.2.

No credit is taken for the plant control system to mitigate the consequences of the event. The PMS is required to function following a feedwater line rupture as analysed here. No single active failure prevents operation of this system. The single failure assumed is the failure of one of the two parallel discharge valves in the PRHR outlet line (see Table 9.0-11).

9.2.8.2.2 DBA Credited SSCs

For the DB, all the claimed SSCs are Class 1. The claimed Class 1 SSCs are listed in Table 9.0-10. The primary core cooling is provided by the PRHR and passive containment cooling. Other SSCs include the CMTs, containment isolation, steam line isolation valves and pressuriser SVs. The PMS provides the following:

- RT on Low-2 SG narrow-range water level in either SG
- PRHR actuation on Low-2 SG WR level
- CMTs and containment isolation on Low-2 steamline pressure
- PCS on High-2 containment pressure

9.2.8.2.3 DBA Results

Calculated plant parameters following a major feedwater line rupture are shown in Figures 9.2.8-1 through 9.2.8-10. The calculated sequence of events for the case analysed is listed in Table 9.2-1.

The results presented in Figures 9.2.8-5 and 9.2.8-7 show that pressures in the reactor coolant system and main steam system remain below 110 percent of the respective design pressures.

In the first part of the transient, due to the conservative analysis assumptions, the system response following the feedwater line rupture is similar to the loss of normal feedwater with consequent loss of ac power (Section 9.2.7). For transient period prior to rod insertion, the feedwater line rupture event is bounded by the turbine trip event presented in Section 9.2.3 with respect to DNB concerns.

After the trip, the core makeup tanks are actuated on Low-2 steam line pressure in the ruptured loop while the PRHR heat exchanger is actuated on a Low-2 steam generator water level (wide range).

The addition of the PRHR heat exchanger and flows from the core makeup tanks help to cool down the primary system and to provide sufficient fluid to keep the core covered with water.

Pressuriser safety valves open due to the mismatch between decay heat and the heat transfer capability of the PRHR heat exchanger. In the first part of the transient, there is a cooling effect due to the core makeup tanks that inject cold water into the reactor coolant system and receive hot water from the cold leg. This effect decreases due to the heatup of the core makeup tanks from recirculation flow. Also, the injection driving head is lowered as the core makeup tanks heat up.

Reactor coolant system temperatures are low (with the hot leg temperature of the faulted loop at approximately 265.56°C (510°F) at about 2,200 seconds) and, in this condition, the PRHR heat exchanger cannot remove the entire decay heat load. Reactor coolant system temperatures then increase until approximately 21,500 seconds due to the limited heat removal capability of the PRHR heat exchanger. At approximately 23,990 seconds, the heat removal capability of the PRHR exceeds the decay heat power and the reactor coolant system pressure begins to decrease. Since subcooling is maintained throughout the transient and the reactor coolant system inventory increases (i.e., net core makeup tank injection exceeds net pressuriser safety valve relief), core cooling capability is maintained.

Appendix 9C provides discussion and analysis of long term safe shutdown for non-LOCA events.

9.2.8.3 Diverse Mitigation

As this is a low probability design basis fault (DBL), a diverse mitigation assessment is not required.

9.2.8.4 Radiological Consequences

Design Basis

With no fuel damage and no threat to containment, a significant release of radioactivity to the environment can only occur if the feedwater line break is outside the containment. Activity release will be limited to that present in the secondary coolant prior the event and any activity present in reactor coolant prior to the event that leaks into the SG during the event. These releases are the same as those considered in main steam line break doses presented in Section 9.1.5.4. Therefore,

the main steam line break doses from Section 9.1.5.4 are presented. The calculated maximum doses for all relevant pathways (inhalation, cloudshine, and groundshine) are as follows:

- Offsite dose: 9.3 mSv Worker dose: 78 mSv

These doses are within the Target 4 BSL for infrequent faults (10 mSv offsite and 200 mSv onsite).

9.2.8.5 As Low As Reasonably Practicable Assessment

For this event, the identification of the primary safety functions (Table 9.2.8-1) as Class 1 SSCs has been shown to be adequate to meet DB requirements.

Diverse mitigation features, similar to those for the loss of normal feedwater event are also available for mitigation of this infrequent fault, although not required. Table 9.2.8-2 lists operator actions available in the event of a primary protection failure.

Refer to Section 9.2.7.5 for additional discussion on DiD levels of defence that are available and on ALARP that applies to this event.

9.2.8.6 Conclusions

Results of the analyses show that for the postulated feedwater line rupture, the capacity of the PRHR heat exchanger is adequate to remove decay heat, to prevent overpressurisation of the reactor coolant system, and to maintain the core cooling capability. Radioactivity doses from postulated ruptures of the feedwater lines are less than those presented for the postulated main steam line break. The evaluation criteria are therefore met.

DBA Radiological consequences are within the Target 4 BSL for infrequent faults (10 mSv offsite and 200 mSv onsite). Thus, the identification of necessary Class 1 SSCs is adequate to meet DB requirements for this fault.

It has been shown that the AP1000 plant design includes adequate systems for the protection of this fault, which limit the radiological consequences such that they are compliant with the SAPs targets and the risks have been reduced to be ALARP.

9.2.9 References

9.2-1 Westinghouse Document WCAP-7769, Rev. 1 (Proprietary), “Topical Report Overpressure Protection for Westinghouse Pressurized Water Reactors,” June 1972. (Also letter NS-CE-622, C. Eicheldinger (Westinghouse) to D. B. Vassallo (NRC), additional information on WCAP-7769, Revision 1, April 16, 1975).

9.2-2 Westinghouse Documents WCAP-7907-P-A, Rev. 0 (Proprietary) and WCAP-7907-A, Rev. 0 (Non-Proprietary), “LOFTRAN Code Description,” April 1984.

9.2-3 ANSI/ANS 5.1-1979, “American National Standard Decay Heat Power in Light Water Reactors,” August 1979.

9.2-4 Westinghouse Documents WCAP-9230 (Proprietary) and WCAP-9231 (Non-Proprietary), “Report on the Consequences of a Postulated Main Feedline Rupture,” January 1978.

9.2-5 Westinghouse Documents WCAP-11397-P-A (Proprietary) and WCAP-11397-A (Non-Proprietary), "Revised Thermal Design Procedure," April 1989.

9.2-6 Westinghouse Documents WCAP-15644-P, Rev. 2 (Proprietary) and WCAP-15644-NP, Rev. 2 (Non-Proprietary), "AP1000 Code Applicability Report," March 2004.

9.2-7 Westinghouse Document WCAP-7908-A (Non-Proprietary), "FACTRAN A FORTRAN-IV Code for Thermal Transients in a UO_2 Fuel Rod," December 1989.

9.2-8 Westinghouse Documents WCAP-14565-P-A, Rev. 0 (Proprietary) and WCAP-15306-NP-A, Rev. 0 (Non-Proprietary), "VIPRE-01 Modeling and Qualification for Pressurized Water Reactor Non-LOCA Thermal-Hydraulic Safety Analysis," October 1999.

9.2-9 Westinghouse Document WCAP-16779-NP, Rev. 1 (Non-Proprietary), "Overpressure Protection Report for AP1000 Nuclear Power Plant," August 2010.

9.2-10 Westinghouse Report UKP-GW-GL-067, Rev. 1, "AP1000 Assessment of Diverse Mitigation of Frequent Faults for the UK," December 2011.

9.2-11 Westinghouse Report UKP-GW-GLR-016, Rev. B, "Evaluation of ATWS Events for UK AP1000™ Pressurized Water Reactor," October 2010.

9.2-12 NUREG/CR-5535, EGG-2596, "RELAP5/MOD3 Code Manual," EG&G Idaho, Inc, June 1990.

9.2-13 Westinghouse Report UKP-SSAR-GLR-001, Rev. 0, "UK Fault Studies Analysis Basis," August 2016.

9.2-14 Westinghouse Report UKP-SSAR-GLR-002, Rev. 0, "UK AP1000® Plant: Summary Report Supporting the Closure of Fault Studies Issue 03," May 2016.

Table 9.2-1 (Sheet 1 of 8). DBA Time Sequence Of Events For Incidents Which Result In A Decrease In Heat Removal By The Secondary System

Accident	Event	Time (seconds)
I. Turbine trip		
A.1. With pressuriser spray, minimum reactivity feedback, with offsite power available	Turbine trip; loss of main feedwater	0.0
	Minimum DNBR occurs	9.9
	Initiation of steam release from steam generator safety valves	11.09
	Overtemperature ΔT reactor trip setpoint reached	19.1
	Rods begin to drop	21.1
A.2. With pressuriser spray, minimum reactivity feedback, without offsite power available	Turbine trip; loss of main feedwater	0.0
	Offsite power lost, reactor coolant pumps begin coasting down	3.0
	Low reactor coolant pump speed reactor trip setpoint reached	3.50
	Rods begin to drop	4.15
	Minimum DNBR occurs	5.9
	Initiation of steam release from steam generator safety valves	15.99

Table 9.2-1 (Sheet 2 of 8). DBA Time Sequence Of Events For Incidents Which Result In A Decrease In Heat Removal By The Secondary System

Accident	Event	Time (seconds)
B.1. With pressuriser spray, maximum reactivity feedback, with offsite power available	Turbine trip; loss of main feedwater flow	0.0
	Minimum DNBR occurs	0.0
	Initiation of steam release from steam generator safety valves	11.2
	Overtemperature ΔT reactor trip setpoint reached	20.9
	Rod motion begins	22.9
B.2. With pressuriser spray, maximum reactivity feedback, without offsite power available	Turbine trip; loss of main feedwater	0.0
	Offsite power lost, reactor coolant pumps begin coasting down	3.0
	Low reactor coolant pump speed reactor trip setpoint reached	3.50
	Rods begin to drop	4.15
	Minimum DNBR occurs	4.9
	Initiation of steam release from steam generator safety valves	17.7

Table 9.2-1 (Sheet 3 of 8). DBA Time Sequence Of Events For Incidents Which Result In A Decrease In Heat Removal By The Secondary System

Accident	Event	Time (seconds)
C.1. Without pressuriser spray, minimum reactivity feedback, with offsite power available	Turbine trip; loss of main feedwater flow	0.0
	High-2 pressuriser pressure reactor trip point reached	5.2
	Rods begin to drop	7.2
	Initiation of steam release from steam generator safety valves	8.5
	Peak RCS pressure occurs	8.7
C.2. Without pressuriser spray, minimum reactivity feedback, without offsite power available	Turbine trip; loss of main feedwater	0.0
	Offsite power lost, reactor coolant pumps begin coasting down	3.0
	Low reactor coolant pump speed reactor trip setpoint reached	3.50
	Rods begin to drop	4.15
	Peak RCS pressure occurs	6.2
	Initiation of steam release from steam generator safety valves	10.2

Table 9.2-1 (Sheet 4 of 8). DBA Time Sequence Of Events For Incidents Which Result In A Decrease In Heat Removal By The Secondary System

Accident	Event	Time (seconds)
D.1. Without pressuriser spray, maximum reactivity feedback, with offsite power available	Turbine trip; loss of main feedwater flow	0.0
	High-2 pressuriser pressure reactor trip	5.1
	Rods begin to drop	7.1
	Peak RCS pressure occurs	8.0
	Initiation of steam release from steam generator safety valves	8.5
D.2. Without pressuriser spray, maximum reactivity feedback, without offsite power available	Turbine trip; loss of main feedwater	0.0
	Offsite power lost, reactor coolant pumps begin coasting down	3.0
	Low reactor coolant pump speed reactor trip setpoint reached	3.50
	Rods begin to drop	4.15
	Peak RCS pressure occurs	5.8
	Initiation of steam release from steam generator safety valves	10.4

Table 9.2-1 (Sheet 5 of 8). DBA Time Sequence Of Events For Incidents Which Result In A Decrease In Heat Removal By The Secondary System

Accident	Event	Time (seconds)
II.A. Loss of ac power to the plant auxiliaries	Offsite ac power is lost, feedwater is lost, RCPs begin to coast down, turbine trip	0.0
	RCP speed-low reactor trip set point is reached	0.5
	Rods begin to drop	1.3
	Pressuriser safety valves open	~ 3.0
	Maximum pressuriser pressure reached	4.0
	Pressuriser safety valves close	~8.0
	Pressuriser safety valves open	49.0 (1)
	Steam generator 1 safety valves open	73.6 (1)
	Steam generator 2 safety valves open	76.0 (1)
	PRHR heat exchanger actuation on low steam generator water level (narrow range coincident with low start up feedwater flow rate)	510.5
	Maximum pressuriser water volume reached	511.0
	PRHR heat exchanger extracted heat matches decay heat	~20000

Note:

1. The pressuriser safety valves cycle open and closed from 49.0 seconds until ~435 seconds. The steam generator safety valves in both Loops 1 and 2 also cycle open and close from approximately 75 seconds, until approximately 2500 seconds. After this time, only the steam generator safety valves for the loop without the PRHR (Loop 2) continued to relieve steam intermittently until ~20,000 seconds.

Table 9.2-1 (Sheet 6 of 8). DBA Time Sequence Of Events For Incidents Which Result In A Decrease In Heat Removal By The Secondary System

Accident	Event	Time (seconds)
III.A. Loss of normal feedwater flow	Feedwater is lost	0.0
	Low-2 steam generator water level (narrow range) reactor trip reached	48.2
	Rods begin to drop	50.2
	Minimum DNBR is reached	51.0
	PRHR heat exchanger actuation on Low-2 steam generator water level (narrow range coincident with Low-2 start up feedwater flow rate)	230.2
	Cold leg temperature reaches Low-2 T_{cold} setpoint	1570.8
	High-2 pressuriser level setpoint reached	1576.0
	Reactor coolant pump trip on Low-2 T_{cold} "S" signal	1577.6
	Steam line isolation on Low-2 T_{cold} "S" signal	1582.9
	Core makeup tank actuation on Low-2 T_{cold} "S" signal	1587.9
	The chemical and volume control system is isolated on "S" signal and pressuriser water level – High-1	1608.4
	Pressuriser safety valves open	2080.0
	High-3 pressuriser level setpoint reached	3128.0
	Operator opens reactor vessel head vent (at least 30 minutes after High-2 pressuriser level setpoint is reached)	4350.0
	Pressuriser safety valves reclose	~4350.0
	Maximum pressuriser water volume reached	5628.0

Table 9.2-1 (Sheet 7 of 8). DBA Time Sequence Of Events For Incidents Which Result In A Decrease In Heat Removal By The Secondary System

Accident	Event	Time (seconds)
III.B. Loss of normal feedwater flow with a consequential loss of ac power	Feedwater is lost	10.0
	Low-2 steam generator water level setpoint is reached	58.2
	Rods begin to drop	60.2
	Minimum DNBR is reached	61.0
	Reactor coolant pump trip due to loss of ac power	68.2
	Steam generator safety valves open	94.3
	Pressuriser safety valves open	~107.0
	PRHR heat exchanger actuation on Low-2 steam generator water level (narrow range coincident with Low-2 startup flow rate)	240.2
	Steam generator safety valves close	~2100.0 (1)
	Pressuriser safety valves close	~2450.0(2)
	PRHR heat extraction matches decay heat addition	~2800.0
	Maximum pressuriser water volume reached	3306.0

Notes:

1. Between 94.3 seconds and 2100 seconds the steam generator safety valves cycle open and closed. After 2100 seconds the steam generator safety valves intermittently relieve steam, but with a relief rate that is minimal and has a negligible effect on the transient.
2. Between approximately 107 seconds and 2450 seconds the pressuriser safety valves cycle open and closed.

Table 9.2-1 (Sheet 8 of 8). DBA Time Sequence Of Events For Incidents Which Result In A Decrease In Heat Removal By The Secondary System

Accident	Event	Time (seconds)
IV. Feedwater system pipe break	Main feedwater flow to both steam generators stops due to interaction between the break and the main feedwater control system	10.0
	Low steam generator water level (narrow range) setpoint reached	60.3
	Rods begin to drop	62.3
	Reverse flow from the faulted steam generator through a full double-ended rupture starts	62.3
	Loss of offsite power	70.3
	Low steam line pressure setpoint is reached	76.7
	Core makeup tank valves fully opened	76.7
	Low steam generator water level (wide range) setpoint reached	81.6
	All steam isolation valves close	88.7
	PRHR heat exchanger actuation on low steam generator water level (wide range)	98.6
	Faulted steam generator empties	122.0
	Intact steam generator safety valves open for the first time	251.7
	Pressuriser safety valves open for the first time	1,718
	PRHR heat exchanger extracted heat matches decay heat	23,990

Table 9.2.3-1. ATWT Time Sequence Of Events For Turbine Trip with PMS CCF

Event	Time (Sec)
Turbine trip	5
Rapid power reduction system drops selected bank of rods to reduce power below 50 percent power	not credited
Turbine bypass start to open in T_{avg} mode	5.4
Pressuriser sprays begins to operate	not credited
CVS control system begins to open letdown valve	not credited
Pressuriser safety valves opens	12.2
SG PORV Loops 1&2 open	43
Pressuriser safety valves closes	63

Table 9.2.6-1 (Sheet 1 of 2). DBA Parameters Used In Evaluating The Radiological Consequences Of A Loss Of Offsite Power

Reactor coolant iodine activity	Initial activity equal to the operating limit for reactor coolant activity of 9.25E6 Bq/kg (0.25 μCi/g) dose equivalent I-131 (see Table 9A-1) with an assumed iodine spike that increases the rate of iodine release from fuel into the coolant (see Table 9A-2) by a factor of 335. Duration of spike is 8 hours.
Reactor coolant noble gas activity	Equal to the operating limit for reactor coolant activity of 2.6E9 Bq/kg (70 μCi/g) dose equivalent Xe-133 (see Table 9A-1)
Reactor coolant alkali metal activity	Design basis activity (see Table 9A-1)
Secondary coolant initial iodine and alkali metal activity	10% of design basis reactor coolant concentrations at maximum equilibrium conditions
Reactor coolant mass	1.684E5 kg (3.713E5 lbm)
Condenser	Not available
Primary to secondary leak rate	0.79(1) kg/min (1.74 lbm/min)
Partition coefficient in steam generators Volatile (iodine) Particulates (iodine, alkali metals)	See Appendix 9A.4 1.0 0.0005
Accident scenario in which startup feedwater is not available Duration of accident Duration of flashing Steam release rate Minimum secondary coolant mass	 1.5 hr 1.5 hr 54.44 kg/sec (120 lbm/sec) 3.4E4 kg (7.5E4 lbm)

Table 9.2.6-1 (Sheet 2 of 2). DBA Parameters Used In Evaluating The Radiological Consequences Of A Loss Of Offsite Power

Accident scenario in which startup feedwater is available Duration of accident Duration of flashing Steam release rate Minimum secondary coolant mass	 8.0 hr Not applicable 27.22 kg/sec (60 lbm/sec) 1.32E5 kg (2.92E5 lbm)
Volatile iodine fraction With primary-to-secondary flashing Without primary-to-secondary flashing	See Appendix 9A.5.3 0.002 0.001
Offsite atmospheric dispersion factors	See Table 9A-5
Control room modelling	See Appendix 9A

Notes:
1. Equivalent to 567.8 L (150 gal) per day per SG cooled liquid at 1000 kg/m^3 (62.4 lbm/ft^3).

Table 9.2.6-2. DBA Loss Of Offsite Power Technical Specifications Used In Dose Analysis

Limit or Condition	Tech Spec Identification and Notes
Primary-to-secondary leakage rate	3.4.7 leak rate to be < 567.8 L (150 gal) per day for any one SG
Primary coolant specific activity	3.4.10 dose equivalent specific activity to be < 9.25E6 Bq/kg (0.25 µCi/g) for I-131 and < 2.6E9 Bq/kg (70 µCi/g) for Xe-133
Secondary coolant specific activity	3.7.4 dose equivalent I-131 specific activity to be < 9.25E5 Bq/kg (0.025 µCi/g)

Table 9.2.7-1. ATWT Time Sequence Of Events For LONF With RCCA Mechanical CCF

Event	Time (Sec.)
Loss of Feedwater	5
Pressuriser sprays begins to operate	12
CVS control system begins to open letdown valve	not credited
Narrow Range Low SG Level reactor trip PMS setpoint reached in loops 1&2 generates turbine trip signal, clears turbine bypass block and switch turbine bypass to pressure mode	51.7
Startup Feedwater Pump actuation	not credited
Turbine is tripped	58.7
Turbine bypass start to open	61.4
Pressuriser safety valves open	62.9
SG PORVs and then safety valves open in loops 1 & 2	63.6
Wide range Low SG Level setpoint reached in loops 1& 2, generates signals for PMS PRHR actuation, DAS CMT actuation, DAS RCP trip	71.3
RCPs are tripped on DAS WR Low SG1+SG2 level signal (1)	78.8
PRHR valves full flow on PMS wide range Low SG level signal (1)	80.8
CMT valves full flow on DAS wide range Low SG1+SG2 level signal (1)	85.8
SG safety valves and then SG PORVs close, in loops 1 & 2	86.6
Low Steam Pressure setpoint 4.14 MPa (600 psi) reached	87.15
Pressuriser fills water solid	88.2
Steam line isolation on Low Steam Pressure	99.2
Peak RCS pressure 19.93 MPa (2890 psia) reached	111.8
Pressuriser safety valves close	183
Saturation reached in loop 2 cold leg	184
Subcooling reached in loop 2 cold leg	295

Note:
1. PRHR, CMT and RCP trip actuation delays include instrumentation and control delays (both – inherent and intentional) and valves alignment.

Table 9.2.7-2. Diverse Core Cooling For LONF With PMS CCF

Event	Time (Sec.)
Loss of Feedwater	0
Turbine trip (low SG WR level)	62
CMT actuated (low SG WR level)	62
RCP trip (low SG WR level)	62
Pressuriser safety valves open	65
Reactor trip (low SG WR level + 5 s)	67
SG safety valves open	80
SG safety valves close	710
ADS stage 1 manual actuation	2400
Pressuriser safety valves close	2415
Accumulator injection start	2520
Peak clad temperature 847°C (1556°F)	2608
Accumulator empty	2890
ADS stage 4 manual actuation	3300
IRWST inject manual actuation	3450

Table 9.2.7-3. Loss Of Normal Feedwater Flow Mitigation Features

Category A Safety Function	Provision	SSCs	Classification
Short-term reactivity control	Primary means	Reactor trip Breakers (PMS)	1
	Diverse means	Motor-generator set field breakers (DAS)	1
Long-term reactivity control	Primary means	CMT Recirculation	1
	Diverse means	Passive feed and bleed	1
Decay heat removal	Primary means	PRHR HX	1
	Diverse means	Passive feed and bleed	1
RCS pressure control	Primary means	Pressuriser safety valve	1
	Diverse means	Pressuriser volume	1
RCS inventory control	Primary means	CMTs	1
	Diverse means	Passive feed and bleed	1
Containment cooling	Primary means	PCS AOVs	1
	Diverse means	PCS MOVs	1

Table 9.2.7-4. Credited SSCs in LONF DBA and Diverse Core Cooling Analysis

	DBA Case	Diverse Core Cooling Case
C&I System	PMS	DAS
Reactor trip	RT breakers	MG set field breakers
RCCA insertion	Yes	Yes
Core heat removal	PRHR	Passive feed and bleed using manual ADS 1-4, accumulators, IRWST gravity injection and natural circulation containment recirculation
RCS makeup / boration	CMTs	
Containment Cooling	PCS AOVs	PCS MOVs

Table 9.2.8-1. Feedwater System Pipe Break Mitigation Features

Category A Safety Function	Provision	SSCs	Classification
Short-term reactivity control	Primary means	Reactor trip Breakers (PMS)	1
Long-term reactivity control	Primary means	CMTs	1
Decay heat removal	Primary means	PRHR HX	1
RCS pressure control	Primary means	Pressuriser safety valve	1
RCS inventory control	Primary means	CMTs	1
Containment cooling	Primary means	PCS AOVs	1

Table 9.2.8-2. Feedwater System Pipe Break Potential Operator Actions

Operator Action	Class
If PRHR fails, activate ADS to allow automatic actuation of recirculation RHR via the IRWST.	1

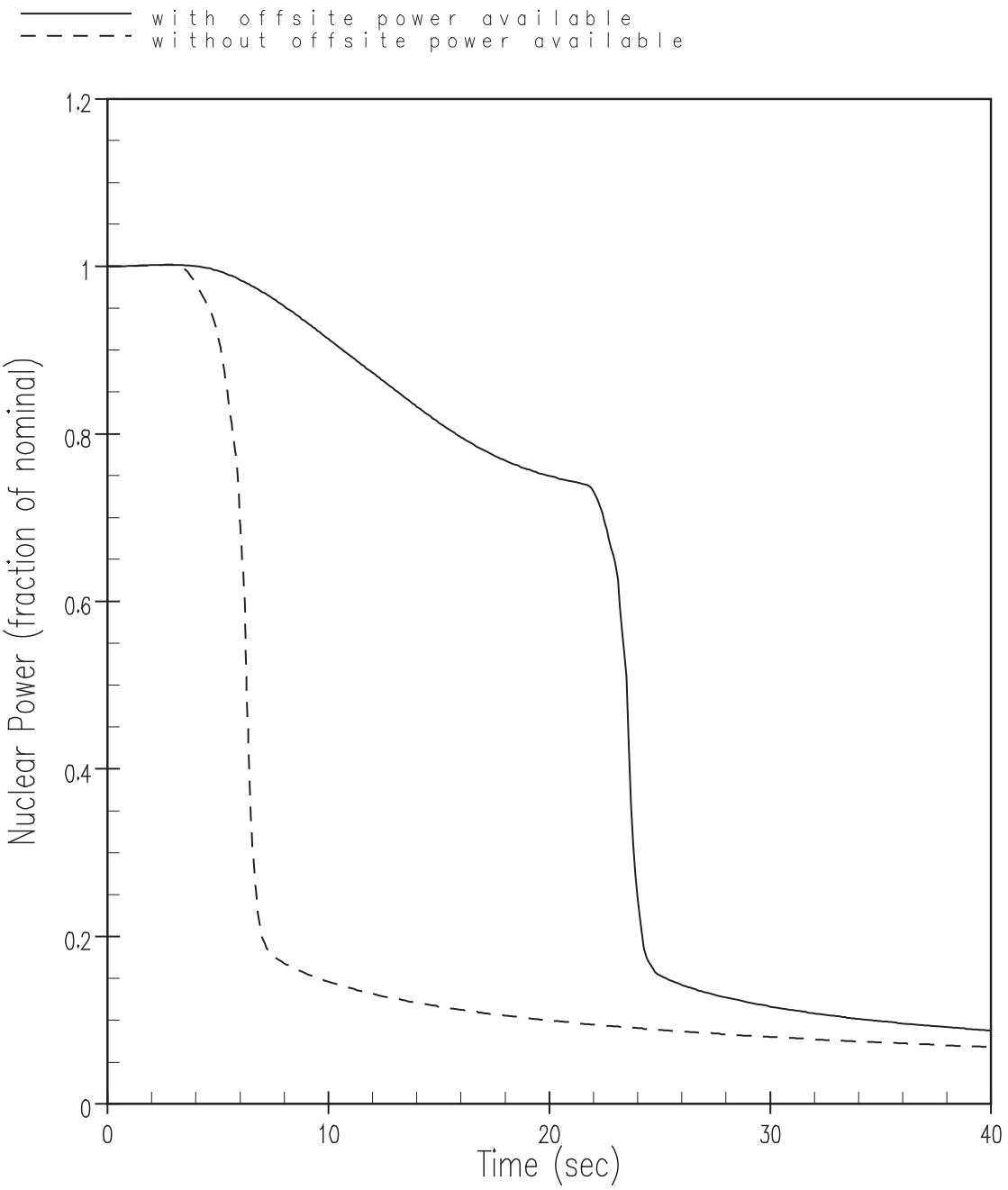


Figure 9.2.3-1. DBA Nuclear Power versus Time for Turbine Trip Accident with Pressuriser Spray and Minimum Moderator Feedback

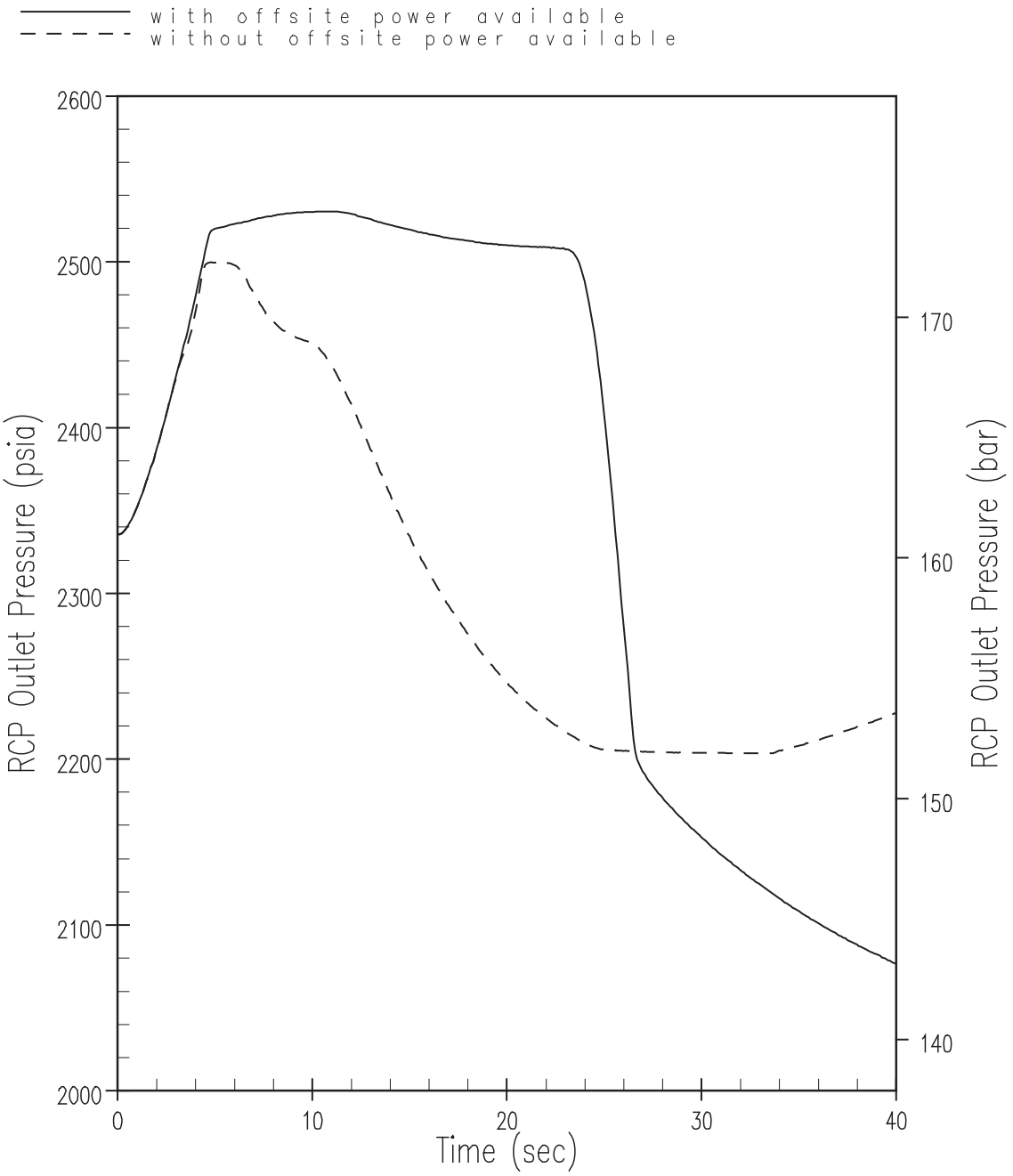


Figure 9.2.3-2. DBA RCP Outlet Pressure versus Time for Turbine Trip Accident with Pressuriser Spray and Minimum Moderator Feedback

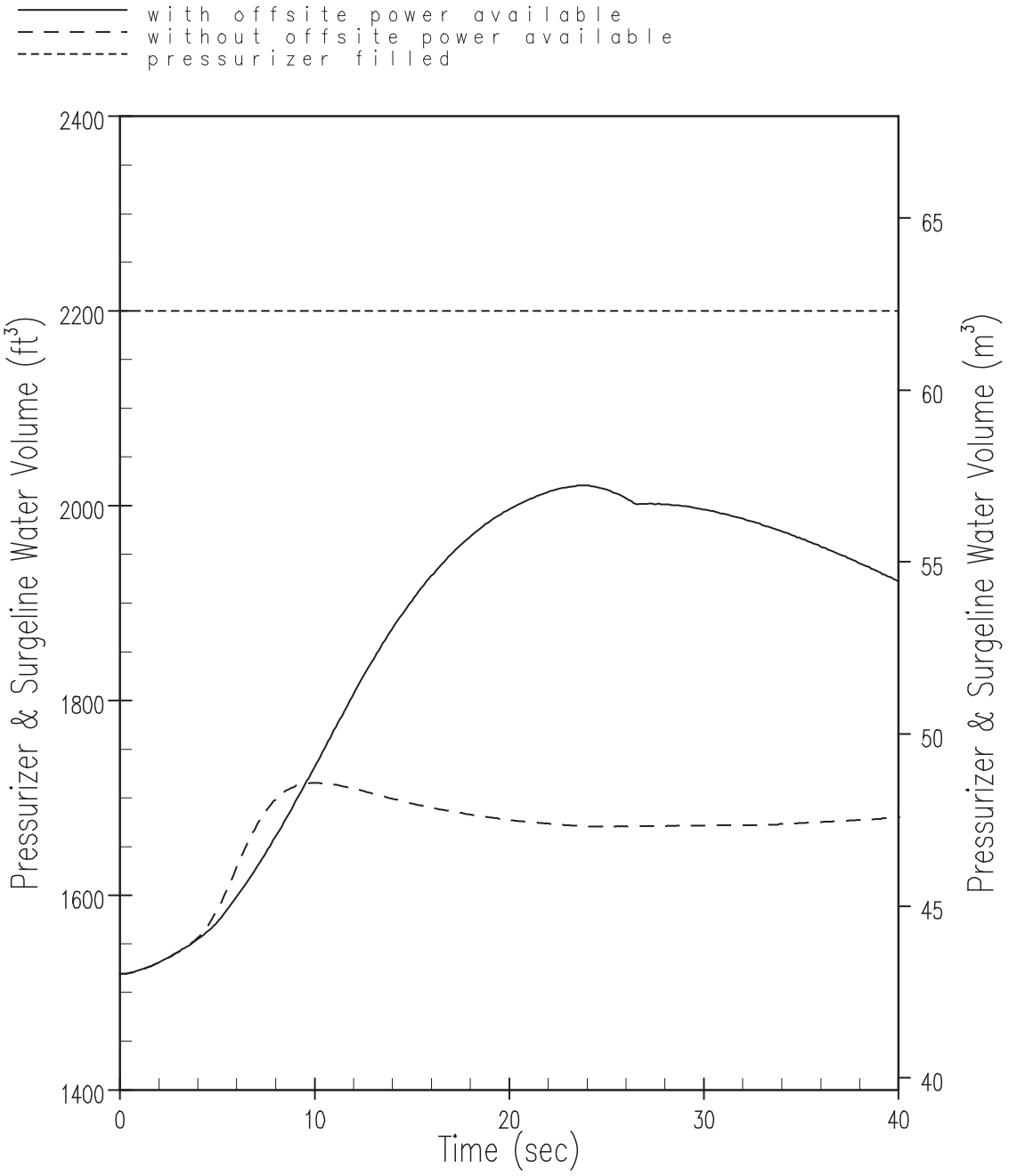


Figure 9.2.3-3. DBA Pressuriser & Surgeline Water Volume versus Time for Turbine Trip Accident with Pressuriser Spray and Minimum Moderator Feedback

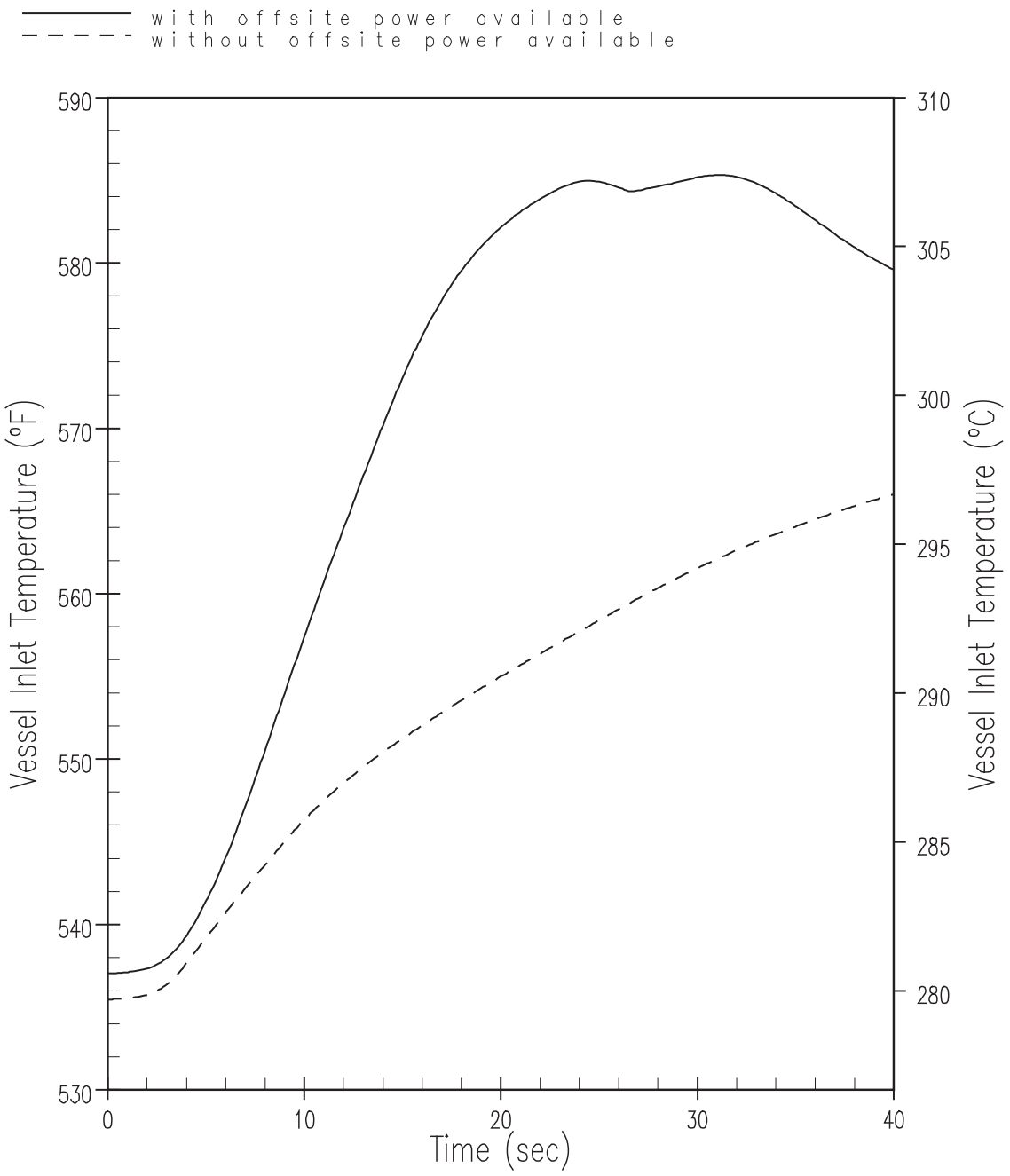


Figure 9.2.3-4. DBA Vessel Inlet Temperature versus Time for Turbine Trip Accident with Pressuriser Spray and Minimum Moderator Feedback

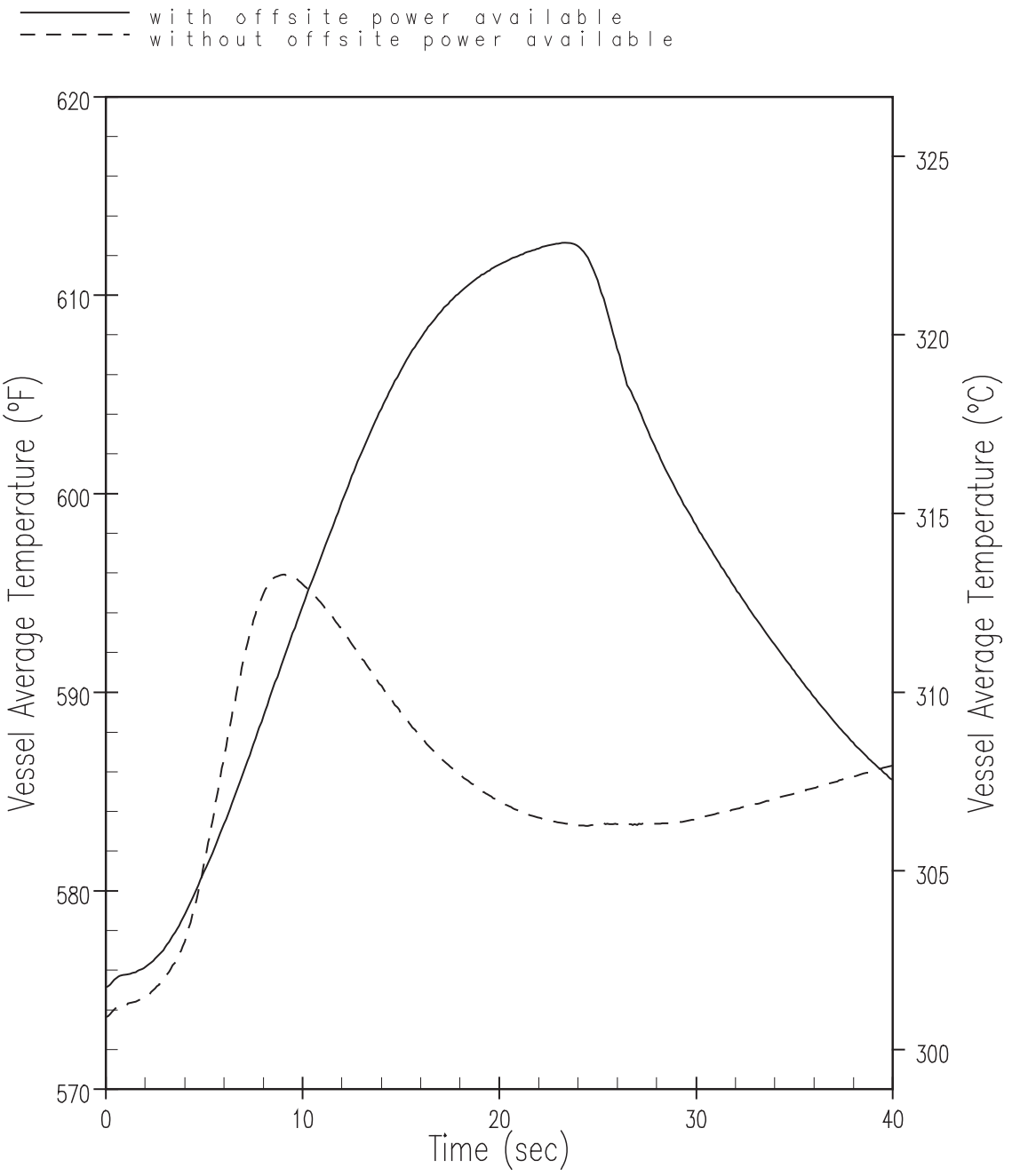


Figure 9.2.3-5. DBA Vessel Average Temperature versus Time for Turbine Trip Accident with Pressuriser Spray and Minimum Moderator Feedback

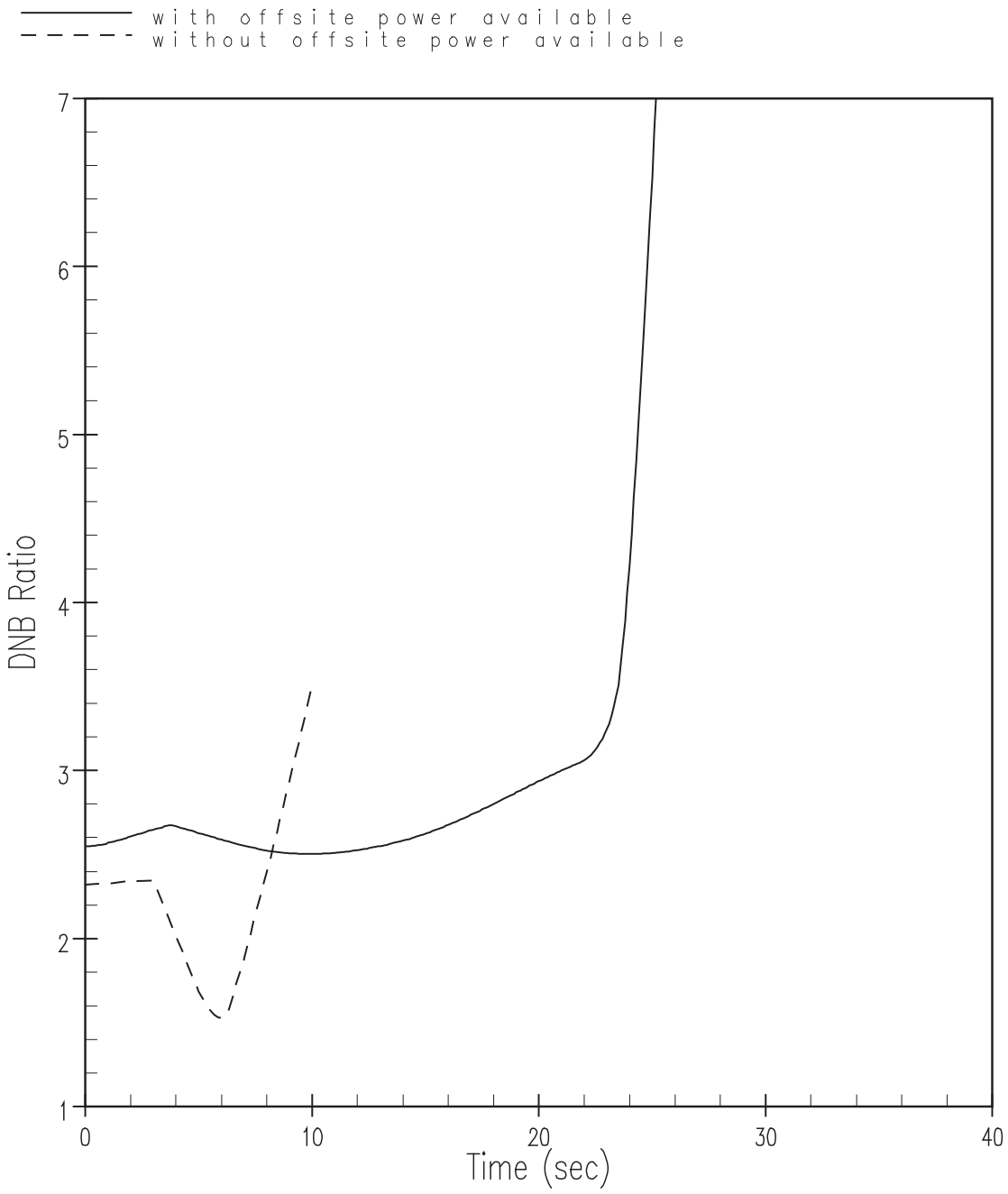


Figure 9.2.3-6. DBA DNBR versus Time for Turbine Trip Accident with Pressuriser Spray and Minimum Moderator Feedback

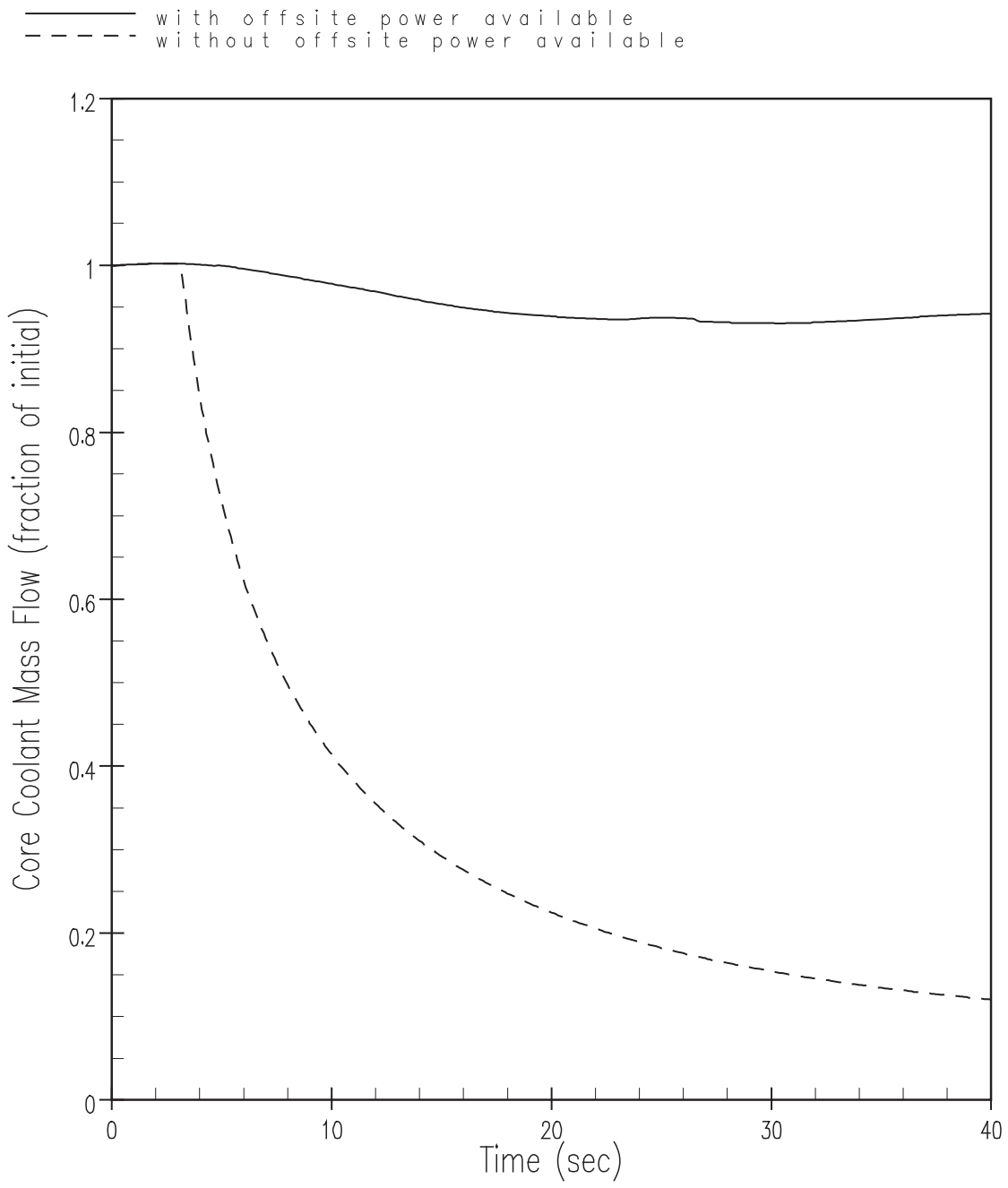


Figure 9.2.3-7. DBA Core Coolant Mass Flow Rate versus Time for Turbine Trip Accident with Pressuriser Spray and Minimum Moderator Feedback

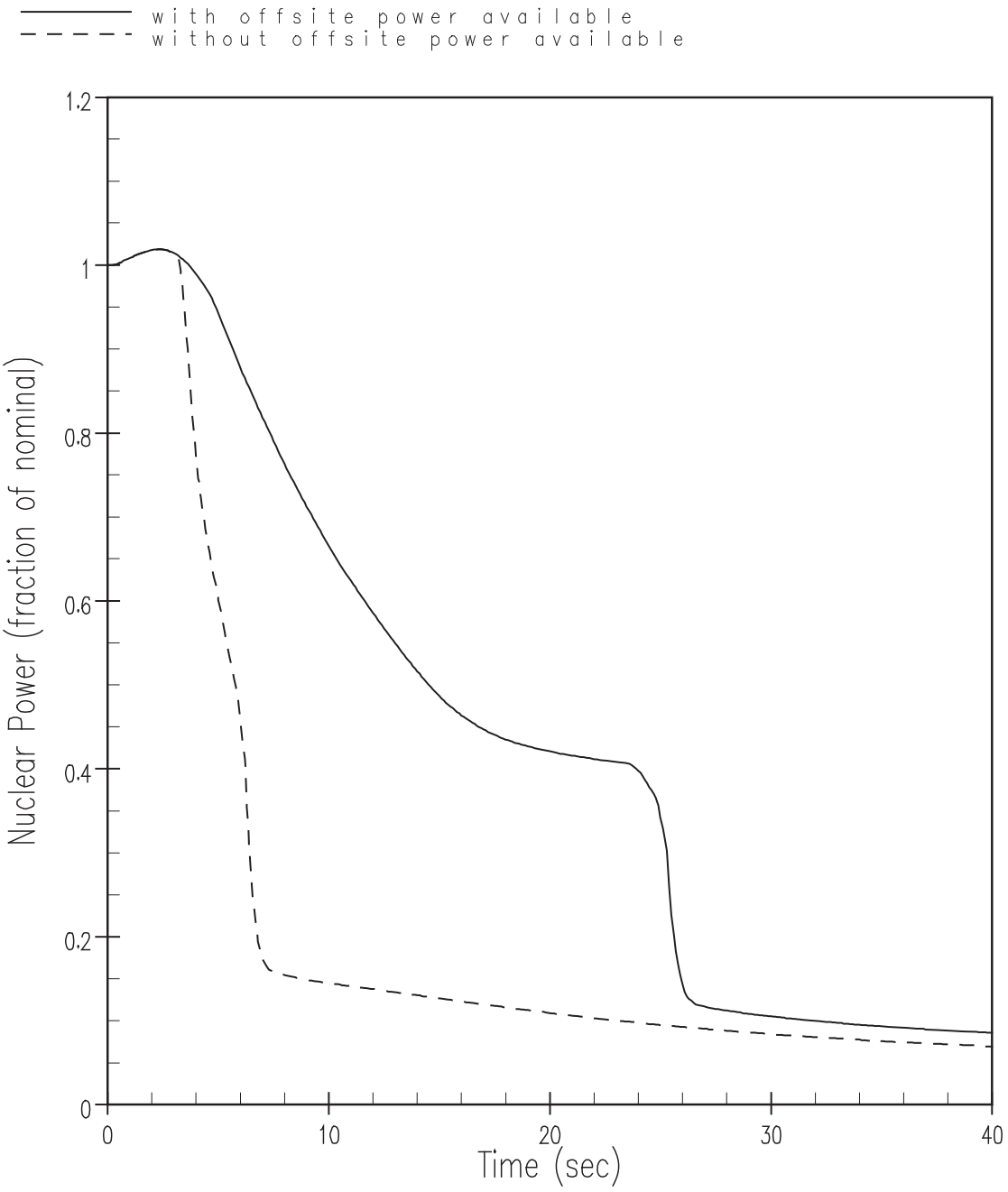


Figure 9.2.3-8. DBA Nuclear Power versus Time for Turbine Trip Accident with Pressuriser Spray and Maximum Moderator Feedback

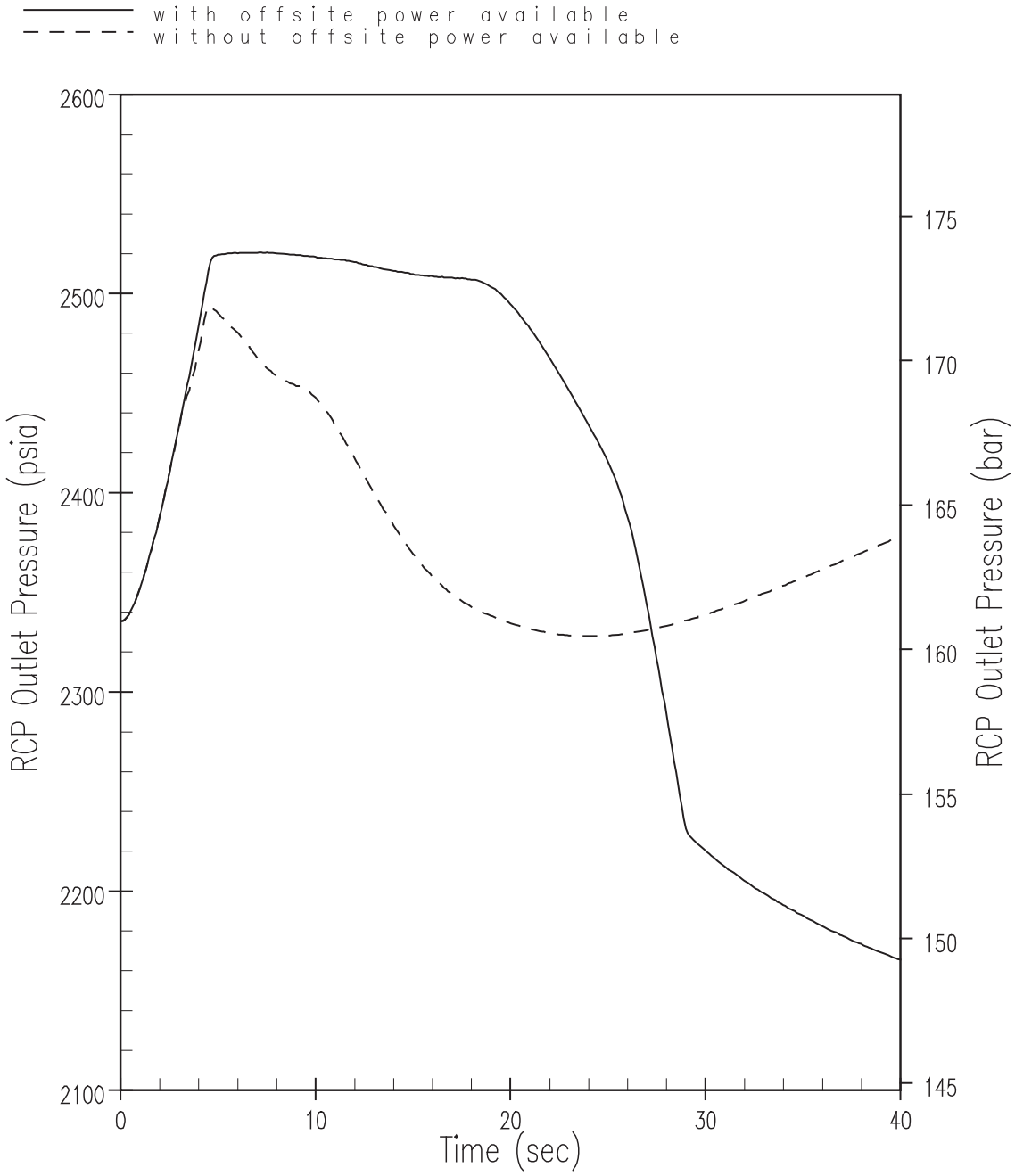


Figure 9.2.3-9. DBA RCP Outlet Pressure versus Time for Turbine Trip Accident with Pressuriser Spray and Maximum Moderator Feedback

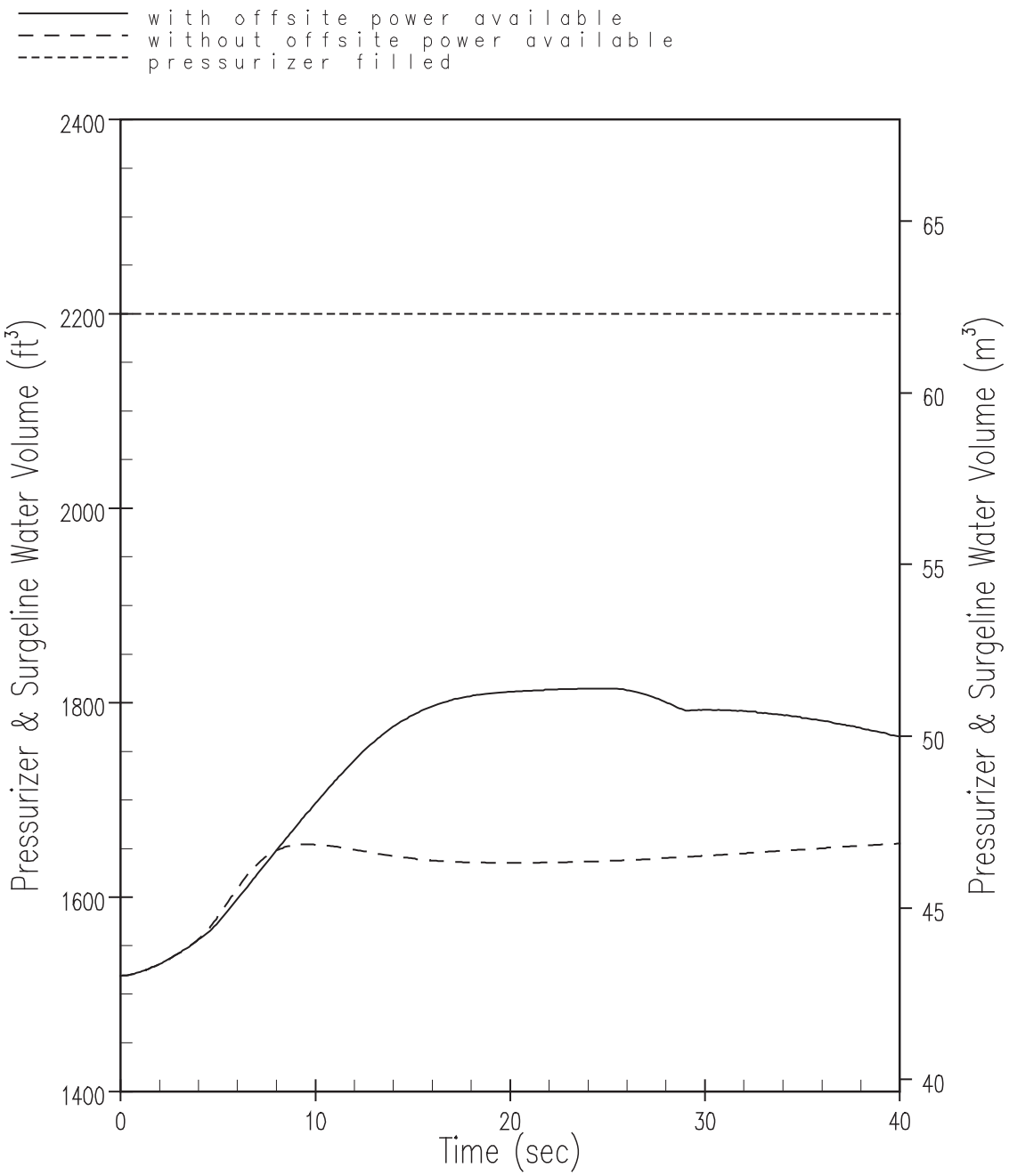


Figure 9.2.3-10. DBA Pressuriser & Surgeline Water Volume versus Time for Turbine Trip Accident with Pressuriser Spray and Maximum Moderator Feedback

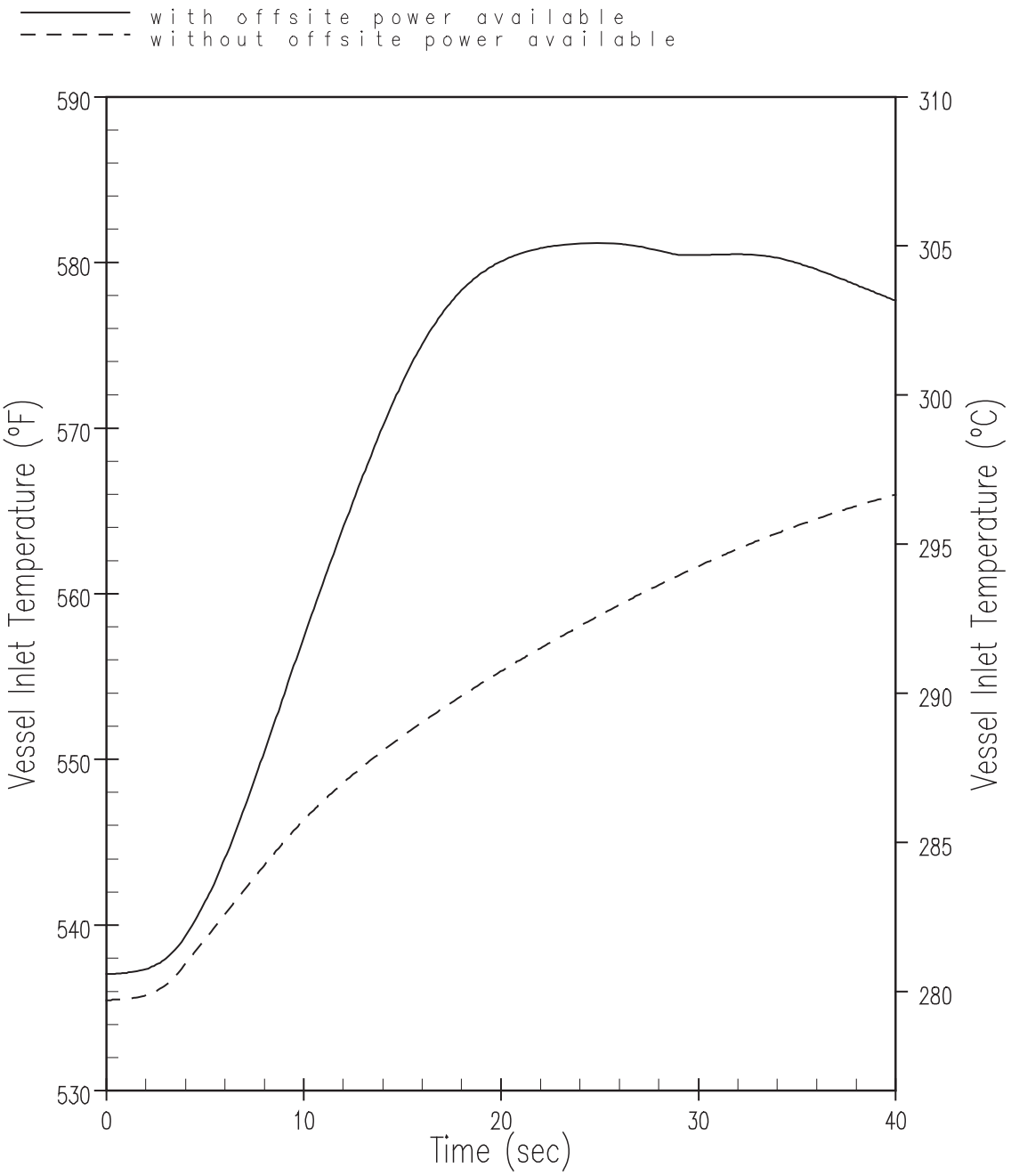


Figure 9.2.3-11. DBA Vessel Inlet Temperature versus Time for Turbine Trip Accident with Pressuriser Spray and Maximum Moderator Feedback

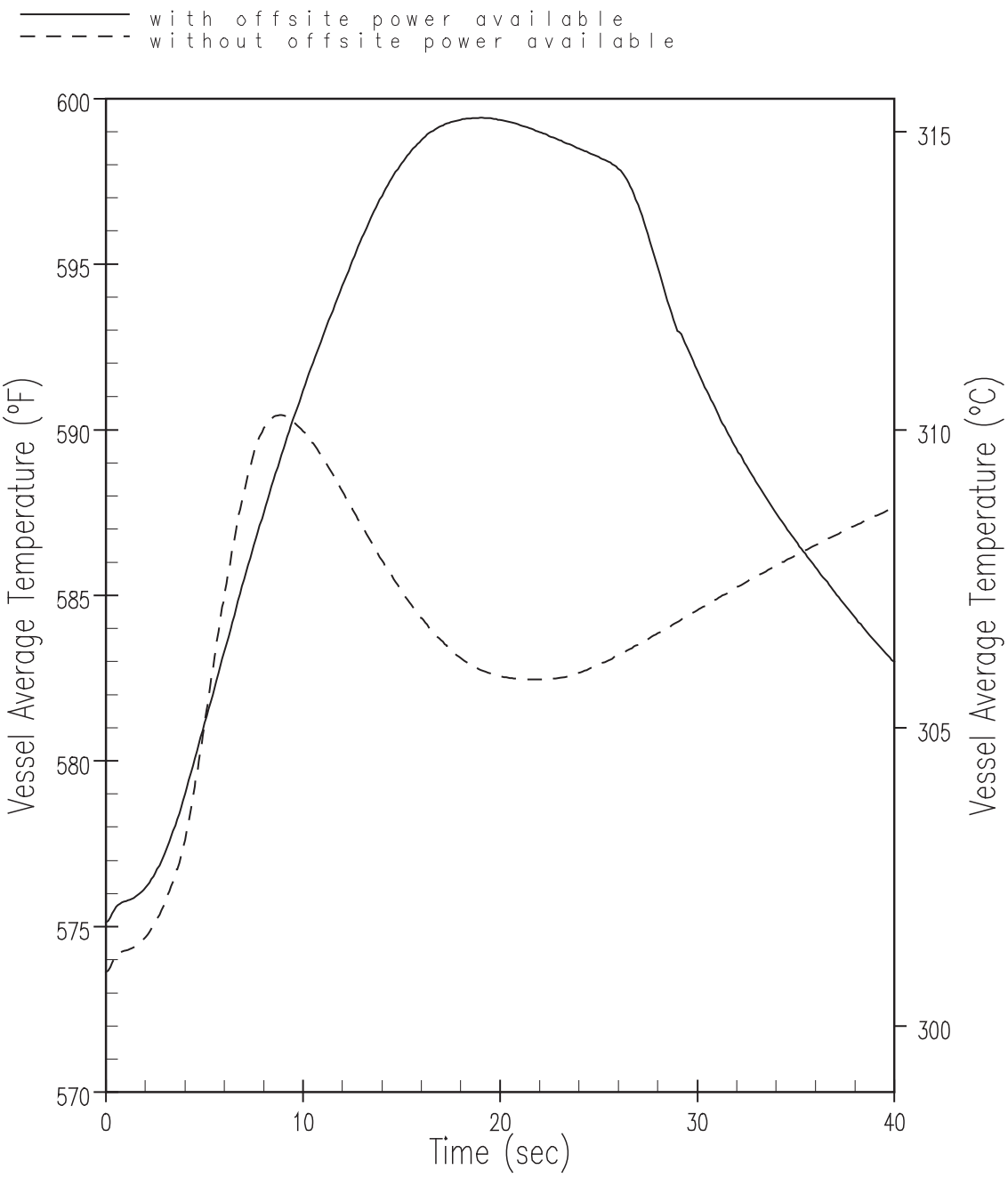


Figure 9.2.3-12. DBA Vessel Average Temperature versus Time for Turbine Trip Accident with Pressuriser Spray and Maximum Moderator Feedback

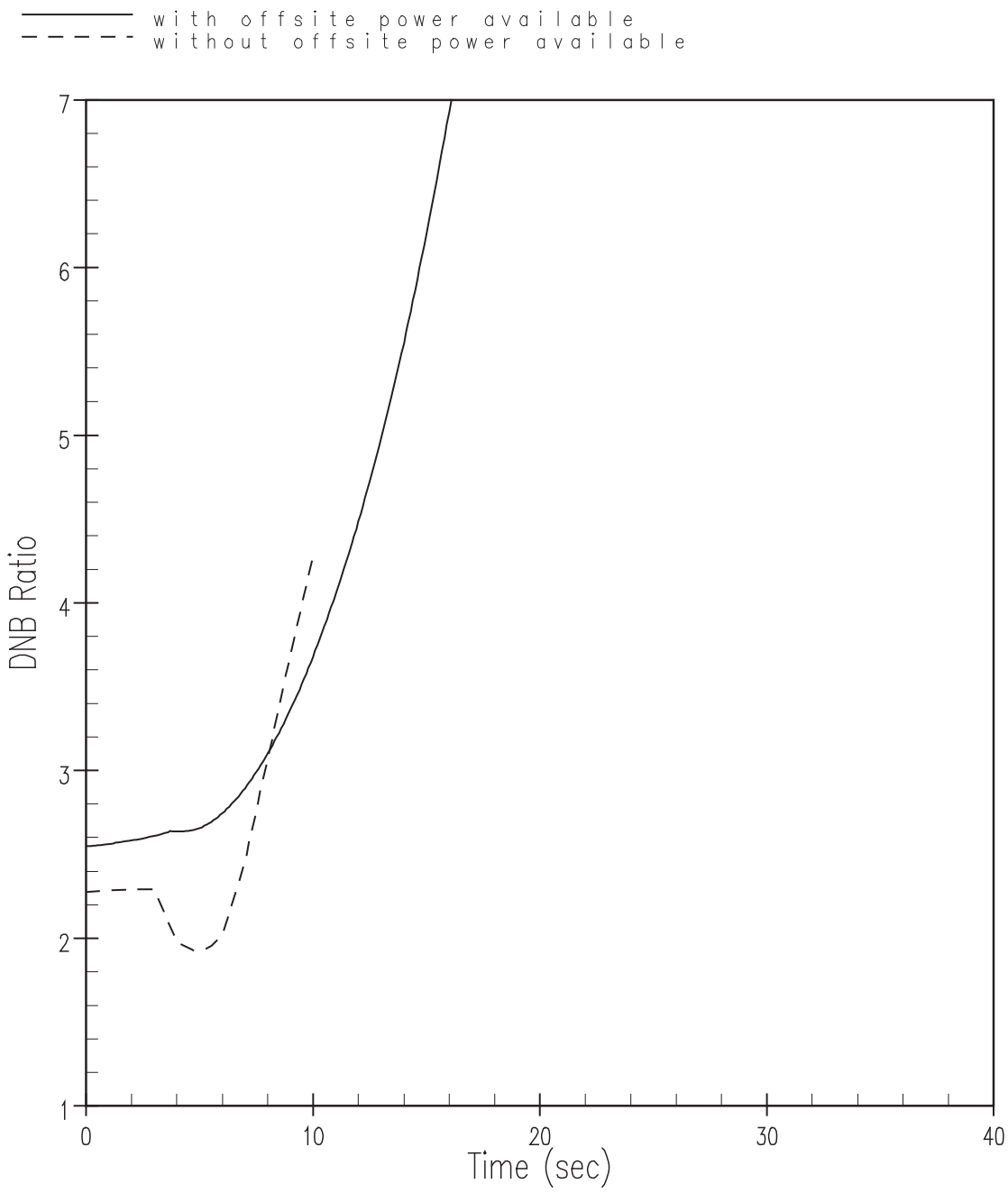


Figure 9.2.3-13. DBA DNBR versus Time for Turbine Trip Accident with Pressuriser Spray and Maximum Moderator Feedback

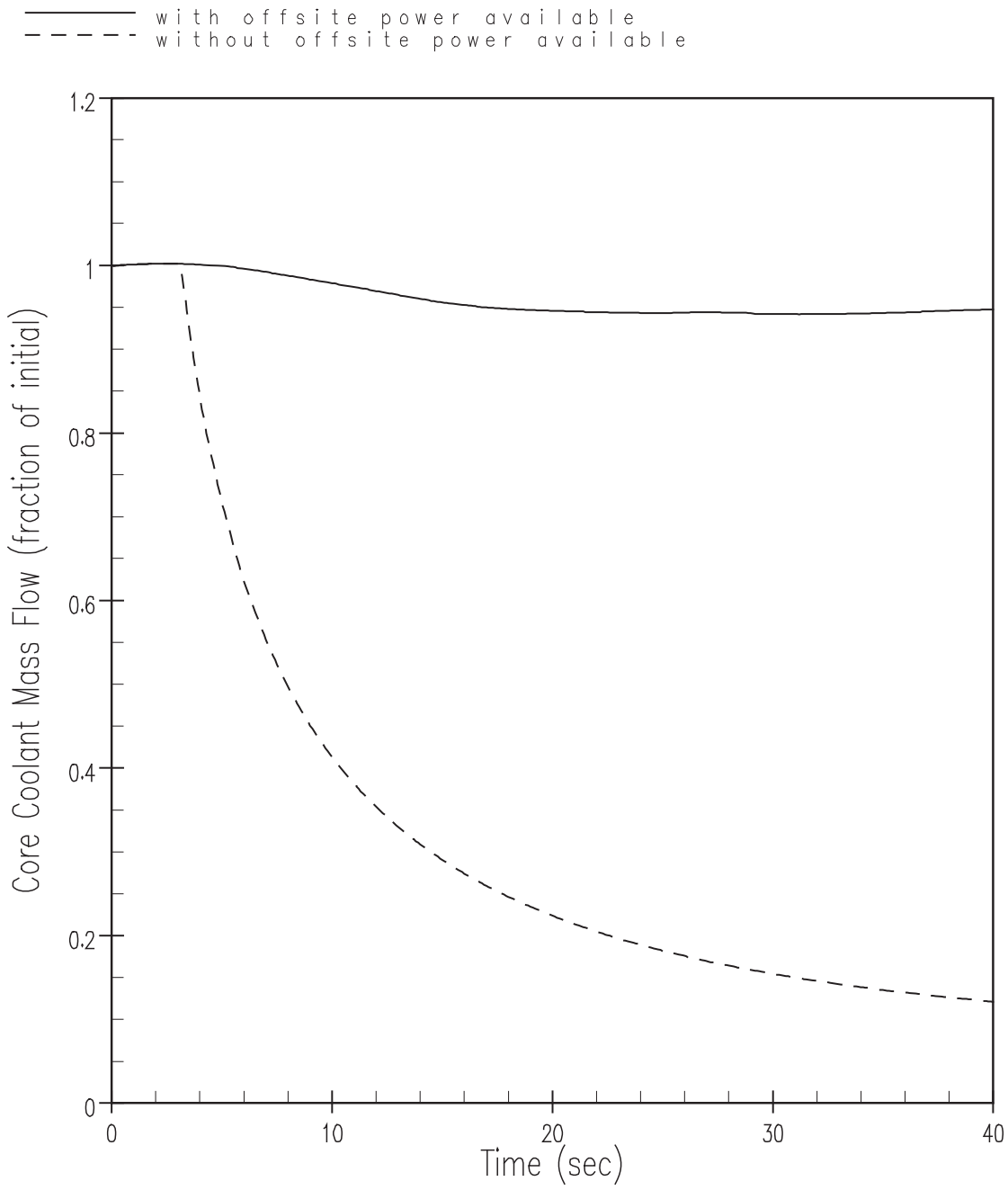


Figure 9.2.3-14. DBA Core Coolant Mass Flow Rate versus Time for Turbine Trip Accident with Pressuriser Spray and Maximum Moderator Feedback

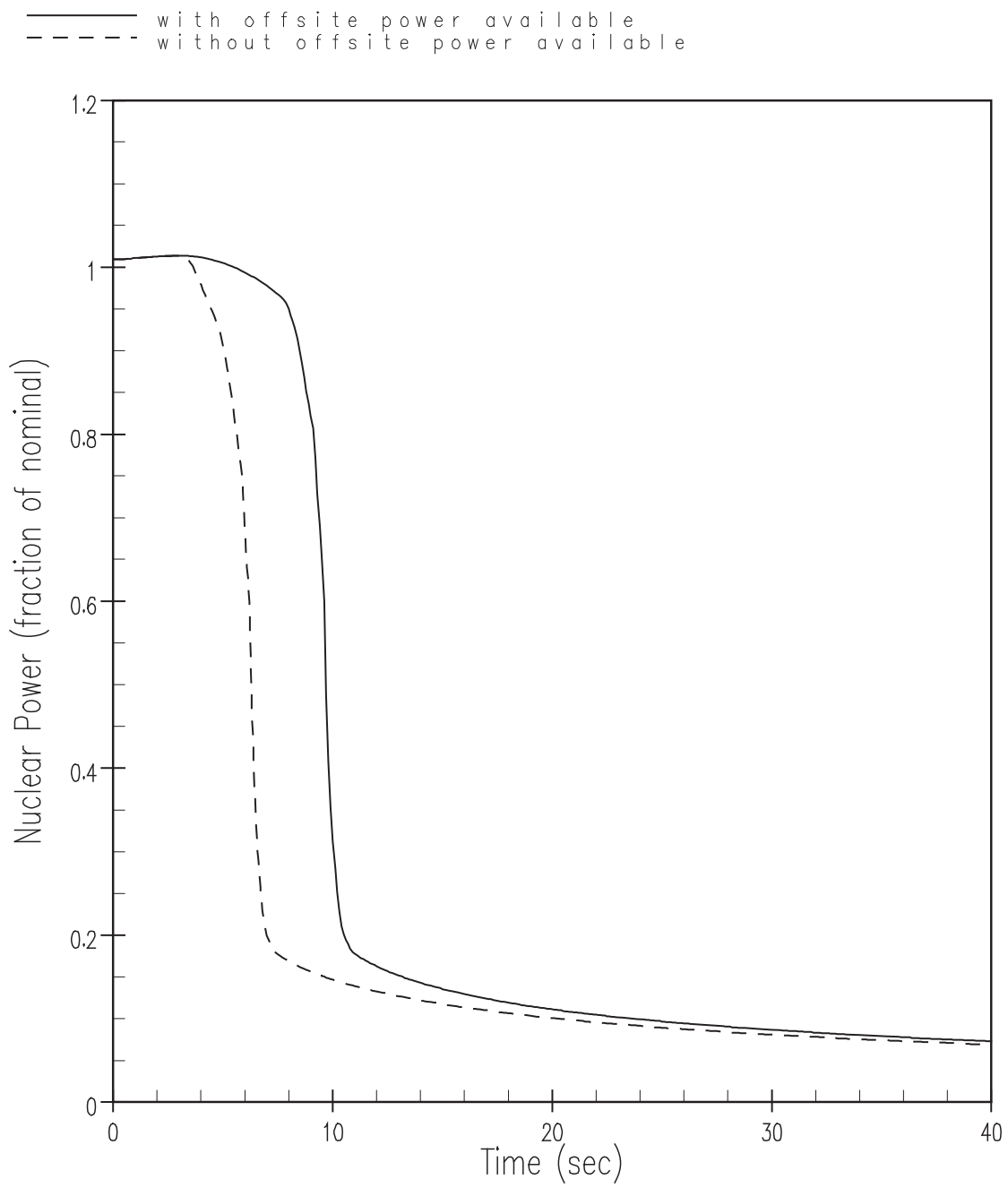


Figure 9.2.3-15. DBA Nuclear Power versus Time for Turbine Trip Accident Without Pressuriser Spray and Minimum Moderator Feedback

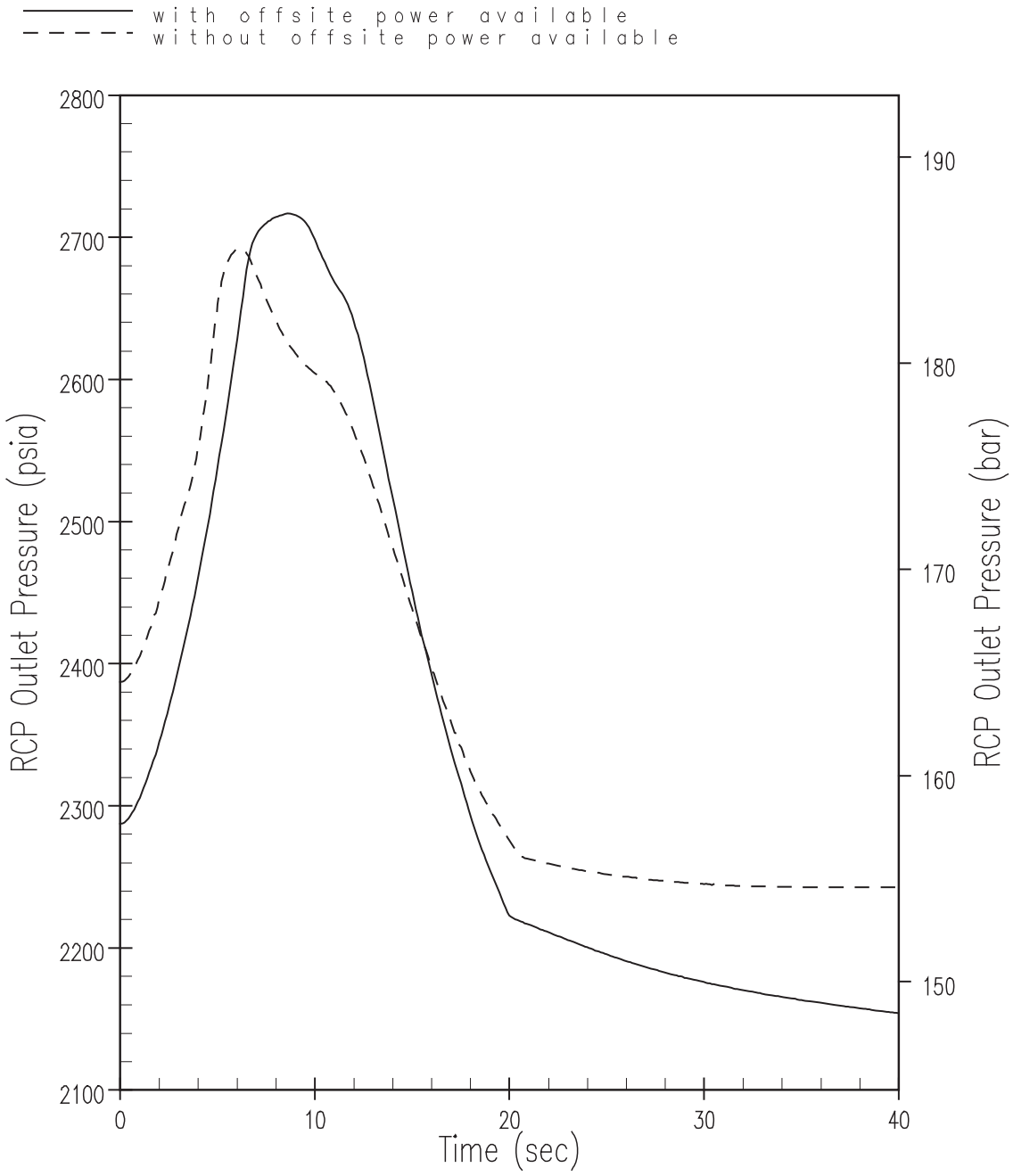


Figure 9.2.3-16. DBA RCP Outlet Pressure versus Time for Turbine Trip Accident Without Pressuriser Spray and Minimum Moderator Feedback

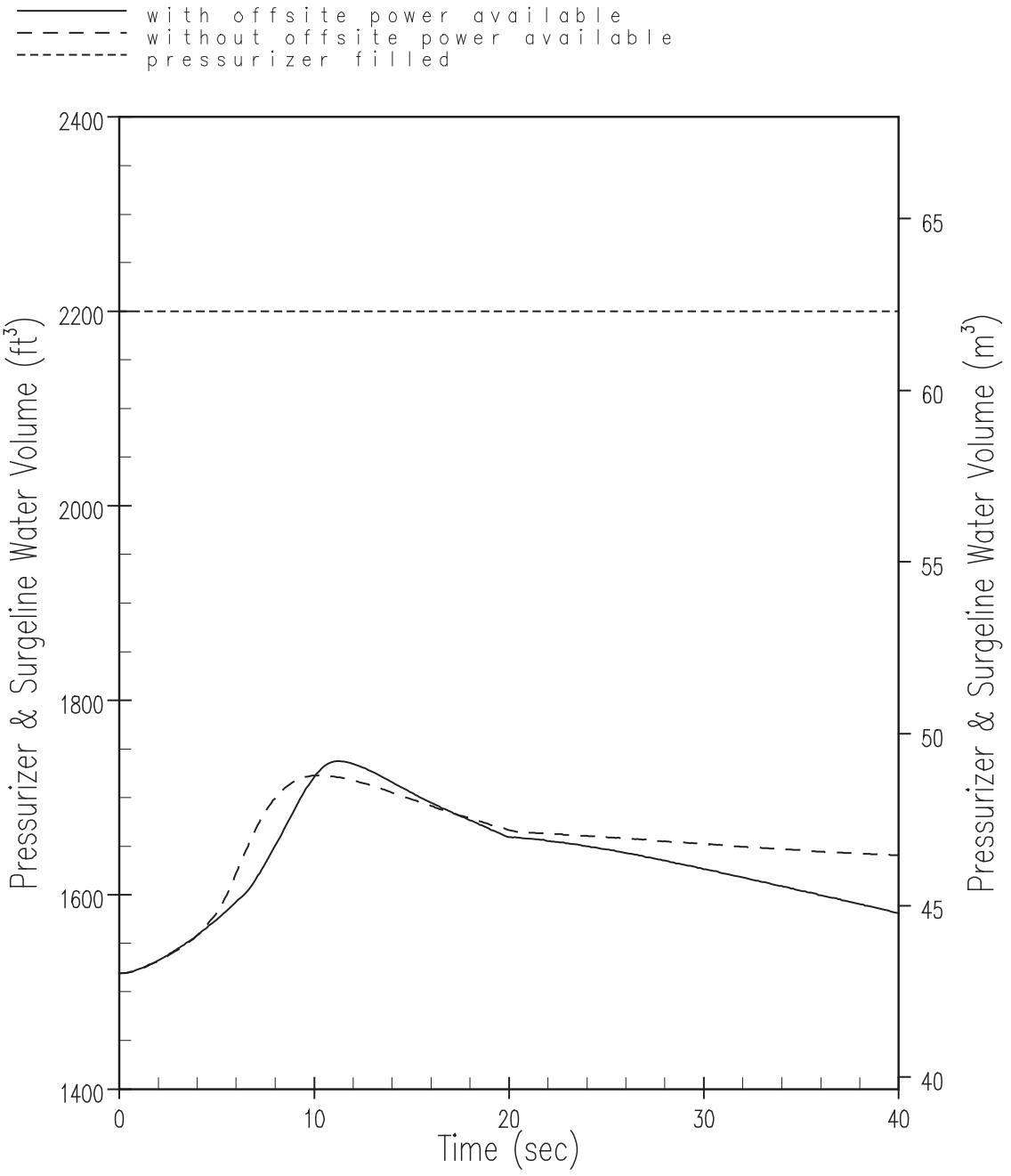


Figure 9.2.3-17. DBA Pressuriser & Surgeline Water Volume versus Time for Turbine Trip Accident Without Pressuriser Spray and Minimum Moderator Feedback

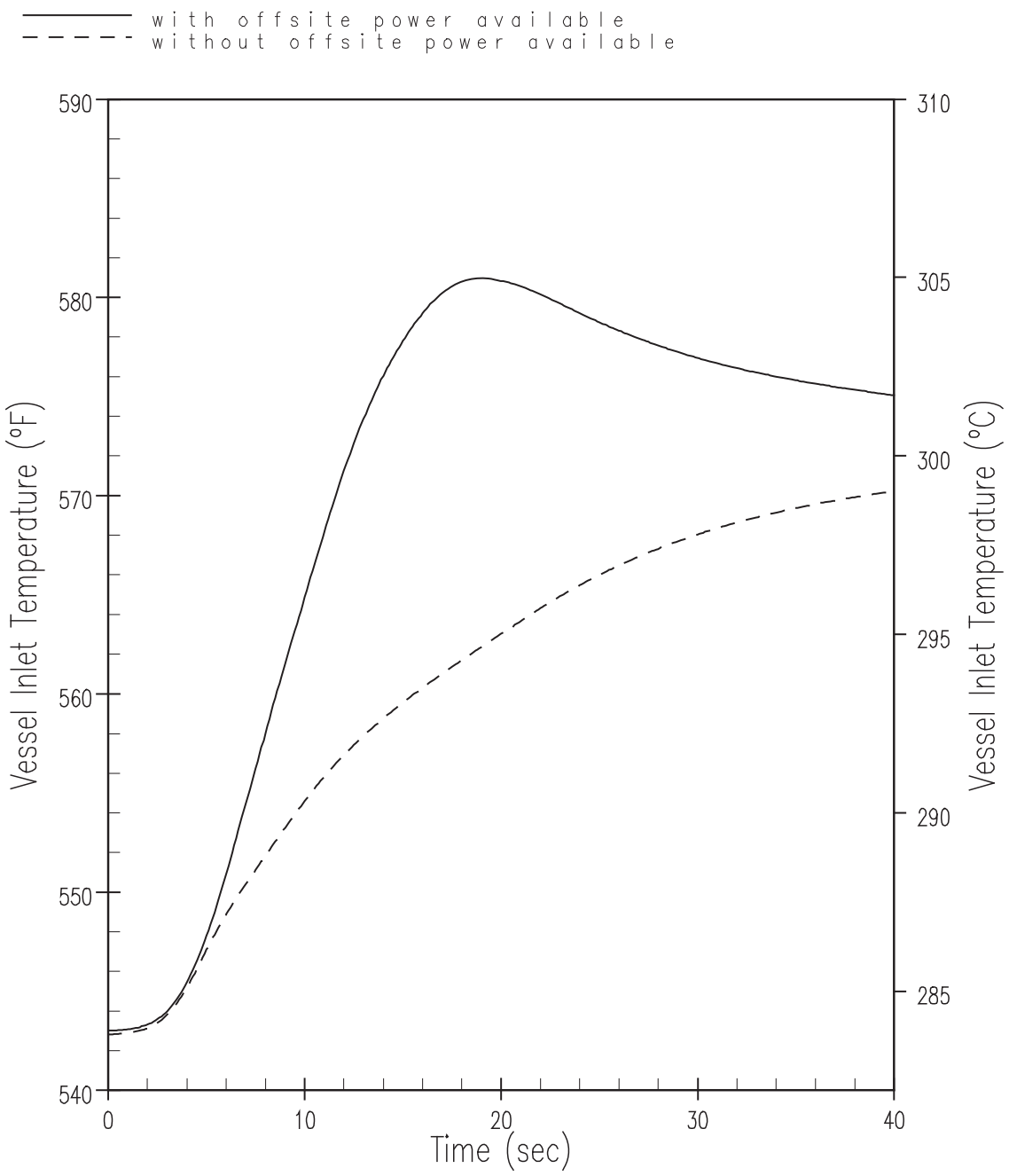


Figure 9.2.3-18. DBA Vessel Inlet Temperature versus Time for Turbine Trip Accident Without Pressuriser Spray and Minimum Moderator Feedback

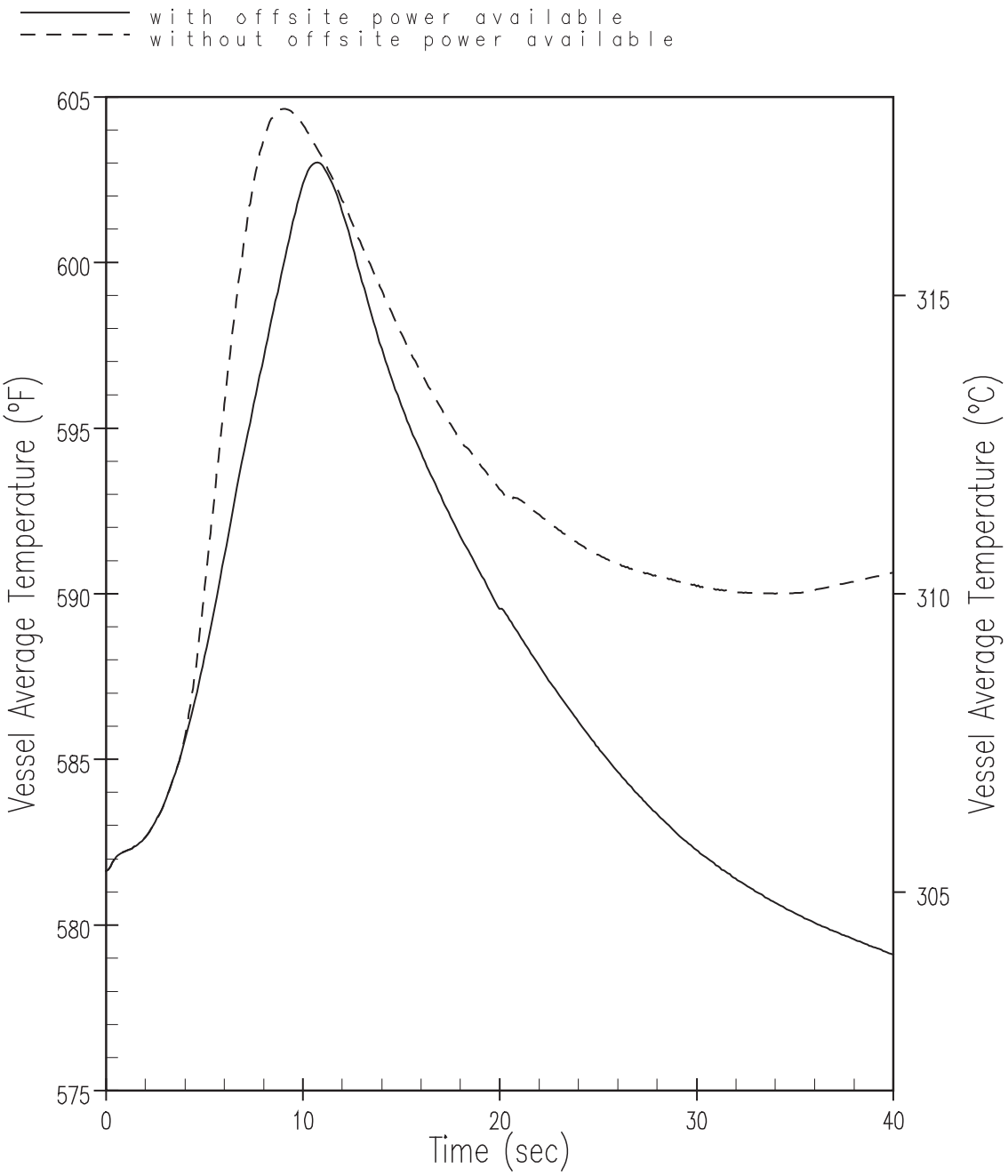


Figure 9.2.3-19. DBA Vessel Average Temperature versus Time for Turbine Trip Accident Without Pressuriser Spray and Minimum Moderator Feedback

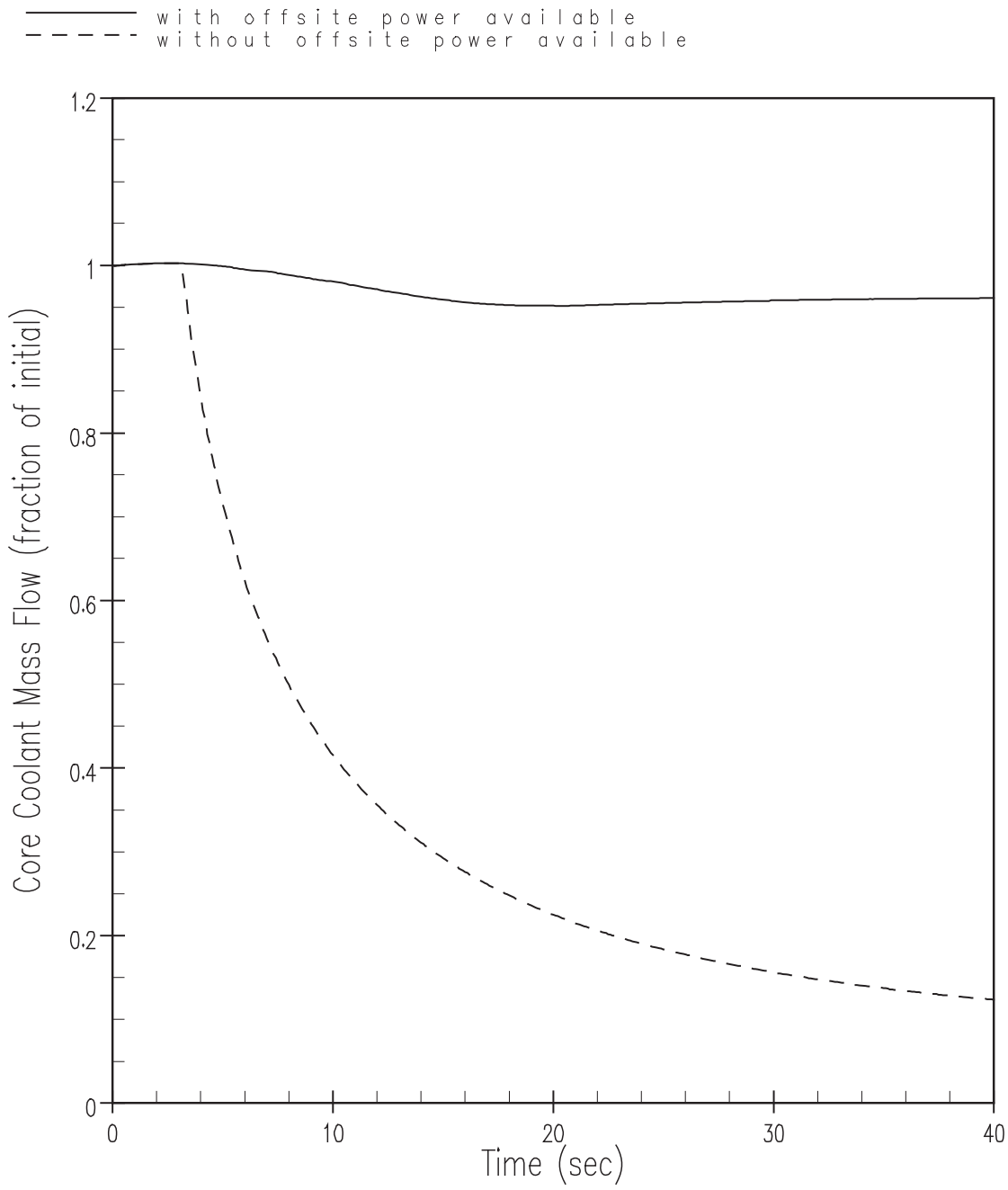


Figure 9.2.3-20. DBA Core Coolant Mass Flow Rate versus Time for Turbine Trip Accident Without Pressuriser Spray and Minimum Moderator Feedback

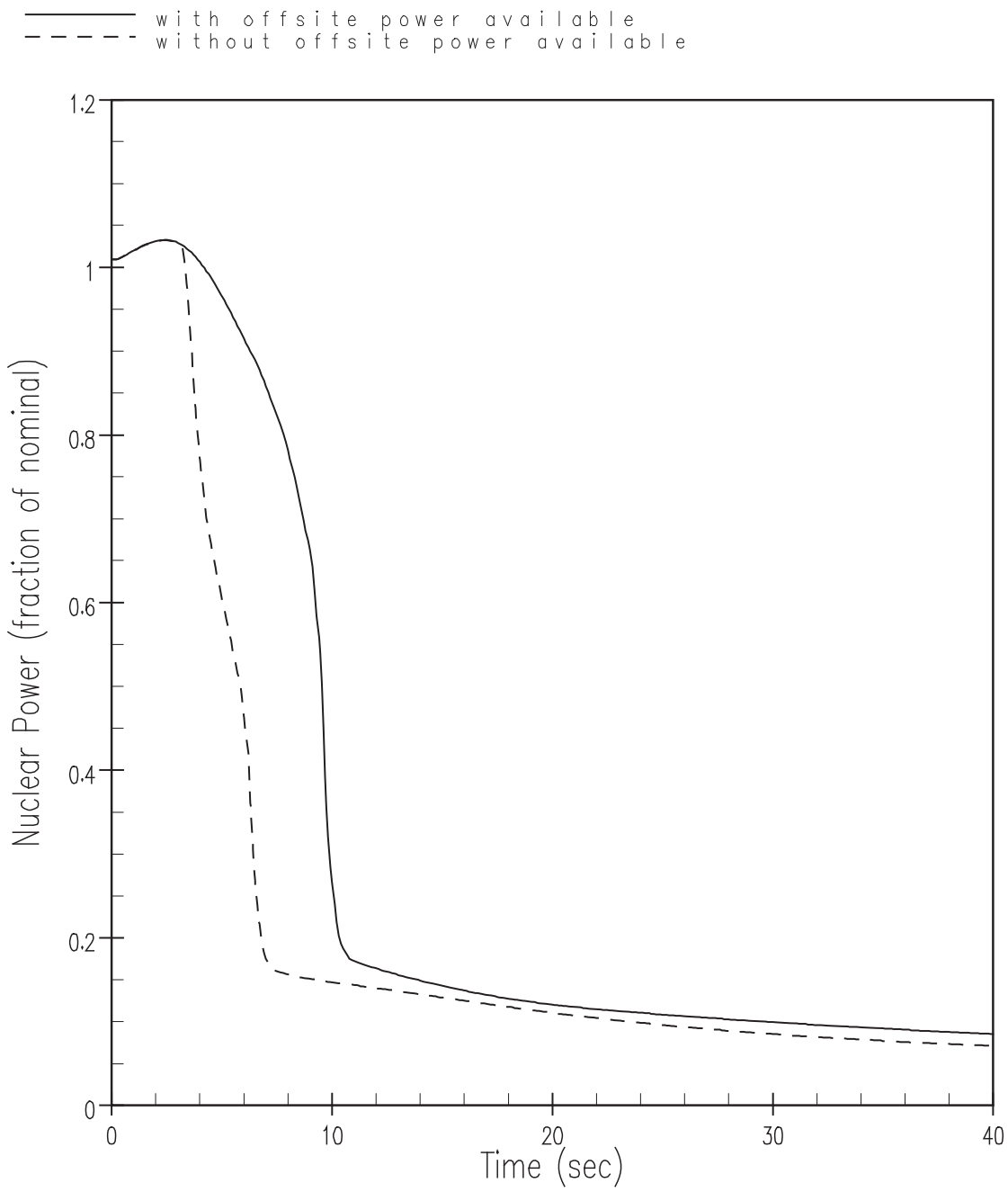


Figure 9.2.3-21. DBA Nuclear Power versus Time for Turbine Trip Accident Without Pressuriser Spray and Maximum Moderator Feedback

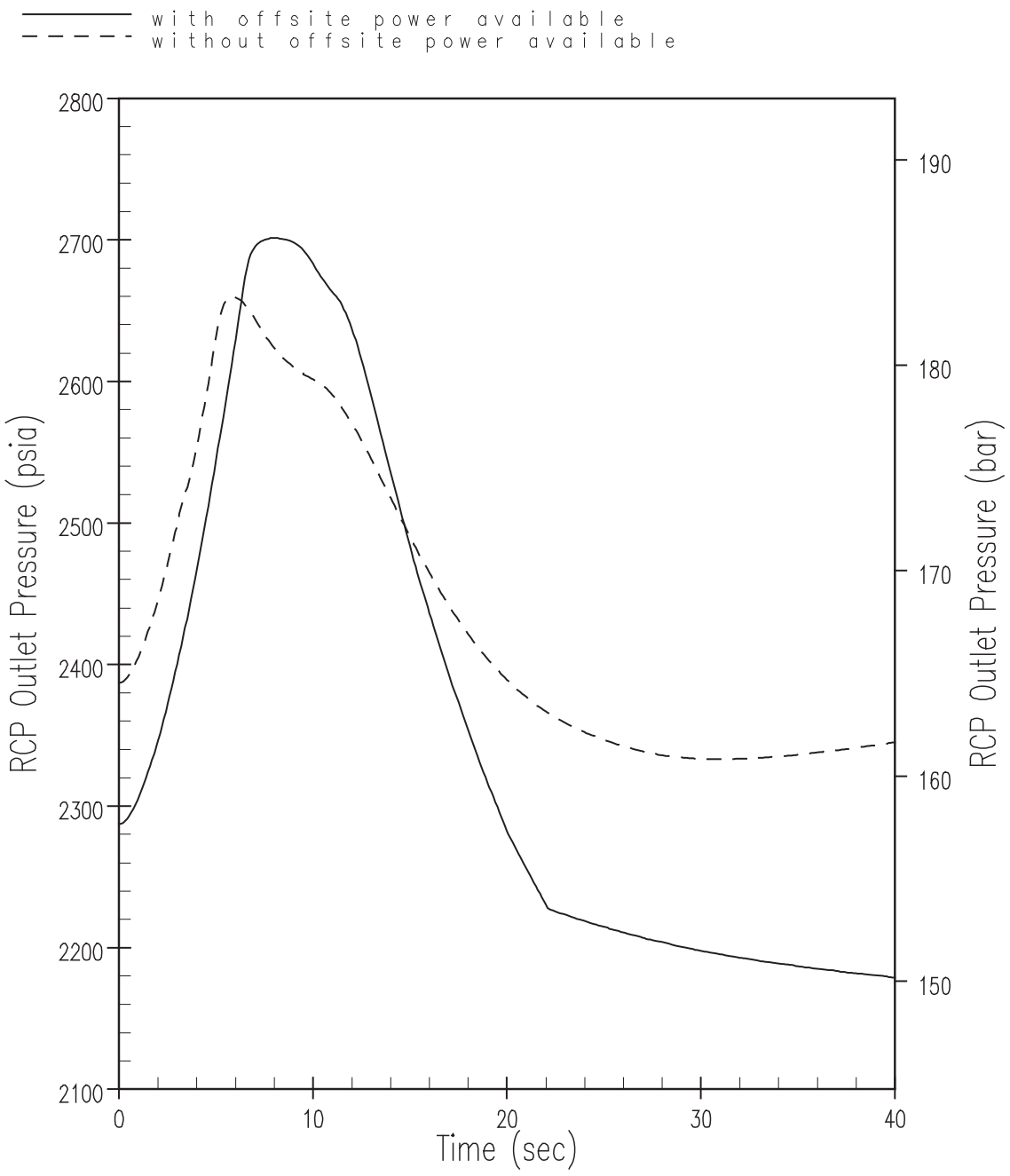


Figure 9.2.3-22. DBA RCP Outlet Pressure versus Time for Turbine Trip Accident Without Pressuriser Spray and Maximum Moderator Feedback

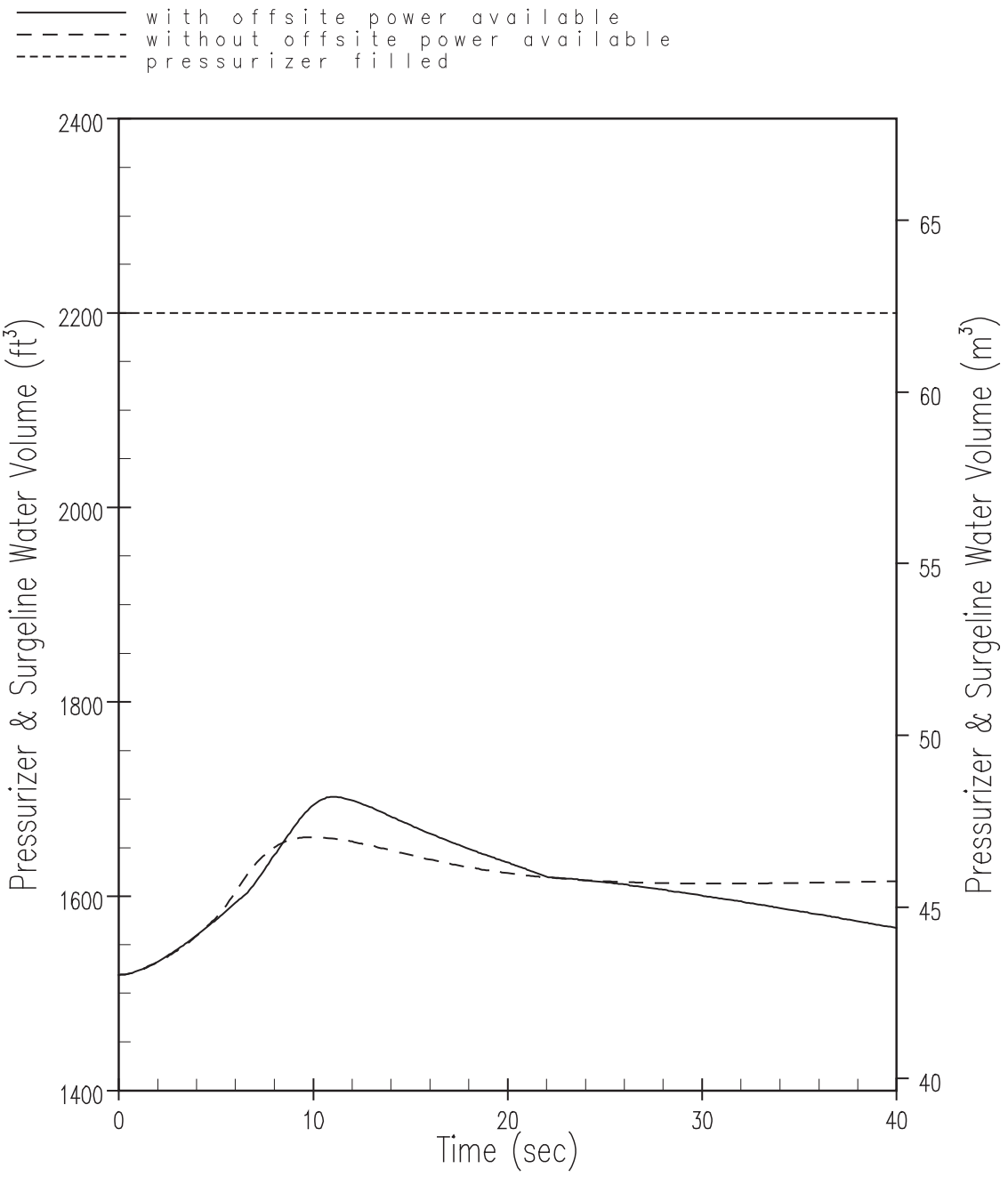


Figure 9.2.3-23. DBA Pressuriser & Surgeline Water Volume versus Time for Turbine Trip Accident Without Pressuriser Spray and Maximum Moderator Feedback

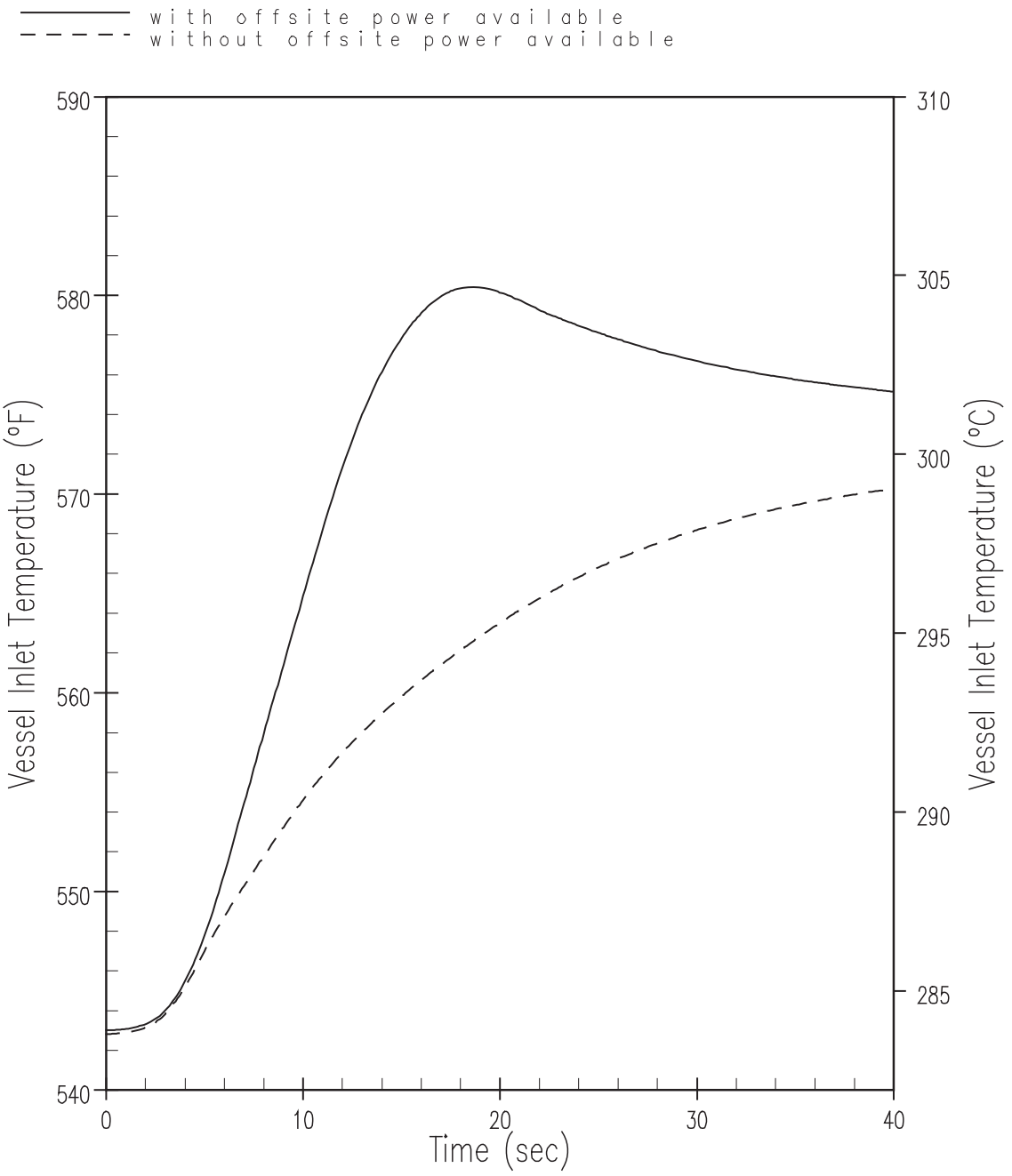


Figure 9.2.3-24. DBA Vessel Inlet Temperature versus Time for Turbine Trip Accident Without Pressuriser Spray and Maximum Moderator Feedback

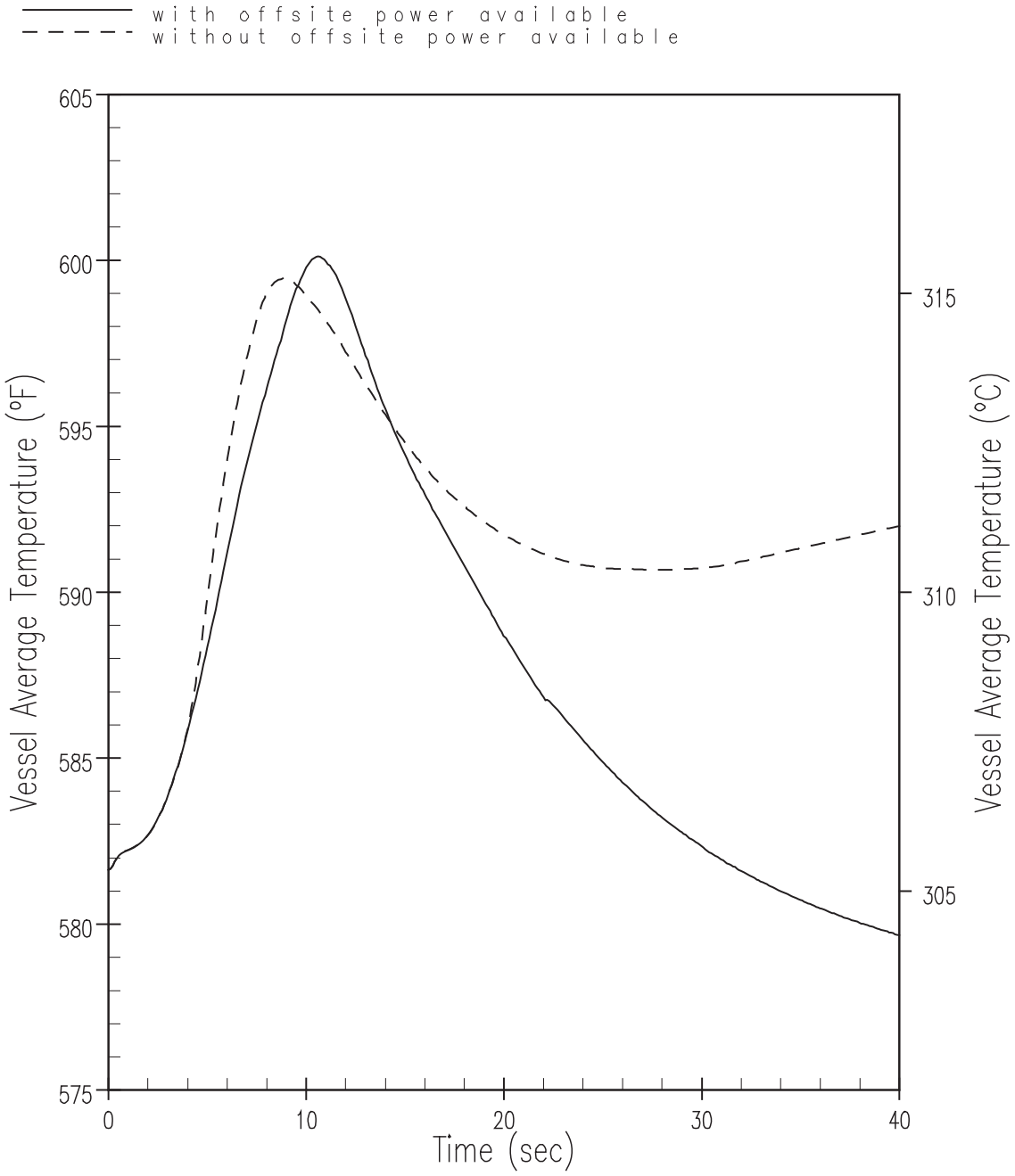


Figure 9.2.3-25. DBA Vessel Average Temperature versus Time for Turbine Trip Accident Without Pressuriser Spray and Maximum Moderator Feedback

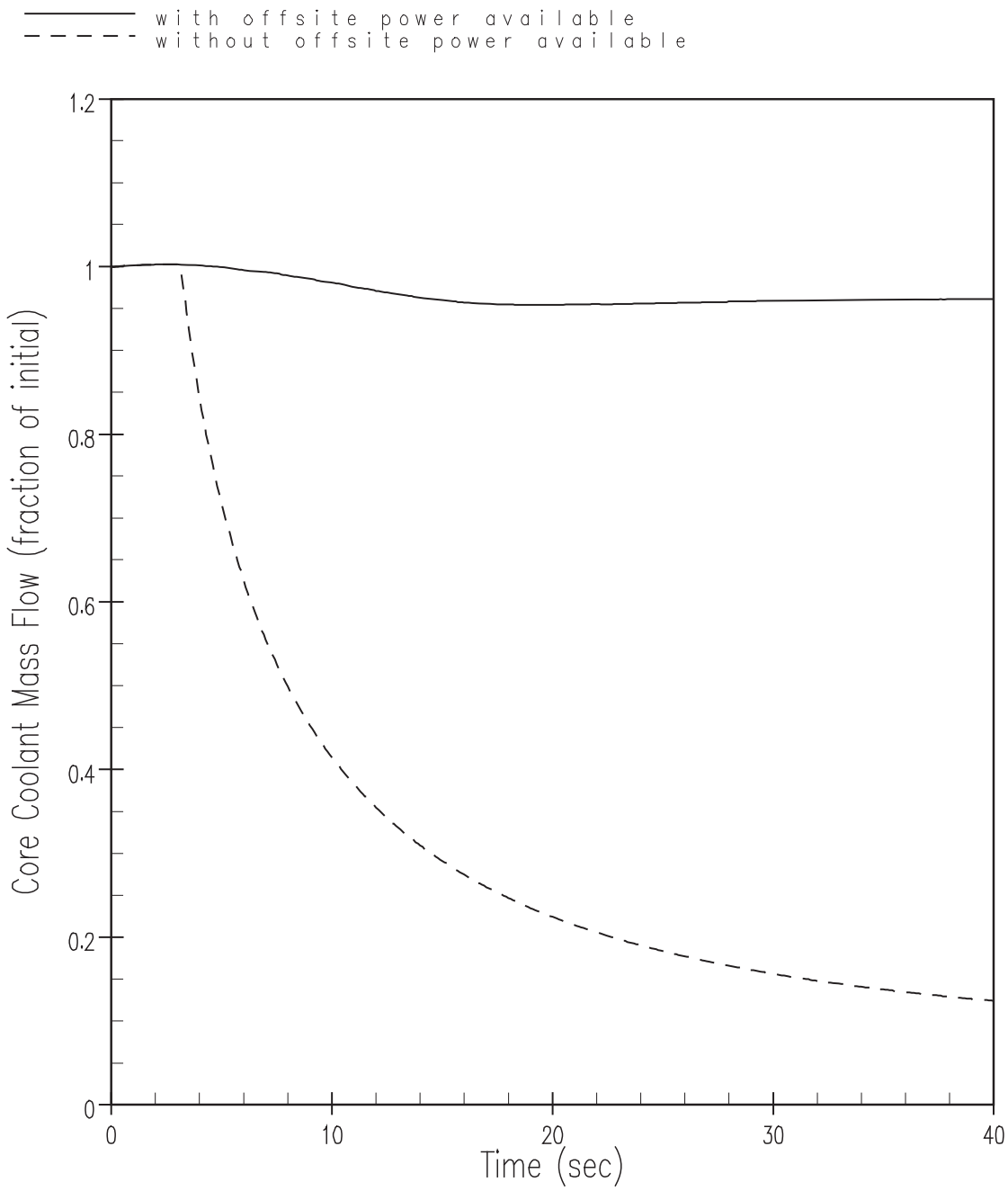


Figure 9.2.3-26. DBA Core Coolant Mass Flow Rate versus Time for Turbine Trip Accident Without Pressuriser Spray and Maximum Moderator Feedback

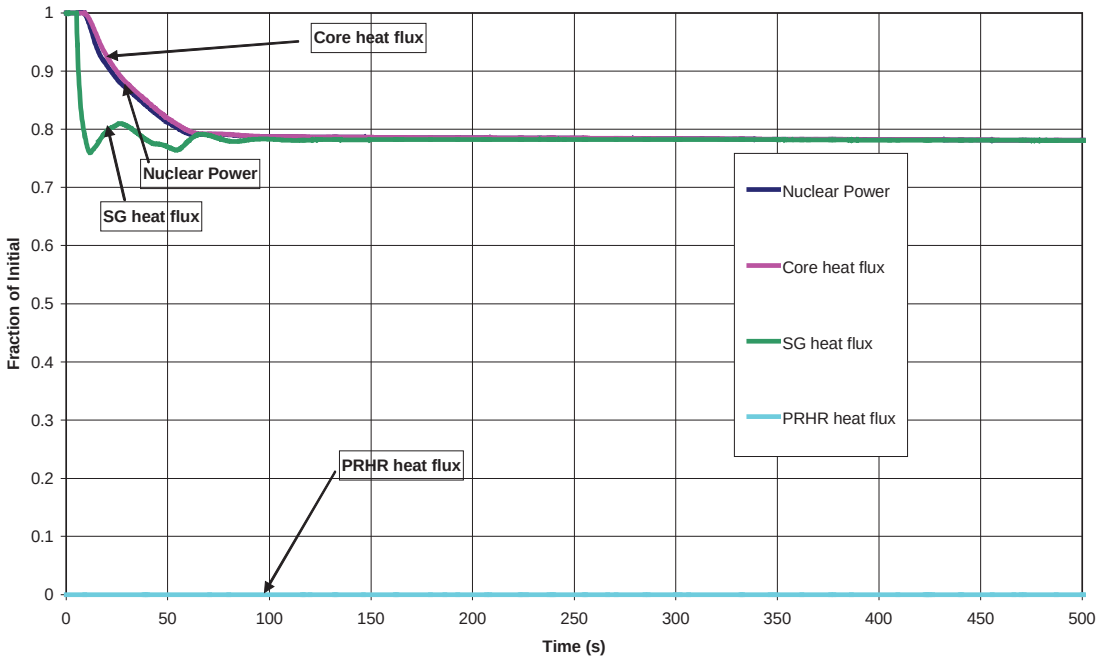


Figure 9.2.3-27. ATWT Power and Heat Transfer for Turbine Trip with PMS CCF

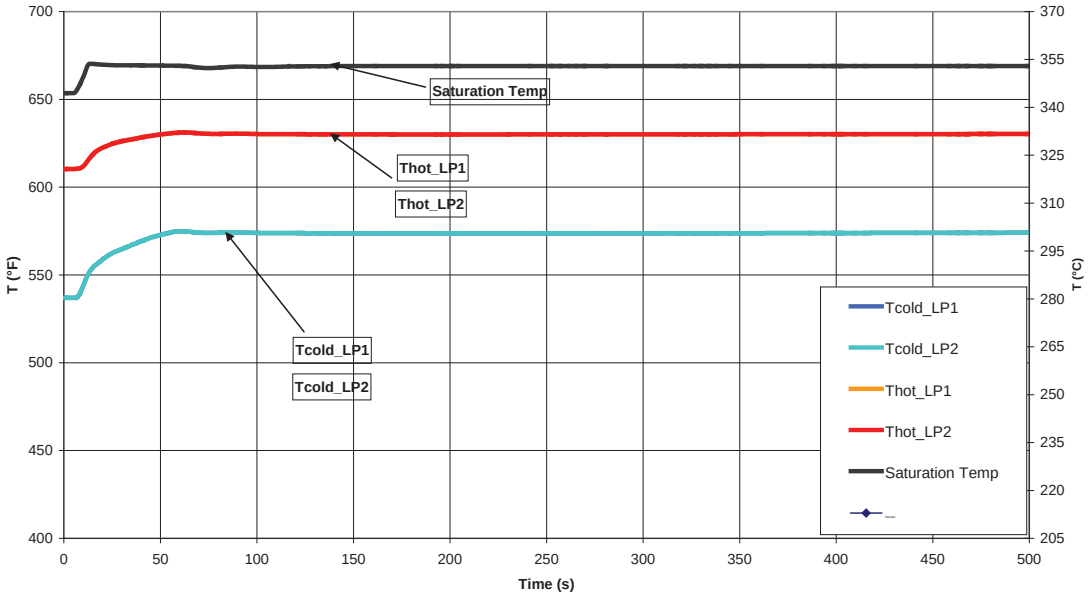


Figure 9.2.3-28. ATWT Primary Loop Temperatures for Turbine Trip with PMS CCF

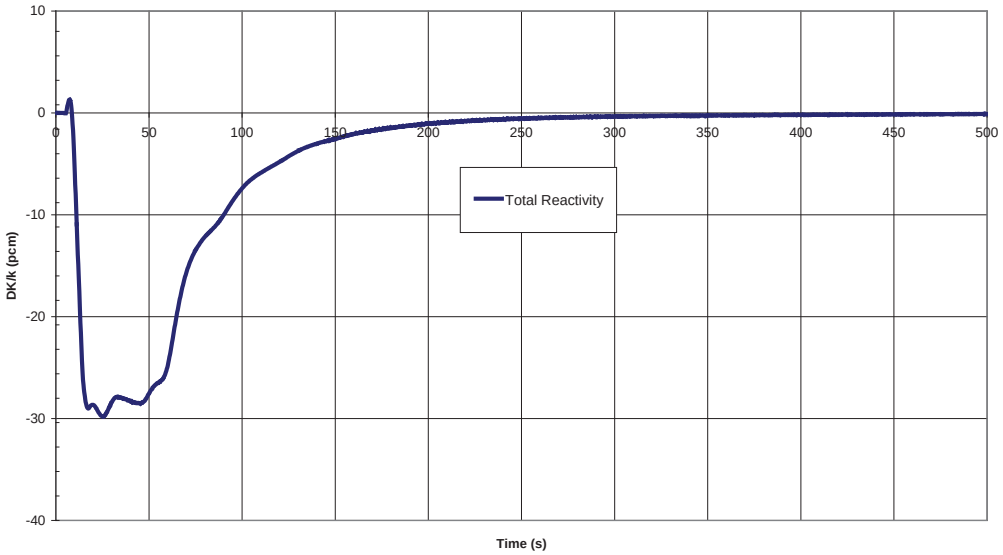


Figure 9.2.3-29. ATWT Core Reactivity for Turbine Trip with PMS CCF

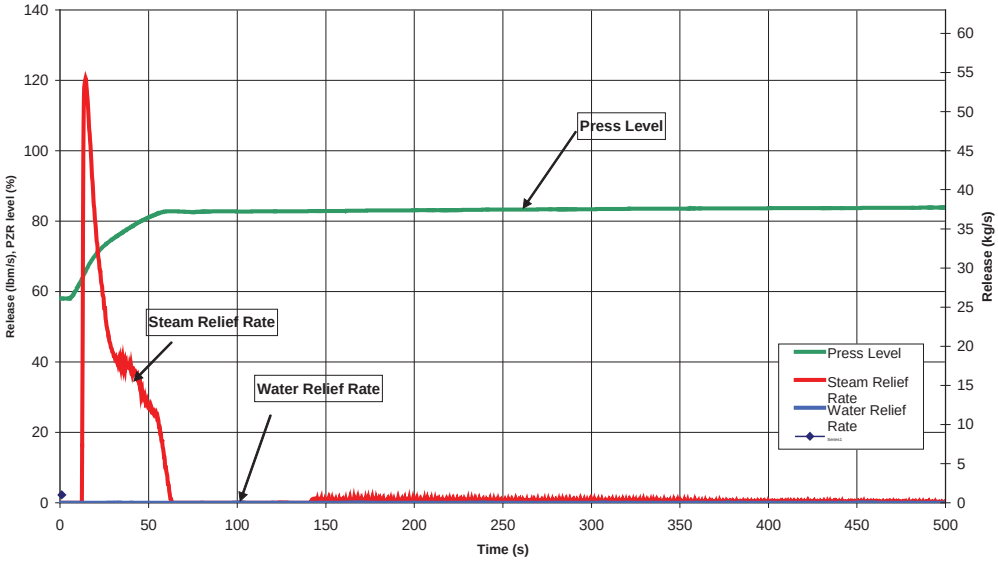


Figure 9.2.3-30. ATWT Pressuriser Level and Safety Valve Relief Rates for Turbine Trip with PMS CCF

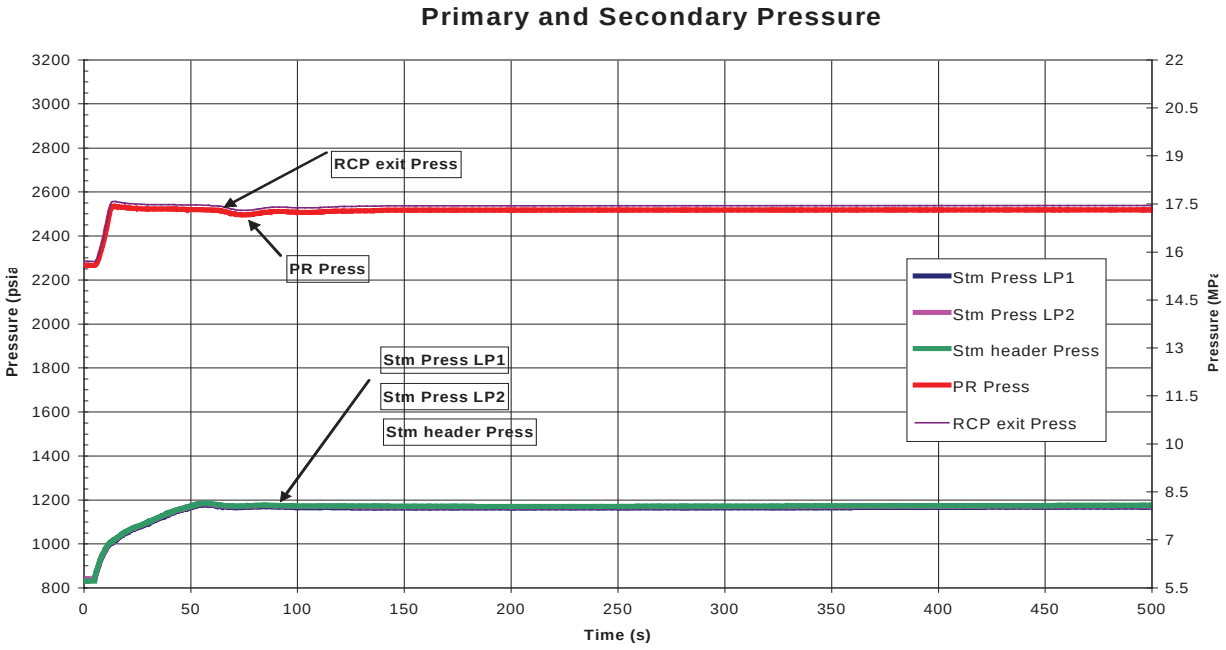


Figure 9.2.3-31. ATWT Primary and Secondary System Pressures for Turbine Trip with PMS CCF

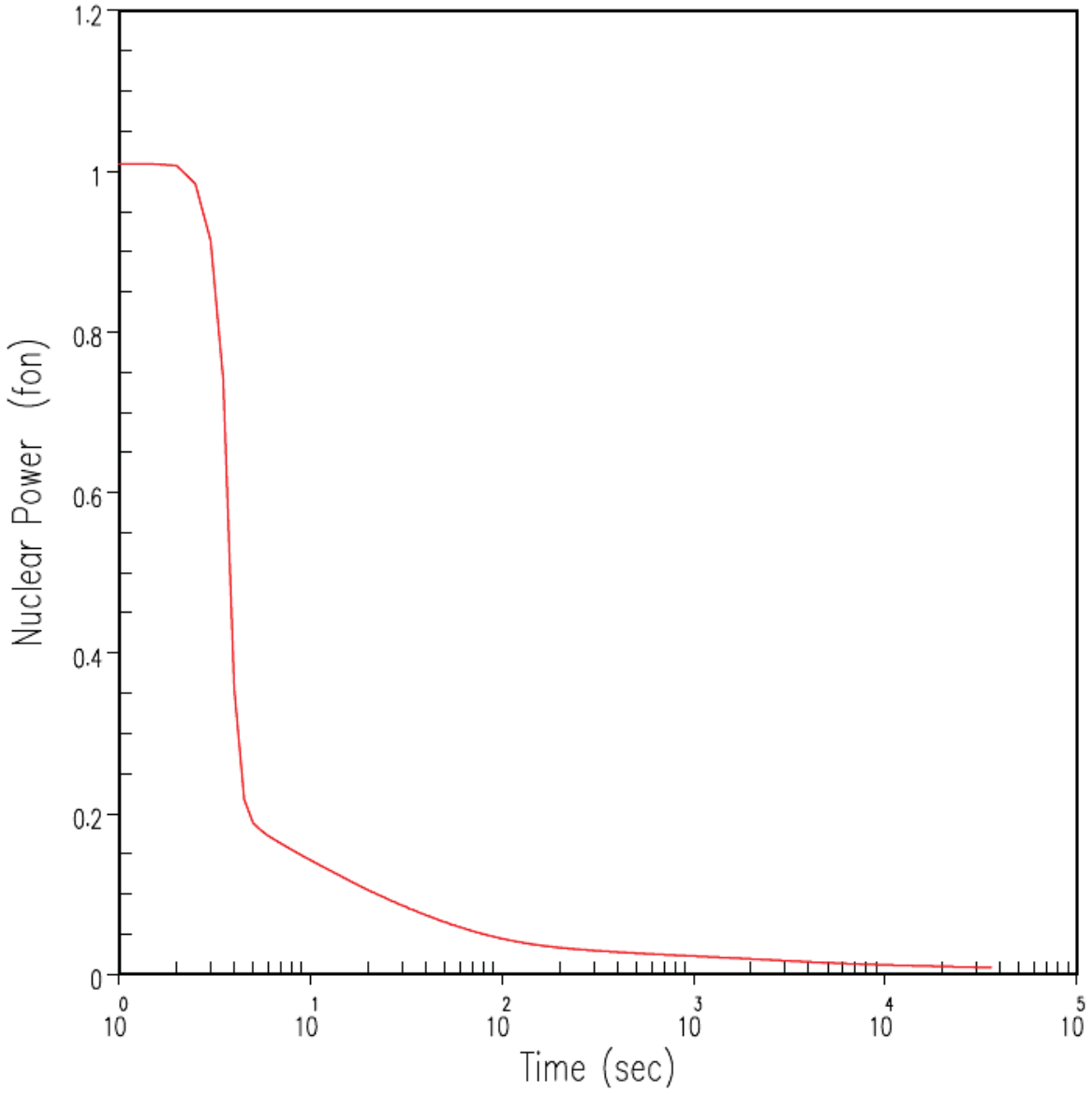


Figure 9.2.6-1. DBA Nuclear Power Transient for Loss of ac Power to the Plant Auxiliaries

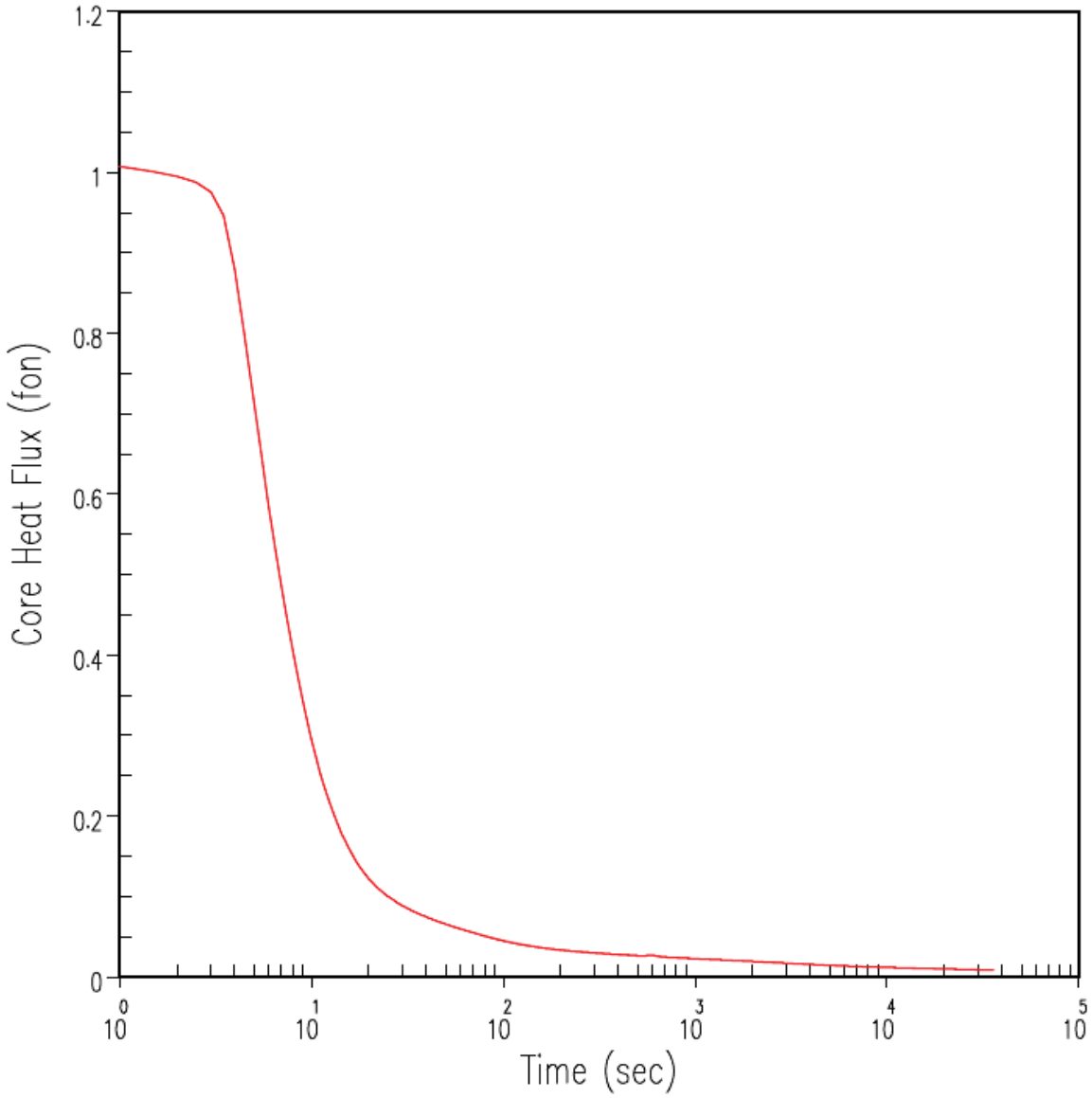


Figure 9.2.6-2. DBA Core Heat Flux Transient for Loss of ac Power to the Plant Auxiliaries

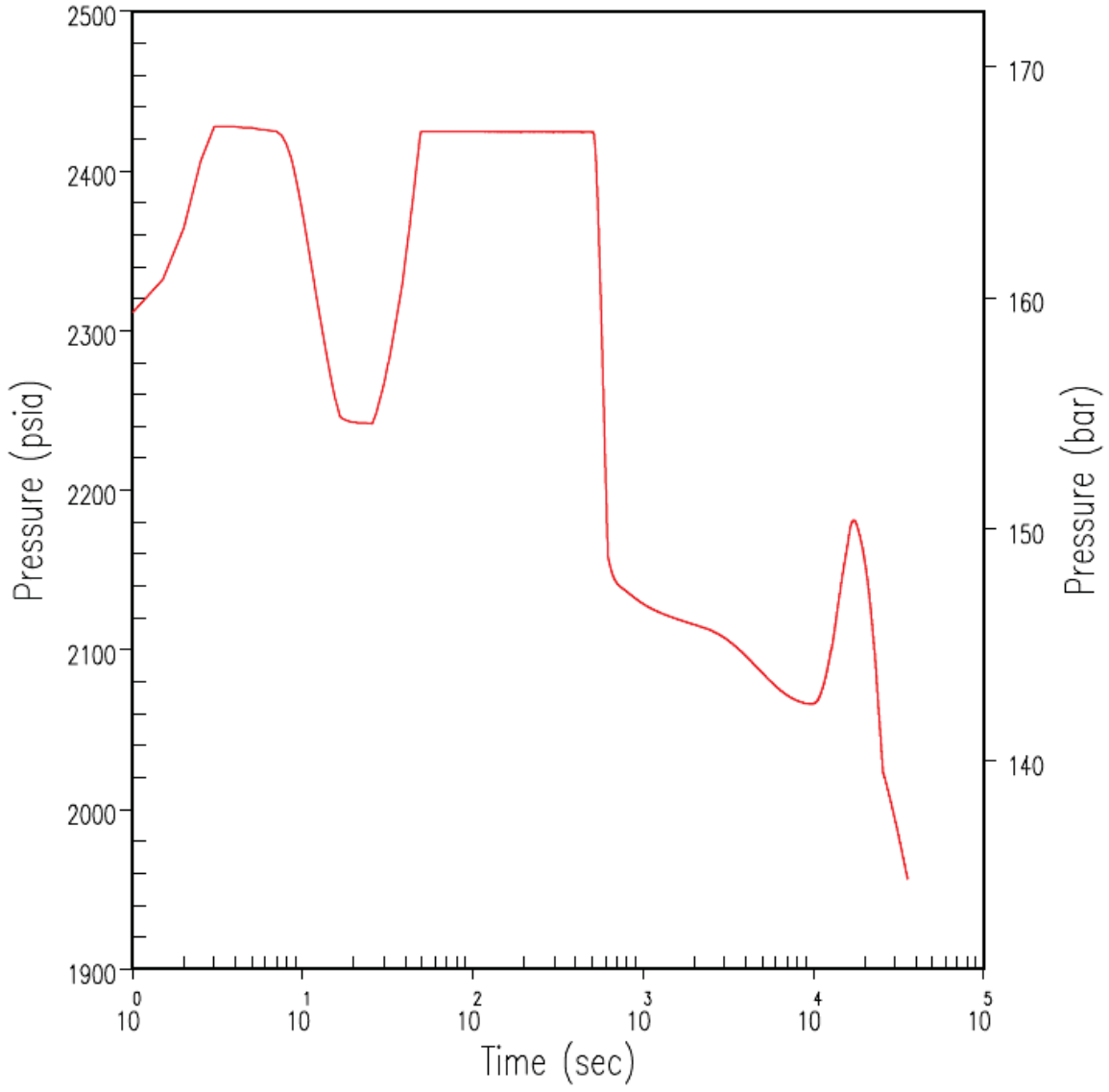


Figure 9.2.6-3. DBA Pressuriser Pressure Transient for Loss of ac Power to the Plant Auxiliaries

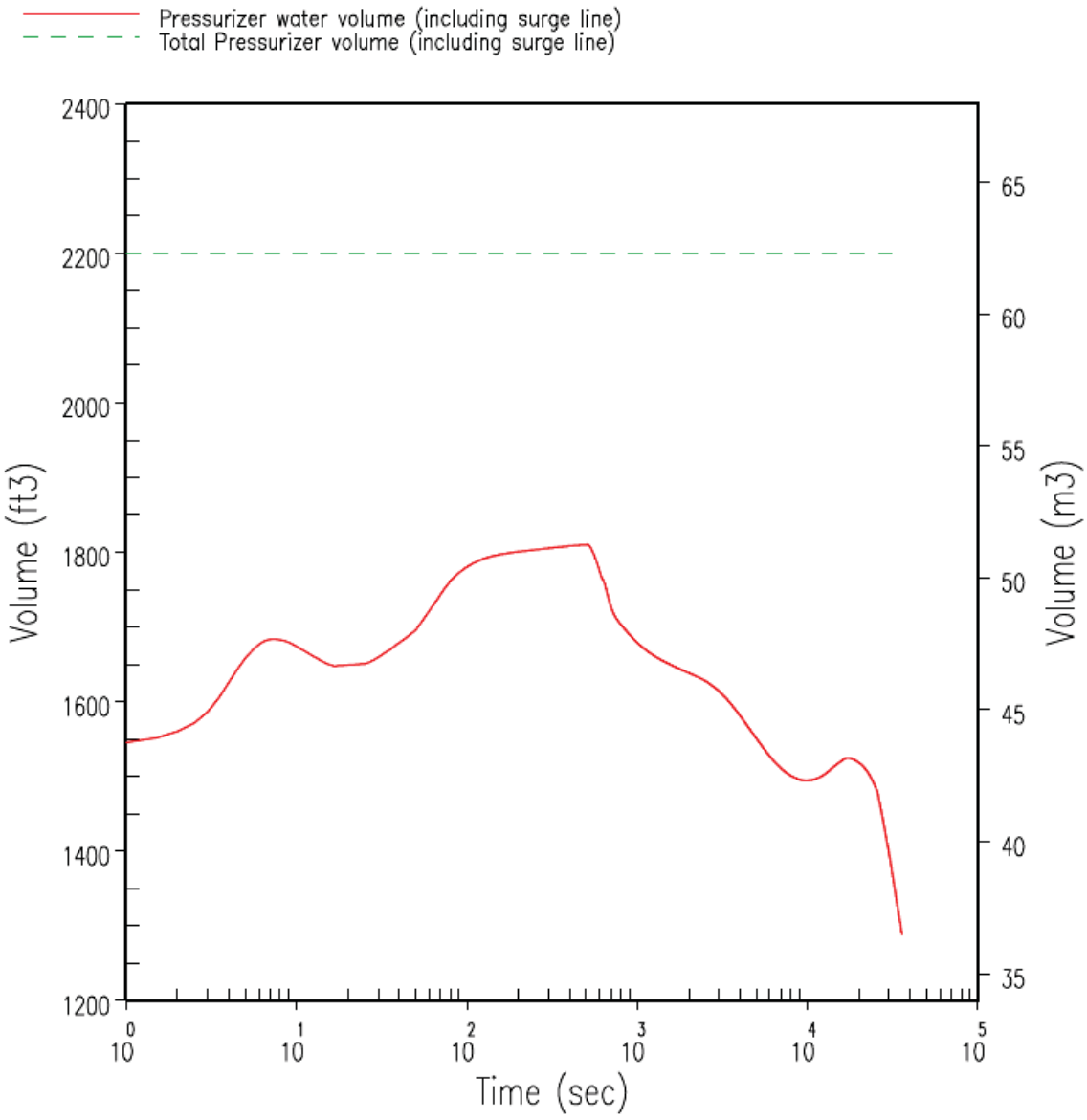


Figure 9.2.6-4. DBA Pressuriser Water Volume Transient for Loss of ac Power to the Plant Auxiliaries

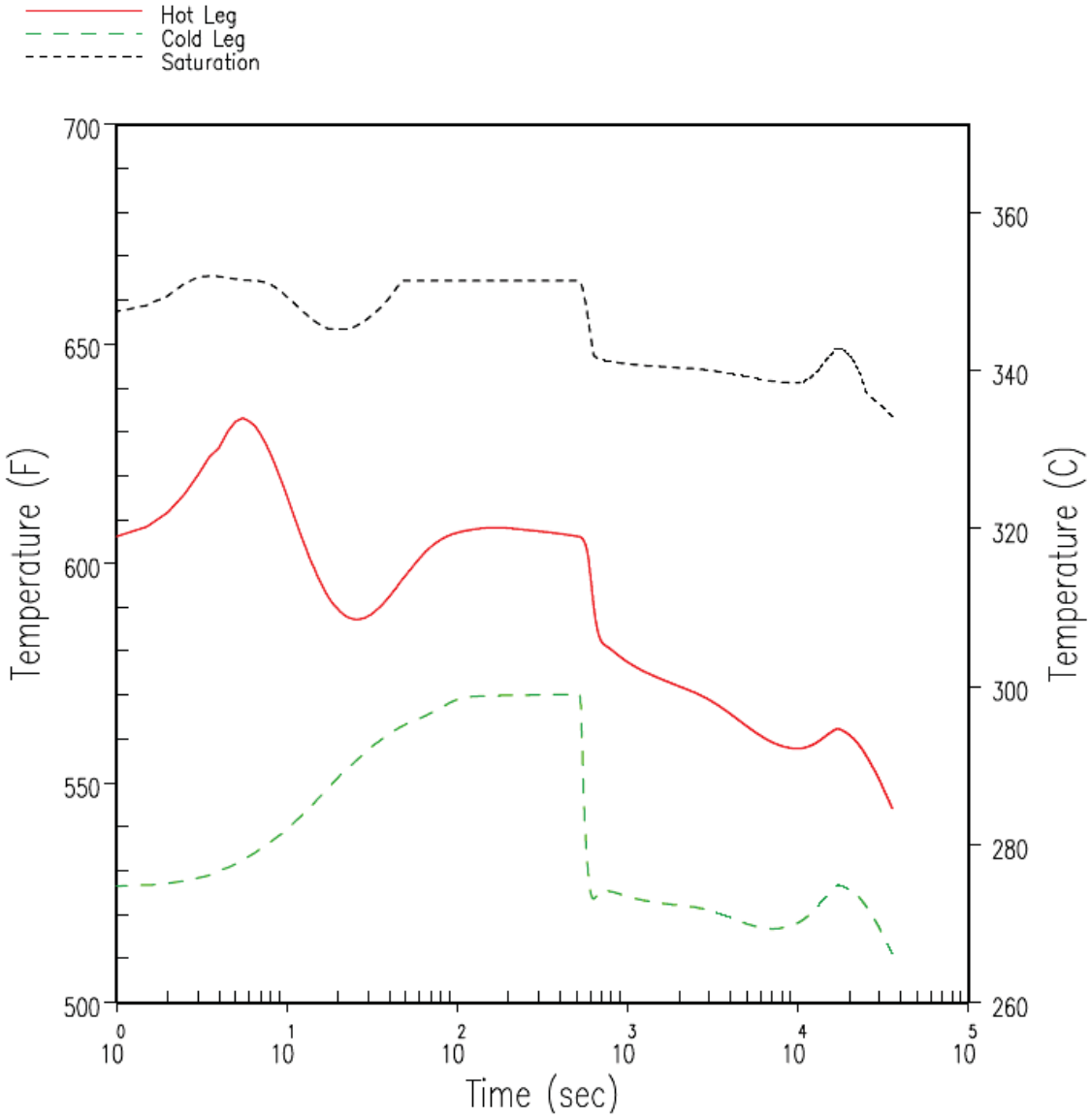


Figure 9.2.6-5. DBA Reactor Coolant System Temperature Transients in Loop Containing the PRHR for Loss of ac Power to the Plant Auxiliaries

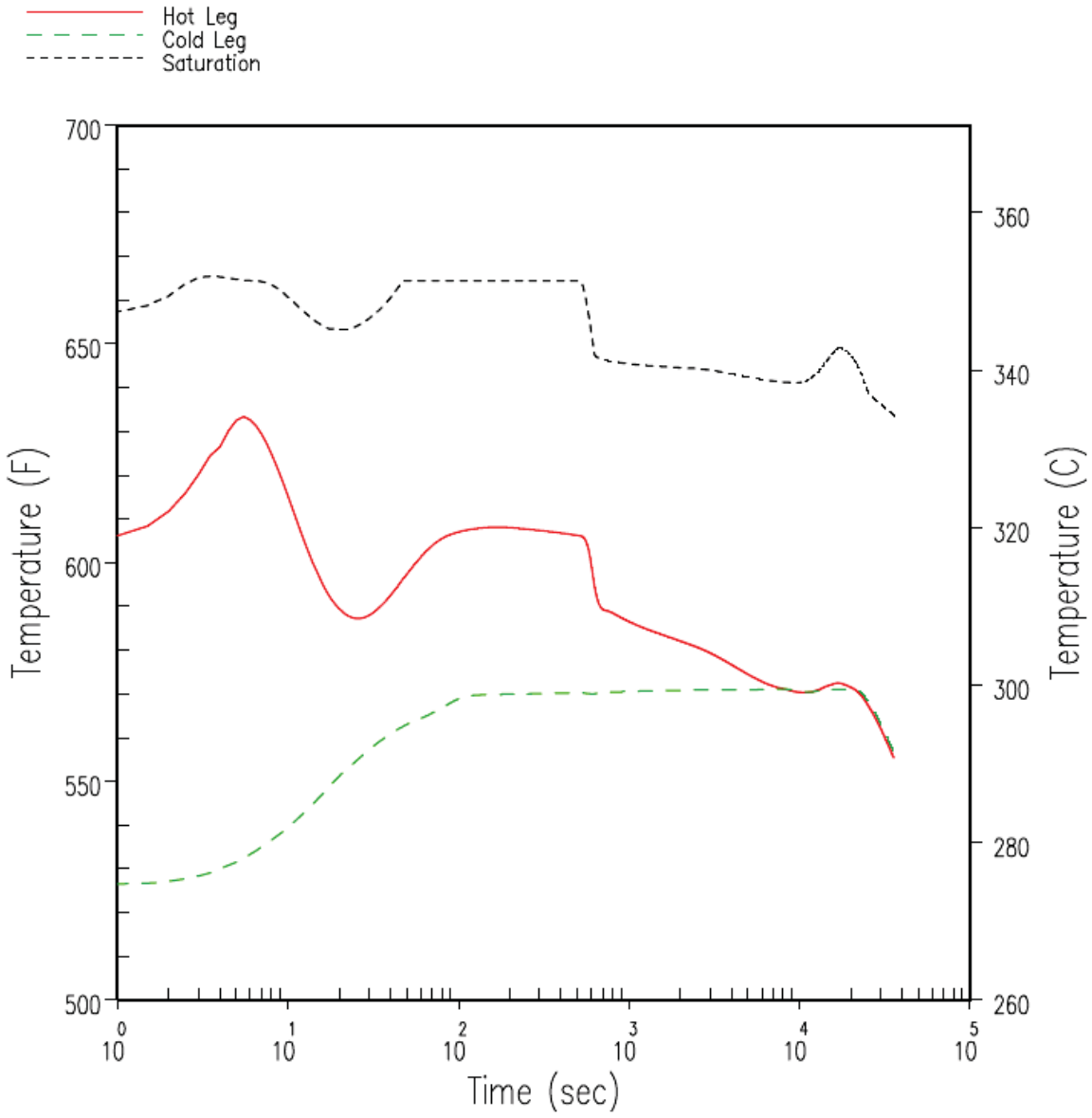


Figure 9.2.6-6. DBA Reactor Coolant System Temperature Transients in Loop Not Containing the PRHR for Loss of ac Power to the Plant Auxiliaries

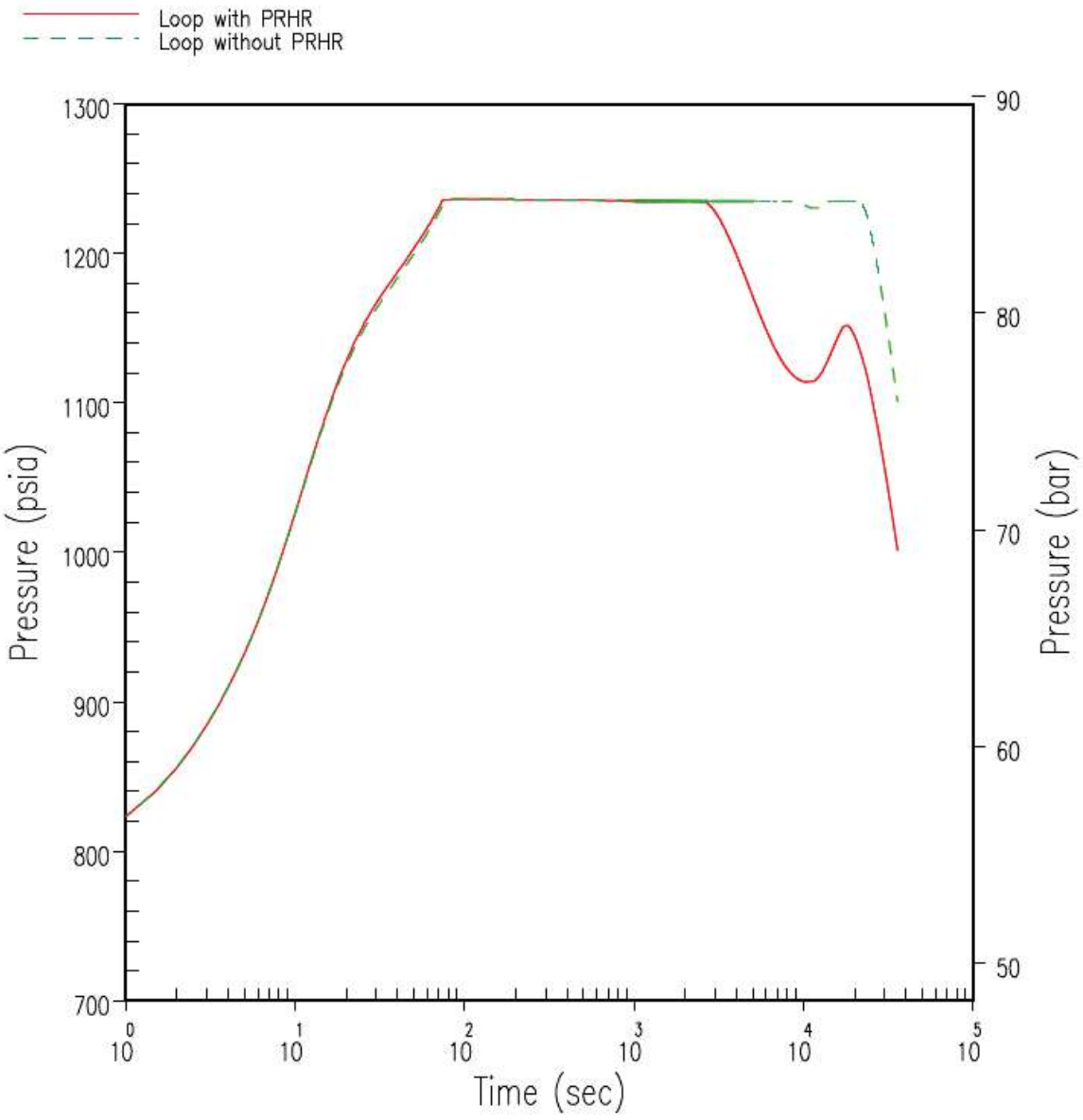


Figure 9.2.6-7. DBA Steam Generator Pressure Transient for Loss of ac Power to the Plant Auxiliaries

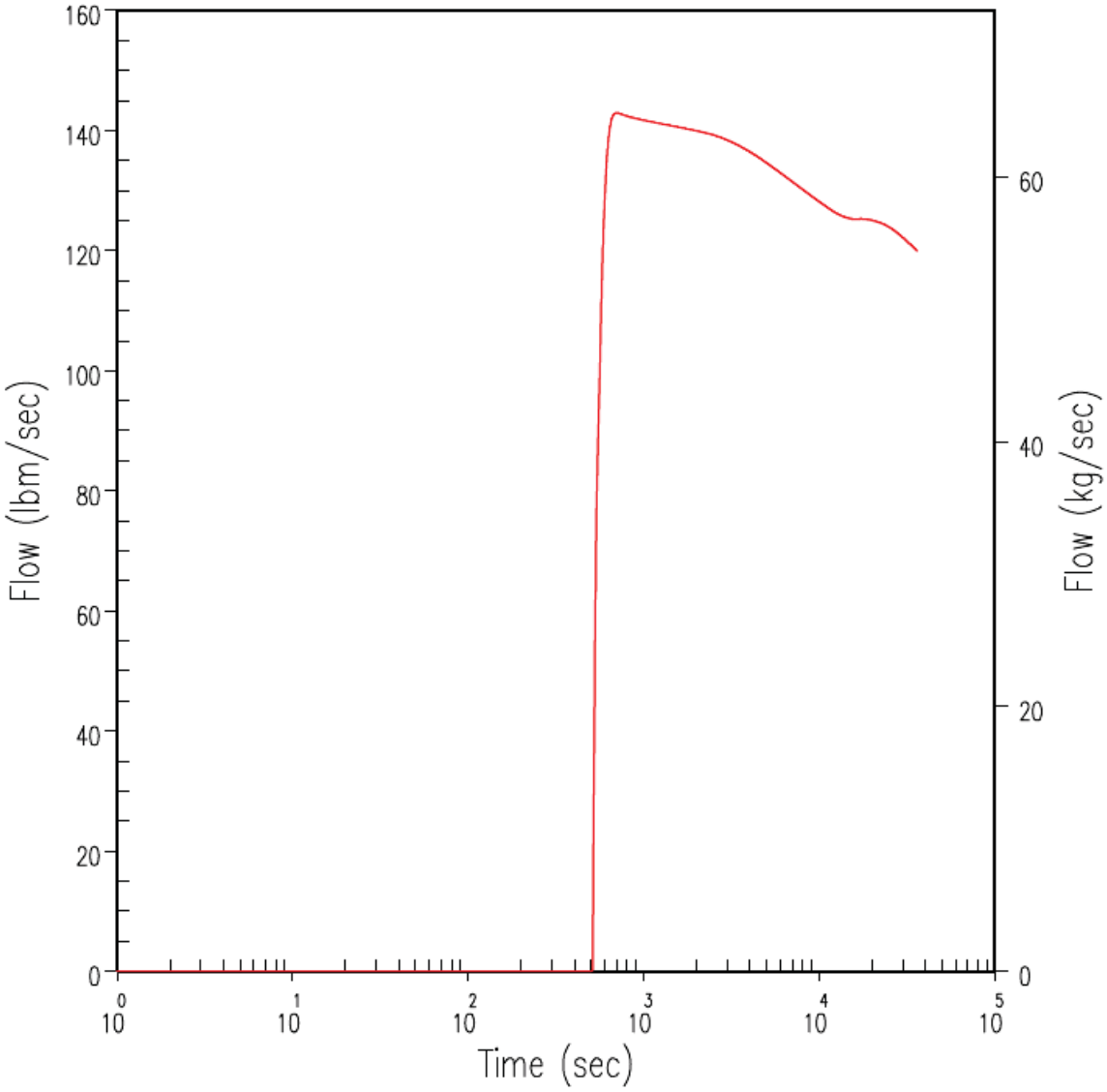


Figure 9.2.6-8. DBA PRHR Flow Rate Transient for Loss of ac Power to the Plant Auxiliaries

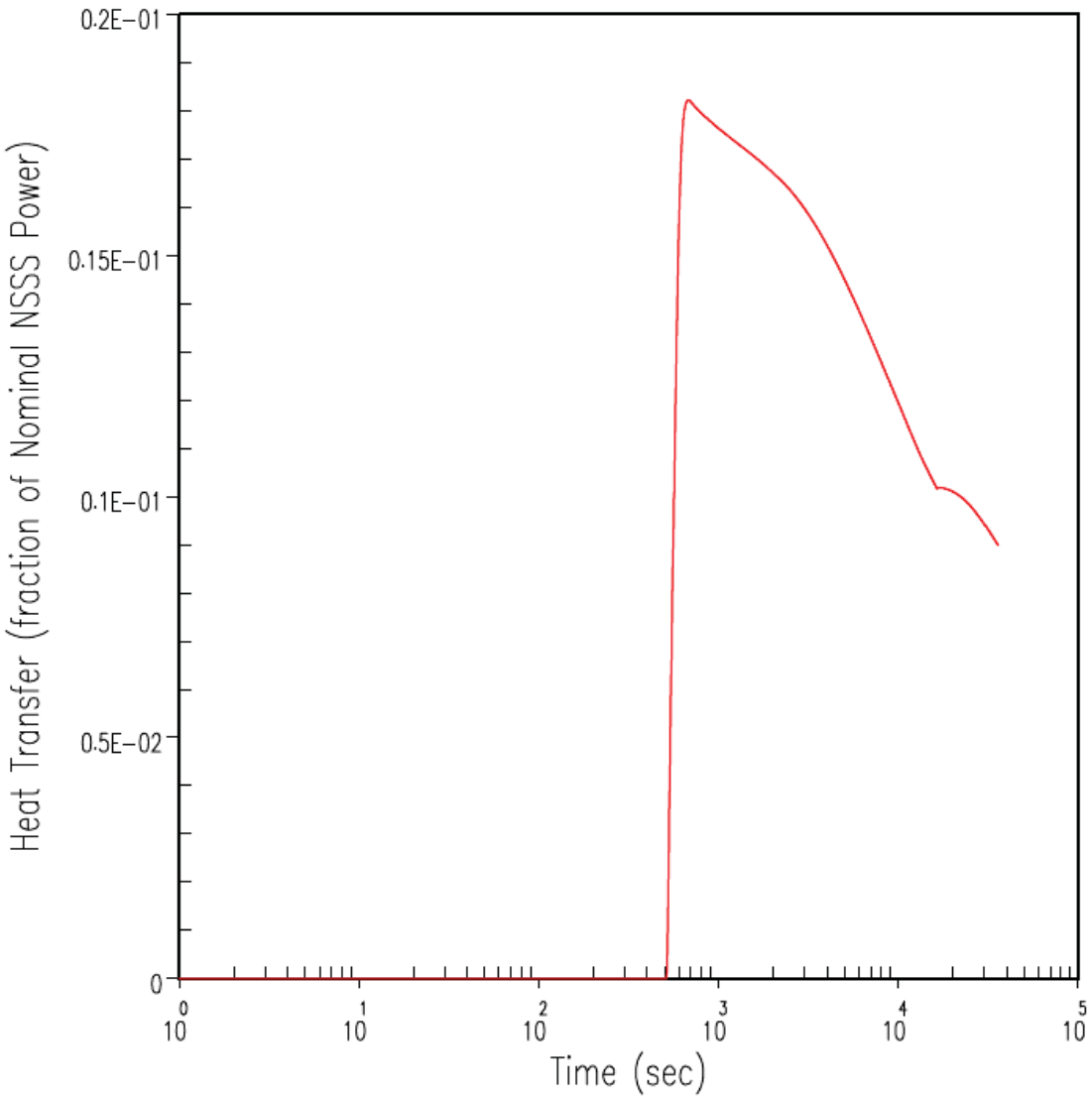


Figure 9.2.6-9. DBA PRHR Heat Transfer Transient for Loss of ac Power to the Plant Auxiliaries

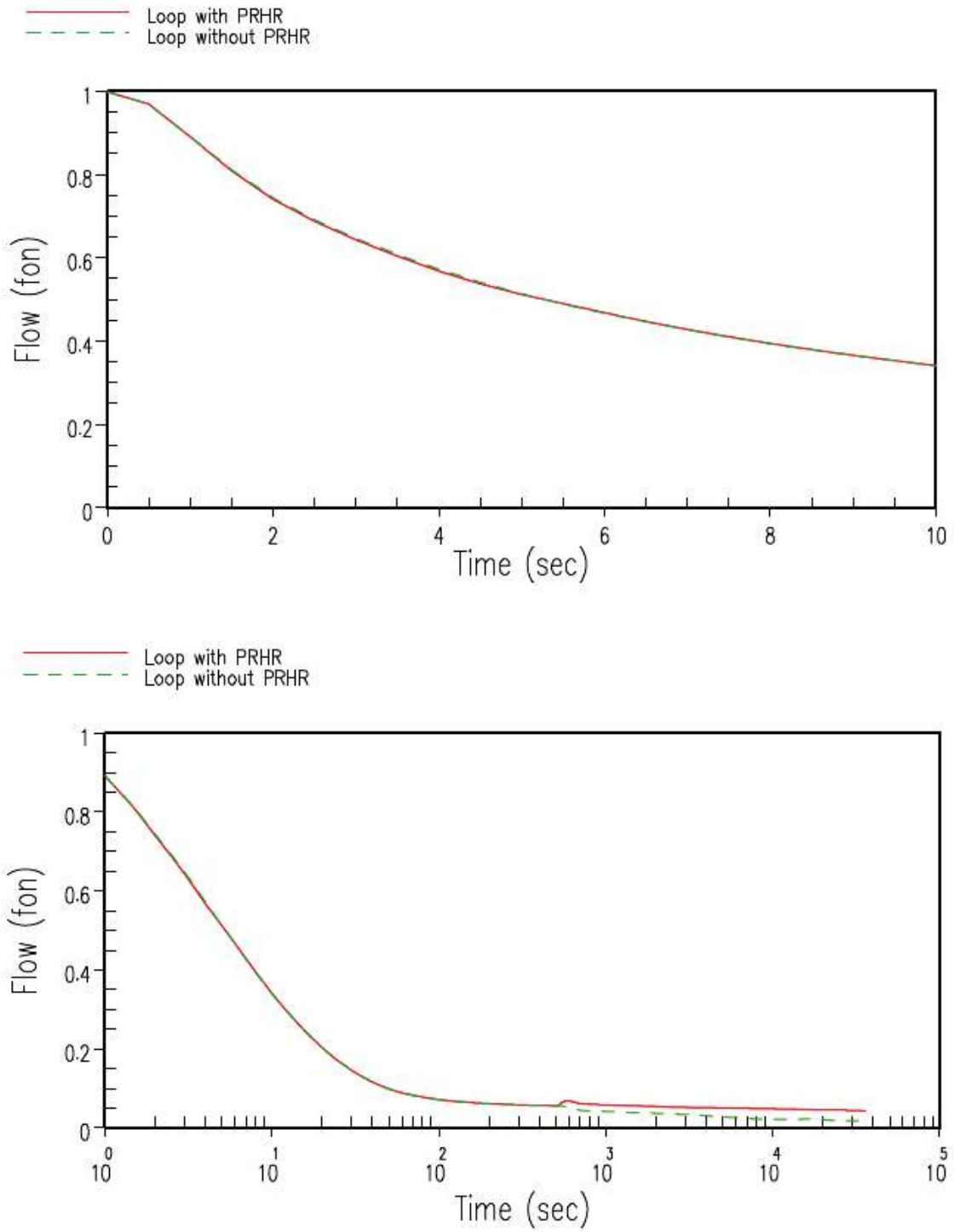


Figure 9.2.6-10. DBA Reactor Coolant Volumetric Flow Rate Transient for Loss of ac Power to the Plant Auxiliaries

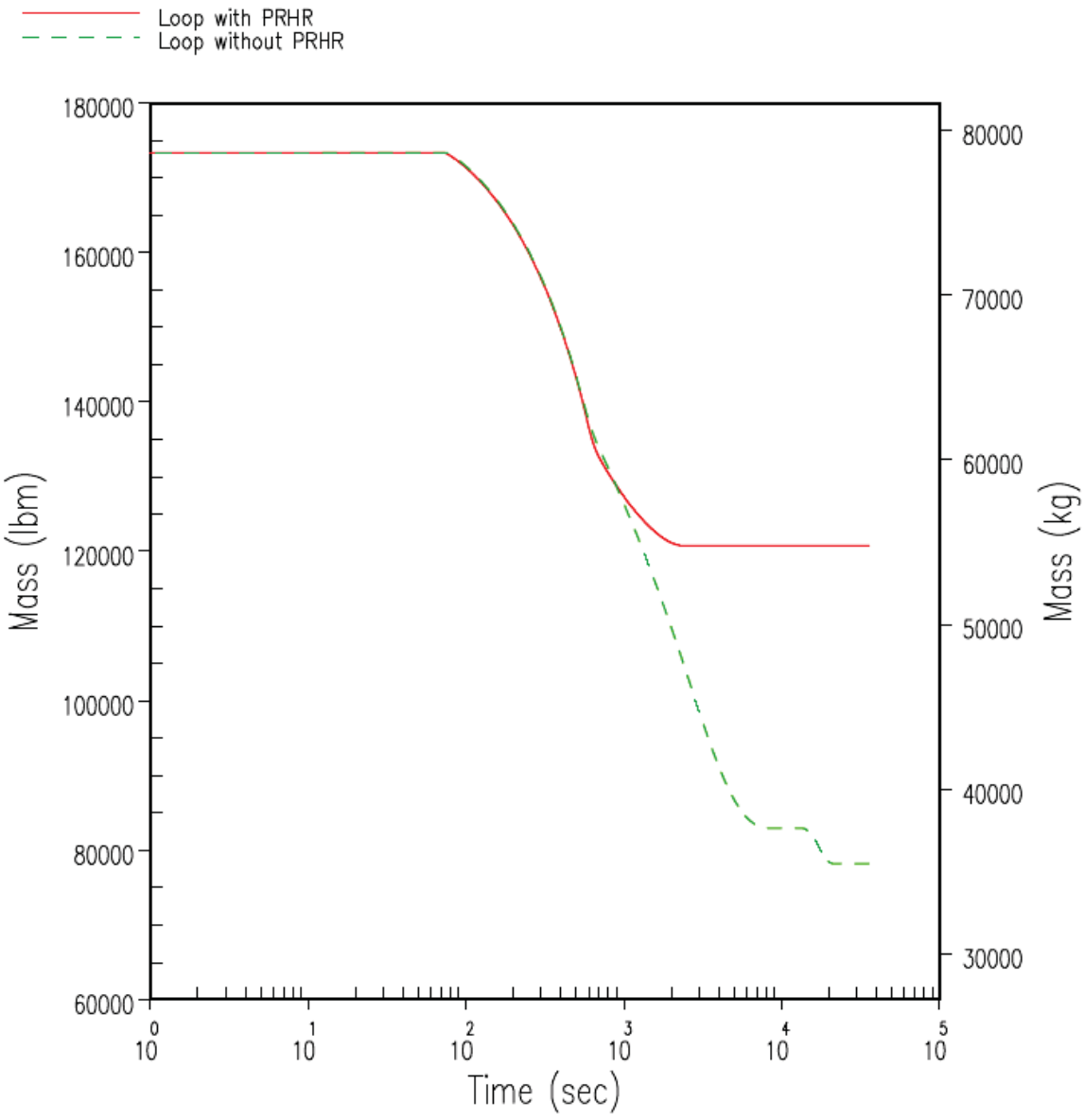


Figure 9.2.6-11. DBA Steam Generator Inventory Transient for Loss of ac Power to the Plant Auxiliaries

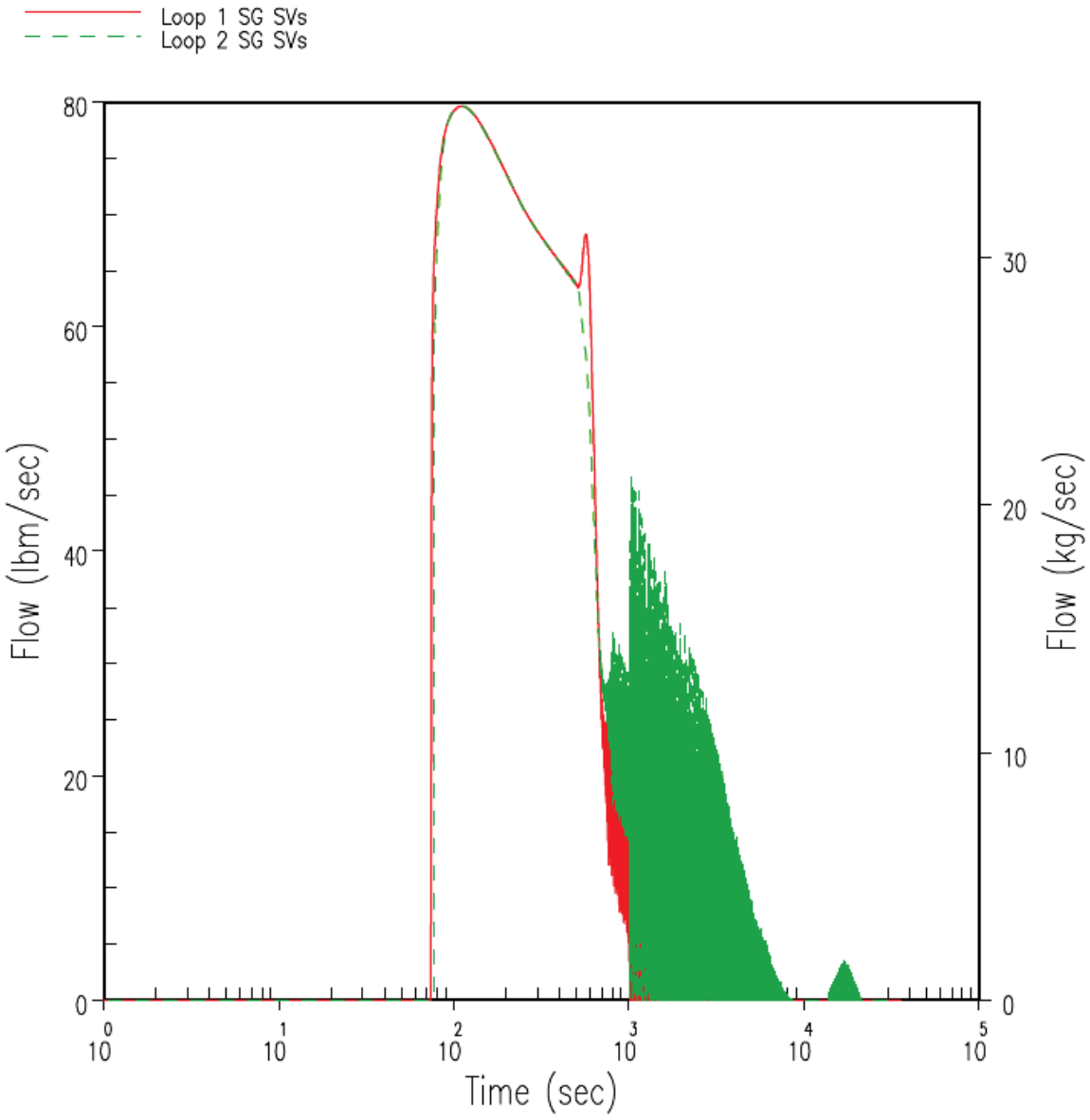


Figure 9.2.6-12. DBA Steam Generator Safety Valve Relief for Loss of ac Power to the Plant Auxiliaries

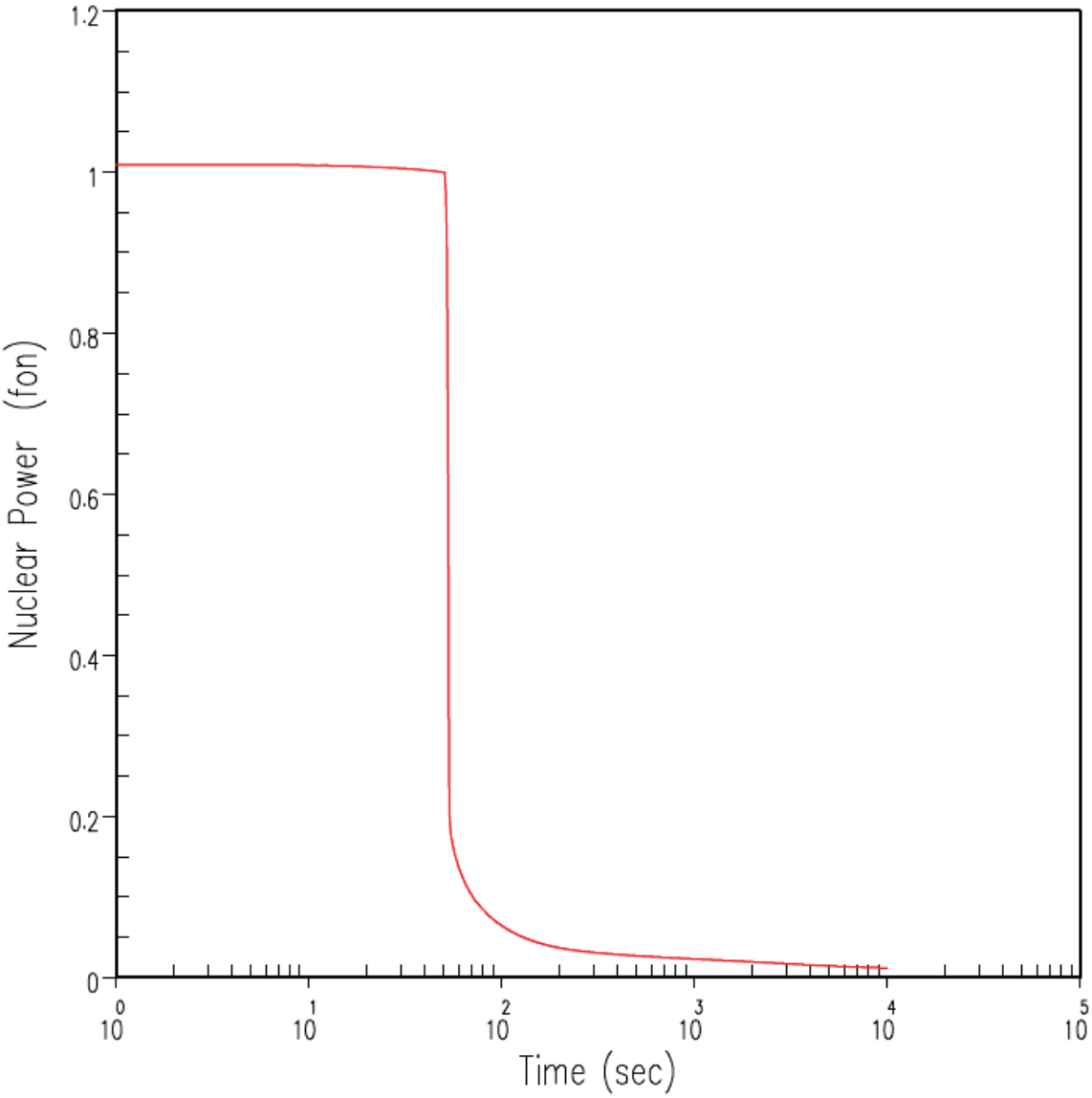


Figure 9.2.7-1. DBA Nuclear Power Transient for Loss of Normal Feedwater

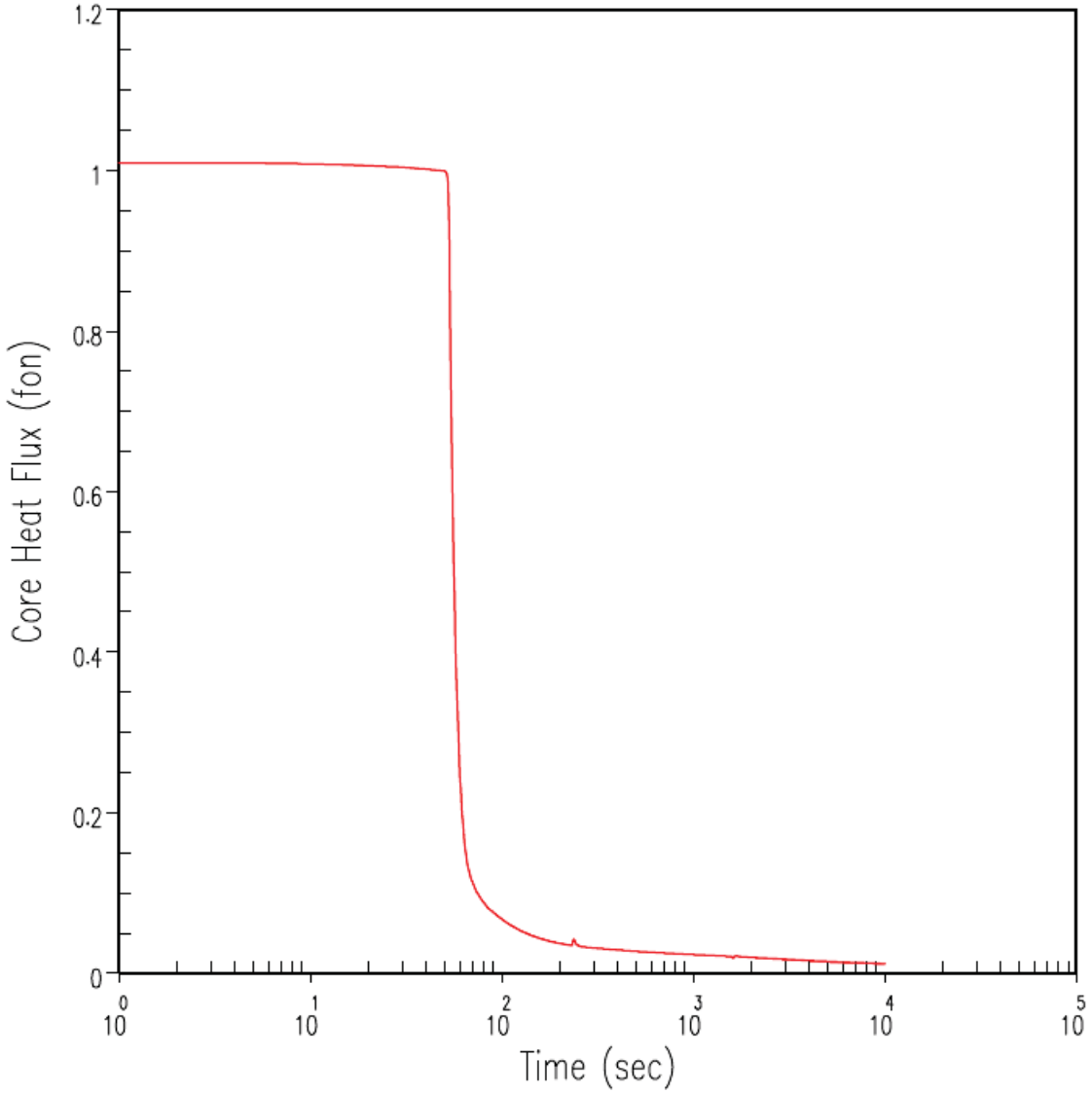


Figure 9.2.7-2. DBA Core Heat Flux Transient for Loss of Normal Feedwater

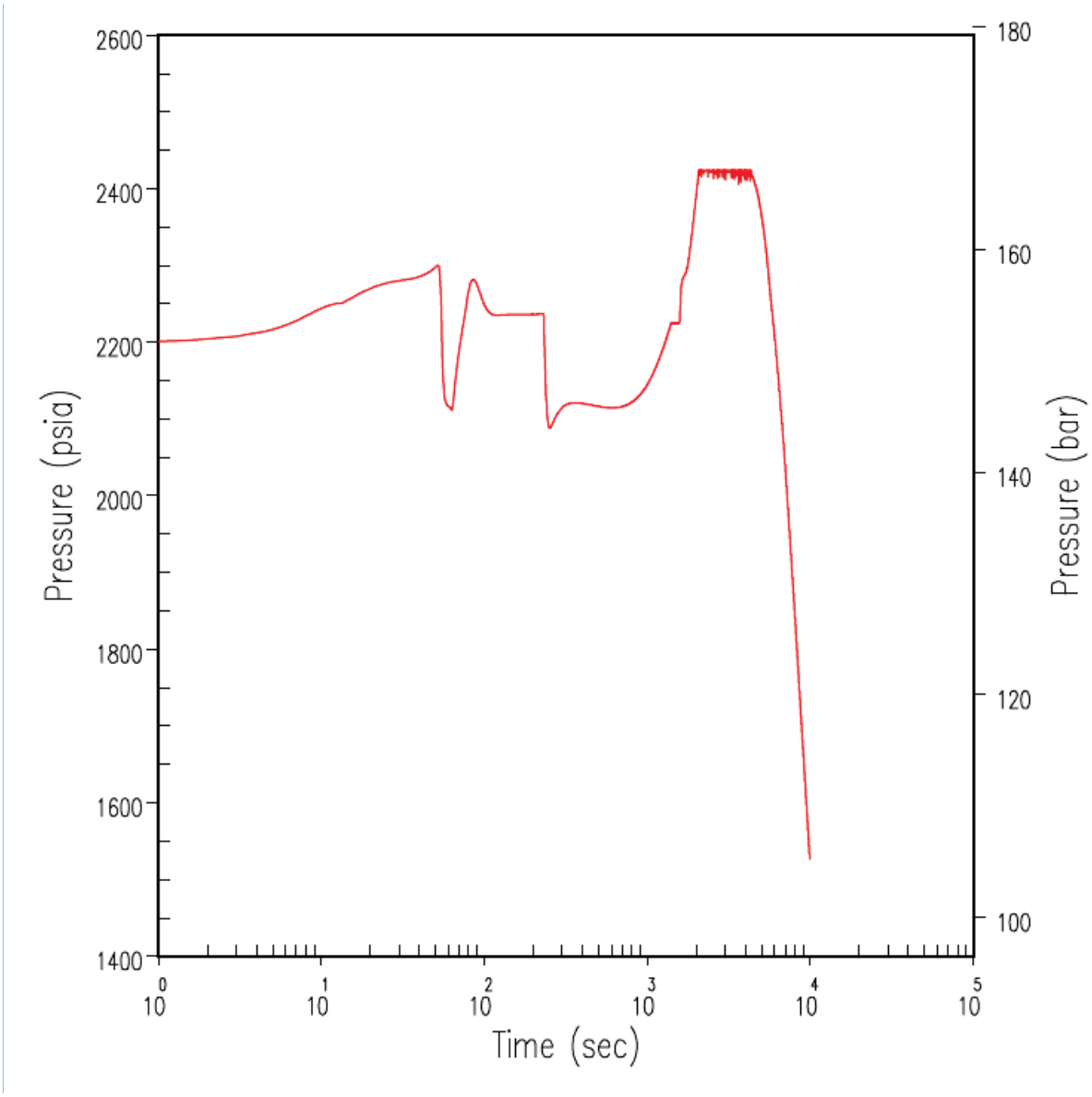


Figure 9.2.7-3. DBA Pressuriser Pressure Transient for Loss of Normal Feedwater

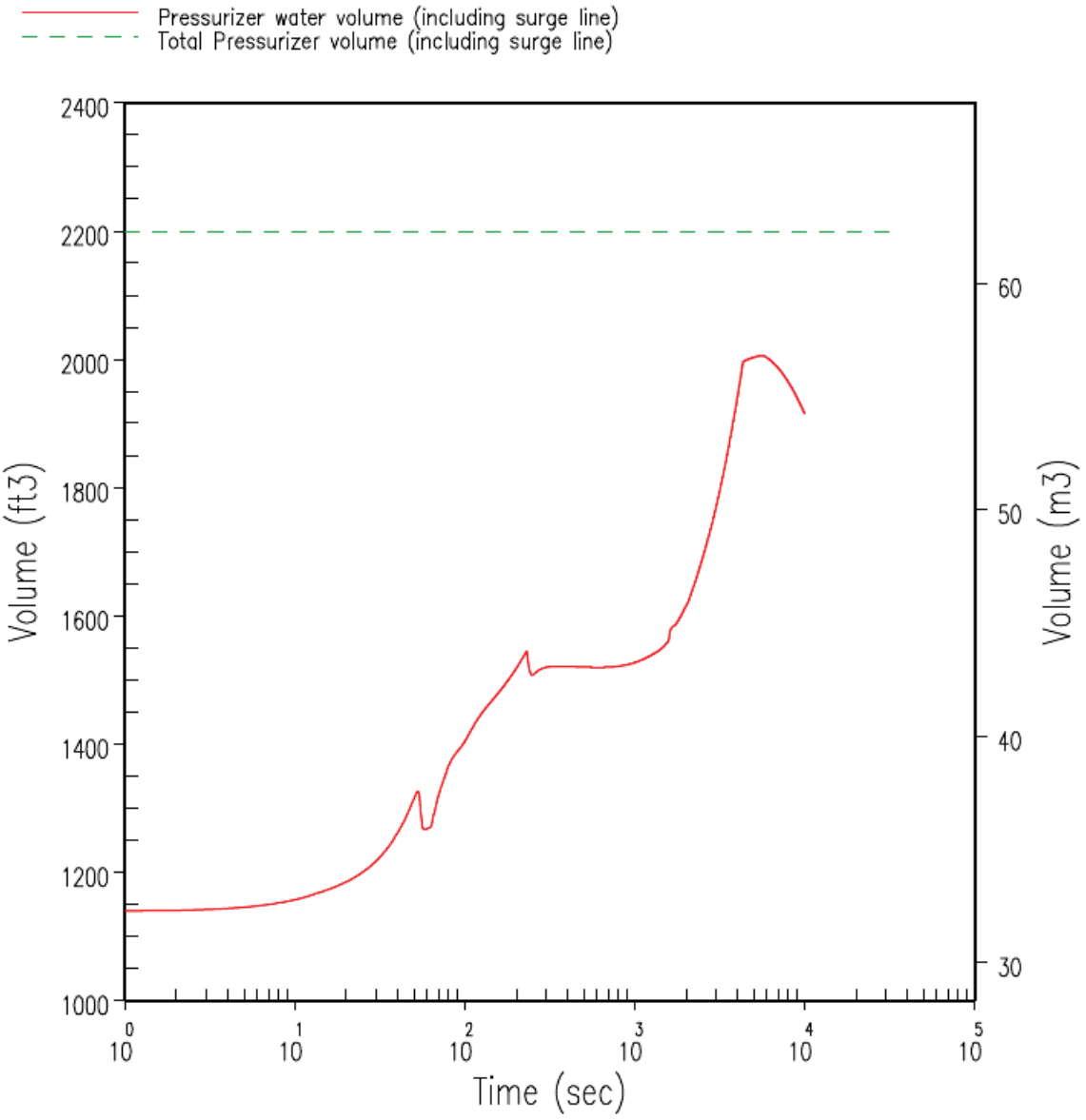


Figure 9.2.7-4. DBA Pressuriser Water Volume Transient for Loss of Normal Feedwater

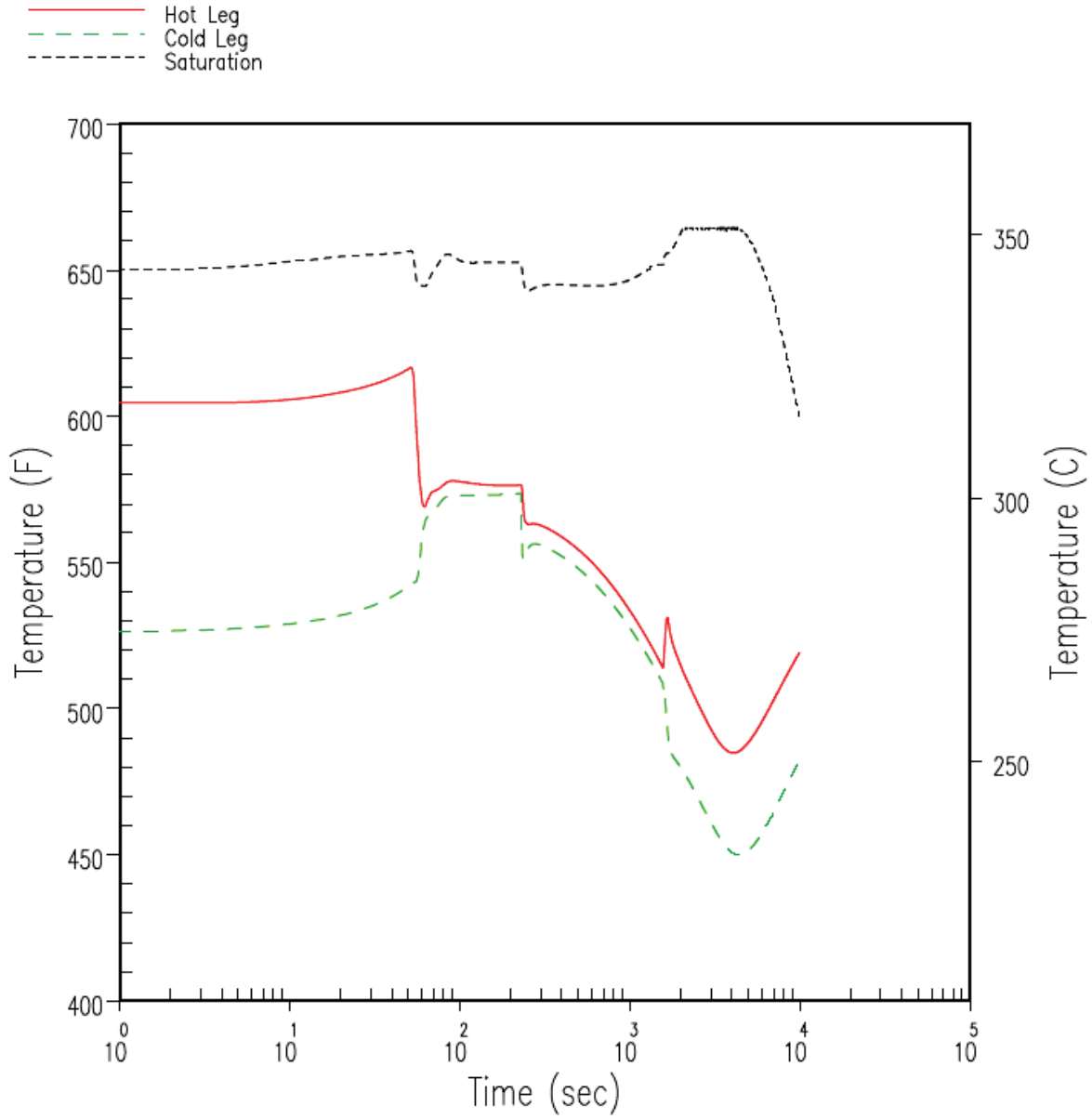


Figure 9.2.7-5. DBA Reactor Coolant System Temperature Transients in Loop Containing the PRHR for Loss of Normal Feedwater Flow

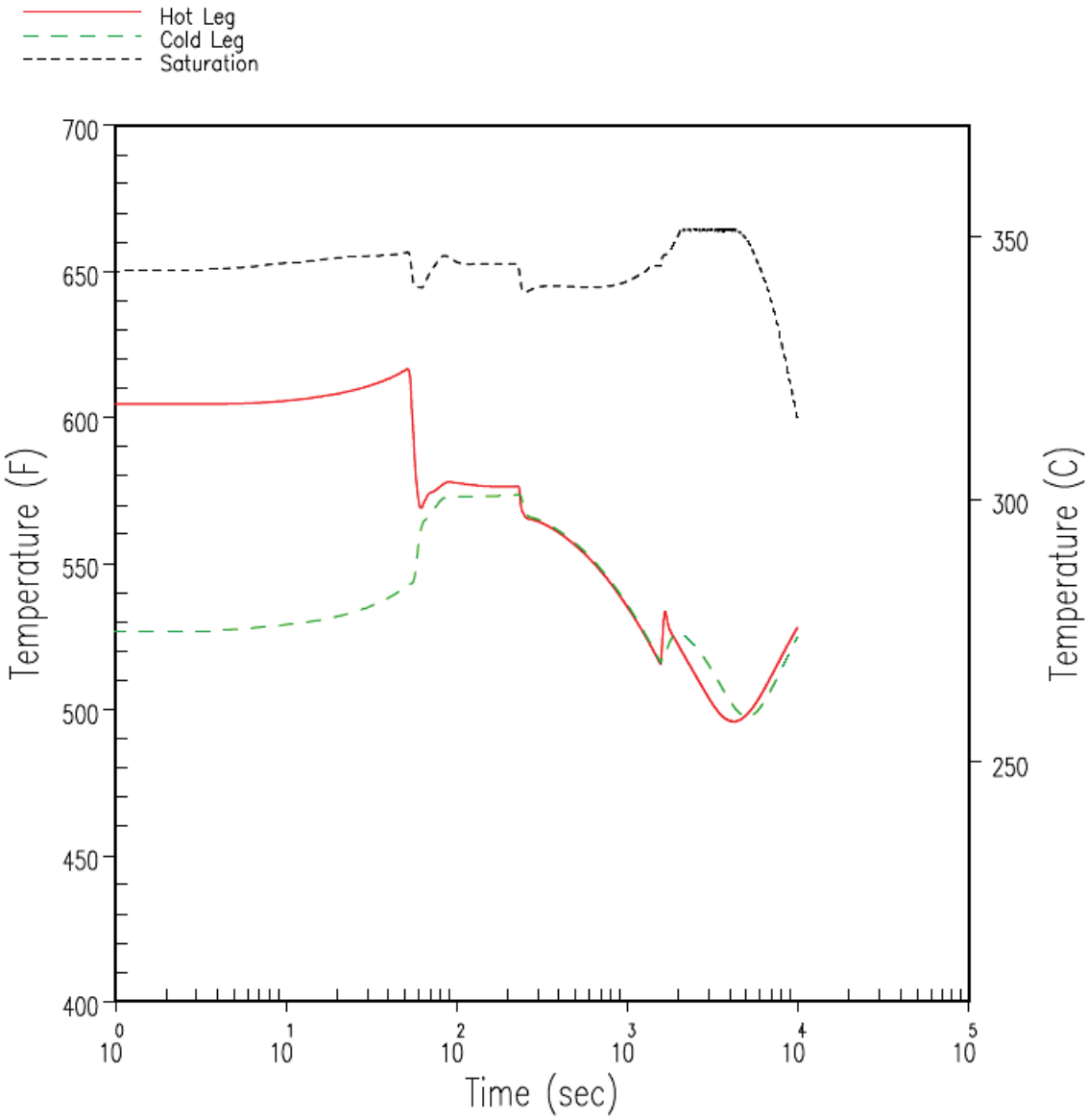


Figure 9.2.7-6. DBA Reactor Coolant System Temperature Transient in Loop Not Containing the PRHR for Loss of Normal Feedwater Flow

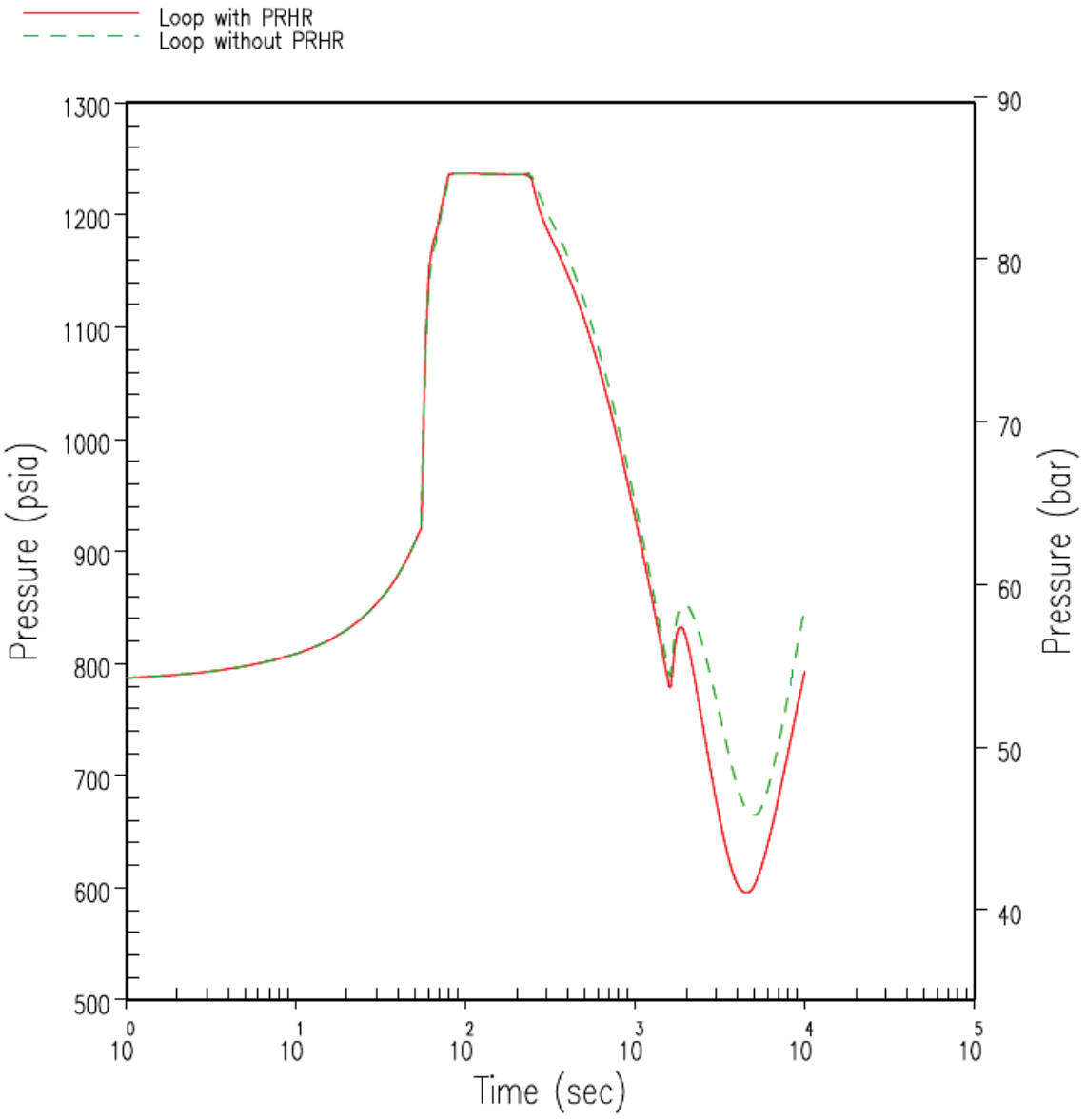


Figure 9.2.7-7. DBA Steam Generator Pressure Transient for Loss of Normal Feedwater

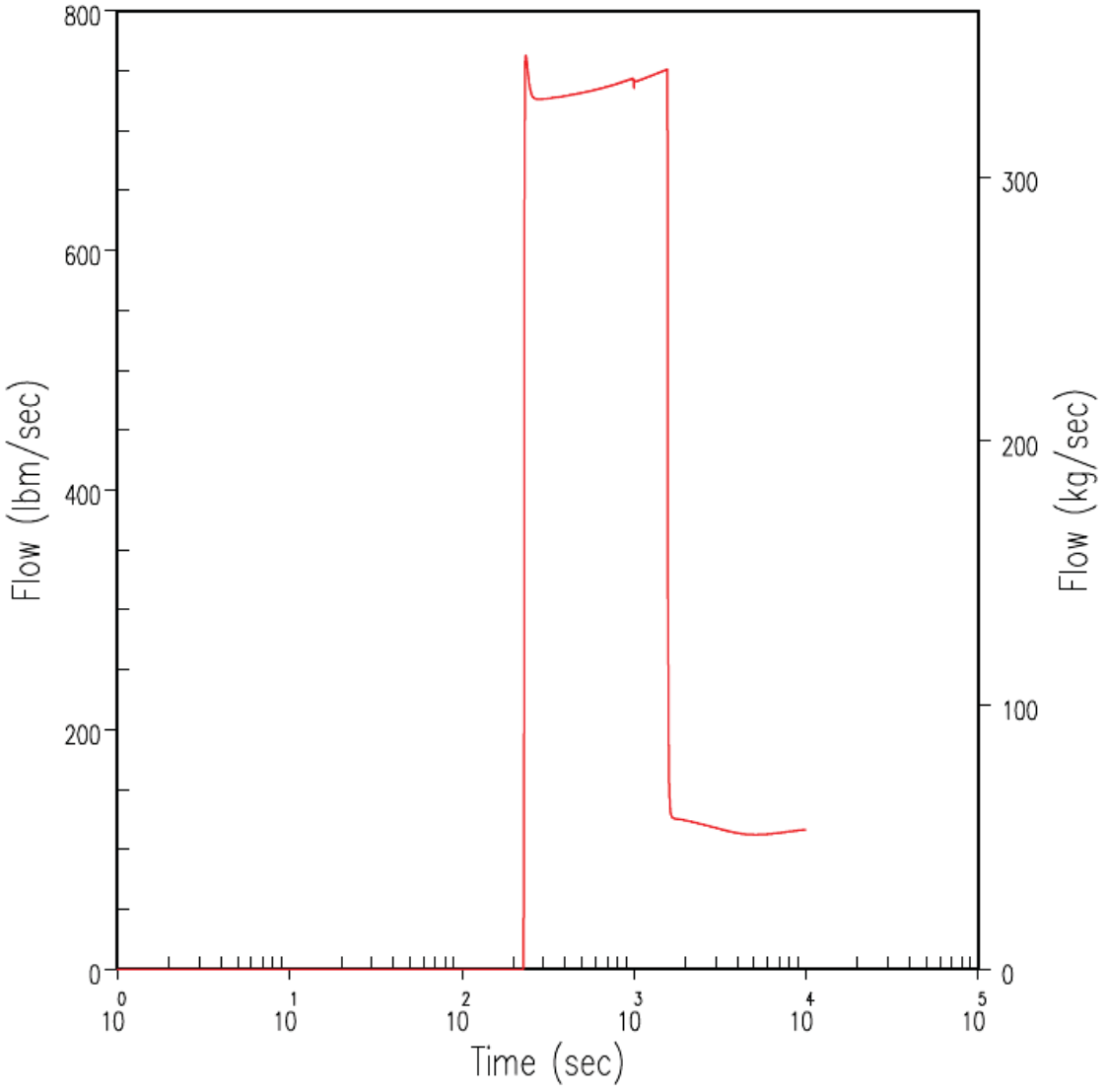


Figure 9.2.7-8. DBA PRHR Flow Rate Transient for Loss of Normal Feedwater

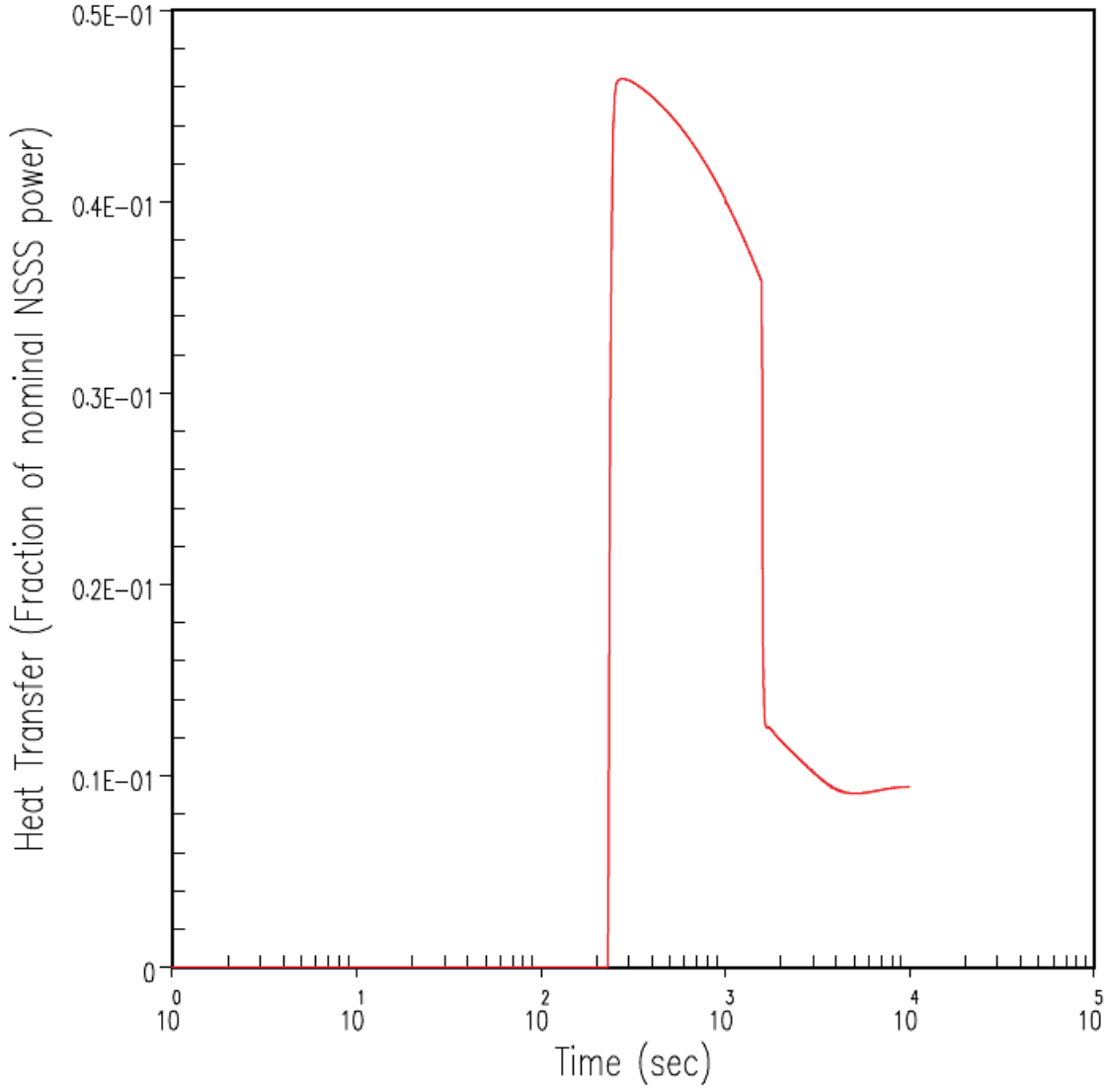


Figure 9.2.7-9. DBA PRHR Heat Transfer Transient for Loss of Normal Feedwater

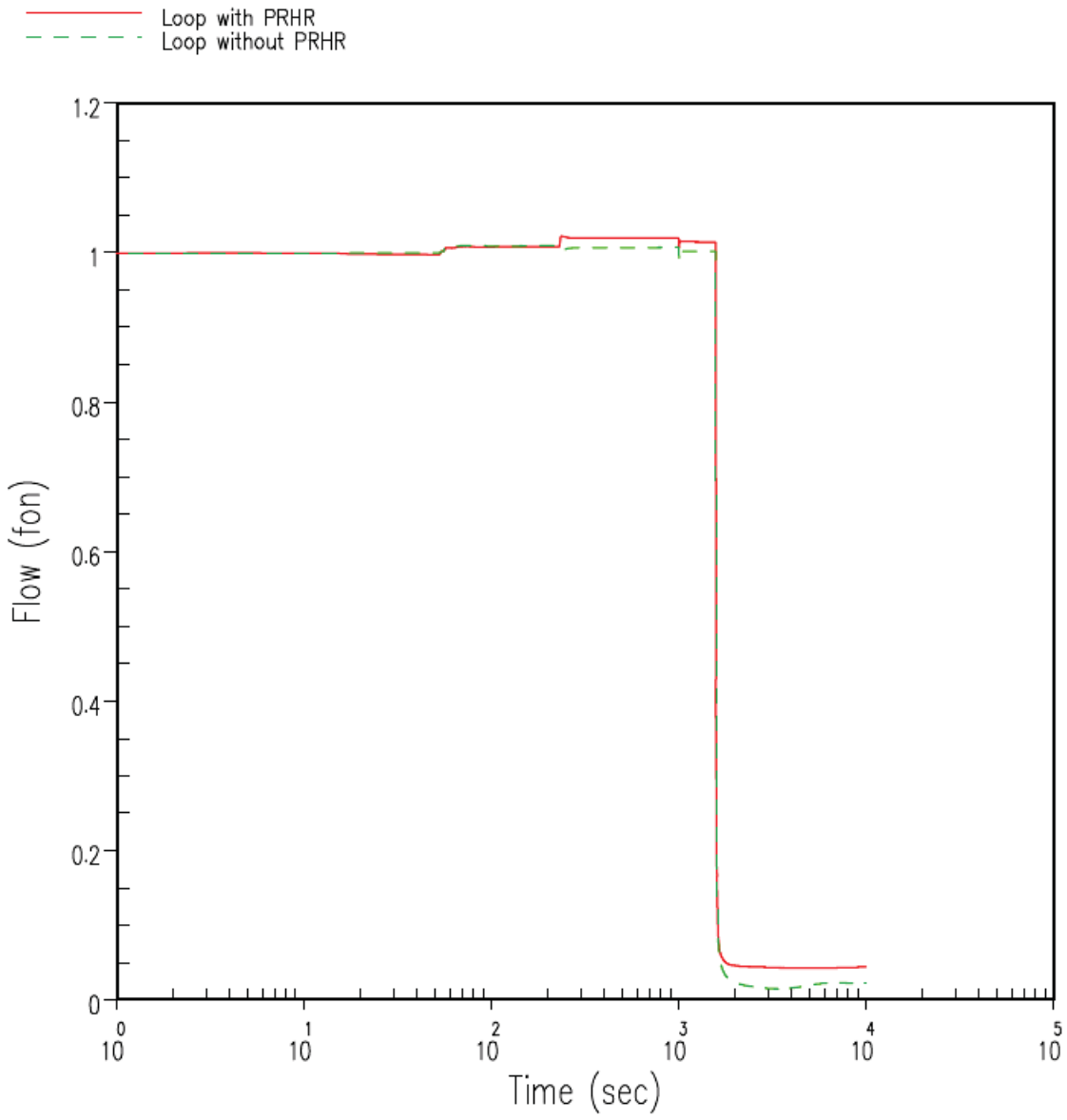


Figure 9.2.7-10. DBA Reactor Coolant Volumetric Flow Transient for Loss of Normal Feedwater

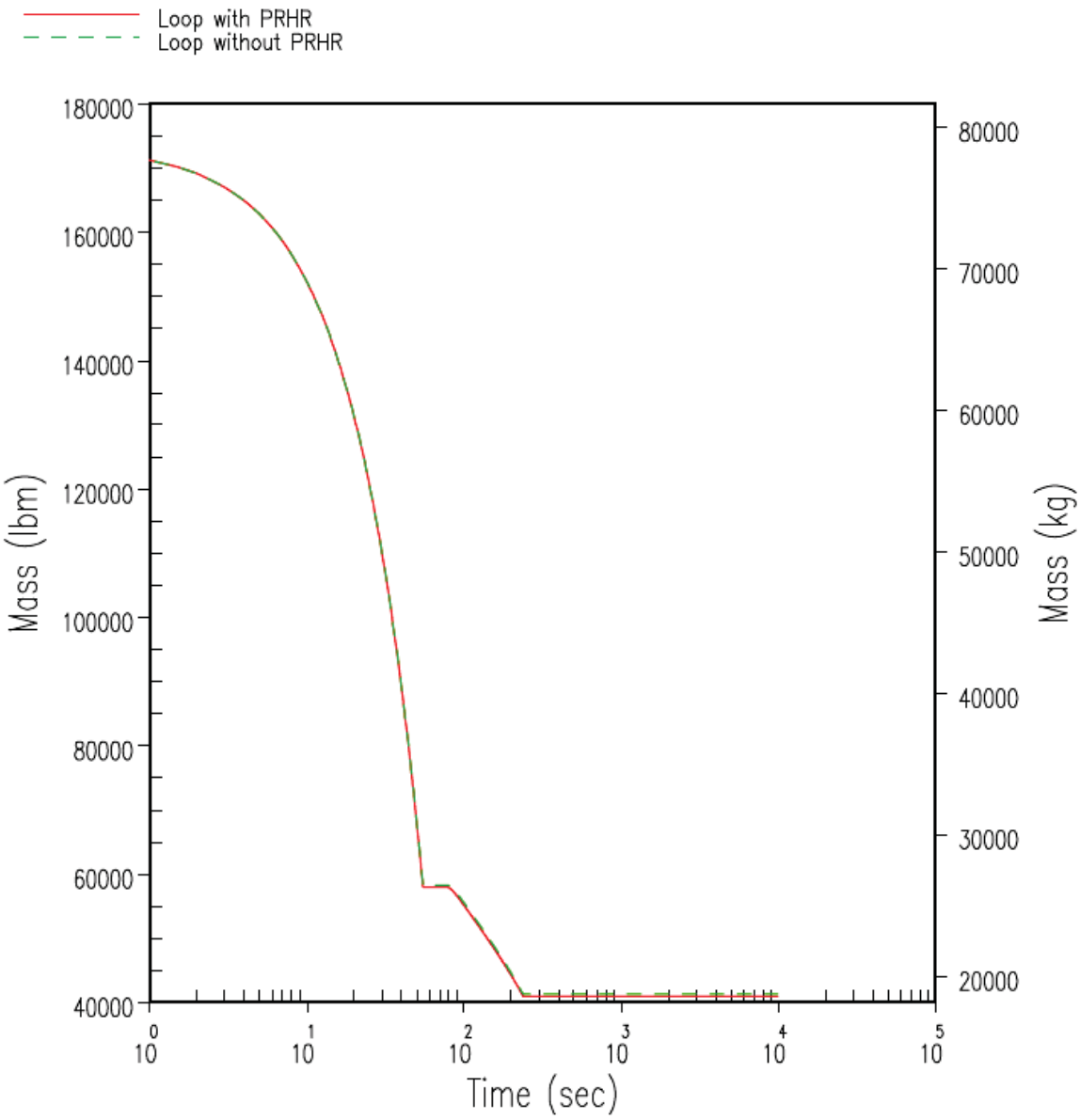


Figure 9.2.7-11. DBA Steam Generator Inventory Transient for Loss of Normal Feedwater

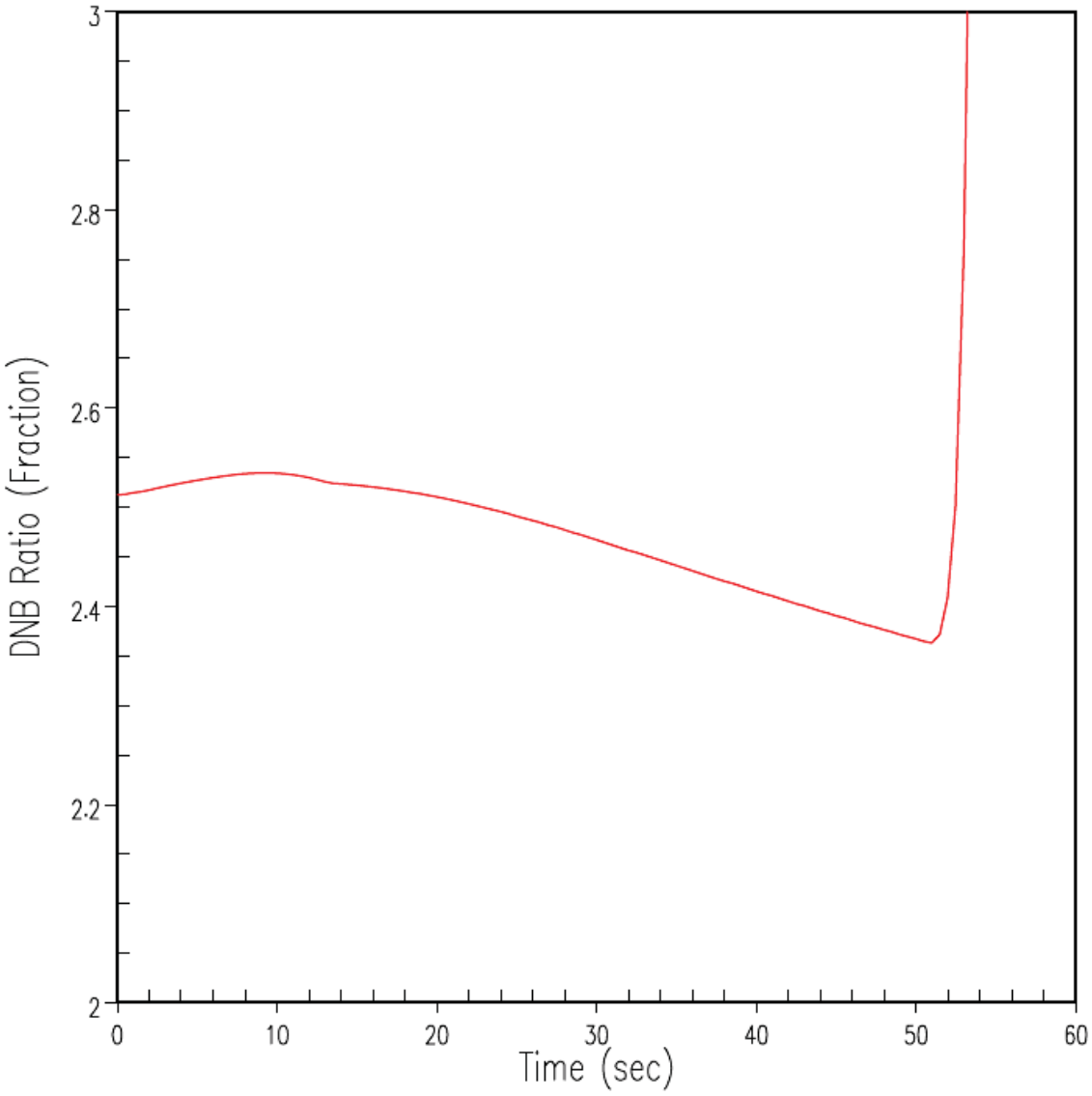


Figure 9.2.7-12. DBA DNB Ratio Transient for Loss of Normal Feedwater

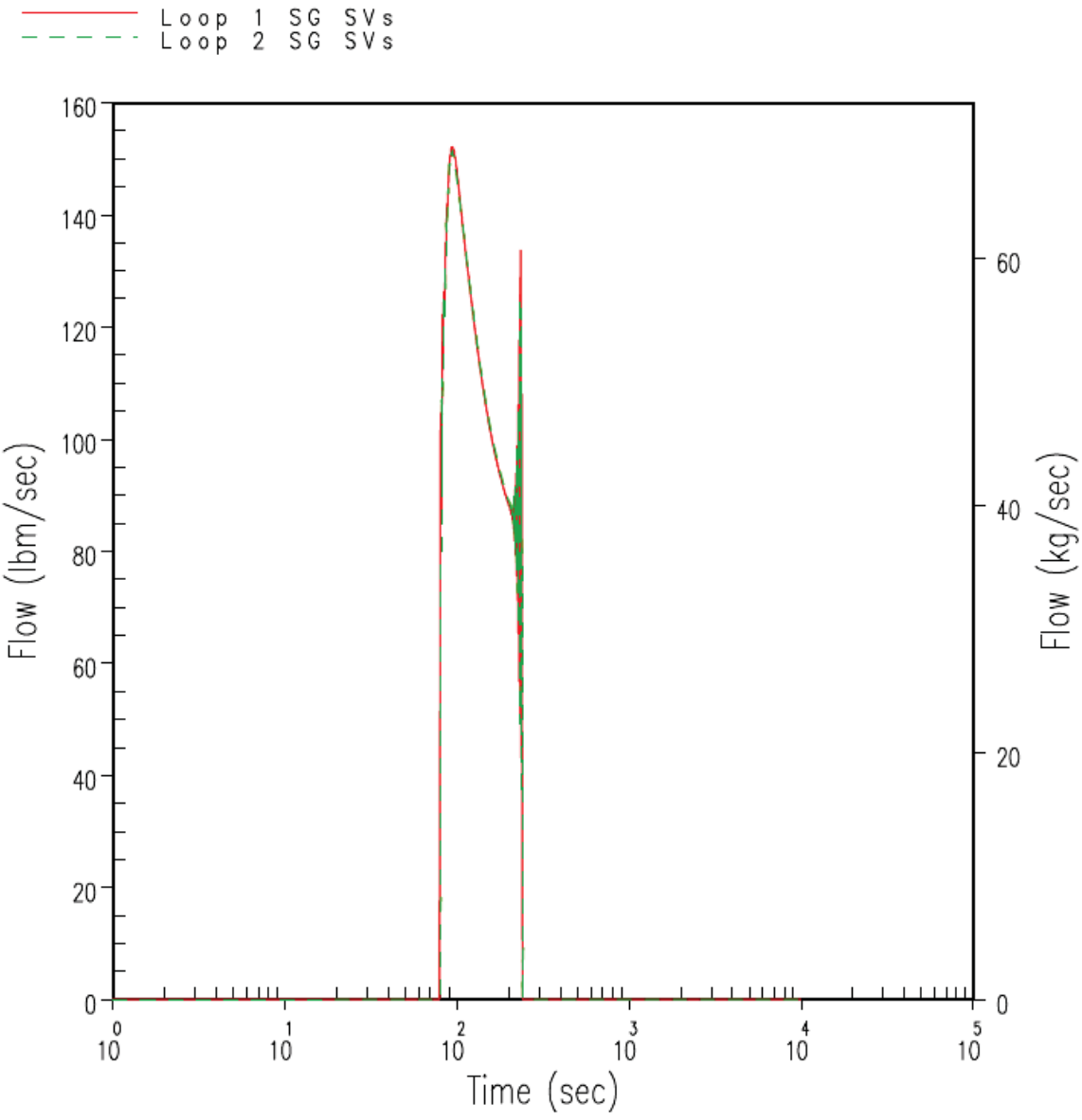


Figure 9.2.7-13. DBA Steam Generator Safety Valve Relief Transient for Loss of Normal Feedwater

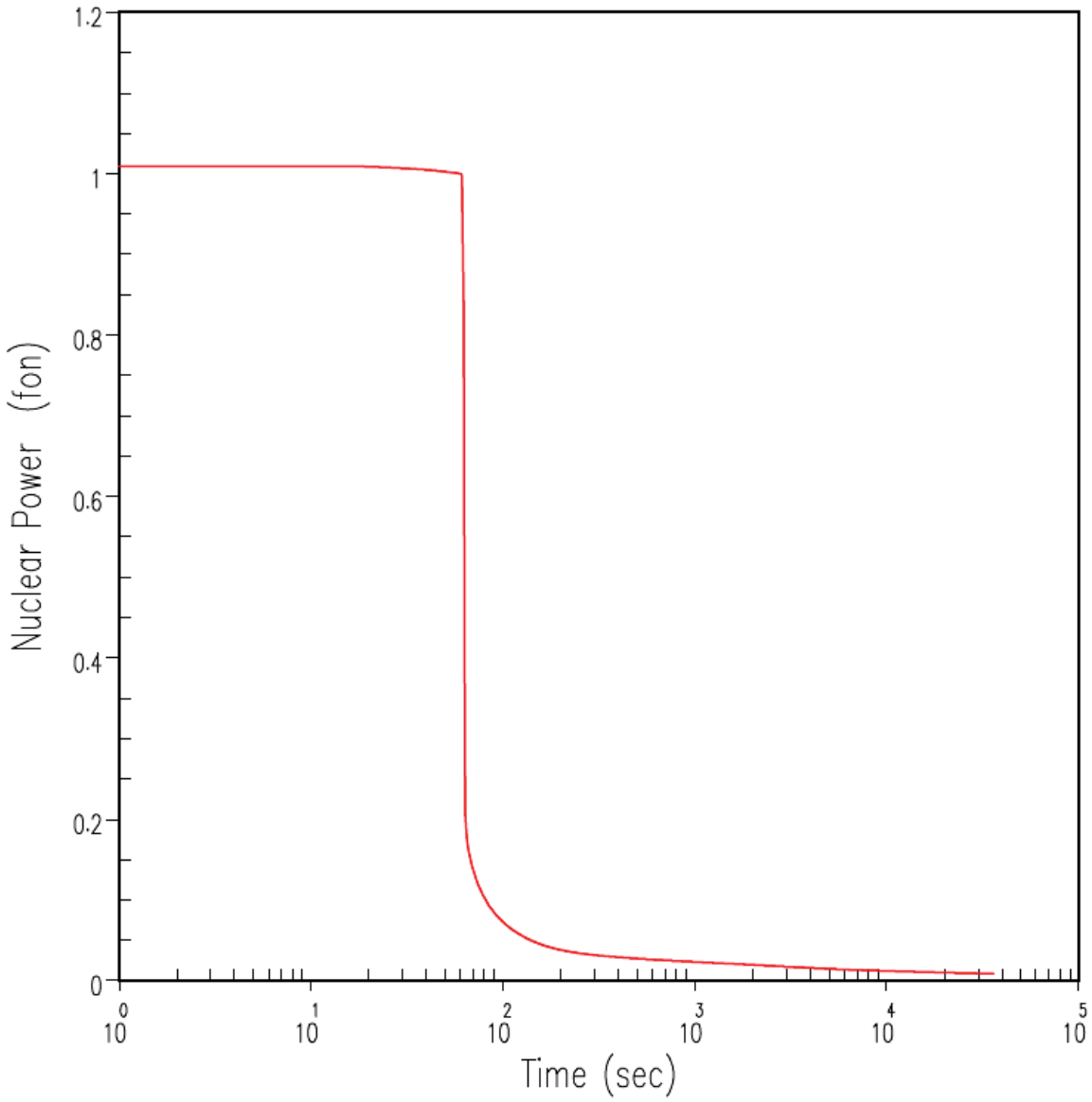


Figure 9.2.7-14. DBA Nuclear Power Transient for Loss of Normal Feedwater with a Consequential Loss of ac Power to the Plant Auxiliaries

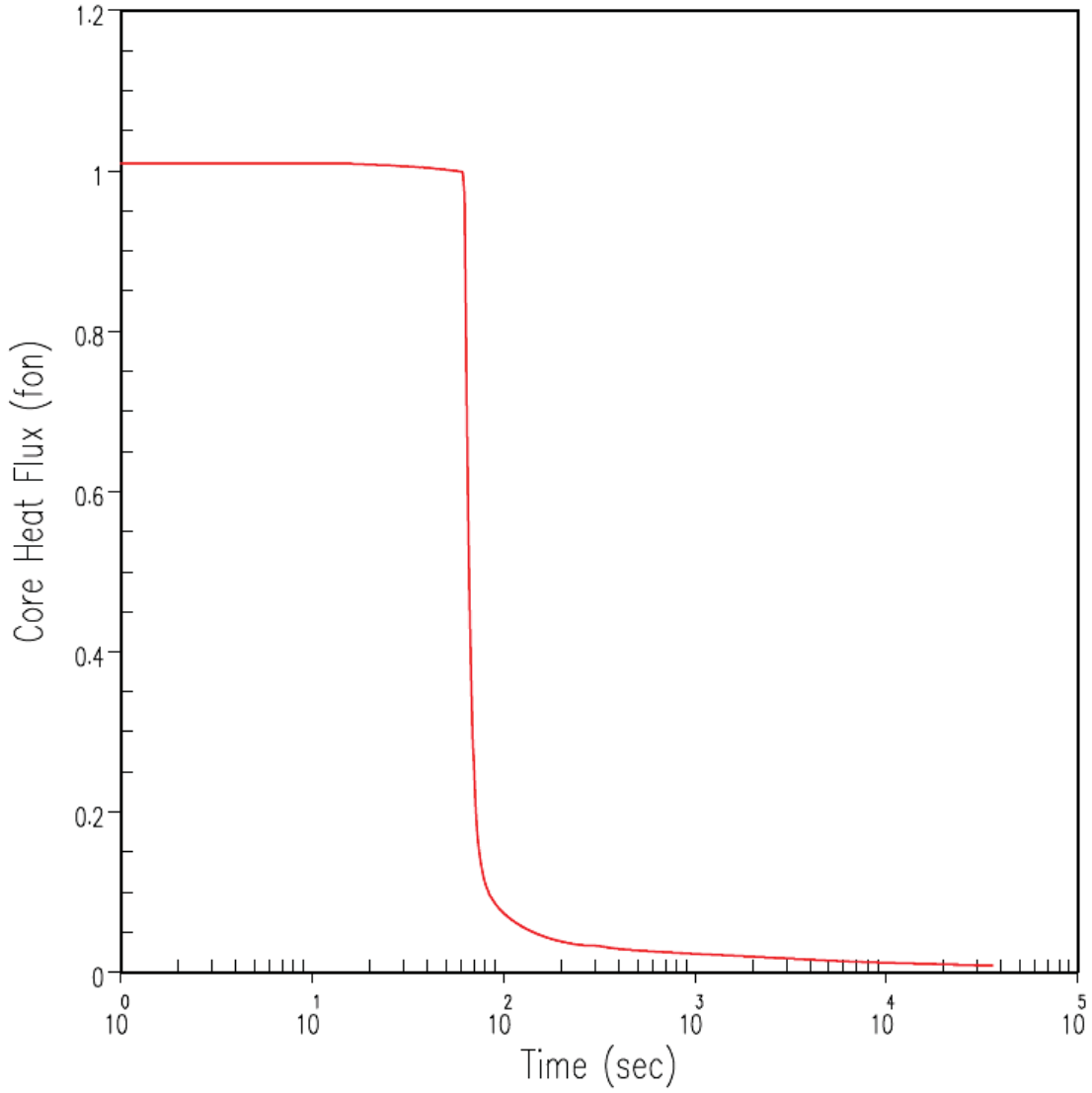


Figure 9.2.7-15. DBA Core Heat Flux Transient for Loss of Normal Feedwater with a Consequential Loss of ac Power to the Plant Auxiliaries

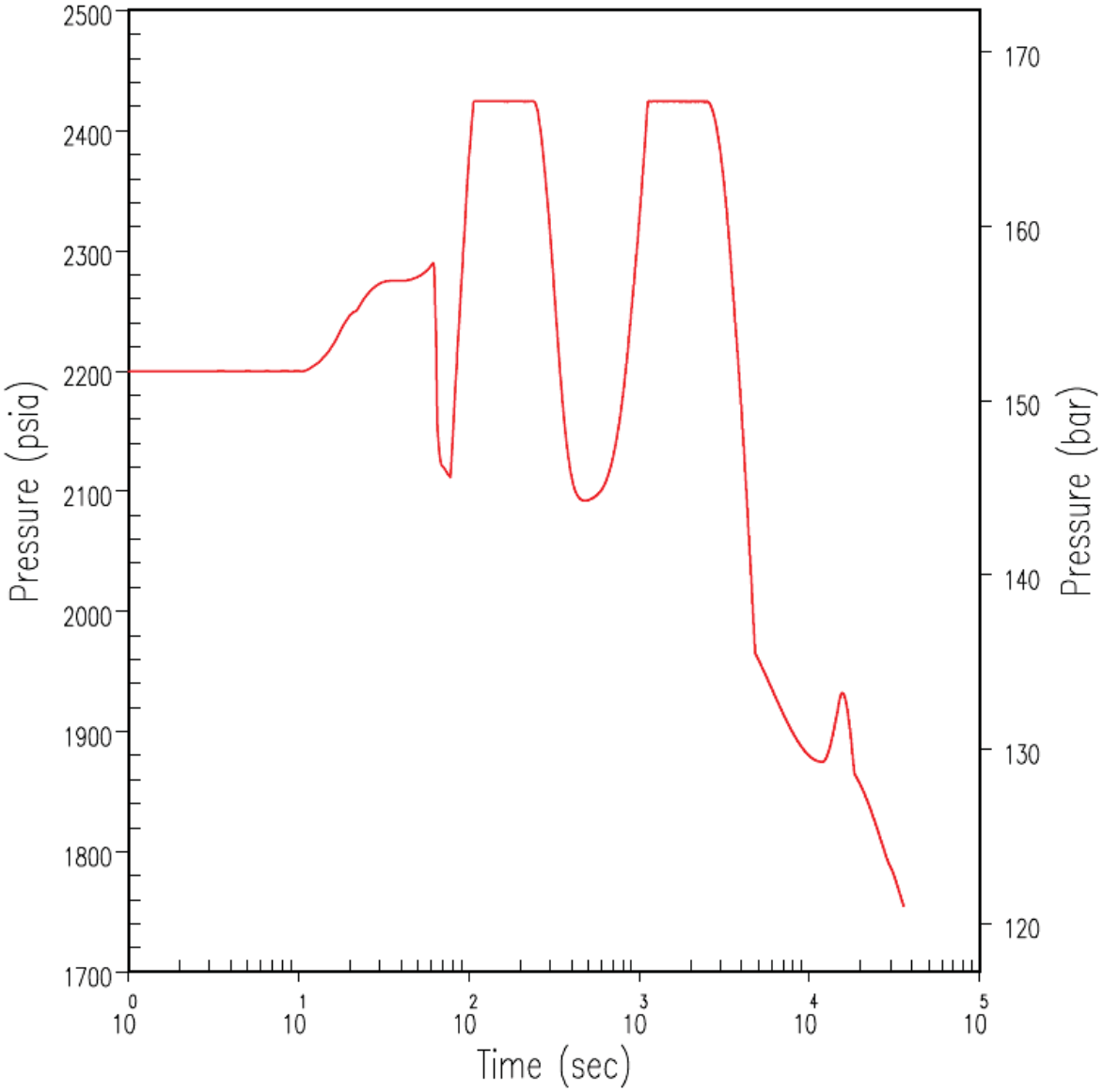


Figure 9.2.7-16. DBA Pressuriser Pressure Transient for Loss of Normal Feedwater with a Consequential Loss of ac Power to the Plant Auxiliaries

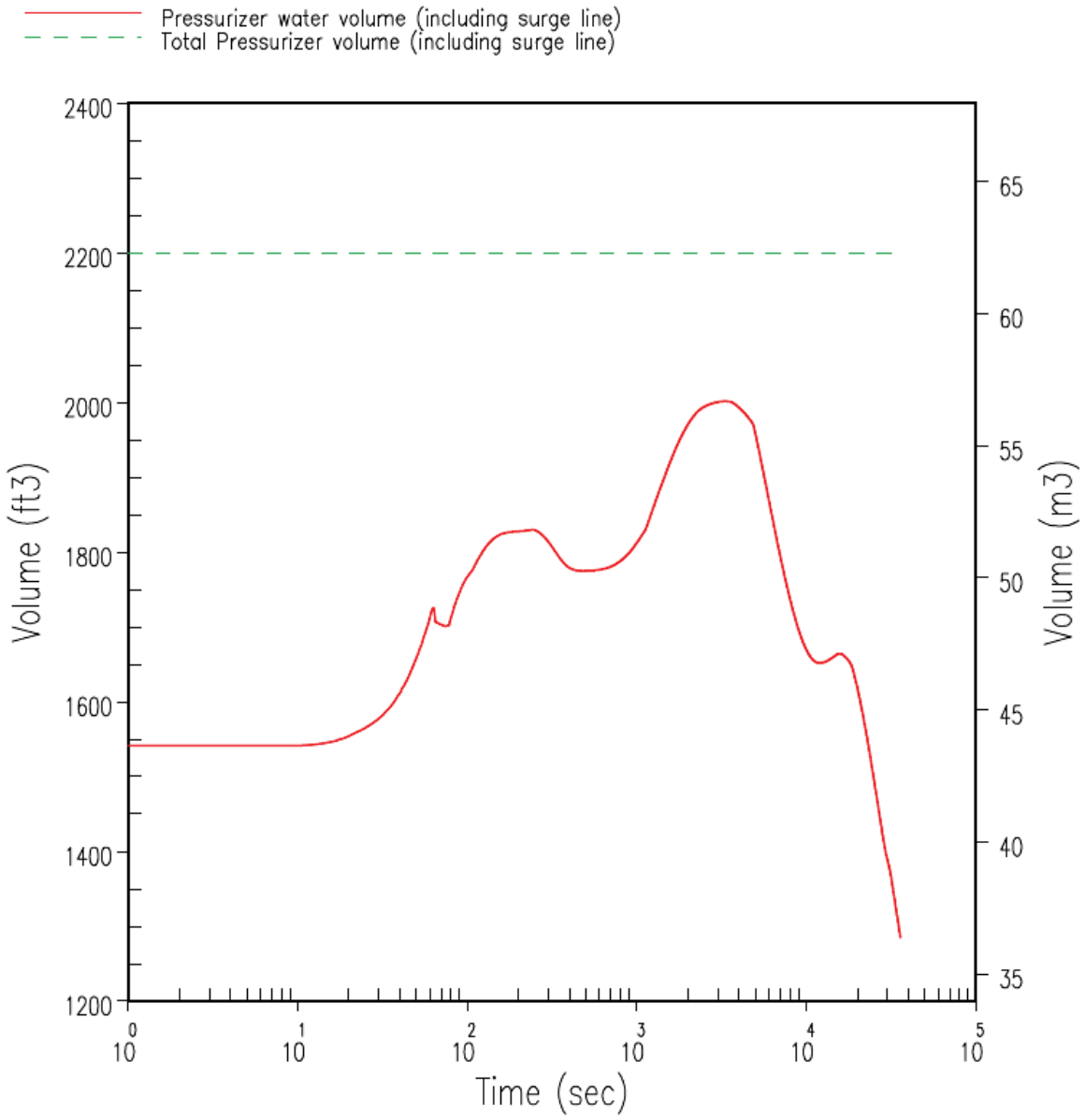


Figure 9.2.7-17. DBA Pressuriser Water Volume Transient for Loss of Normal Feedwater with a Consequential Loss of ac Power to the Plant Auxiliaries

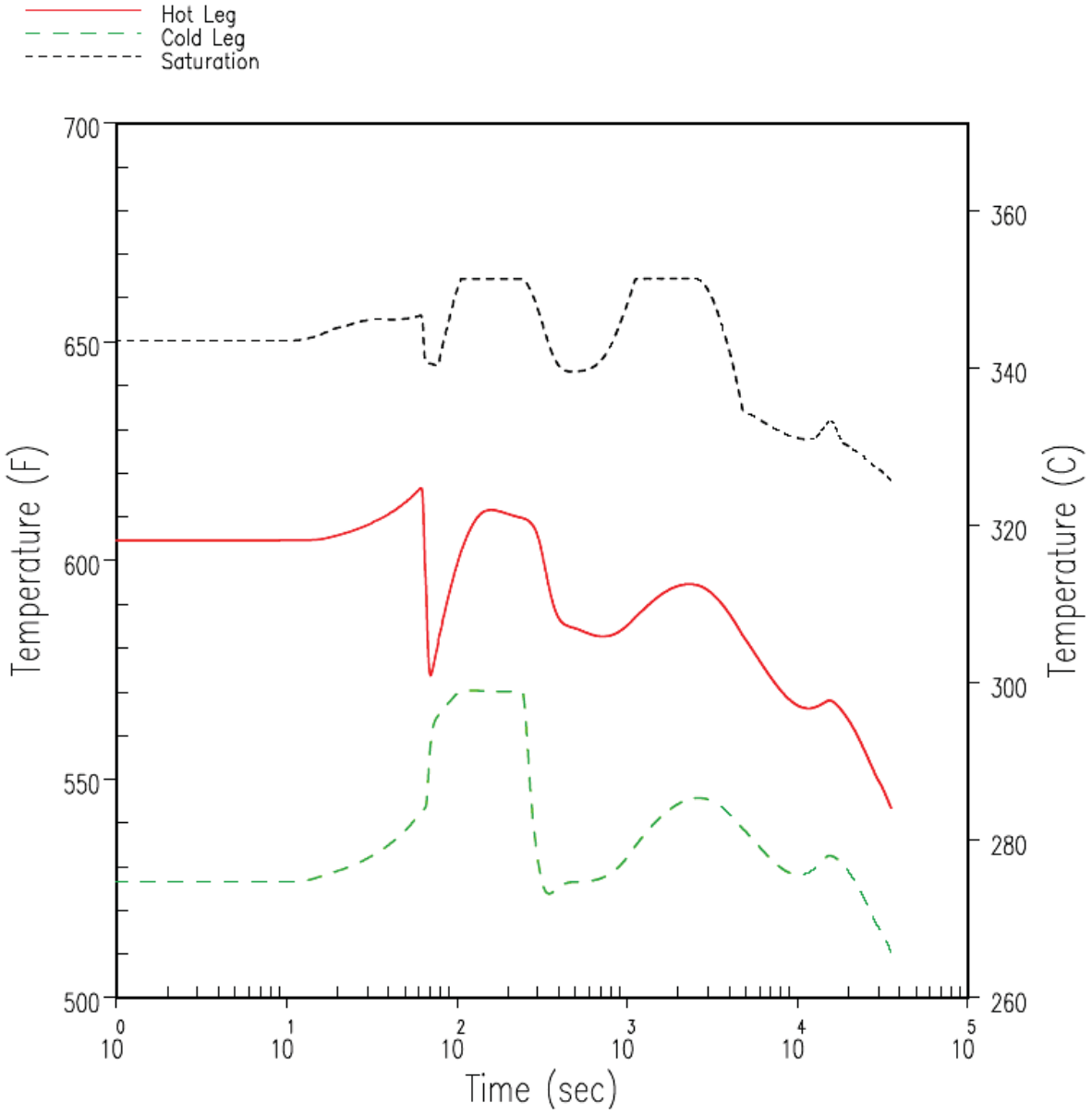


Figure 9.2.7-18. DBA Reactor Coolant System Temperature Transients in Loop Containing the PRHR for Loss of Normal Feedwater with a Consequential Loss of ac Power to the Plant Auxiliaries

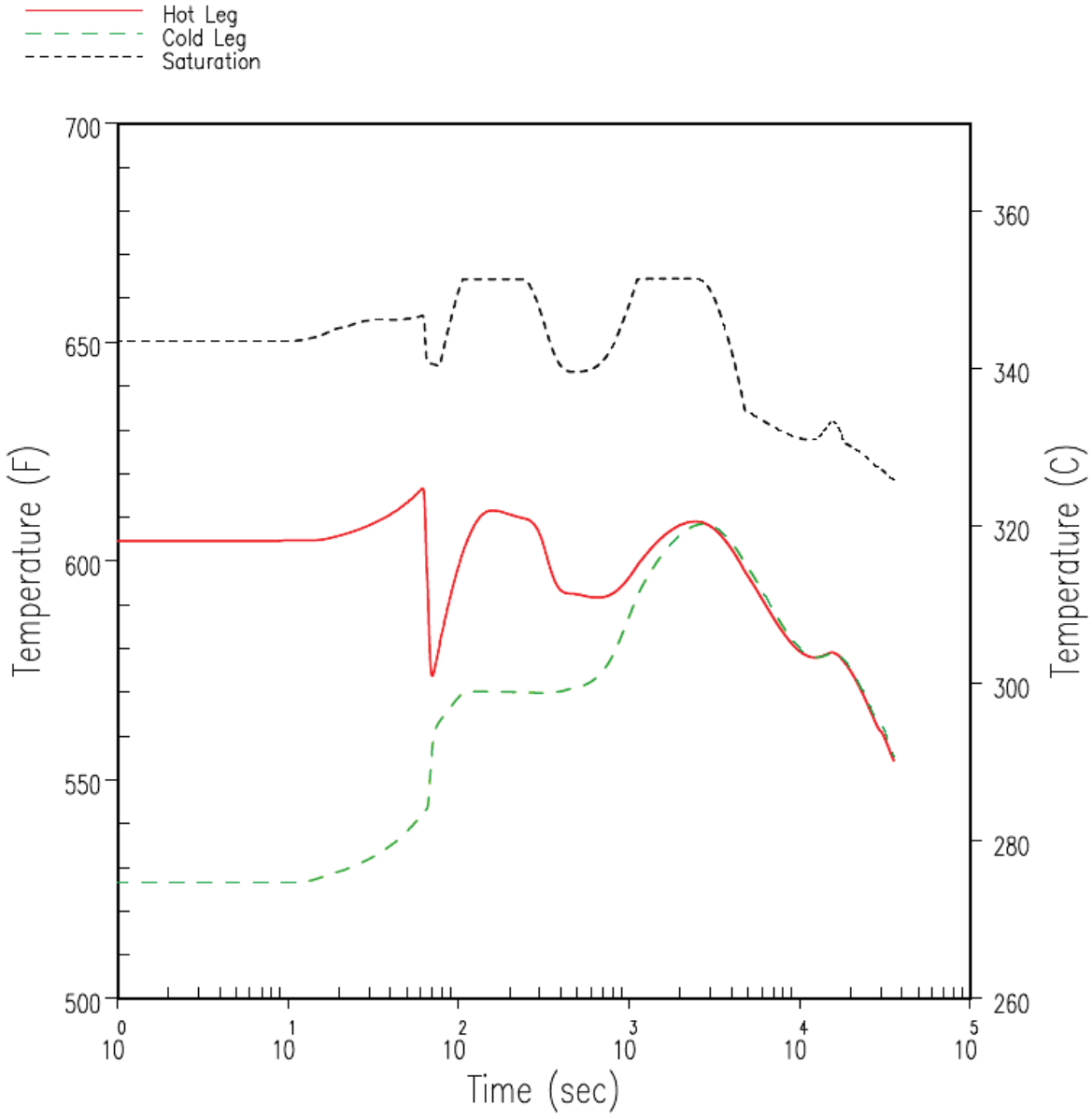


Figure 9.2.7-19. DBA Reactor Coolant System Temperature Transients in Loop Not Containing the PRHR for Loss of Normal Feedwater with a Consequential Loss of ac Power to the Plant Auxiliaries

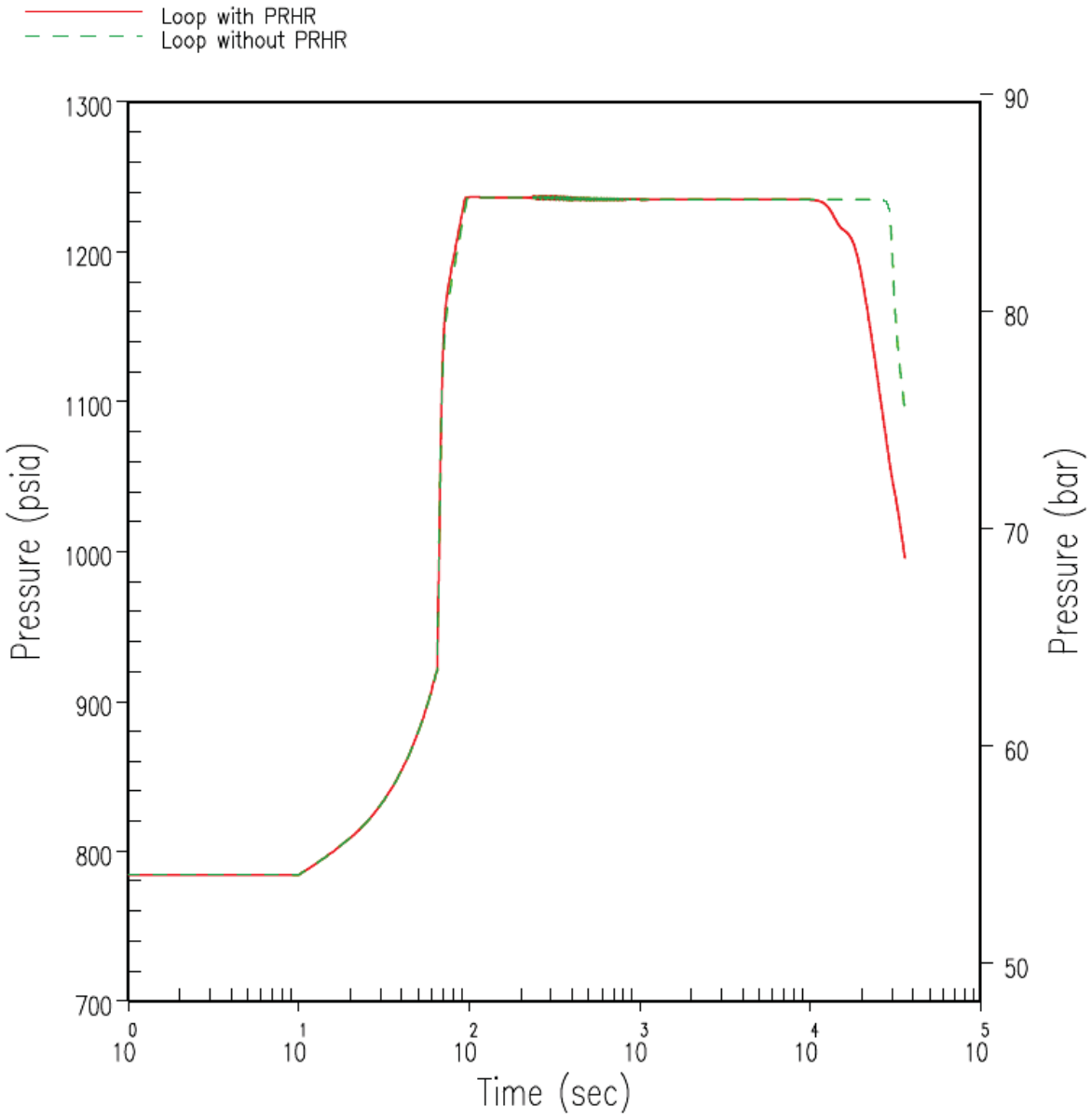


Figure 9.2.7-20. DBA Steam Generator Pressure Transient for Loss of Normal Feedwater with a Consequential Loss of ac Power to the Plant Auxiliaries

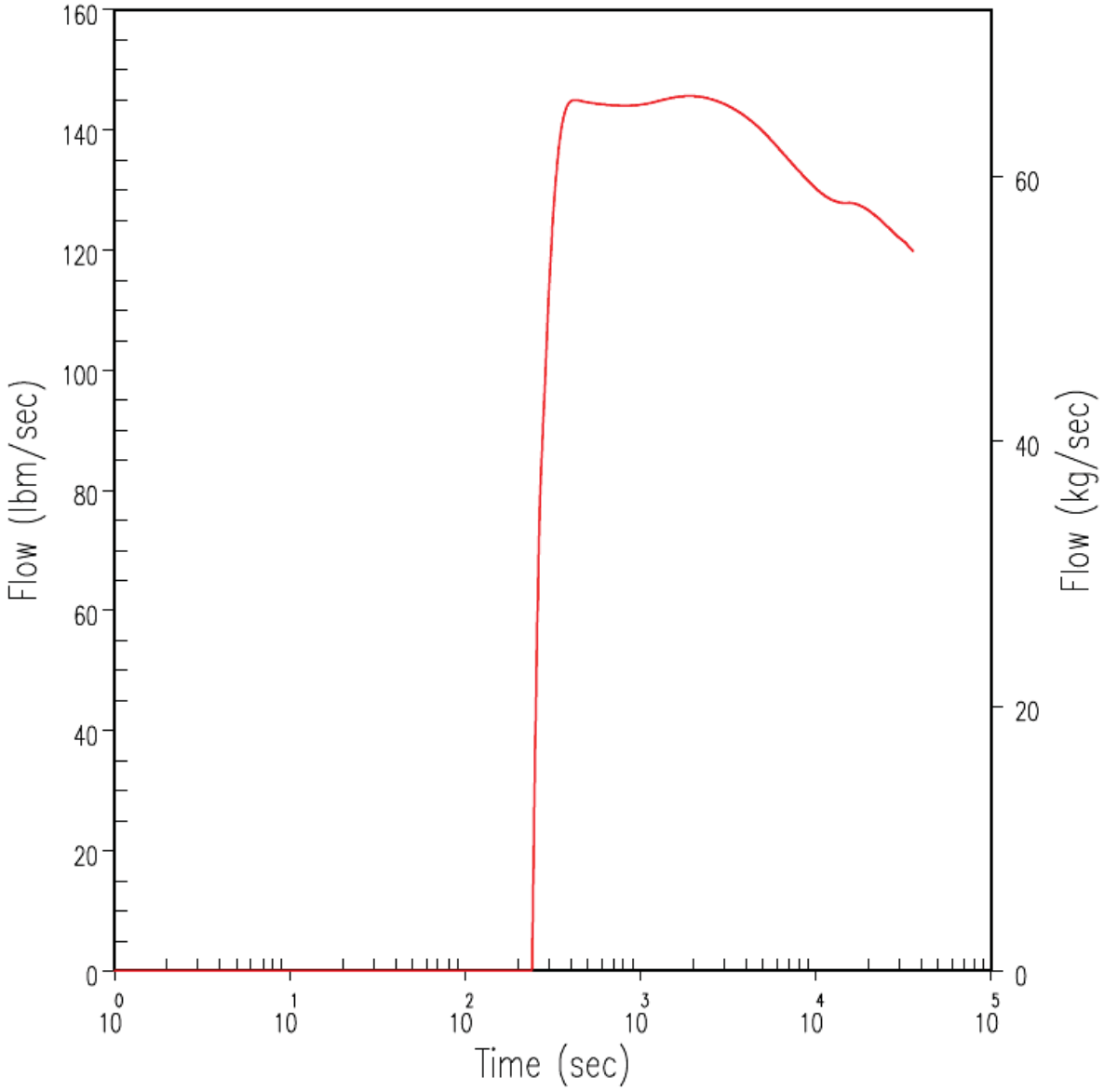


Figure 9.2.7-21. DBA PRHR Flow Rate Transient for Loss of Normal Feedwater with a Consequential Loss of ac Power to the Plant Auxiliaries

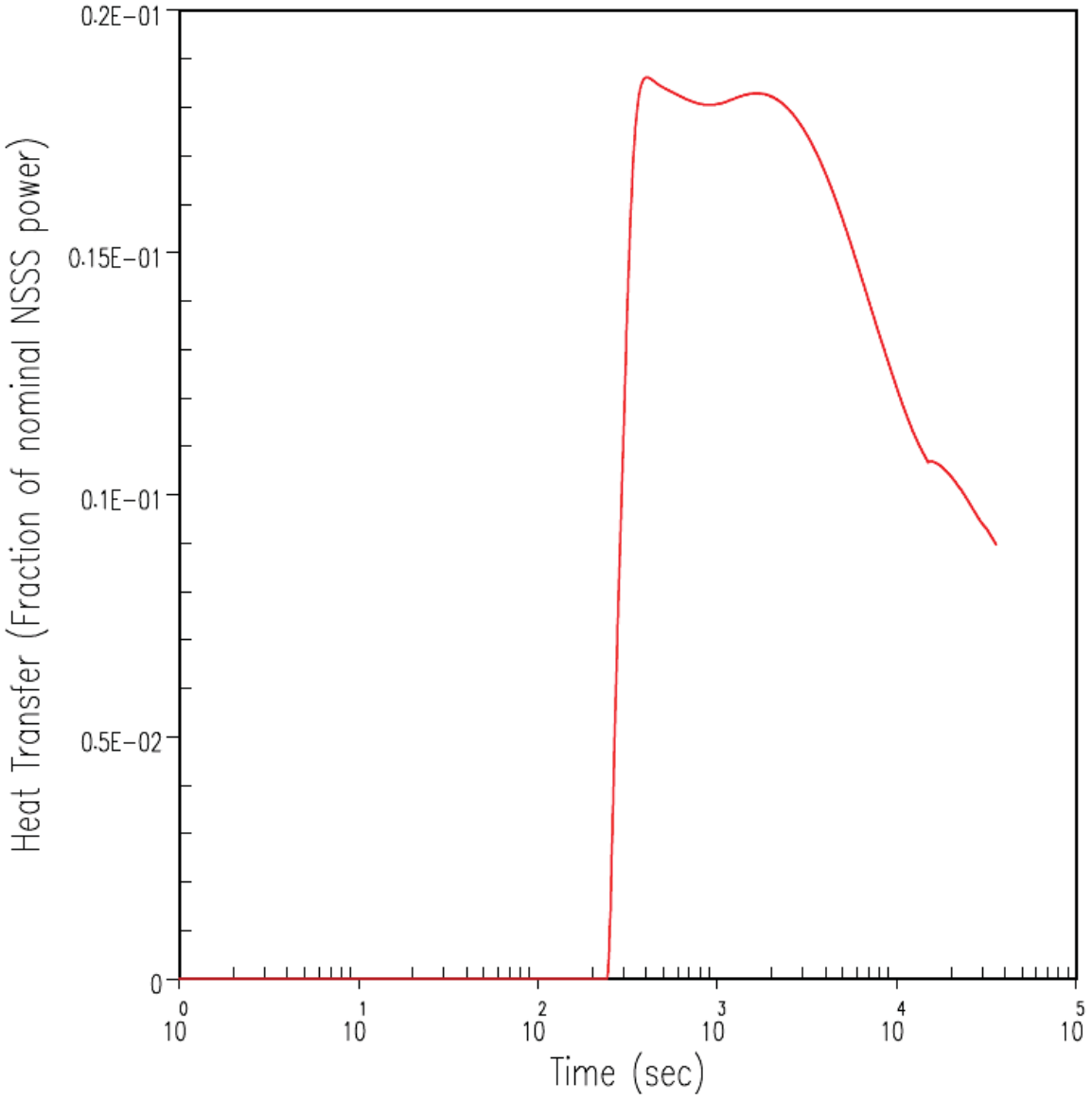


Figure 9.2.7-22. DBA PRHR Heat Transfer Transient for Loss of Normal Feedwater with a Consequential Loss of ac Power to the Plant Auxiliaries

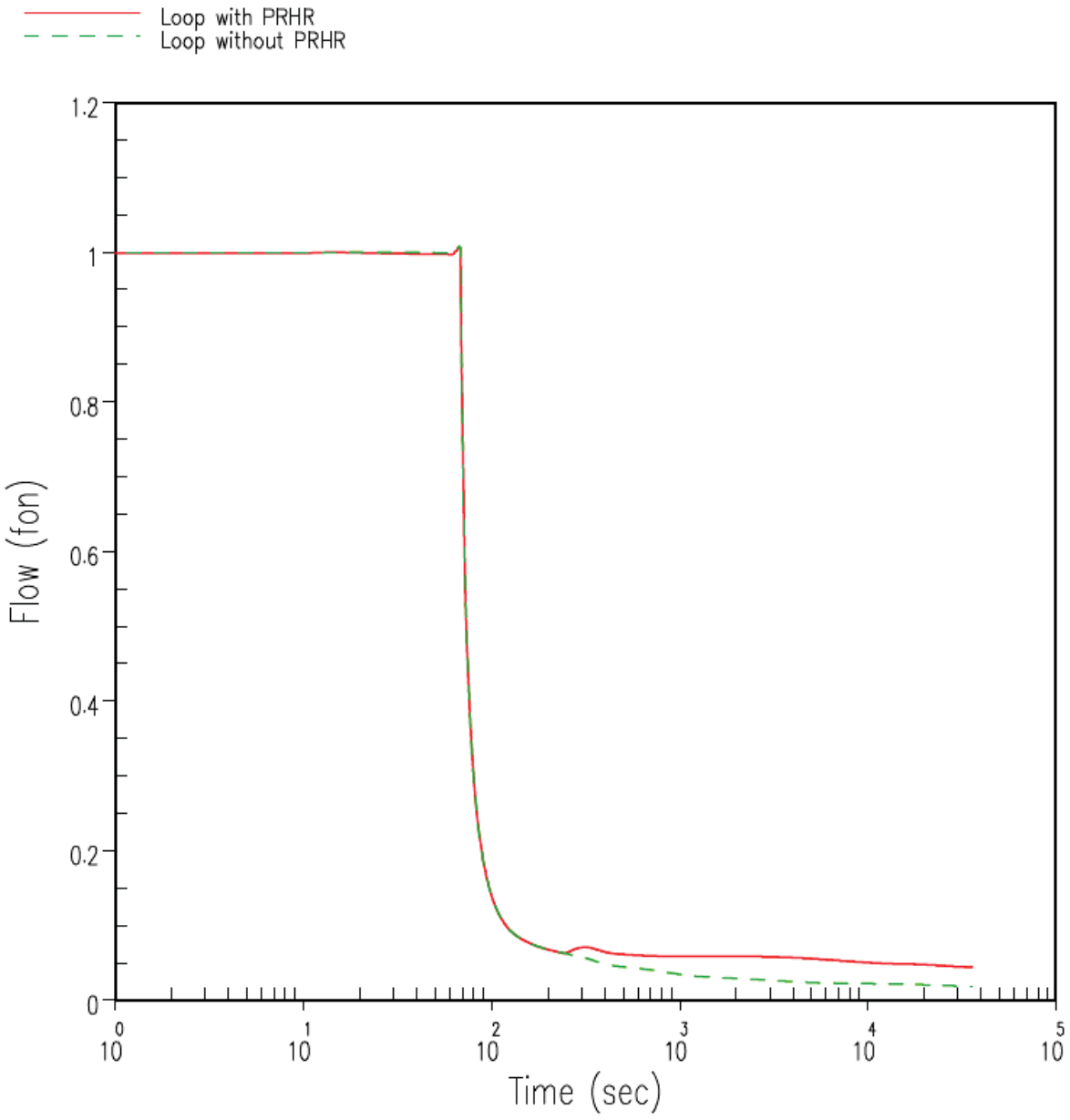


Figure 9.2.7-23. DBA Reactor Coolant Volumetric Flow Transient for Loss of Normal Feedwater with a Consequential Loss of ac Power to the Plant Auxiliaries

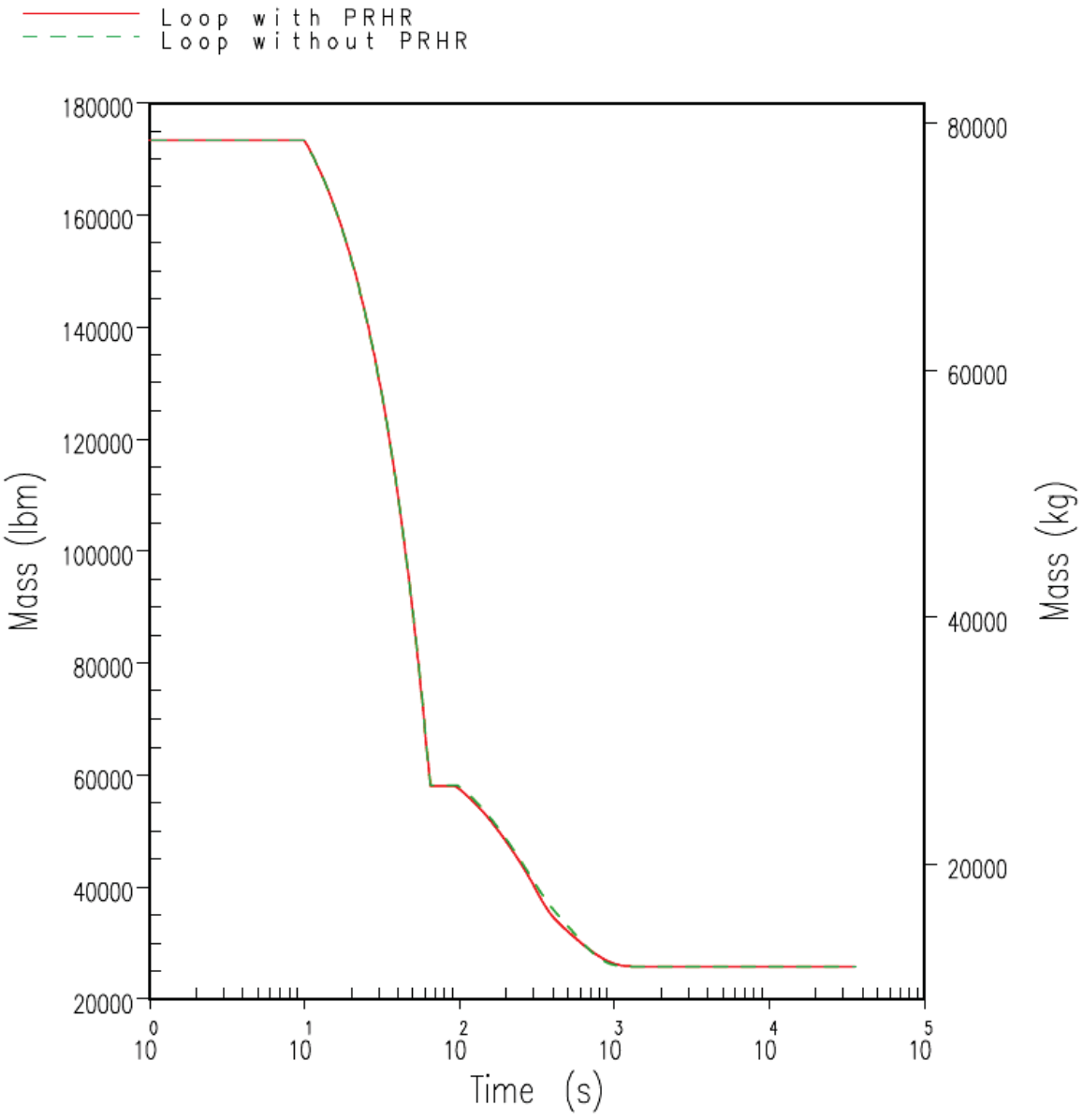


Figure 9.2.7-24. DBA Steam Generator Inventory Transient for Loss of Normal Feedwater with a Consequential Loss of ac Power to the Plant Auxiliaries

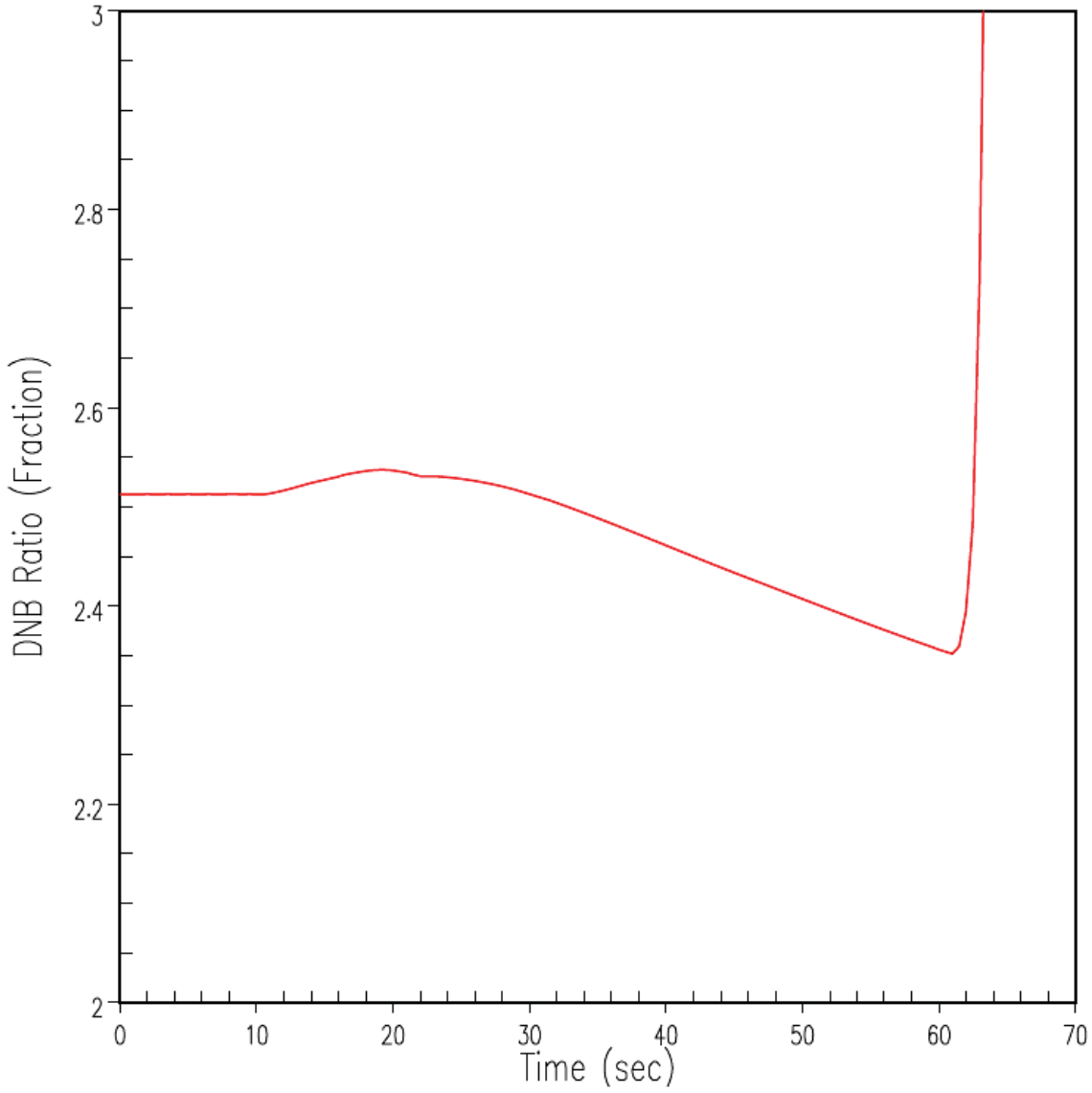


Figure 9.2.7-25. DBA DNB Ratio Transient for Loss of Normal Feedwater with a Consequential Loss of ac Power to the Plant Auxiliaries

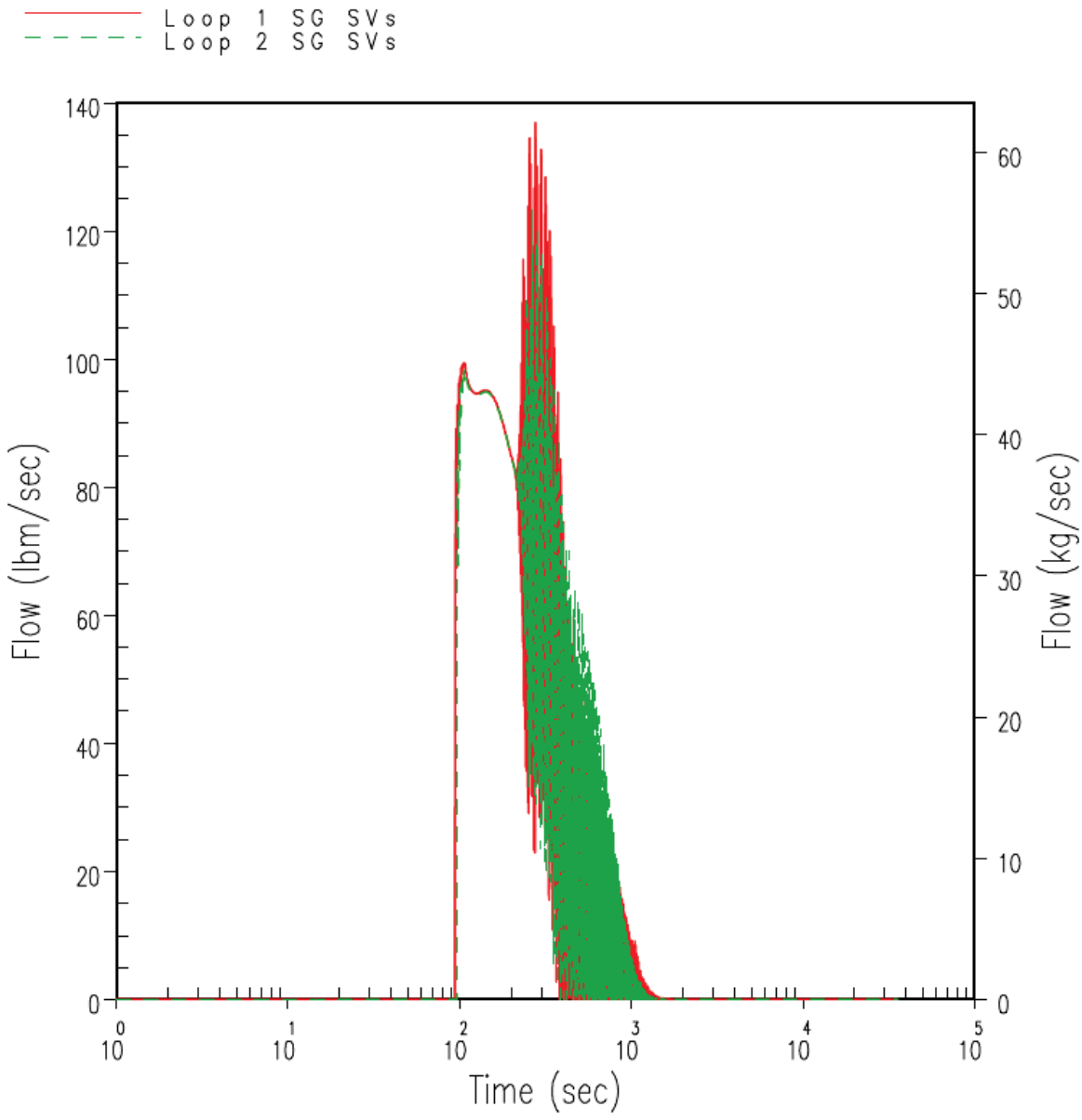


Figure 9.2.7-26. DBA Steam Generator Safety Valve Relief Transient for Loss of Normal Feedwater with a Consequential Loss of ac Power to the Plant Auxiliaries

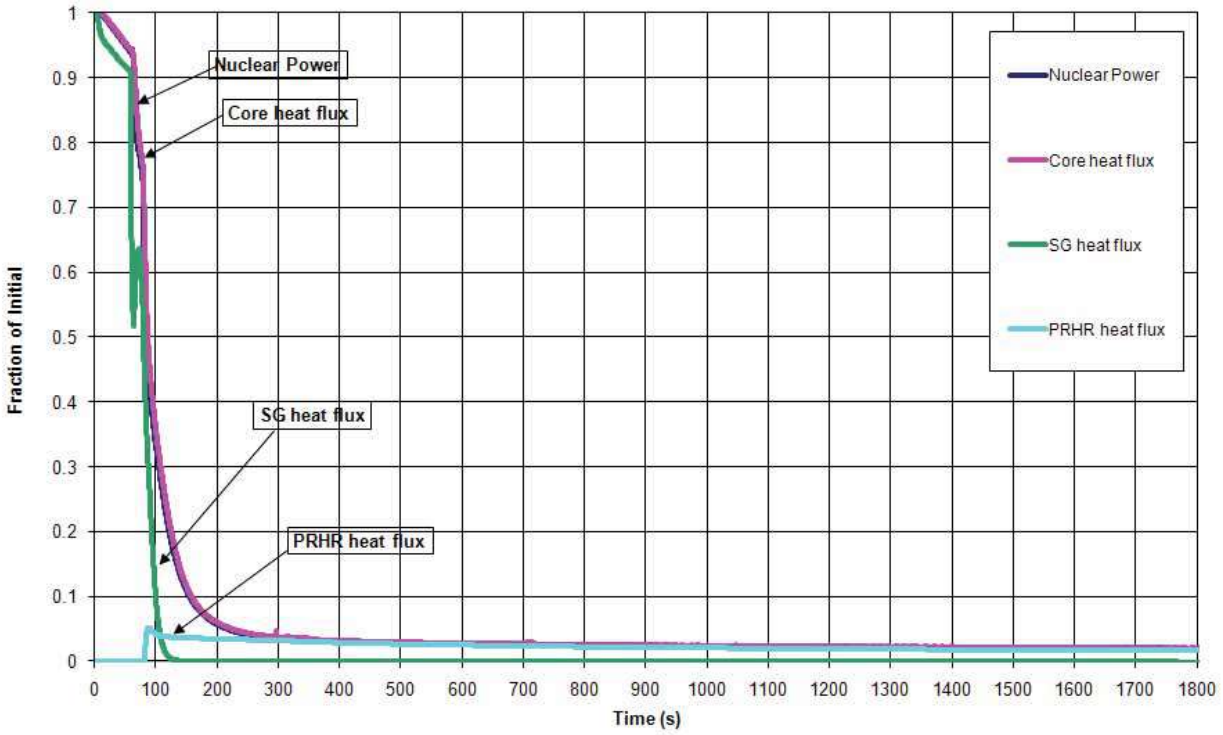


Figure 9.2.7-27. ATWT Power and Heat Transfer for Complete LONF with a RCCA CCF

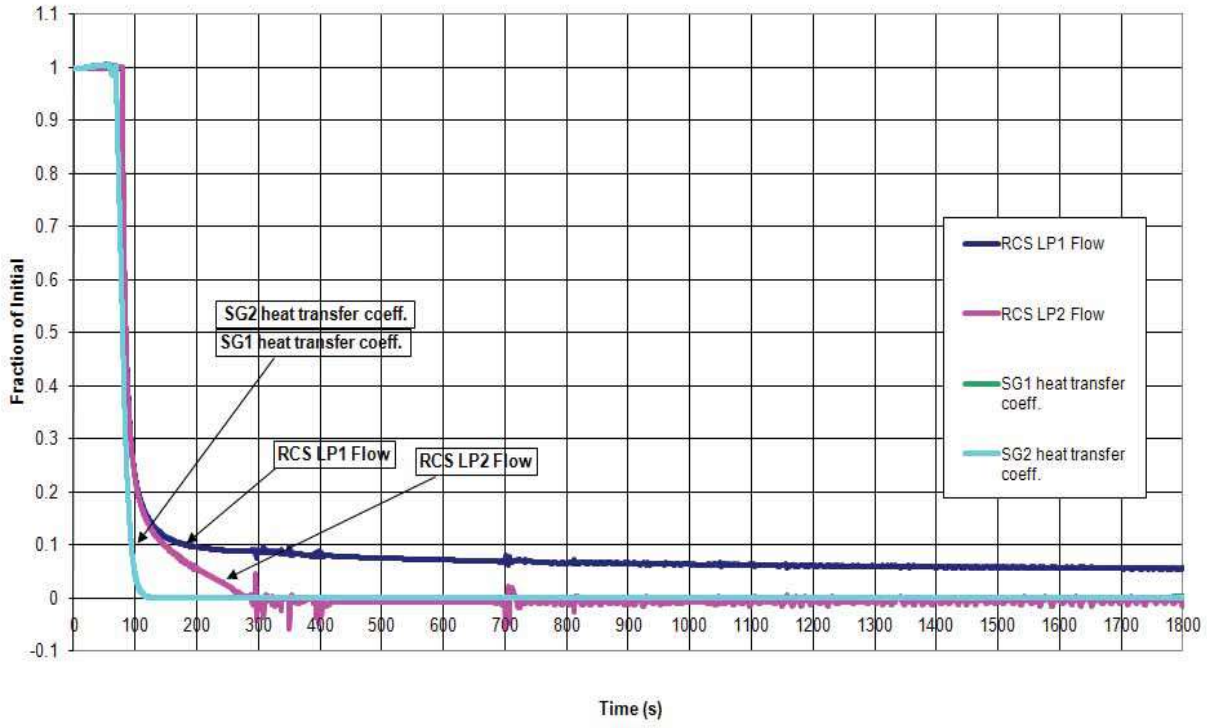


Figure 9.2.7-28. ATWT RCS Volumetric Flow and SG Heat Transfer Coefficients for Complete LONF with a RCCA CCF

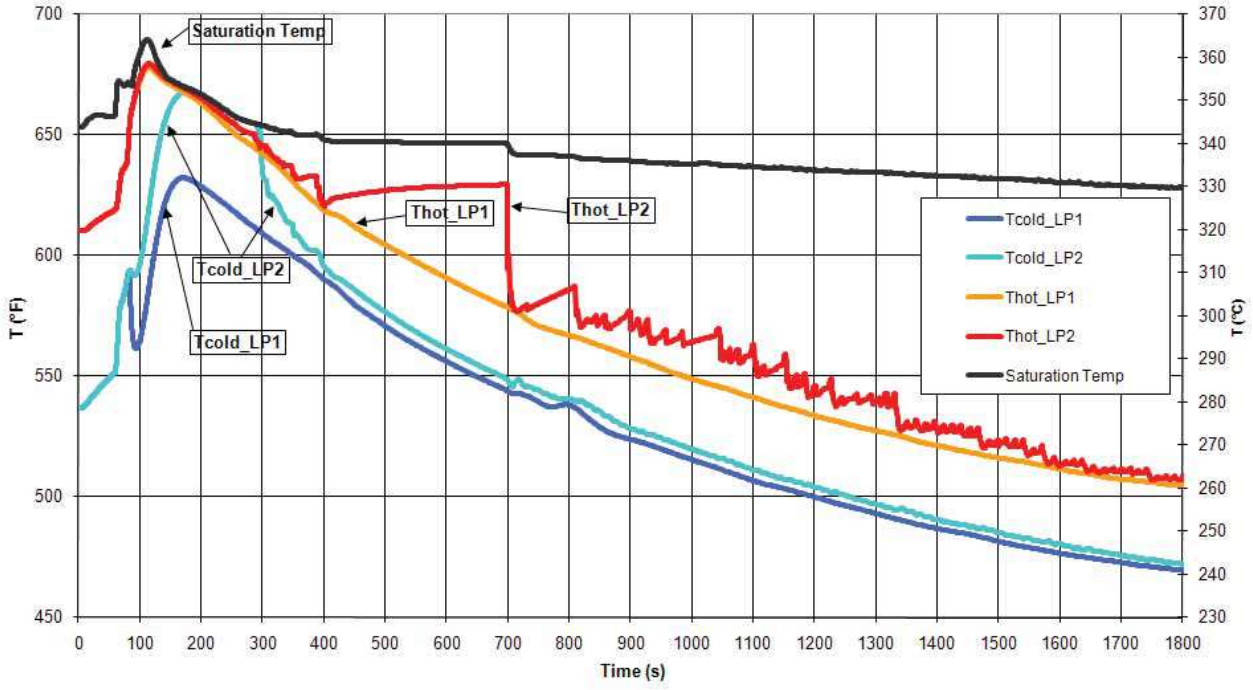


Figure 9.2.7-29. ATWT Primary Loop Temperatures for Complete LONF with a RCCA CCF

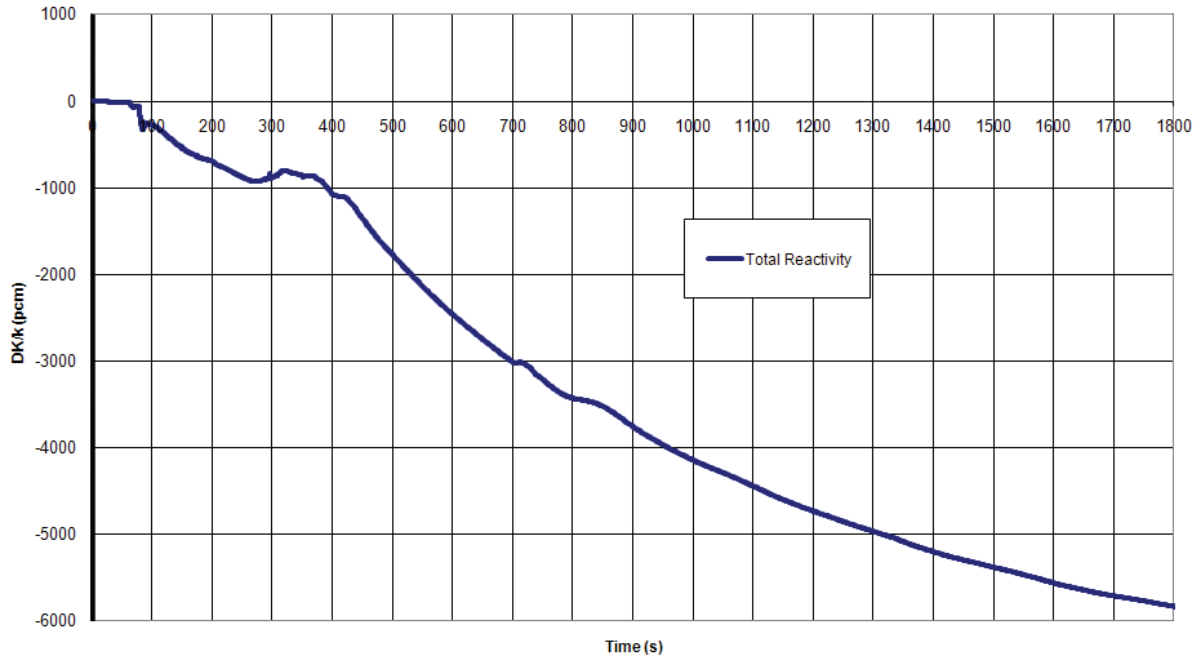


Figure 9.2.7-30. ATWT Core Reactivity for Complete LONF with a RCCA CCF

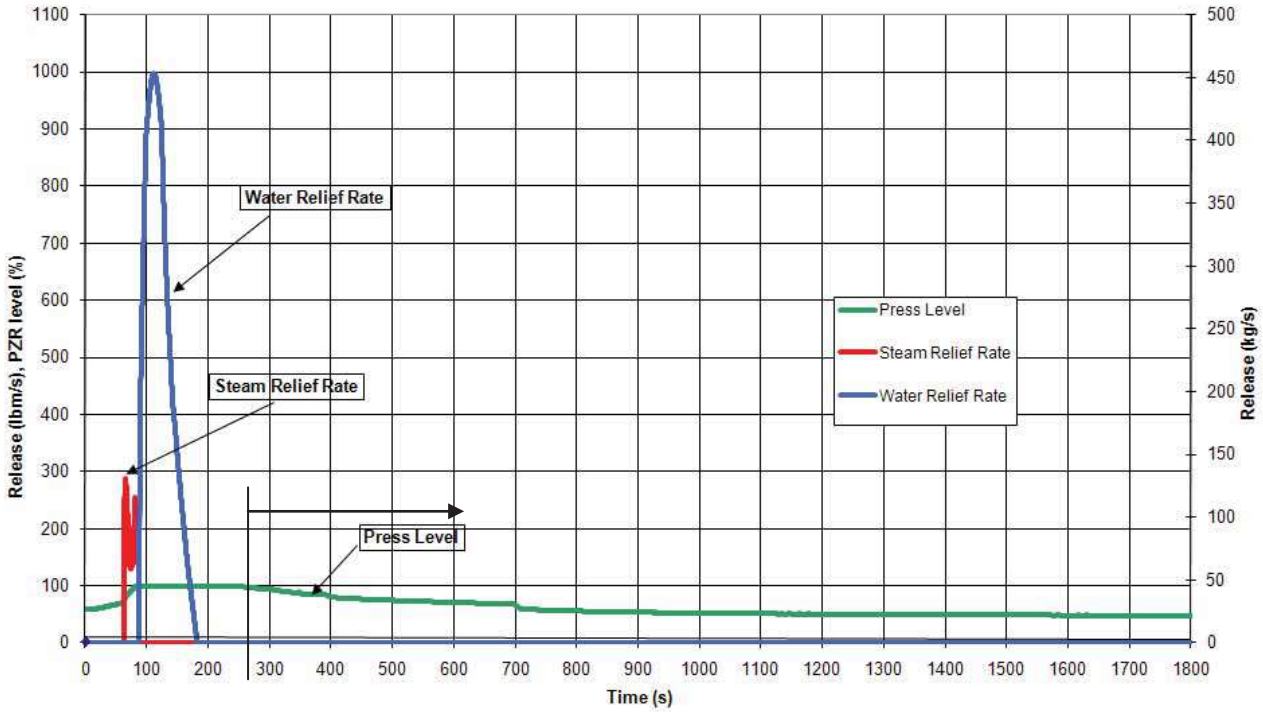


Figure 9.2.7-31. ATWT Pressuriser Level and Safety Valve Relief Rates for Complete LONF with a RCCA CCF

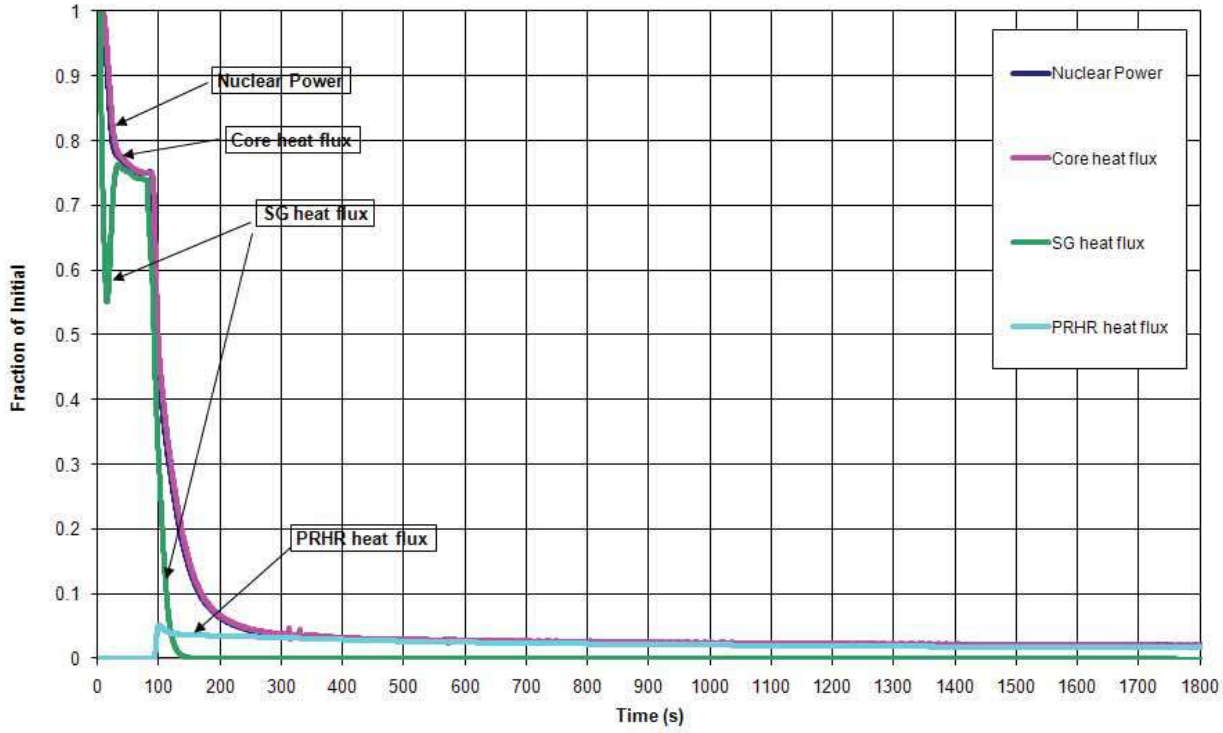


Figure 9.2.7-32. ATWT Primary and Secondary System Pressures for Complete LONF with a RCCA CCF

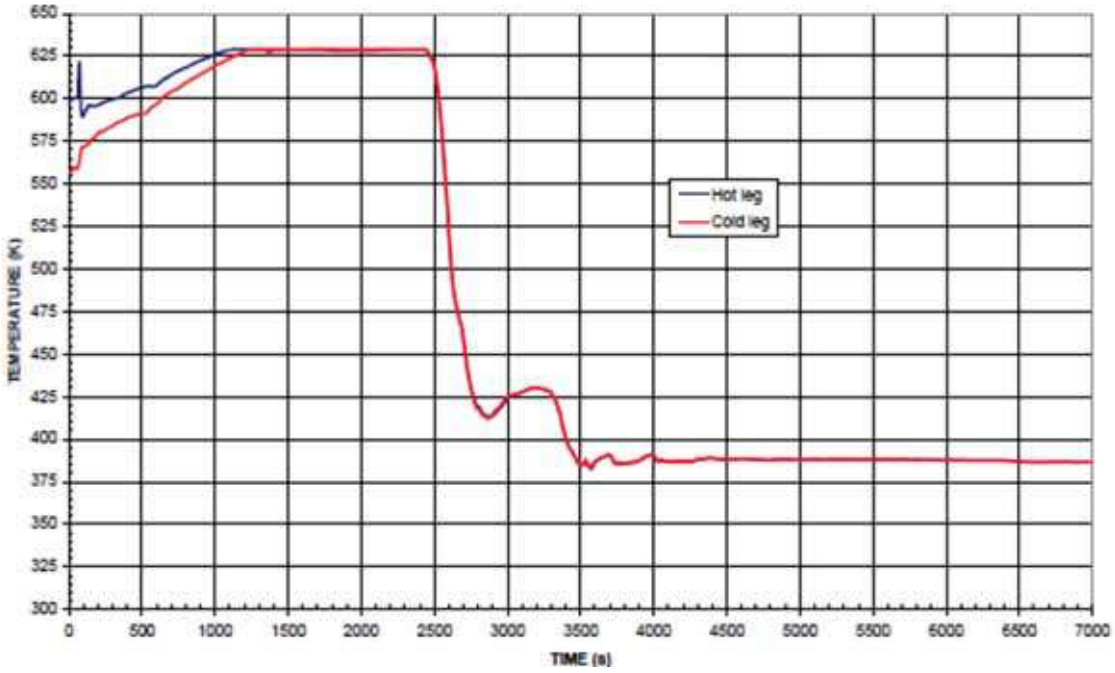


Figure 9.2.7-33 Diverse Core Cooling for LONF, RCS Loop Temperatures

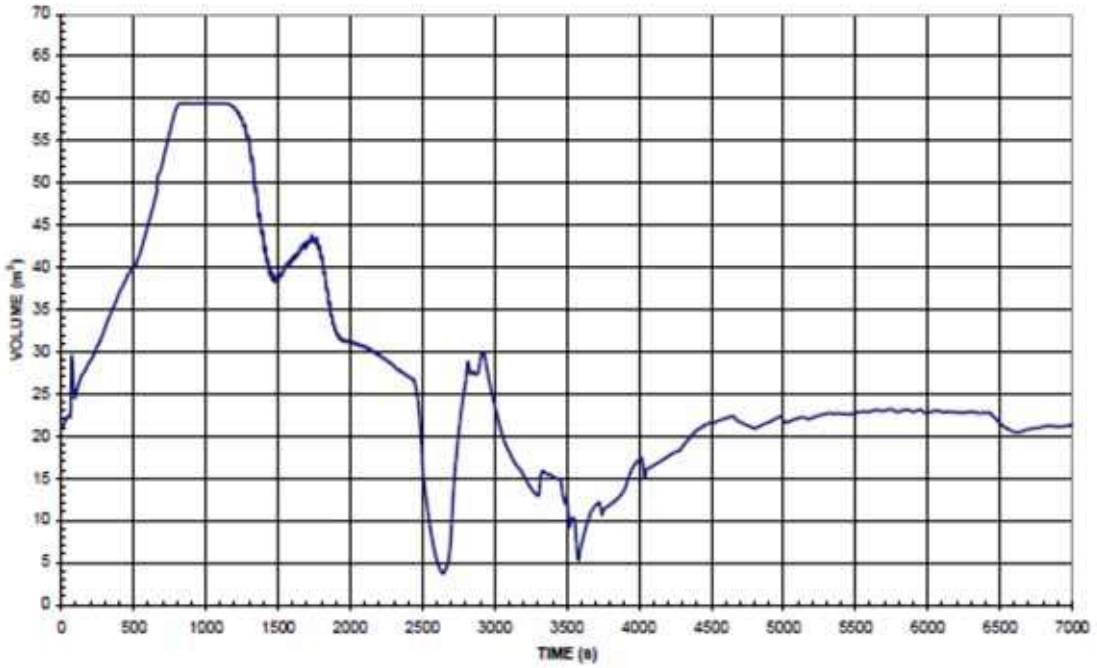


Figure 9.2.7-34. Diverse Core Cooling for LONF, Pressuriser Volume

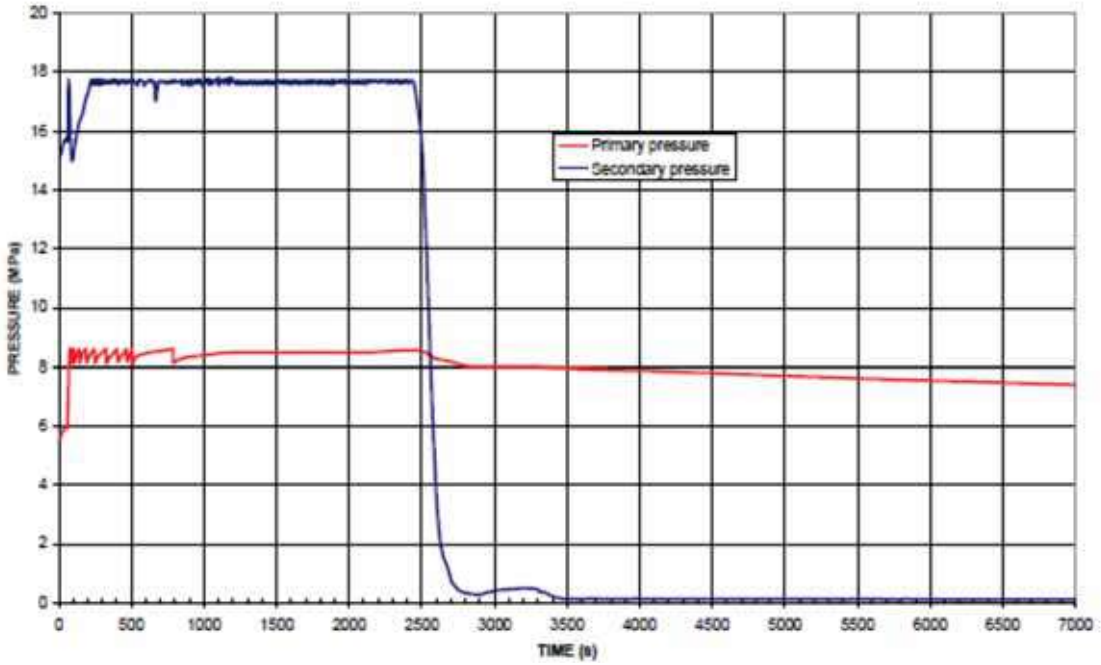


Figure 9.2.7-35. Diverse Core Cooling for LONF, Primary and Secondary Pressures

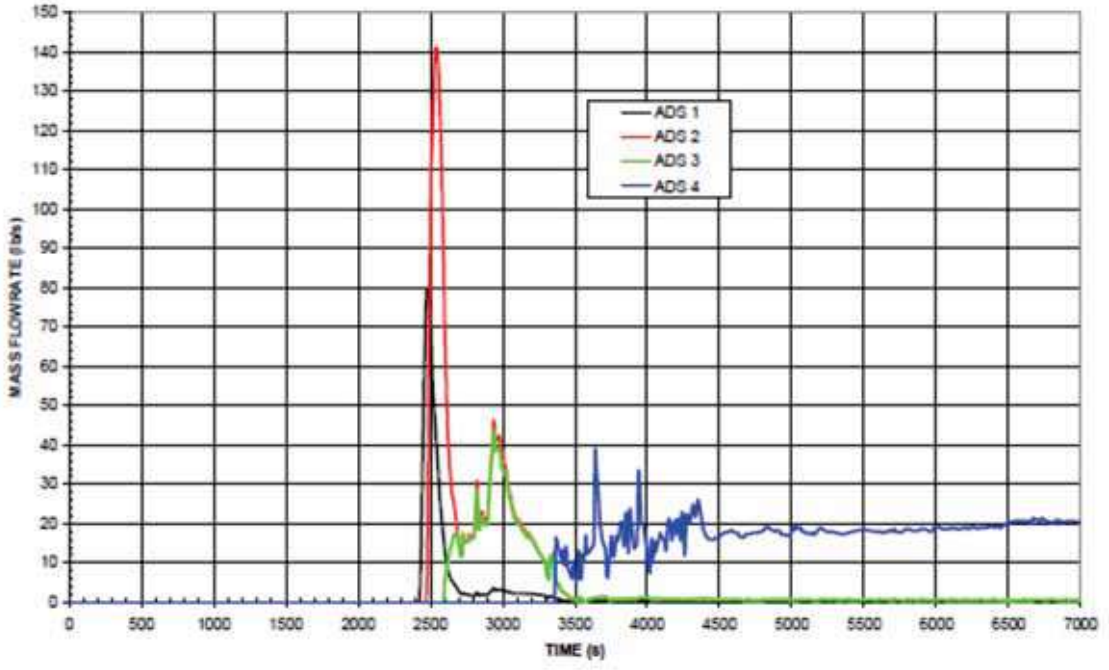


Figure 9.2.7-36. Diverse Core Cooling for LONF, ADS Mass Flow

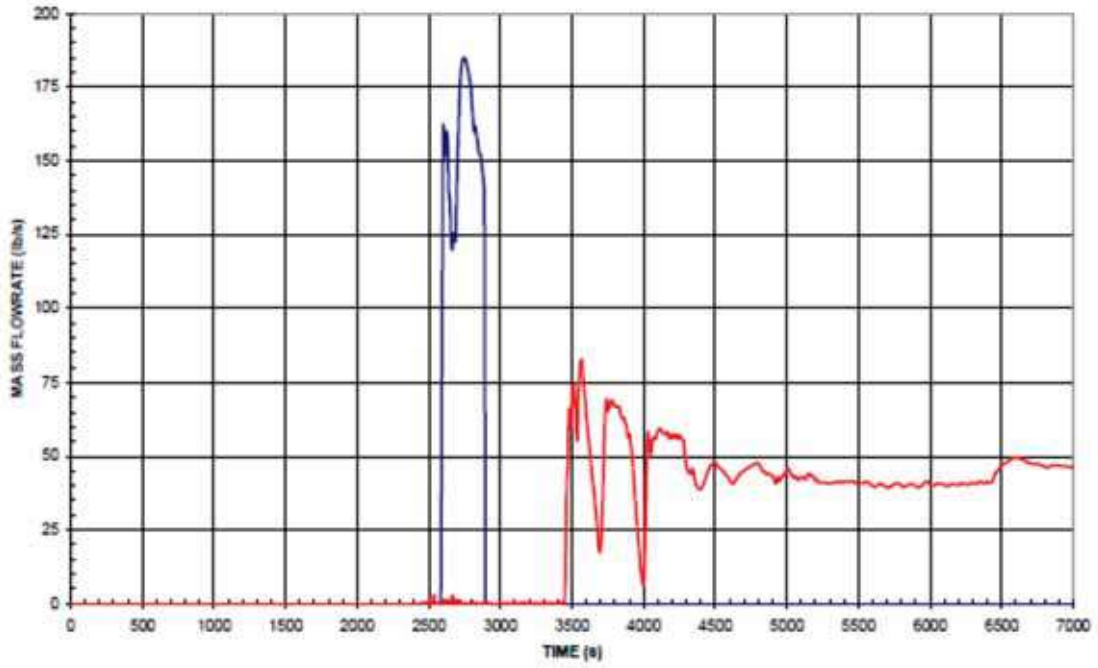


Figure 9.2.7-37. Diverse Core Cooling for LONF, Accumulator and IRWST Mass Flows

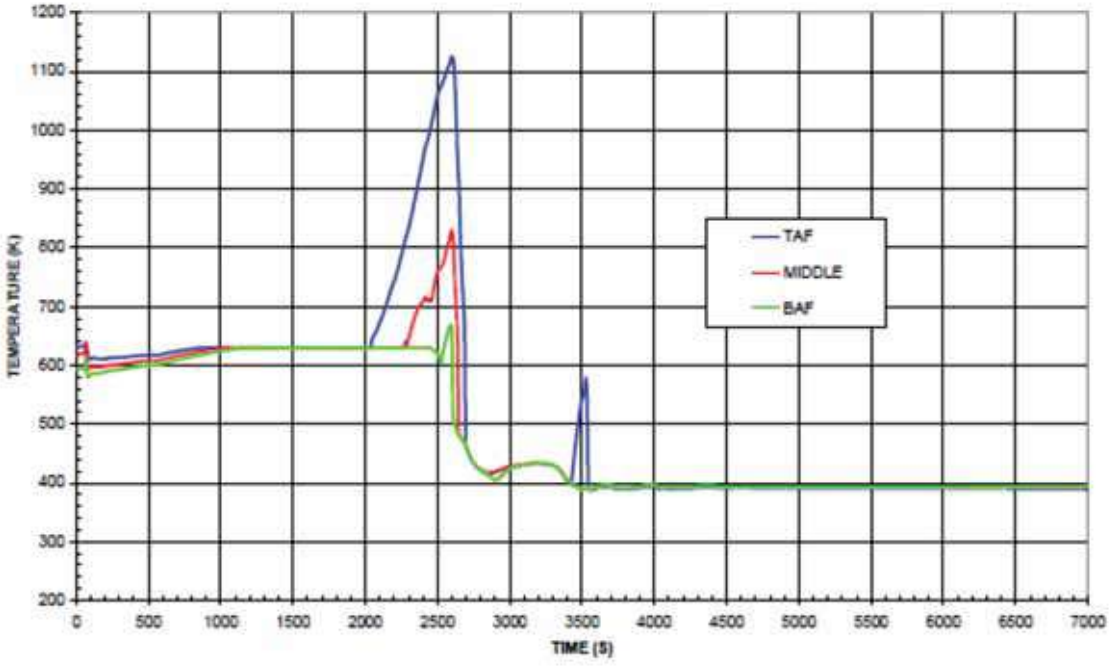


Figure 9.2.7-38. Diverse Core Cooling for LONF, Fuel Clad Temperature (Hot Rod)

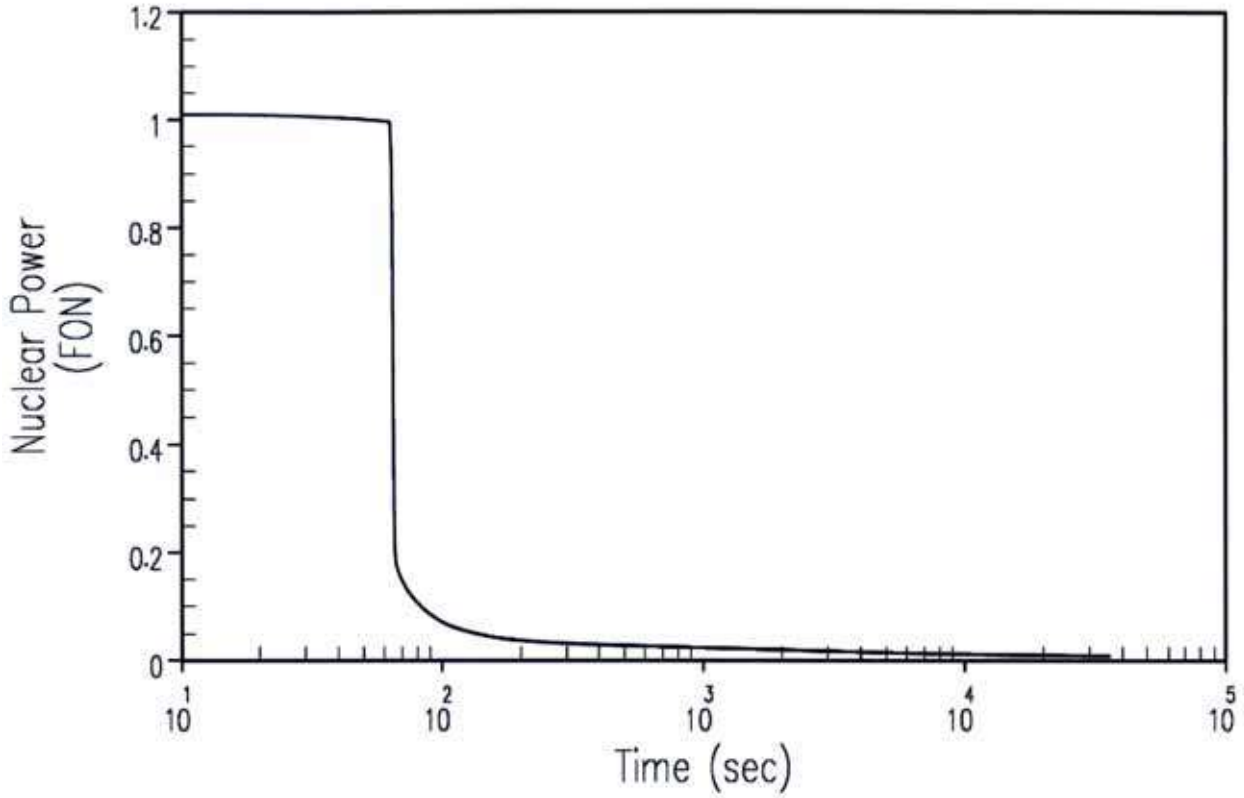


Figure 9.2.8-1. DBA Nuclear Power Transient for Main Feedwater Line Rupture

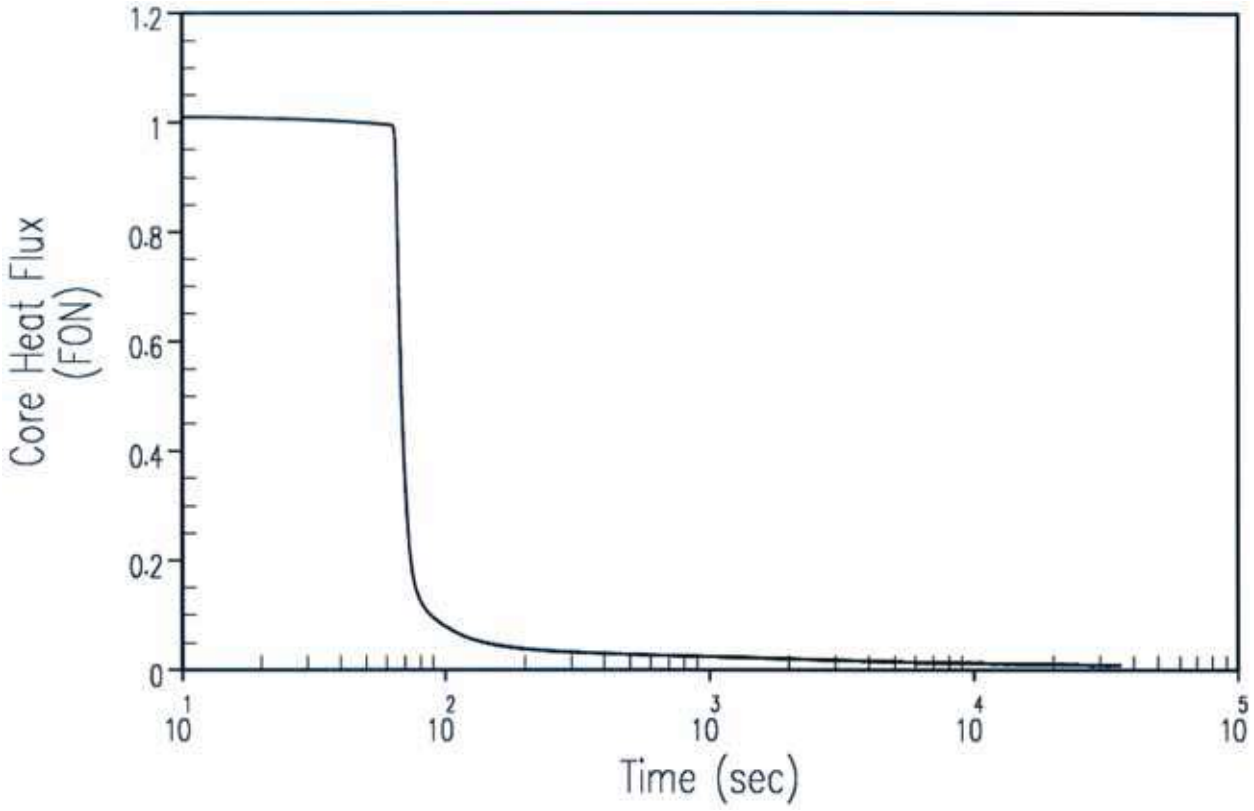


Figure 9.2.8-2. DBA Core Heat Flux Transient for Main Feedwater Line Rupture

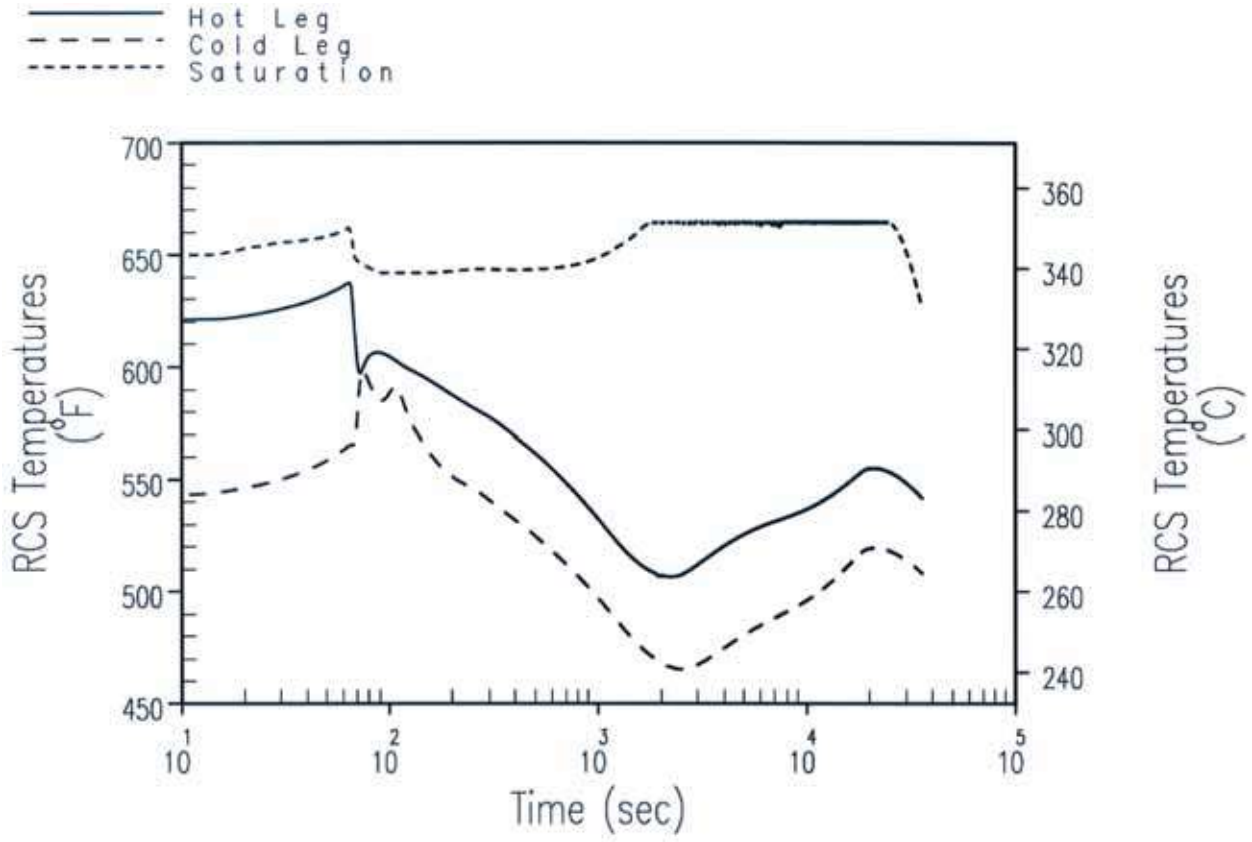


Figure 9.2.8-3. DBA Faulted Loop Reactor Coolant System Temperature Transients for Main Feedwater Line Rupture

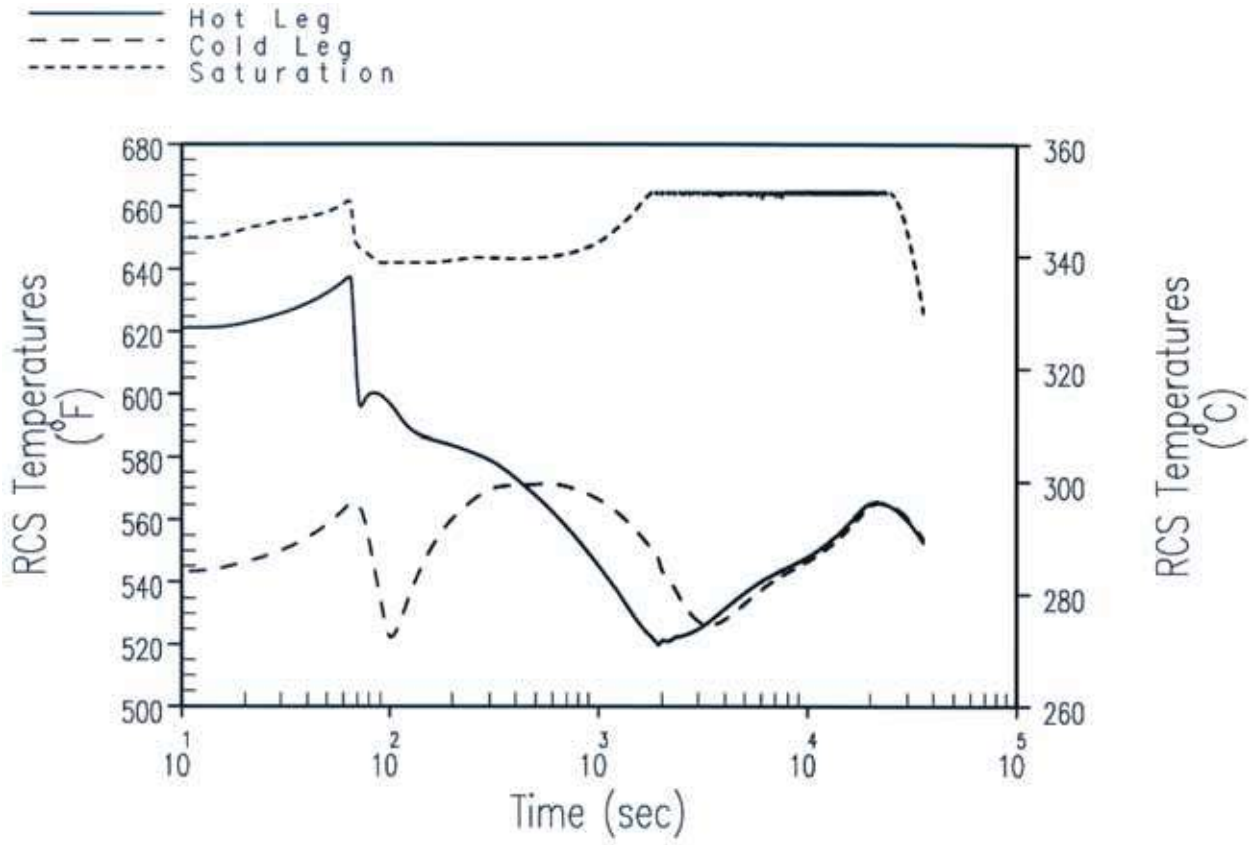


Figure 9.2.8-4. DBA Intact Loop Reactor Coolant System Temperature Transients for Main Feedwater Line Rupture

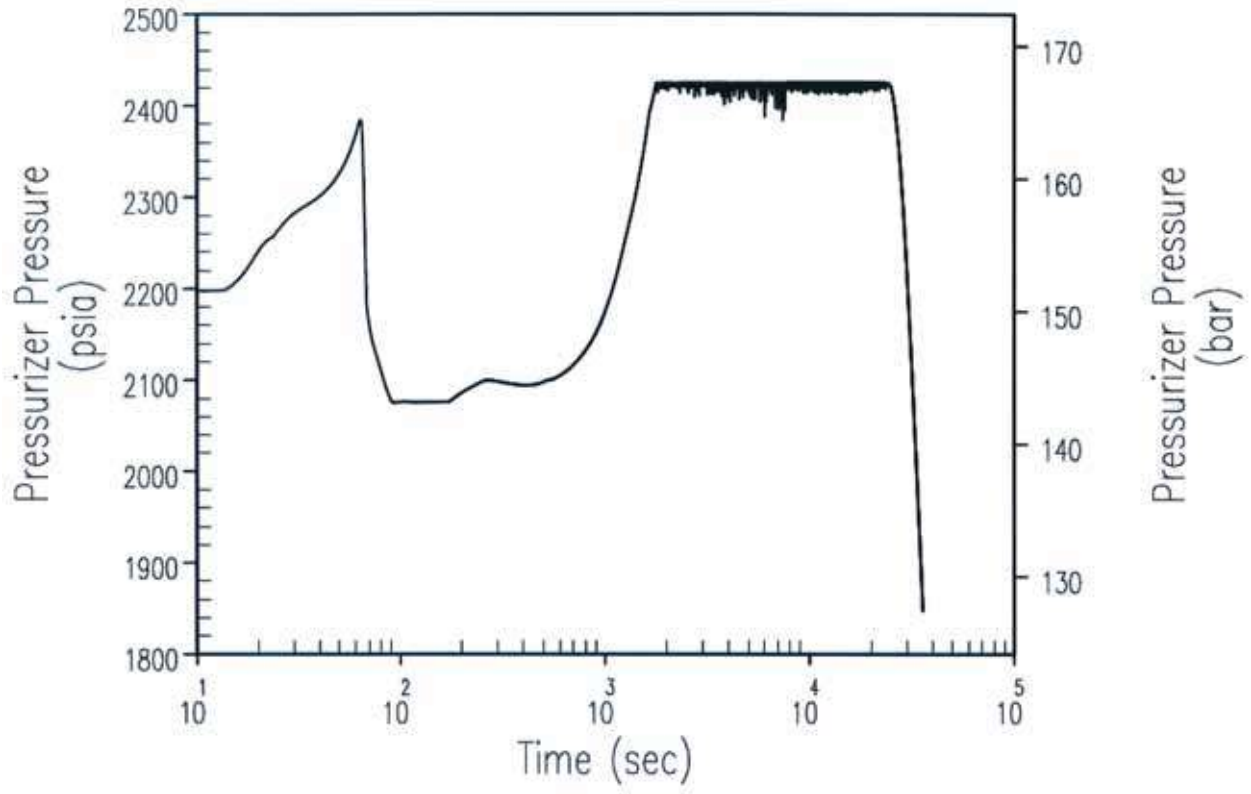


Figure 9.2.8-5. DBA Pressuriser Pressure Transient for Main Feedwater Line Rupture

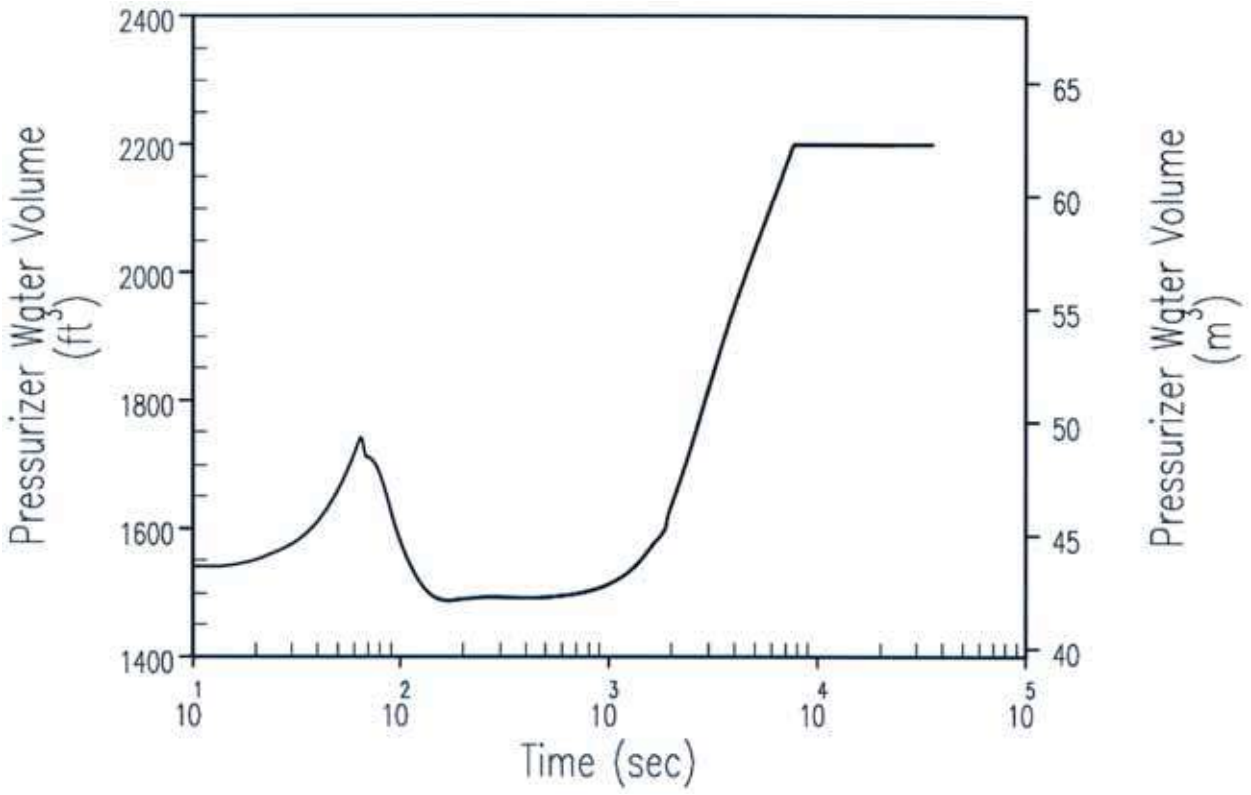


Figure 9.2.8-6. DBA Pressuriser Water Volume Transient for Main Feedwater Line Rupture

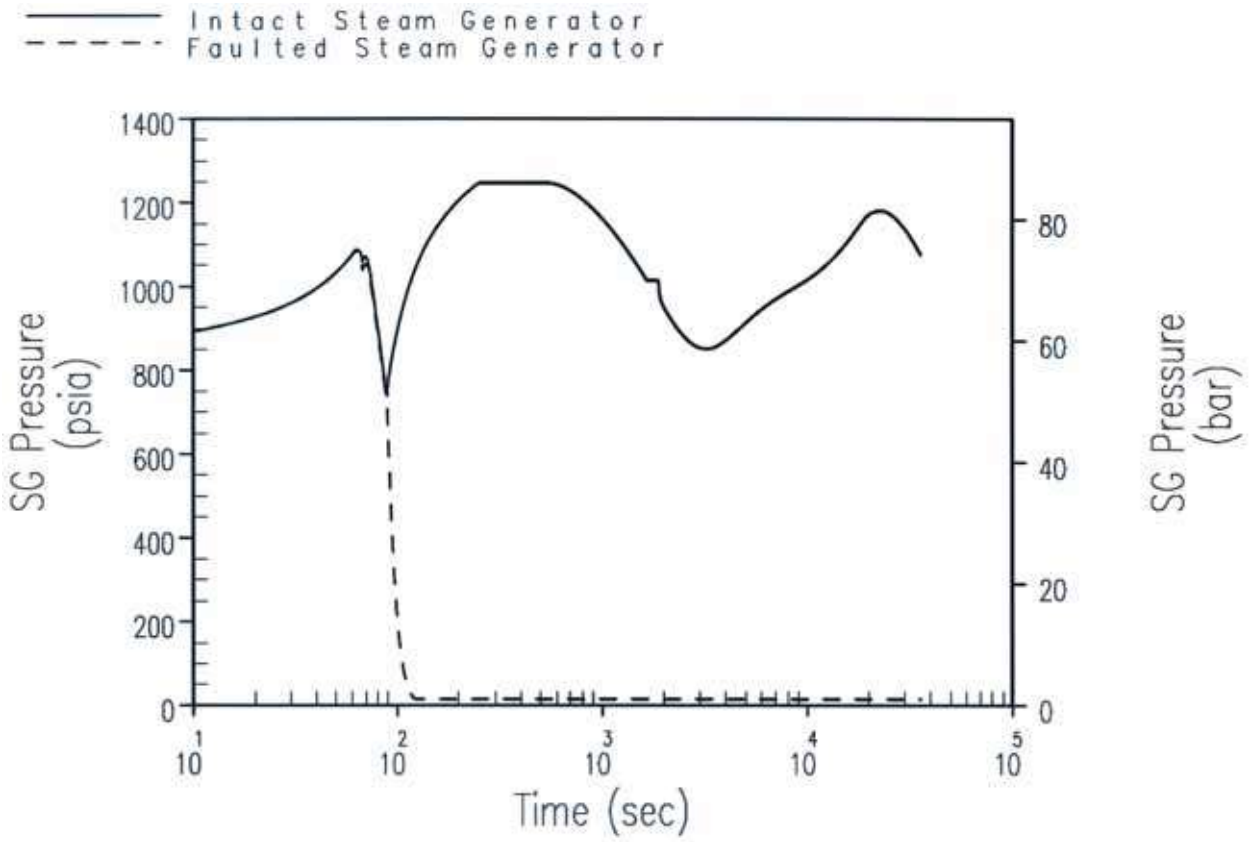


Figure 9.2.8-7. DBA Steam Generator Pressure Transient for Main Feedwater Line Rupture

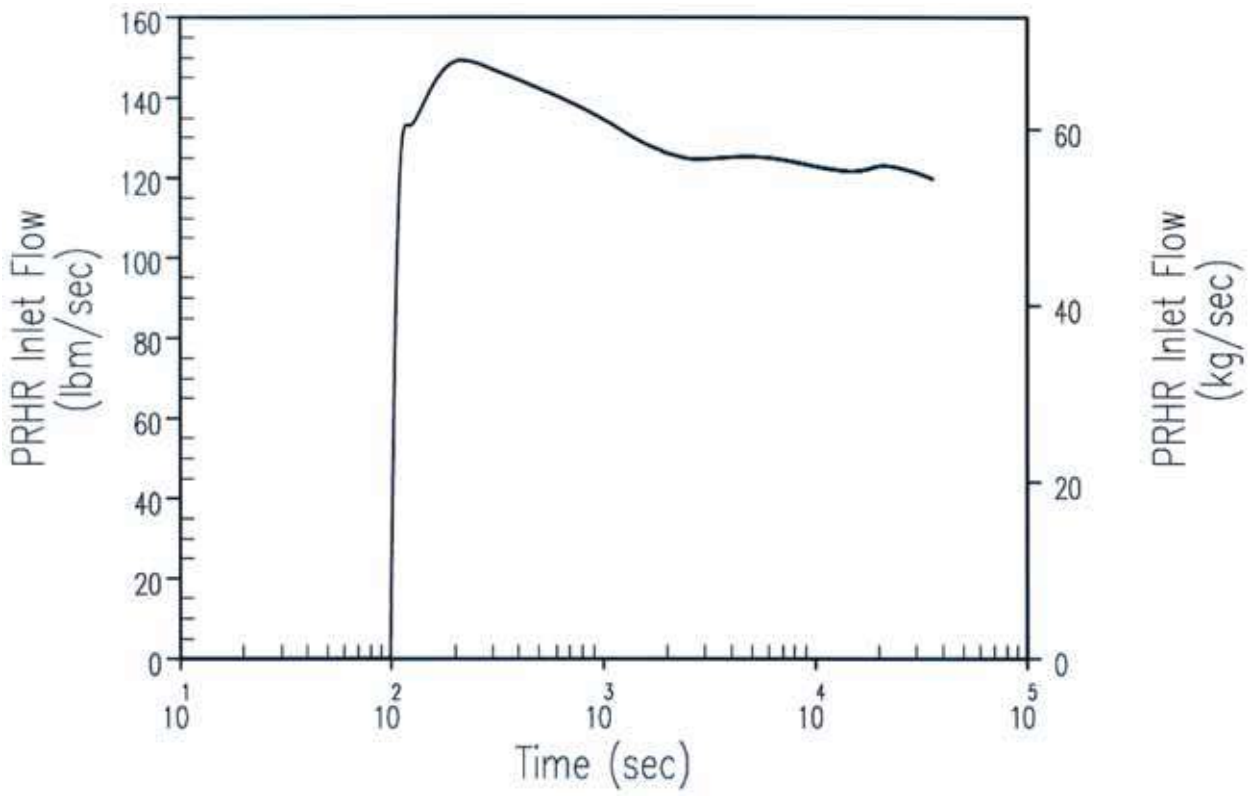


Figure 9.2.8-8. DBA PRHR Flow Rate Transient for Main Feedwater Line Rupture

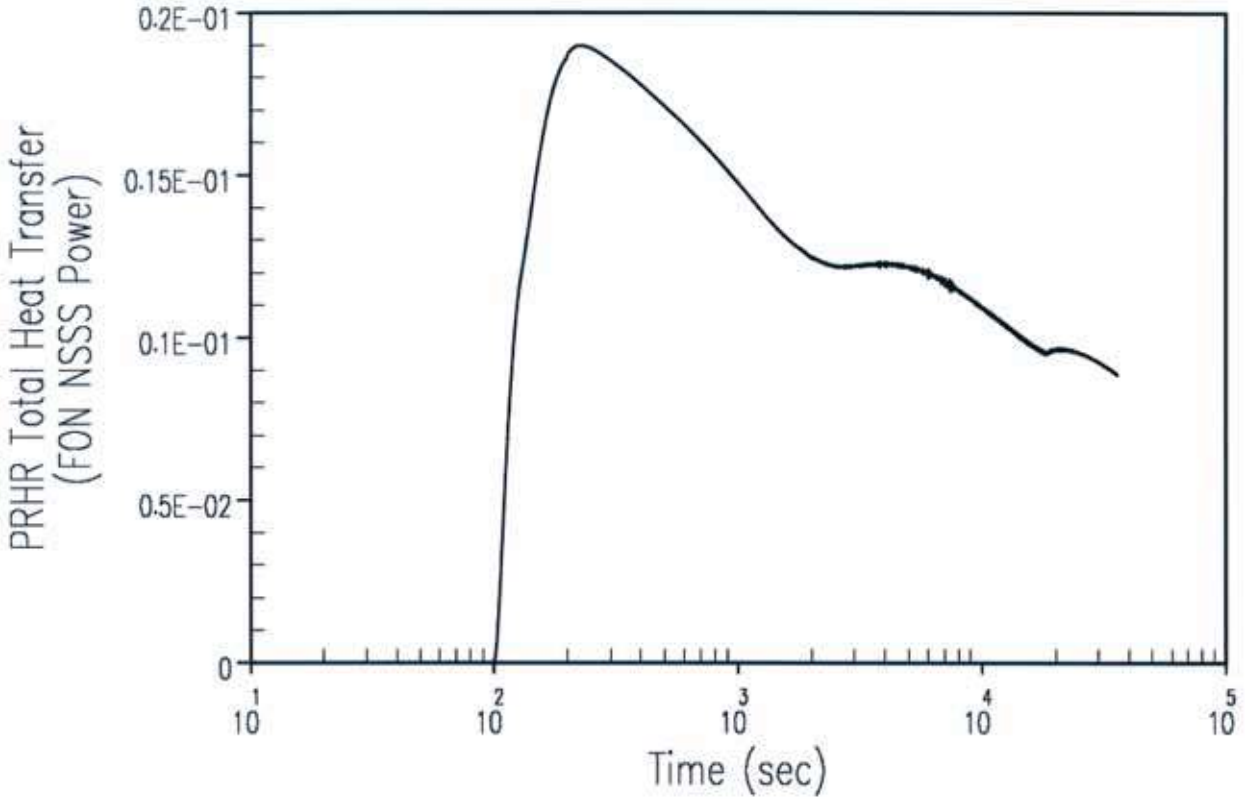


Figure 9.2.8-9. DBA PRHR Heat Flux Transient for Main Feedwater Line Rupture

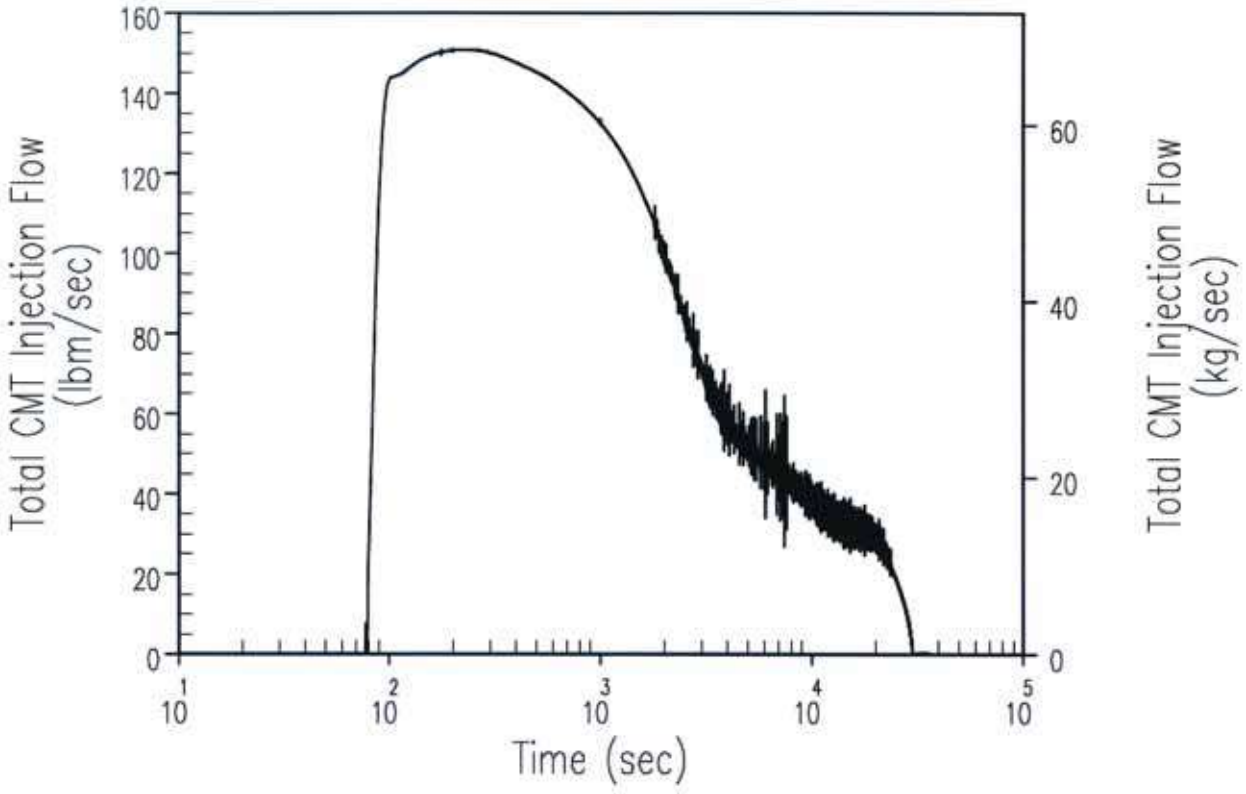


Figure 9.2.8-10. DBA CMT Injection Flow Rate Transient for Main Feedwater Line Rupture

9.3 Decrease in Reactor Coolant System Flow Rate

A number of faults that could result in a decrease in the reactor coolant system flow rate are postulated. The events are discussed in this section. Detailed analyses are presented for the most limiting of the RCS flow decrease events.

9.3.0 Introduction and Overview of the Faults

Decrease in reactor coolant flow as a consequence of RCP failure can be caused by a number of initiating faults that are split into two parts:

- Loss of forced reactor coolant flow (excluding major mechanical pump failure)
    - Partial loss of flow (PLOF)
        - Failure of power supply to the RCP
        - Random failure of pump variable speed controller
        - Flow blockage
        - Pump cavitation during start-up
        - Partial loss of forced reactor coolant flow – maintenance or operator error
    - Complete loss of flow (CLOF)
        - Complete loss of forced reactor coolant flow - maintenance or operator error
        - Common cause failure of pumps – loss of electrical supply
        - Common cause failure of pump bearings due to gas build-up during start-up
        - Loss of component cooling water to RCS pumps either directly, due to operator error or mechanical failure or, indirectly, due to the loss of service water
- Major mechanical failure of a single RCP
    - Pump rotor impinges on stationary member and completely seizes
    - Pump shaft break due to corrosion/pre-existing defect

The behaviour of faults involving a major mechanical failure of a single RCP differs somewhat from the other loss of forced reactor coolant flow faults, because the pump that suffers the major mechanical failure will not coast down. These faults are therefore considered separately.

Reference 9.3-12 lists loss of forced reactor coolant flow (excluding major mechanical pump failure) as a frequent fault based on the frequency of these events being greater than 1E-3/yr. A frequent fault should demonstrate that diverse mitigation is provided. Sections 9.3.1.3 and 9.3.2.3 present the diverse mitigation features for the partial and complete loss of forced reactor coolant flow events and the analyses that demonstrate that the diverse mitigation is adequate for these frequent faults.

A major mechanical failure of a single RCP has an event frequency less than 1E-4/yr (Table 8A-2). This does not qualify as a frequent fault or a cliff edge fault (faults not sufficiently lower than 1E-3/yr as defined in Reference 9.3-12); therefore a diverse safety case is not assessed. This is considered an infrequent event.

Section 9.3 considers these faults in turn. Each fault is first described; the initial event frequency and the design basis class are provided and the bounding fault or faults are identified (if needed). The analysed faults are presented individually in Table 8A-2.

The analysed fault(s) are described in additional detail in the subsequent sections to complete the safety case for each fault, including:

- Identification of Causes and Accident Description
- Design Basis Analysis of Effects and Consequences
- Assessment of the Radiological Consequences for the DBA
- Diverse Mitigation and ATWT for Frequent Faults
- ALARP Assessment
- Conclusions

ATWT analyses presented herein are based on Reference 9.3-10.

9.3.0.1 Loss of Forced Reactor Flow (Excluding Major Mechanical Pump Failure)

Description

There are a number of faults in which reactor coolant flow is lost when one or more RCP coasts down as a result of one of the following pump failures (see also Sections 9.3.1.1 and 9.3.2.1):

- Mechanical failure of a pump[1]
- Electrical failure of a pump
- Loss of power supply to one or more pumps
- Loss of component cooling water to one or more pumps, which causes a pump trip

The loss of forced reactor coolant flow is considered a complete loss of all reactor coolant flow if all four pumps are affected (Fault 1.13.1a) or a partial loss of reactor coolant flow if less than four of the pumps are affected (Fault 1.13.1).

Separate analyses for the complete and partial loss of reactor coolant flow events determine the adequacy of the primary reactor trip setpoints. The complete and partial loss of reactor coolant flow events are analysed individually since there are different PMS reactor trip sensors considered for each event. For the loss of reactor coolant flow events, the low primary coolant flow reactor trip signal and the reactor coolant pump under-speed reactor trip signal can be used to mitigate the transient.

The reactor trip on RCP under-speed is also provided to trip the reactor for an under-frequency condition (i.e., a frequency decay) resulting from frequency disturbances on the power grid. This trip protects the core from under-frequency events if the grid frequency decay rate is less than approximately 5 Hz/s. As part of the resolution to GI-AP1000-FS-03, a complete loss of flow case following an electrical grid frequency perturbation (not only a constant frequency decay) was specifically analysed (Reference 9.3-4). This case is discussed further in Section 9.3.2.

The reactor trip on low primary coolant loop flow is provided to protect against loss of flow conditions that affect only one or two reactor coolant loop cold legs. This function is generated by two-out-of-four, low-flow signals per reactor coolant loop hot leg. Above permissive P10, low flow in either hot leg actuates a reactor trip. Additionally, this trip function would also protect the

[1] Includes initiating events arising from maintenance or operator errors.

core from an under-frequency condition if the grid frequency decay rate is less than approximately 5 Hz/s.

The partial loss of forced reactor coolant flow is discussed in more detail in Section 9.3.1. Section 9.3.2 describes the complete loss of forced reactor coolant flow in more detail.

Initiating Event Frequency[2]

The AP1000 plant PSA gives the IEF for the failure of power supply to the RCPs as 1.7E-2/yr (Table 8A-2). This frequency includes a number of initiating events potentially resulting in a loss of flow; the loss of flow fault also covers other faults with comparable probabilities, such as a loss of component cooling (which would also lead to a consequential loss of flow). This is considered to be a frequent fault.

Design Basis Class

The unmitigated consequences of a loss of reactor coolant flow are assumed to be greater than the Target 4 BSL for frequent faults (1 mSv offsite and 20 mSv onsite). Given the IEF above, the event is in the DB2 class.

9.3.0.2 Major Mechanical Failure of a Single Reactor Coolant Pump

Description

There are two faults that can cause a major mechanical failure of single RCP, causing a decrease in RCS flow rate (see also Sections 9.3.3.1 and 9.3.4.1):

- RCP impeller seizure (locked rotor) (Fault 1.13.11)
- RCP shaft break (or coupling failure) (Fault 1.13.12)

For both faults, there is no inertial coastdown of the affected pump, so flow through the single affected reactor coolant loop is rapidly reduced. The reactor trip would occur on a low-flow signal in the affected loop. The initial rate of reduction of reactor coolant flow is greater for the RCP rotor seizure event. However for a RCP shaft break event, the impeller is free to spin in the reverse direction; this results in a lower or negative flow in the reactor coolant loop later in the transient. The locked rotor transient analysis is done conservatively such that it bounds the RCP shaft break event.

The RCP locked rotor event is discussed in more detail in Section 9.3.3. Section 9.3.4 provides a brief discussion on the RCP shaft break event.

[2] As discussed in Chapter 8, the frequency for initiating events from the PSA is used in both Chapters 8 and 9 with the sole purpose of supporting the categorisation of the fault to a specific DB category. As noted in Chapter 8, these probabilities should not be considered to be representative of actual frequency of the events, and for several events they can be significantly conservative. Detailed PSA results and their basis are discussed in Chapter 10.

Initiating Event Frequency[3]

Each RCP mechanical failure fault is classified as having a frequency <1.0E-04/yr (Table 8A-2). The summed frequency is therefore <2.0E-04/yr, which makes the fault an infrequent fault.

Design Basis Class

The unmitigated consequences of the major mechanical failure of an RCP are assumed to be greater than the Target 4 BSL for frequent faults (1 mSv offsite and 20 mSv onsite). Given the IEF above, the event is in the DB1 class.

9.3.1 Partial Loss of Forced Reactor Coolant Flow (Fault 1.13.1)

9.3.1.1 Identification of Causes and Accident Description

A partial loss of coolant flow accident can result from a mechanical or an electrical failure of a reactor coolant pump or from a fault in the power supply to the pump or pumps. If the reactor is at power at the time of the event, the immediate effect of the loss of coolant flow is a rapid increase in the coolant temperature. For the AP1000 plant design, there are two potential partial loss of flow scenarios. These scenarios include the coast down of one reactor coolant pump and the coast down of two reactor coolant pumps in diametrically opposite loops. Although both scenarios are analysed, the loss of two reactor coolant pumps bounds the loss of one pump since it results in a more severe flow coast down. Thus, the two pump partial loss of flow is used as the basis for the discussion within this section.

Normal power for the pumps is supplied through four busses connected to the generator. When a generator trip occurs, the busses are supplied from offsite power and the pumps continue to operate.

Protection against this event is provided by the Low-2 primary coolant flow reactor trip signal, which is actuated by two-out-of-four low-flow signals. Above permissive P10, Low-2 flow in either hot leg actuates a reactor trip (see Section 19.2).

The effects of a loss of offsite power are considered in evaluating partial loss of forced reactor coolant flow transients. As discussed in Section 9.0.12, the loss of offsite power is considered to be a potential consequence of the event due to disruption of the electrical grid following a turbine trip during the event. A delay of 3 seconds is assumed between the turbine trip and the loss of offsite power. In addition, turbine trip occurs 5 seconds following a reactor trip condition being reached. This delay on turbine trip is a feature of the AP1000 reactor trip system. The primary effect of the loss of offsite power is to cause the remaining operating reactor coolant pumps to coast down. However, since the loss of offsite power would occur no earlier than 8 seconds into the event, it is well beyond the critical time frame of interest for the partial loss of flow events (i.e., time of rod insertion). Thus, it is not explicitly modelled in the analysis.

[3] As discussed in Chapter 8, the frequency for initiating events from the PSA is used in both Chapters 8 and 9 with the sole purpose of supporting the categorization of the fault to a specific DB category. As noted in Chapter 8, these probabilities should not be considered to be representative of actual frequency of the events, and for several events they can be significantly conservative. Detailed PSA results and their basis are discussed in Chapter 10.

9.3.1.2 Design Basis Mitigation

Analysis is performed to demonstrate the adequacy of the PMS to detect and mitigate the fault and show that the safety analysis criteria are satisfied including:

- No fuel failures (confirmed using minimum DNBR),
- The RCS pressure criterion is met,
- The MSS pressure criterion is met, and
- The pressuriser does not fill (which could result in a LOCA)

It is noted that this event is bounded by the Section 9.2.3 analysis with respect to RCS/MSS pressure criteria, therefore, these limits are not explicitly confirmed for this event. Also, pressuriser filling is not challenged for this event and is not explicitly confirmed.

9.3.1.2.1 DBA Method of Analysis

This transient is analysed using three computer codes. First, the LOFTRAN code (References 9.3-1 and 9.3-8) is used to calculate the core flow during the transient based on the input loop flows, the nuclear power transient, and the primary system pressure and temperature transients. The FACTRAN code (Reference 9.3-2) or the VIPRE-01 fuel rod model (Reference 9.3-7), which is equivalent to FACTRAN, is then used to calculate the heat flux transient based on the nuclear power and flow from LOFTRAN. Finally, the VIPRE-01 code is used to calculate the DNBR during the transient, based on the heat flux from FACTRAN and the flow from LOFTRAN (or directly from LOFTRAN statepoints if the the transient VIPRE-01 method is used). The calculated DNBR transient represents the minimum of the typical cell or the thimble cell. The objective of the analysis is to demonstrate that the DNBR criterion is met.

Initial Conditions

Initial reactor power, pressuriser pressure, and reactor coolant system temperature are assumed to be at their nominal values. Uncertainties in initial conditions are statistically accounted for in the DNBR limit, as described in WCAP-11397-P-A (Reference 9.3-5).

Plant characteristics and initial conditions assumed in this analysis are further discussed in Section 9.0.2.

A loss of forced reactor coolant flow at full power produces the greatest heat-up in the reactor core, placing the greatest demand on the protection systems and minimising the DNBR. Therefore, the partial loss of reactor coolant flow event during Mode 1 option at full power is the limiting condition.

Reactivity Coefficients

The reactivity feedback parameters are chosen to maximize the energy transferred to the primary coolant during the flow coastdown. A most-negative Doppler-only power coefficient (see Figure 9.0-3) is applied to maximize the positive reactivity addition during the reactor trip and rod motion, which acts to slow the rate of power reduction; the equivalent total integrated Doppler reactivity from 0 to 100-percent power is 0.016 Δk. As there is an initial heatup due to the reduction in RCS flow, a least-negative (minimum feedback) moderator temperature coefficient is most conservative. Therefore, a constant moderator density coefficient of 0.0 $\Delta k/g/cc$ is modelled. Finally, a curve of trip reactivity versus time based on a 2.7-second rod cluster control assembly insertion time to the dashpot is applied (see Section 9.0.6).

Flow Coastdowns

Conservative flow coastdowns are used to simulate the transient. The flow coastdowns are calculated externally to the LOFTRAN code using the COAST computer code which is described in Section 9.0.9.5.

9.3.1.2.2 DBA Credited SSCs

For the DB, all of the claimed SSCs are Class 1. The claimed Class 1 SSCs are listed in Table 9.0-10. The presented DBA ends shortly after reactor trip; however, essential safety functions for the long term safe shutdown analysis (Appendix 9C) bound safe shutdown response for this event. The diverse core cooling is provided by the PRHR and passive containment cooling. Other SSCs include the CMTs, containment isolation, and pressuriser SVs. The PMS provides the following:

- RT on Low-2 RCS flow, one out of two loops
- PRHR actuation on Low-2 SG NR level coincident with Low-2 SFW flow
- CMTs and containment isolation on Low-2 CL temperature
- PCS on High-2 containment pressure

9.3.1.2.3 DBA Results

The calculated sequence of events for the case analysed is shown in Table 9.3-1.

Figures 9.3.1-1 through 9.3.1-6 show the transient response for the loss of two reactor coolant pumps with offsite power available. Figure 9.3.1-6 demonstrates that the DNBR is always greater than the safety analysis limit value, which demonstrates that the DNB design basis is met. The DNB design basis is described in Section 22.7.1.1.

The affected reactor coolant pumps coast down, and the core flow reaches a new equilibrium value. The plant is tripped by the low-flow trip rapidly enough so that the capability of the reactor coolant to remove heat from the fuel rods is not greatly reduced. The average fuel and cladding temperatures do not increase significantly above their initial values. With the reactor tripped, a stable plant condition is attained and plant shutdown may then proceed.

In the event that a loss of offsite power occurs as a consequence of a turbine trip during a partial loss of reactor coolant flow, the DNB design basis continues to be met as discussed in Section 9.3.1.1.

Appendix 9C provides discussion and analysis of long term safe shutdown for non-LOCA events.

9.3.1.3 Diverse Mitigation

In addition to the Class 1 passive systems credited in the DBA, the plant also provides diverse mitigation capability that is able to supply the Category A safety functions for frequent faults. The diverse features are also Class 1 except for the C&I, which is Class 2.

Two different diverse mitigation analyses are discussed in the following subsections. One demonstrates the reactor can be shut down when a CCF prevents control rod insertion. Such an event is defined as an ATWT. The other demonstrates that adequate core cooling can be provided

when a CCF affects the core cooling credited in the DBA. In the diverse core cooling case rod insertion is assumed to occur.

The diverse core cooling is provided by passive feed and bleed using PXS injection and ADS venting (Class 1). The DAS provides diverse reactor trip and safety system actuation (Class 2).

Table 9.3-4 summarizes the SSCs credited in these diverse fault assessments. The information provided in Table 9.3-4 is from Reference 9.3-12, which documents the diversity for the frequent faults and provides additional information on the diverse mitigation functions.

The following sections provide the evaluation and results of the diverse mitigation analysis cases for the partial loss of forced reactor coolant system flow.

9.3.1.3.1 Diverse Mitigation for ATWT

A number of cases were considered to address different potential CCFs that can affect the PMS and its ability to insert RCCAs. The analysis documented in this section is performed to bound the following events:

- Partial loss of flow with a PMS CCF – The CCF prevents all PMS reactor trips signals and engineered safeguards features signals. The DAS is assumed to be completely operable. Offsite power and turbine bypass are also assumed available.

- Partial loss of flow with a PMS reactor trip breaker CCF - This failure prevents the PMS from inserting the rods; however, PMS logic continues to function, and all engineered safeguards features signals are operable. DAS is completely operable, including its capability to drop rods. Offsite power and turbine bypass are also assumed to be available.

- Partial loss of flow with a RCCA mechanical CCF - The PMS, DAS, and control systems are assumed to be operable except that RCCAs do not insert into the core on a trip signal.

This analysis is performed to demonstrate the adequacy of the operable portions of the PMS (considering the impact of the CCF) as well as the DAS to detect and actuate mechanical SSCs to mitigate the fault. The following ATWT acceptance criteria are applicable to this event:

- The RCS does not overpressurise due to reactor coolant heatup. The ATWT pressure limit is 22.06 MPa-rel (3200 psig).

- There is no significant fuel damage.

- The rate and duration of energy release to containment is much less than for the design basis LOCA. This demonstrates that the containment does not overpressurise due to the energy release to the containment.

9.3.1.3.1.1 Diverse ATWT Method of Analysis

Partial loss of reactor coolant flow has no potential for RCS overpressurisation and is bounded by loss of normal feedwater analysed in Section 9.2.7 for RCS overpressurisation. This section addresses partial loss of flow ATWT core damage potential.

The partial loss of flow event diverse mitigation analyses assumptions are:

- Plant initial conditions are at the nominal full power values

- The flow coastdown curves and time when reactor trip on low coolant flow in any hot leg is reached are calculated externally using the COAST computer code and input in the LOFTRAN code.

  The only credible cause for the two of four RCPs loss is the loss of electrical power supply at corresponding transformers. Loss of voltage at ZAS-ET-2A causes loss of RCP 1A and 2A; loss of voltage at ZAS-ET-2B causes loss of RCP 1B and 2B. RCPs 1A and 1B take suction from the SG 1 cold plenum, and RCPs 2A and 2B take suction from the SG 2 cold plenum. There is no credible single failure that could cause loss of RCPs 1A and 1B or loss of RCPs 2A and 2B.

- Core kinetics parameters and initial boron concentration are both assumed to be at BOC values.

- MTC is modelled as discussed in Reference 9.3-10.

- Pressuriser pressure and level control systems are assumed to be operable.

- The turbine bypass system is assumed to be operable. The turbine bypass system control logic blocks turbine bypass opening unless there is a sudden decrease in turbine load. The turbine bypass control is set for T_{avg} control prior to a reactor trip signal. When the T_{avg} mode is selected, the turbine bypass valves would be automatically actuated only if either a large rapid turbine load rejection or a turbine trip is detected. After a reactor trip signal is generated in PMS or DAS, the turbine bypass switches to pressure control automatically.

9.3.1.3.1.2 Diverse ATWT Credited SSCs

For the diverse ATWT, the plant stabilizes at new power and flow conditions; manual operator action would be necessary to end transient. The available SSCs are listed in Table 9.0-14.

- DAS PRHR actuation on High hot leg temperature (T_{hot}) available for possible for 2 of 4 RCP partial loss of flow with RCCA insertion failures only

9.3.1.3.1.3 Diverse ATWT Results

1 of 4 Reactor Coolant Pumps Partial Loss of Flow with a PMS CCF

At the start of the event one RCP is assumed to be tripped. Core power decreases due to the initial increase in coolant average temperature and moderator density feedback results in an equilibrium power value which is equal to the energy removal rate of the turbine system.

The setpoint for the PMS reactor trip on low coolant flow is reached but no PMS action occurs due to the PMS CCF. There are no parameters monitored by DAS which would cause DAS system intervention. To shut down the reactor from these conditions, operator action will be necessary.

Figures 9.3.1-7 to 9.3.1-9 show the event progression.

2 of 4 Reactor Coolant Pumps Partial Loss of Flow with a PMS CCF

At the start of the event, one RCP in each loop is assumed to be tripped. The setpoint for the PMS reactor trip on low reactor coolant pump speed is reached, but no PMS action occurs due to the PMS CCF. Core power decreases due to the initial increase in coolant average temperature and moderator density feedback results in an equilibrium power value, which is equal to the energy removal rate of the turbine system.

The only parameter monitored by DAS that would potentially be available to initiate reactor trip is High T_{hot} in both hot legs. However, due to the fact that turbine continues to absorb steam from steam generators and thus keeps steam pressure relatively low, the primary temperature does not reach the value for High T_{hot} reactor trip. To shut down the reactor from these conditions, operator action will be necessary.

Figures 9.3.1-10 to 9.3.1-12 show the event progression.

1 of 4 RCPs Partial Loss of Flow with a Reactor Trip Breaker CCF

This scenario is very similar to the 1 of 4 RCPs PLOF with a PMS CCF scenario above. The only difference is that after the first PMS reactor trip setpoint is reached the turbine is tripped and turbine bypass control switches to the pressure control mode. Pressuriser safety valves temporarily open for a short time after turbine trip. There are no parameters monitored by DAS which would cause DAS system intervention. To shut down the reactor from these conditions, operator action will be necessary.

The turbine trip and turbine bypass switch to pressure control mode results in higher secondary pressure and higher coolant average temperature comparing to the 1 of 4 RCPs PLOF with PMS CCF scenario. As a result equilibrium power is significantly lower for the reactor trip breaker CCF scenario than for the PMS CCF scenario.

2 of 4 Reactor Coolant Pumps Partial Loss of Flow with a Reactor Trip Breaker CCF

This scenario begins in the same manner as the 2 of 4 RCPs PLOF with PMF CCF scenario above. The difference is that after the first PMS reactor trip setpoint is reached, the turbine is tripped and turbine bypass switches to the pressure control mode.

The turbine trip results in increased secondary pressure and increased RCS temperature and pressure. Pressuriser safety valves temporarily open a short time after turbine trip. Hot-leg temperature increases close to the DAS high hot-leg temperature setpoint. Depending on the time response of the turbine bypass system, the high hot-leg temperature setpoint may be reached which will actuate PRHR and a reactor trip via M-G sets being de-energised.

If the DAS high hot-leg temperature setpoint is not reached, core power would stay at an equilibrium value which is equal to the energy removal rate of the turbine bypass system. The turbine trip and turbine bypass switch to pressure control mode would result in higher secondary pressure and higher coolant average temperature compared to the PMF CCF scenario, and equilibrium power would be significantly lower for the reactor trip breaker CCF scenario than for the PMS CCF scenario.

This section describes a partial loss of flow with a mechanical CCF that prevents rods from inserting. The PMS, DAS and PLS are assumed to be operable, except that RCCAs do not insert into the core on a trip signal.

1 of 4 Reactor Coolant Pumps PLOF with an RCCA Mechanical CCF

Because there are no parameters monitored by DAS that would cause DAS system intervention for 1 of 4 RCPs PLOF, the RCCA mechanical CCF is the same as the reactor trip breaker CCF scenario.

2 of 4 Reactor Coolant Pumps PLOF with an RCCA Mechanical CCF

This scenario is the same as the 2 of 4 RCPs PLOF with reactor trip breaker CCF scenario, except that for the case when DAS high hot-leg temperature setpoint is reached, only PRHR will be actuated but RCCAs will not be dropped into the core. Actuation of PRHR will increase energy removal from the primary system. However, since the turbine is already tripped, core power will stay at an equilibrium value, which is equal to the energy removal rate of the turbine bypass system and the PRHR. This equilibrium power is significantly lower for the RCCA mechanical CCF scenario than for the PMS CCF scenario.

Departure from Nucleate Boiling Ratio Evaluation

The above scenarios were analysed for DNB using the WRB−2M correlation. DNB calculations were done using design power shape including design $F_{\Delta H}$ and flow maldistribution factors. Figure 9.3.1-13 shows WRB-2M DNBR. As can be seen from the figure, there is significant margin to the DNBR limit during PLOF ATWT scenarios.

9.3.1.3.2 Diverse Mitigation for Core Cooling

The loss of normal feedwater diverse core cooling, as analysed in Section 9.2.7.3.2, was determined to be bounding of all non-LOCA events.

9.3.1.4 Radiological Consequences

Design Basis

In the case where offsite power remains available, there is no release of activity to the environment and the Target 4 BSOs (0.01 mSv offsite and 0.1 mSv onsite) are met.

In the case where offsite power is lost, a small release of activity may occur as a result of steam dump to the atmosphere due to unavailability of the condensers. With no fuel damage and primary and secondary circuits intact, the initiating event has no impact on the doses. The doses are a consequence of the assumed loss of offsite power. Therefore, the loss of offsite power doses from Section 9.2.6.4 are presented. The calculated maximum doses for all relevant pathways (inhalation, cloudshine, and groundshine) are as follows:

- Offsite dose: 0.05 mSv Worker dose: 1.5 mSv

These doses are within the Target 4 BSL for frequent faults (1 mSv offsite and 20 mSv onsite).

Diverse Mitigation

Both the diverse ATWT and diverse core cooling scenarios demonstrate that the RCS does not overpressurise and there is no fuel damage. For a diverse mitigation radiological consequences analysis better estimate assumptions would be credited. This would include reactor coolant system activity levels significantly lower than those modelled for the DBA and better activity retention in containment and in the steam generators. In addition better estimate atmospheric

dispersion factors would be used. Therefore, a diverse mitigation radiological consequences analysis would show that the doses for the diverse ATWT scenario would be less than those reported for the non-LOCA DBAs and doses for the diverse core cooling scenario would be much less than for the design basis LOCA. The diverse mitigation analyses would not have to meet the Target 4 BSL for frequent faults and would meet the Target 4 BSL for infrequent faults.

9.3.1.5 As Low as Reasonably Practicable Assessment

For this event, the identification of the primary safety functions as Class 1 SSCs has been shown to be adequate to meet DB requirements.

The diverse mitigation functions, including other Class 1 safety functions and the DAS function, which is Class 2, is also shown by analysis to meet the corresponding requirements for the partial loss of forced reactor coolant flow. See Reference 9.3-12 for additional discussions on these diverse mitigation features.

Additionally, the AP1000 plant design has a third level of redundancy/diversity that is provided by the Class 2 DiD systems. The applicable DiD functions include:

- CVS boration for long-term reactivity control
- CVS make-up for RCS inventory control
- Pressuriser spray and pressuriser auxiliary spray for RCS pressure control
- SFW with steam dump for short-term decay heat removal
- RNS cooling of the RCS for long-term decay heat removal
- Control by the PLS C&I

The characteristics of the above features were compared to improvements that were evaluated for the RNS for its mitigation of cliff edge small LOCAs. First it should be recognized that in this situation the RNS provides the second level of defence for this event and is therefore more important than the above DiD features which provide a 3rd level of defence. The RNS improvements included making the RNS alignment and actuation automatic, increasing the RNS pump head, and adding a RNS suction supply tank that is separate from the Class 1 system. None of these potential improvements were found to be ALARP (See Section 9.1.4.5). However, the SFW and CVS already include characteristics similar to these proposed improvements. Another improvement that could be made to these DiD systems is to upgrade them to Class 1. This would be very expensive especially and would have wide reaching impacts to the design of SSCs; notable would be the impact on component and building design to address hazards including seismic and storm winds/missiles. Such a change would not be ALARP because the cost would be grossly disproportional to its benefit.

As discussed in Chapter 9.0.15, the AP1000 has incorporated ALARP thinking throughout its development. In addition, the current risk of a large radioactivity release is significantly less than the SAP Target 9 BSO (1E-7 pa). Considering the ALARP thinking that went into the AP1000 development, its low risk profile and the additional level of defence discussed above (including their performance characteristics), improving the Class 2 DiD to better remove decay heat or shutdown the reactor would be grossly disproportional to the risk reduction that might be achieved. As a result, the current design is considered ALARP.

9.3.1.6 Conclusions

The DB analysis shows that for the partial loss of reactor coolant flow, the DNBR does not decrease below the safety analysis limit value at any time during the transient, which demonstrates that the DNB design basis is met. The DNB design basis is described in Section 22.7.1.1.

The ATWT acceptance criteria are met for this event. This event was not explicitly analysed for the change in the current design reference point in the UK as described in Reference 9.3-14. However, the evaluation conducted to closeout FS-03 demonstrated with a subset of events (Reference 9.3-4) that there is little impact on the key analysis trends, results, and margin to the applicable acceptance criteria. Therefore, the subset of events confirmed the change in design reference point would not invalidate the conclusions presented for this event.

Diverse core cooling capabilities have been demonstrated.

DBA radiological consequences are within the Target 4 BSL for frequent faults (1 mSv offsite and 20 mSv onsite). Thus, the identification of necessary Class 1 SSCs is adequate to meet DB requirements.

It has been shown that the AP1000 plant design includes adequate systems for the protection of this fault, which limit the radiological consequences such that they are compliant with the SAPs targets and the risks have been reduced to be ALARP.

9.3.2 Complete Loss of Forced Reactor Coolant Flow (Fault 1.13.1a)

9.3.2.1 Identification of Causes and Accident Description

A complete loss of flow accident may result from a simultaneous loss of electrical supplies to the reactor coolant pumps. If the reactor is at power at the time of the event, the immediate effect of a loss of coolant flow is a rapid increase in the coolant temperature. Electric power for the reactor coolant pumps is normally supplied through busses, connected to the generator through the unit auxiliary transformers. When a generator trip occurs, the busses receive power from external power lines and the pumps continue to supply coolant flow to the core.

The following signals provide protection against this event:

- Reactor coolant pump under-speed
- Low primary coolant loop flow

The reactor trip on reactor coolant pump under-speed protects against conditions that can cause a loss of voltage to two-out-of-four reactor coolant pumps. This function is blocked below approximately 10-percent power (permissive P10). The reactor trip on reactor coolant pump under-speed protects against conditions that can cause a loss of voltage to two-out-of-four reactor coolant pumps. This function is blocked below approximately 10-percent power (permissive P10). The reactor trip on reactor coolant pump under-speed also protects against a frequency decay condition resulting from frequency disturbances on the power grid, as long as the grid frequency decay rate is less than approximately 5 hertz per second. WCAP-8424-R1 (Reference 9.3-3), provides analyses of grid frequency disturbances and the resulting protection requirements that are applicable to the AP1000 plant design. As part of addressing GI-AP1000-FS-03, a complete loss of flow was postulated to occur following a grid frequency perturbation (not just grid frequency decay) in UKP-SSAR-GLR-002 (Reference 9.3-4).

9.3.2.2 Design Basis Mitigation

Analysis is performed to demonstrate the adequacy of the PMS to detect and mitigate the fault and show that the safety analysis criteria are satisfied including:

- No fuel failures (confirmed using minimum DNBR),
- The RCS pressure criterion is met,
- The MSS pressure criterion is met, and

- The pressuriser does not fill (which could result in a LOCA)

It is noted that this event is bounded by the Section 9.2.3 analysis with respect to RCS/MSS pressure criteria, therefore, these limits are not explicitly confirmed for this event. Also, pressuriser filling is not challenged for this event and is not explicitly confirmed.

9.3.2.2.1 DBA Method of Analysis

The complete loss of flow transient is analysed for a loss of power to four reactor coolant pumps.

For the scenario of a complete loss of voltage, which results in all the reactor coolant pumps coasting down, the method of analysis and the assumptions made regarding initial operating conditions and reactivity coefficients are identical to those discussed in Section 9.3.1, with two exceptions. Following the loss of power supply to all pumps at power, a reactor trip is actuated by the reactor coolant pump under-speed trip instead of the low primary coolant flow trip. Also, rather than the bounding value of 0.0 $\Delta k/g/cc$, a less limiting, yet still conservative, moderator density coefficient (MDC) curve (MDC as a function of coolant density) was modelled. Due to all pumps coasting down, a rod drop time of 2.3 seconds is assumed (see Section 9.0.6).

For the scenario of a complete loss of flow following a grid frequency perturbation, the frequency disturbance was initiated at the same initial conditions as the loss of voltage case, above. However, the frequency perturbation caused a slightly more limiting power condition at the time the reactor coolant pumps were assumed to coast down, primarily due to an increase in main feedwater pump speed caused by a grid overfrequency fault and the associated reactivity-induced power increase. The most limiting grid frequency perturbation case assumed a grid overfrequency with operable variable frequency drives on the reactor coolant pumps. This case causes an increase in feedwater pump speed, but with RCPs remaining at nominal speed. The limiting case also modelled automatic rod control, and the coastdown of all four RCPs was assumed to occur at the peak power level caused by rod control overshoot. This case is described in detail in UKP-SSAR-GSC-002 (Reference 9.3-4).

A complete loss of forced primary coolant flow can also result from a constant decay in the reactor coolant pump motor supply frequency. However, the results of the complete loss of voltage scenario (i.e., free spinning pump coastdown) bound the results of the complete loss of flow initiated by a frequency decay of up to 5 hertz per second. This is due to the reactor coolant pump design, which initially (during the critical time frame of the transient) has a more rapid coastdown as a free spinning pump than for an electrical frequency decay.

The results of the complete loss of voltage case and the grid frequency perturbation case are presented in Section 9.3.2.2.3.

9.3.2.2.2 DBA Credited SSCs

For the DB, all of the claimed SSCs are Class 1. The claimed Class 1 SSCs are listed in Table 9.0-10. The presented DB analysis ends shortly after reactor trip; however, essential safety functions for the long term safe shutdown analysis (Appendix 9C) bound safe shutdown response for this event. The primary core cooling is provided by the PRHR and passive containment cooling. Other SSCs include the CMTs, containment isolation, and pressuriser SVs. The PMS provides the following:

- RT on Low-2 RCP Speed (requires 2 of 4 RCPs underspeed)

- PRHR actuation on Low-2 SG NR level coincident with Low-2 SFW flow
- CMTs and containment isolation on Low-2 CL temperature
- PCS on High-2 containment pressure

9.3.2.2.3 DBA Results

Figures 9.3.2-1 through 9.3.2-6 show the transient response for the complete loss of voltage to all four reactor coolant pumps. Figures 9.3.2-7 through 9.3.2-12 show the transient response for the complete loss of flow following a grid frequency perturbation. The results of both cases are very similar. In both cases, the reactor is tripped on the reactor coolant pump under-speed signal. Figures 9.3.2-6 and 9.3.2-12 demonstrate that the DNBR is always greater than the safety analysis limit value, which demonstrates that the DNB design basis is met. The DNB design basis is described in Section 22.7.1.1.

The calculated sequence of events for the two cases are shown in Table 9.3-1. With respect to the DNB concerns, the event is essentially over shortly after reactor trip. However, if the event was extended beyond the time frame analysed for DNB, the reactor coolant pumps continue to coast down, and natural circulation flow would be established, as demonstrated in Section 9.2.6. With the reactor tripped, a stable plant condition is attained and plant shutdown may then proceed.

Appendix 9C provides discussion and analysis of long term safe shutdown for non-LOCA events.

9.3.2.3 Diverse Mitigation

In addition to the passive systems credited in the DBA, the plant also has a diverse mitigation capability that is able to supply the Category A safety functions for frequent faults. For this frequent fault event the diverse features are also Class 1 except for the C&I, which is Class. 2

The diverse core cooling is provided by passive feed and bleed using PXS injection and ADS venting (Class 1). The DAS provides diverse reactor trip and safety system actuation (Class 2).

Table 9.3-7 summarizes the SSCs from this fault assessment. As this is a frequent fault, a diverse means of providing the Category A safety functions is provided. The information provided in Table 9.3-7 is from Reference 9.3-12, which documents the diversity for the frequent faults and provides additional information on the diverse mitigation functions. Table 9.3-8 provides the operator actions utilized in the diverse safety case.

The following sections provide the evaluation and results of the diverse mitigation analysis cases for the complete loss of forced reactor coolant system flow.

9.3.2.3.1 Diverse Mitigation for ATWT

The AP1000 design has several automatic RCP trip features that introduce mechanisms for complete loss of RC forced circulation that do not exist on standard Westinghouse PWRs. For ATWT consideration, that is a safety benefit, as a flow coastdown will cause a rapid reduction in core power because of moderator reactivity feedback.

A number of cases were considered to address different potential CCFs that can affect the PMS and its ability to insert RCCAs. The analysis documented in this section is performed to bound the following events:

- Complete loss of flow with a PMS CCF – The CCF prevents all PMS reactor trips signals and engineered safeguards features signals. The DAS is assumed to be completely operable. Offsite power and turbine bypass are also assumed available.

- Complete loss of flow with a PMS reactor trip breaker CCF - This failure prevents the PMS from inserting the rods; however, PMS logic continues to function, and all engineered safeguards features signals are operable. DAS is completely operable, including its capability to drop rods. Offsite power and turbine bypass are also assumed to be available.

- Complete loss of flow with a RCCA mechanical CCF - The PMS, DAS, and control systems are assumed to be operable except that RCCAs do not insert into the core on a trip signal.

This analysis is performed to demonstrate the adequacy of the operable portions of the PMS (considering the impact of the CCF) as well as the DAS to detect and actuate mechanical SSCs to mitigate the fault. The following ATWT acceptance criteria are applicable to this event:

- The RCS does not overpressurise due to reactor coolant heatup. The ATWT pressure limit is 22.06 MPa-rel (3200 psig).

- There is no significant fuel damage.

- The rate and duration of energy release to containment is much less than for the design basis LOCA. This demonstrates that the containment does not overpressurise due to the energy release to the containment.

An ATWT loss of RCS flow does not have the potential to cause RCS overpressure. In fact, it provides defence against overpressurisation since it causes [ ]
For that reason, the analysis in this section focuses on the potential for core damage (i.e., core DNB). Further, long-term recovery from a loss of flow ATWT is covered by the analysis and discussion of the loss of feedwater event in Section 9.2.7.5.

This section covers the evaluation of the various scenarios caused by different initiating events or with differing assumed failures.

9.3.1.3.1.1 Diverse ATWT Method of Analysis

The causes for trip of all RCPs are:

- Loss of all ac power to the station auxiliaries

- PMS CMT actuation (on Low-2 pressuriser water level, low wide range water level in both SGs coincident with High-1 T_{hot}, First Stage ADS actuation, or manual)

- DAS CMT actuation (Low wide range water level in both SGs, Low pressuriser water level, or manual)

- High RCP bearing water temperature in any RCP

These are evaluated in the following sections.

Bounding Loss of Reactor Coolant System Flow Scenarios

Many different scenarios can be considered. To limit the large number of cases to be addressed, a small number of limiting DNB scenarios can be constructed that can be shown to bound the core consequences of other scenarios. For the purposes of this report, two bounding scenarios are considered for DNB concerns. Other scenarios are evaluated and are shown to be less limiting for DNB, as well as shown to be covered by other analyses for other limits and long-term recovery. The two bounding scenarios are:

- Case 1: Simultaneous Trip of all RCPs from Initial Steady-State
- Case 2: Trip of all RCPs from an Elevated RCS Temperature

9.3.2.3.1.2 Diverse ATWT Credited SSCs

For the diverse ATWT, the presented ATWT cases only credit turbine trip from DAS and stabilize at a new power and flow condition; a manual operator action would be required to terminate the event. The available Class 1 SSCs are listed in Table 9.0-14. DNB limits are met for this stabilised transient condition. DAS provides the following:

- Turbine trip on High hot leg temperature (T_{hot})

9.3.2.3.1.3 Diverse ATWT Results

Case 1: Simultaneous Trip of all RCPs from Initial Steady-State

Simultaneous trip of all RCPs is the initiating event with failure of control rods to insert (PMS and PLS and DAS failure) and failure of all other PMS and DAS protective actions except turbine trip on DAS high T_{hot}. The NSSS would come to a quasi-steady-state condition, with core power equal to steam load, natural circulation being driven by core power generation, and reactivity balance (all reactivity contributors summing to zero). The exact power, flow, and steam pressure will depend upon reactivity coefficients and plant conditions such as turbine bypass pressure control settings. This quasi-steady-state power will continue until some automatic or manual actuation occurs, or SG fluid inventory could no longer sustain the core power level. If adequate feedwater cannot be sustained, then the event becomes a loss of feedwater ATWT initiated from a low initial power level. Long-term recovery is covered by the analysis and discussion of the loss of feedwater ATWT event in Section 9.2.7.5. The short-term event is covered by the analysis discussed below.

Case 1 is analysed at BOC because at end of cycle (EOC) the stronger negative moderator feedback causes a much faster core power reduction than at BOC conditions.

The BOC system transient for this case is shown on Figures 9.3.2-13 to 9.3.2-16. As shown in Figures 9.3.2-13 and 9.3.2-14, the core nuclear power and heat flux decrease rapidly with the loss of flow, even though the moderator feedback is minimised at BOC. At 20 seconds, the bulk core exit begins to boil, causing the dip and small oscillations shown in Figure 9.3.2-14 at that time. (This particular oscillation is probably due to the single thermal hydraulic channel and use of the core density difference reactivity coefficient described in Reference 9.3-10). Hot-leg temperature rises rapidly, as shown in Figure 9.3.2-15, causing the DAS T_{hot} circuit to trip the turbine and reactor and actuate PRHR. (The T_{hot} setpoint was taken as 343.3°C (650°F) in this analysis, but reactor trip and PRHR actuation were not modelled.)

These conditions were then analysed for DNB using the standard Westinghouse methodology for safety analyses (i.e., design power shape including design $F_{\Delta h}$ and flow maldistribution factors) with no credit for either axial or radial power shape change during the flow coastdown. This is very conservative, as the heating of coolant in the hot channels and top of the core changes the power shape and substantially increases margins to DNB.

Two DNB correlations were considered: WRB-2M and WLOP. The WRB-2M correlation is valid up to [ ] but high steam quality may exceed its correlation limits. The WRB-2M DNB calculations did not credit any pressures above this value. However, the quality limit was exceeded about 9 seconds after the RCP trip. The WLOP correlation is valid for high quality but has an upper pressure limit that does not extend to normal operating pressure. Therefore, the DNB calculation for WLOP assumed [ ] instead of the actual system pressure. Since the critical heat flux increases with pressure (other variables being equal), the calculated DNB ratio is conservatively underestimated when the system pressure is above the correlation limit. The DNB ratios for those two correlations are shown in Figure 9.3.2-17.

The AP1000 design basis for DNB prevention uses the WRB-2M correlation. The correlation meets the 95/95 criterion for DNBR. Its use is discussed in Section 22.7.1.1. As discussed in that section, the 95/95 DNBR limit when used with the RTDP is [ ]. The RTDP includes uncertainty for flow, power, temperature, and pressure (and those uncertainties need not be included in an ATWT analysis). The 95/95 DNB ratio limit for WLOP is [ ].

Both correlations indicate the minimum DNB ratio occurs relatively early in the flow coast down. Although the WRB-2M correlation quality limit is exceeded in the later part of the flow coastdown, the WLOP correlation demonstrates that the DNB ratio is improving and continues to improve after that time.

Figure 9.3.2-18 displays the core reactivity, as calculated by LOFTRAN during the transient using the BOC reactivity coefficients described in Reference 9.3-10. The neutronics code (ANC) statepoint reactivity calculation for the transient conditions is also calculated by LOFTRAN. These were calculated using the same methodology that Westinghouse uses for steam line break analysis (see Section 9.1). That is, LOFTRAN calculated inlet temperature, flow, pressure, and total core power at various times in the transient were input into ANC and the reactivity calculated. The ANC calculation of reactivity is always significantly less than the reactivity calculated by LOFTRAN. This verifies that the reactivity coefficients used by LOFTRAN are conservative; a more exact analysis would have shown a faster drop in core power.

Case 2: Trip of all RCPs from an Elevated RCS Temperature

This bounding case assumed a loss of feedwater (which causes some initial RCS heatup and core power reduction), followed by partial SG dryout, rapid RCS heating, actuation of turbine trip and RCP trip on DAS low SG water level, and failure of all other PMS, PLS, and DAS functions. This scenario differs from Case 1 only because the loss of RCS flow begins from a higher inlet temperature and lower power. The specific analysed scenario was a very conservative total loss of feedwater with early turbine trip, delayed RCP trip, and no PRHR or CMT actuation or reactor trip. These assumptions tended to drive the core inlet temperature quite high before RCP trip.

The system transient for this case is shown on Figures 9.3.2-23 to 9.3.2-25. These cases were analysed for DNB with the same very conservative methodology as described for Case 1 above; i.e., design power distribution without credit for radial or axial beneficial improvement

in the power shape during the transient, and no credit for pressure above the correlation limit. The DNB ratio is shown in Figure 9.3.2-26 for both the WRB-2M correlation (with pressures above [ ] not credited) and the WLOP correlation (with calculations based on [ ]. The WRB-2M quality limit is not exceeded for this transient.

Figure 9.3.2-27 displays the core reactivity, as calculated by LOFTRAN during the transient for Case 2. Similar to Case 1, the ANC calculation of reactivity is always less than the reactivity calculated by LOFTRAN. This verifies that the reactivity coefficients used by LOFTRAN are conservative; a more exact analysis would have shown a faster drop in core power.

As noted previously, the loss of flow ATWT is bounded by the loss of feedwater ATWT event for peak RCS pressure concerns. Long-term recovery from a loss of flow ATWT is covered by the analysis and discussion of the loss of feedwater event in Section 9.2.7.5

9.3.2.3.2 Diverse Mitigation for Core Cooling

The loss of normal feedwater diverse core cooling, as analysed in Section 9.2.7.3.2, was determined to be bounding of all non-LOCA events.

9.3.2.4 Radiological Consequences

Design Basis

In the case where offsite power remains available, there is no release of activity to the environment and the Target 4 BSOs (0.01 mSv offsite and 0.1 mSv onsite) are met.

In the case where offsite power is lost, a small release of activity may occur as a result of steam dump to the atmosphere due to unavailability of the condensers. With no fuel damage and primary and secondary circuits intact, the initiating event has no impact on the doses. The doses are a consequence of the assumed loss of offsite power. Therefore, the loss of offsite power doses from Section 9.2.6.4 are presented. The calculated maximum doses for all relevant pathways (inhalation, cloudshine, and groundshine) are as follows:

- Offsite dose: 0.05 mSv Worker dose: 1.5 mSv

These doses are within the Target 4 BSL for frequent faults (1 mSv offsite and 20 mSv onsite).

Diverse Mitigation

Both the diverse ATWT and diverse core cooling scenarios demonstrate that the RCS does not overpressurise and there is no fuel damage. For a diverse mitigation radiological consequences analysis better estimate assumptions would be credited. This would include reactor coolant system activity levels significantly lower than those modelled for the DBA and better activity retention in containment and in the steam generators. In addition better estimate atmospheric dispersion factors would be used. Therefore, a diverse mitigation radiological consequences analysis would show that the doses for the diverse ATWT scenario would be less than those reported for the non-LOCA DBAs and doses for the diverse core cooling scenario would be much less than for the design basis LOCA. The diverse mitigation analyses would not have to meet the Target 4 BSL for frequent faults and would meet the Target 4 BSL for infrequent faults.

9.3.2.5 As Low as Reasonably Practicable Assessment

Refer to the ALARP discussion in Section 9.3.1.5

9.3.2.6 Conclusions

The DB analysis demonstrates that for the complete loss of forced reactor coolant flow, the DNBR does not decrease below the safety analysis limit value at any time during the transient, which demonstrates that the DNB design basis is met. The DNB design basis is described in Section 22.7.1.1.

The ATWT acceptance criteria are met for this event.

This event was not explicitly analysed for the change in the current design reference point in the UK as described in Reference 9.3-14. However, the evaluation conducted to closeout FS-03 demonstrated with a subset of events (Reference 9.3-4) that there is little impact on the key analysis trends, results, and margin to the applicable acceptance criteria. Therefore, the subset of events confirmed the change in design reference point would not invalidate the conclusions presented for this event.

Diverse core cooling capabilities have been demonstrated.

DBA radiological consequences are within the Target 4 BSL for frequent faults (1 mSv offsite and 20 mSv onsite). Thus, the identification of necessary Class 1 SSCs is adequate to meet DB requirements.

It has been shown that the AP1000 plant design includes adequate systems for the protection of this fault, which limit the radiological consequences such that they are compliant with the SAPs targets and the risks has been reduced to be ALARP.

9.3.3 Reactor Coolant Pump Shaft Seizure (Locked Rotor) (Fault 1.13.11)

9.3.3.1 Identification of Causes and Accident Description

The accident postulated is an instantaneous seizure of a reactor coolant pump rotor. Flow through the affected reactor coolant loop is rapidly reduced, leading to a reactor trip on a low-flow signal.

Following the reactor trip, heat stored in the fuel rods continues to be transferred to the coolant, causing the coolant temperature to increase and expand. At the same time, heat transfer to the shell side of the steam generator in the faulted loop is reduced because: 1) the reduced flow results in a decreased tube-side film coefficient, and 2) the reactor coolant in the tubes cools down while the shell-side temperature increases. (Consistent with the AP1000 design, the peak pressure and fuel rod thermal analyses assume a 5-second delay in turbine trip following reactor trip.) The rapid expansion of the coolant in the reactor core, combined with reduced heat transfer in the steam generators, causes an insurge into the pressuriser and a pressure increase throughout the reactor coolant system. The insurge into the pressuriser compresses the steam volume, actuates the automatic spray system, and opens the pressuriser safety valves, in that sequence. For conservatism, the pressure-reducing effect of the spray is not included in the analysis.

9.3.3.2 Design Basis Mitigation

Analysis is performed to demonstrate the adequacy of the protection and safety monitoring system to detect and mitigate the fault and show that the safety criteria are satisfied including:

- The RCS pressure criterion is met,
- The percentage of fuel rods-in-DNB are confirmed to be bounded by failed rod assumed for radiological dose evaluation, and
- Core coolability is demonstrated by confirming that limits for peak cladding temperature and zirconium-water reaction are met.

It is noted that transient secondary system transient pressure for this event is bounded results for the turbine trip DB analysis of Section 9.2.3 and, therefore, need not considered herein.

Some fuel damage may occur as a consequence of infrequent faults, such as the locked rotor accident. The acceptability of this fuel damage is judged by the radiological consequences.

9.3.3.2.1 DBA Method of Analysis

Two digital computer codes are used to analyse this transient. The LOFTRAN code (References 9.3-1 and 9.3-8) calculates the resulting core flow transient following the pump seizure and the nuclear power following reactor trip. This code is also used to determine the peak pressure. The thermal behaviour of the fuel located at the core hot spot is investigated by using the FACTRAN code (Reference 9.3-2) used for the presented DBA or the VIPRE-01 fuel rod model (Reference 9.3-7), which is equivalent to FACTRAN. This fuel thermal calculation uses the core flow and the nuclear power calculated by LOFTRAN. The FACTRAN code includes a film-boiling heat transfer coefficient.

At the beginning of the postulated locked rotor accident (at the time the shaft in one of the reactor coolant pumps is assumed to seize), the plant is assumed to be in operation under the most adverse steady-state operating conditions, that is, maximum steady-state thermal power, maximum steady-state pressure, and maximum steady-state coolant average temperature. Plant characteristics and initial conditions are further discussed in Section 9.0.2. The accident is evaluated for both cases with and without offsite power available. For the case without offsite power available, power is lost to the unaffected pumps at 3.0 seconds following turbine/generator trip. Turbine trip occurs 5.0 seconds following a reactor trip condition being reached. This delay on turbine trip is a feature of the AP1000 reactor trip system.

For the peak pressure evaluation, the initial pressure is conservatively estimated as 0.345 MPa (50 psi) above nominal pressure (15.513 MPa [2250 psia]), which allows for errors in the pressuriser pressure measurement and control channels. This is done to obtain the highest possible rise in the coolant pressure during the transient. To obtain the maximum pressure in the primary side, conservatively high loop pressure drops are added to the calculated pressuriser pressure.

Plant systems and equipment available to mitigate the effects of the accident are discussed in Section 9.0.4 and listed in Table 9.0-10. No single active failure in any of these systems or equipment adversely affects the consequences of the accident.

9.3.3.2.1.1 Evaluation of the Pressure Transient and Fuel Rod Thermal Design Transient

After pump seizure, the neutron flux is rapidly reduced by control rod insertion. Rod motion is assumed to begin 1.45 seconds after the flow in the affected loop reaches the reactor trip setpoint. No credit is taken for the pressure-reducing effect of the pressuriser spray, steam dump, or controlled feedwater flow after plant trip. Although these operations are expected to result in a lower peak reactor coolant system pressure, an additional conservatism is provided by ignoring their effect.

The pressuriser safety valves are fully open at 17.75 MPa (2575 psia). Their capacity for steam relief is described in Section 17.3.2.

For this accident, an evaluation of the consequences with respect to fuel rod thermal transients is performed. Results obtained from analysis of this "hot spot" condition represent the upper limit with respect to cladding temperature and zirconium-water reaction.

In the evaluation, the rod power at the hot spot is conservatively assumed to be 3 times the average rod power (that is, $F_Q = 3.0$) at the initial core power level.

9.3.3.2.1.2 Evaluation of Departure from Nucleate Boiling in Core During Accident

An analysis is performed to determine the percentage of fuel rods that experience DNB. The percentage is determined to be less than the limit value used for the fraction of fuel rods that are predicted to experience a DNB in the radiological consequences calculations reported in Section 9.3.3.4.

9.3.3.2.1.3 Film-Boiling Coefficient

The film-boiling coefficient is calculated in the FACTRAN code (Reference 9.3-2) using the Bishop-Sandberg-Tong film-boiling correlation. The fluid properties are evaluated at film temperature (average between wall and bulk temperatures). The program calculates the film coefficient at every time step, based upon the actual heat transfer conditions at the time. The nuclear power, system pressure, bulk density, and mass flow rate as a function of time are used as program input.

For this analysis, the initial values of the pressure and the bulk density are used throughout the transient because they are the most conservative with respect to cladding temperature response. For conservatism, DNB is assumed to start at the beginning of the accident.

9.3.3.2.1.4 Fuel Cladding Gap Coefficient

The magnitude and time dependence of the heat transfer coefficient between fuel and cladding (gap coefficient) have a pronounced influence on the thermal results. The larger the value of the gap coefficient, the more heat is transferred between the pellet and the cladding. Based on investigations on the effect of the gap coefficient upon the maximum cladding temperature during the transient, the gap coefficient is assumed to increase from a steady-state value consistent with the initial fuel temperature to 56.8 kW/m^2-°C (10,000 Btu/h-ft^2-°F) at the initiation of the transient. Thus, the large amount of energy stored in the fuel because of the small initial value of the gap coefficient is released to the cladding at the initiation of the transient.

9.3.3.2.1.5 Zirconium-Steam Reaction

The zirconium-steam reaction can become significant above a cladding temperature of 982.2°C (1800°F). The Baker-Just parabolic rate equation is used to define the rate of the zirconium-steam reaction:

$$\frac{d(w^2)}{dt} = 33.3 \times 10^6 \exp\left(-\frac{45{,}500}{1.986\,T}\right)$$

where:

w = amount reacted (mg/cm^2)

t = time (s)

T = temperature (Kelvin)

The reaction heat is 6322 kJ/kg (1510 cal/g)

The effect of the zirconium-steam reaction is included in the calculation of the hot spot cladding temperature transient.

9.3.3.2.2 DBA Credited SSCs

For the DB analysis, all the claimed SSCs are Class 1. The available Class 1 SSCs are listed in Table 9.0-10. The presented DB analysis ends shortly after reactor trip; however, essential safety functions for the long term safe shutdown analysis (Appendix 9C) bound safe shutdown response for this event. The primary core cooling is provided by the PRHR and passive containment cooling. Other SSCs include the CMTs, containment isolation, pressuriser SVs and SG relief valves. The PMS provides the following:

- RT on Low-2 RCS flow
- PRHR actuation on Low-2 SG NR level coincident with Low-2 SFW flow
- CMTs and containment isolation on Low-2 CL temperature
- PCS on High-2 containment pressure

9.3.3.2.3 DBA Results

Figures 9.3.3-1 through 9.3.3-7 show the transient results for one locked rotor with four reactor coolant pumps in operation. The without-offsite-power case bounds the results for the case with offsite power. The results of these calculations are also summarized in Table 9.3-2. The peak reactor coolant system pressure reached during the transient is less than that which causes stresses to exceed the faulted condition stress limits of the ASME Code, Section III. Also, the peak cladding surface temperature is considerably less than 1482°C (2700°F). The cladding temperature is conservatively calculated, assuming that DNB occurs at the initiation of the transient. These results represent the most limiting conditions with respect to the locked rotor event or the pump shaft break.

The calculated sequence of events for the case analysed is shown in Table 9.3-1. With the reactor tripped, a stable plant condition is eventually attained. Normal plant shutdown may then proceed.

9.3.3.3 Diverse Mitigation

Diverse mitigation for this event is not required as it is an infrequent fault classified as DB1.

9.3.3.4 Radiological Consequences

Design Basis

The evaluation of the radiological consequences of a postulated locked reactor coolant pump rotor accident assumes that the reactor has been operating with a limited number of fuel rods containing cladding defects and that leaking steam generator tubes have resulted in a build-up of activity in the secondary coolant.

A conservative analysis has been performed assuming 10 percent of the rods are damaged such that the activity contained in the fuel-cladding gap is released to the reactor coolant. Activity carried over to the secondary side because of primary-to-secondary leakage is available for release to the environment via the steam line safety valves or the power-operated relief valves. The conservative analysis assumes a loss of offsite power which results in steam releases from the steam generator relief valves.

Two separate accident scenarios are addressed. In the first scenario, it is assumed that the non-safety grade SFW is not available to provide feedwater to the steam generators. In this event, the water level in the steam generators drops, resulting in PRHR actuation. The period of steaming is terminated when the capacity of the PRHR system exceeds the decay heat generation rate.

In the second scenario, it is assumed that SFW is available to maintain water level in the steam generators such that PRHR is not actuated, resulting in a longer period of steaming releases. The period of steaming is terminated when RNS is in service and its capacity exceeds the decay heat generation rate.

9.3.3.4.1 Source Term

The significant radionuclide releases due to the locked rotor accident are the iodines, alkali metals (caesiums, rubidiums) and noble gases. All activity in the fuel rod gap of the damaged fuel is assumed to be released to the coolant. Based on Table 7.3 of Reference 9.3-13, the gap fraction is assumed to be 3 percent of the core inventory for iodines, 10 percent for noble gases, and 4 percent for alkali metals. To address the fact that the failed fuel rods may have been operating at power levels above the core average, the source term is increased by a lead rod radial peaking factor of 1.75 which bounds the COLR limit of 1.72.

Initial reactor coolant and secondary coolant activities are of secondary importance compared to the release of the gap inventory of fission products from the portion of the core assumed to fail because of the accident.

9.3.3.4.2 Release Pathways

The reactor coolant leaking into the steam generators is assumed to mix with the secondary coolant. As steam is released, a portion of the iodine and alkali metal activity in the coolant is released. The fraction of activity released is defined by the reducing conditions within the steam generator. Volatile (elemental) iodines are treated as a direct release from the RCS to the environment. Non-volatile (particulate) iodines and alkali metals are assumed to enter the secondary coolant. Release from the secondary coolant is limited by the assumed moisture carryover. The noble gas activity entering the secondary side is released to the environment. These releases are terminated when the steam releases stop.

9.3.3.4.3 Dose Calculation Models

The models used to calculate offsite and control room doses are provided in Appendix 9A.

9.3.3.4.4 Analytical Assumptions and Parameters

The assumptions and parameters used in the analysis are listed in Table 9.3-3.

9.3.3.4.5 Doses

Design Basis

In the case where offsite power remains available, there is no release of activity to the environment and the Target 4 BSOs (0.01 mSv offsite and 0.1 mSv onsite) are met.

In the case where offsite power is lost, a small release of activity may occur as a result of steam dump to the atmosphere due to unavailability of the condensers. The highest doses are found to be for the case with SFW available. The calculated maximum doses for all relevant pathways (inhalation, cloudshine, and groundshine) are as follows:

- Offsite dose: 2.8 mSv Worker dose: 11 mSv

These doses are within the Target 4 BSL for infrequent faults (10 mSv offsite and 200 mSv onsite).

The limiting conditions for operation of the Technical Specifications used in the dose assessment are provided in Table 9.3-12. The Table 9.3-12 values ensure the Target 4 BSL are met.

9.3.3.5 As Low As Reasonably Practicable Assessment

For this event, the identification of the primary safety functions as Class 1 SSCs has been shown to be adequate to meet DB requirements. This event is not a frequent fault and as a result diverse mitigation is not required. Although not required, the AP1000 does have two additional levels of defence as discussed in Section 9.3.1.5 and for the reasons discussed in this section the design is ALARP.

9.3.3.6 Conclusions

The DB analysis demonstrates that for the locked rotor event, the RCS pressure and cladding temperature DNB design bases are met. Fuel failures based on the rods-in-DNB value are confirmed to be less than fuel failures assumed in dose analysis

Radiological consequences are within the Target 4 BSL for infrequent faults (10 mSv offsite and 200 mSv onsite). Thus, the identification of necessary Class 1 SSCs is adequate to meet DB requirements.

It has been shown that the AP1000 plant design includes adequate systems for the protection of this fault, which limit the radiological consequences such that they are compliant with the SAPs targets and the risks has been reduced to be ALARP.

9.3.4 Reactor Coolant Pump Shaft Break (Fault 1.13.12)

9.3.4.1 Identification of Causes and Accident Description

The accident is postulated as an instantaneous failure of a reactor coolant pump shaft. Flow through the affected reactor coolant loop is rapidly reduced, though the initial rate of reduction of coolant flow is greater for the reactor coolant pump rotor seizure event. Reactor trip occurs on a low-flow signal in the affected loop.

Following the reactor trip, heat stored in the fuel rods continues to be transferred to the coolant, causing the coolant to expand. At the same time, heat transfer to the shell side of the steam generator in the faulted loop is reduced because: 1) the reduced flow results in a decreased tube-side film coefficient, and 2) the reactor coolant in the tubes cools down while the shell-side

temperature increases. The rapid expansion of the coolant in the reactor core, combined with reduced heat transfer in the steam generators, causes an insurge into the pressuriser and a pressure increase throughout the reactor coolant system. The insurge into the pressuriser compresses the steam volume, actuates the automatic spray system, and opens the pressuriser safety valves, in that sequence. For conservatism, the pressure-reducing effect of the spray is not included in the analysis.

9.3.4.2 Conclusion

With a failed shaft, the impeller could be free to spin in a reverse direction as opposed to being fixed in position as is the case when a locked rotor occurs. This results in a decrease in the end point (steady-state) core flow. For both the shaft break and locked rotor incidents, reactor trip occurs very early in the transient. In addition, the locked rotor analysis conservatively assumes that DNB occurs at the beginning of the transient. The calculated results presented for the locked rotor analysis bound the reactor coolant pump shaft break event.

It has been shown that the AP1000 plant design includes adequate systems for the protection of this fault, which limit the radiological consequences such that they are compliant with the SAPs targets and the risks has been reduced to be ALARP.

9.3.5 References

9.3-1 Westinghouse Documents WCAP-7907-P-A, Rev. 0 (Proprietary) and WCAP-7907-A, Rev. 0 (Non-Proprietary), "LOFTRAN Code Description," April 1984.

9.3-2 Westinghouse Document WCAP-7908-A (Non-Proprietary), "FACTRAN A FORTRAN-IV Code for Thermal Transients in a UO_2 Fuel Rod," December 1989.

9.3-3 Westinghouse Document WCAP-8424-R1 (Non-Proprietary), "An Evaluation of Loss of Flow Accidents Caused by Power System Frequency Transients in Westinghouse PWRs," May 1975.

9.3-4 Westinghouse Document UKP-SSAR-GLR-002, Revision 0, "UK AP1000® Plant: Summary Report Supporting the Closure of Fault Studies Issue 03," May 2016.

9.3-5 Westinghouse Documents WCAP-11397-P-A (Proprietary) and WCAP-11397-A (Non-Proprietary), "Revised Thermal Design Procedure," April 1989.

9.3-6 Not Used.

9.3-7 Westinghouse Documents WCAP-14565-P-A, Rev. 0 (Proprietary) and WCAP-15306-NP-A, Rev. 0 (Non-Proprietary), "VIPRE-01 Modeling and Qualification for Pressurized Water Reactor Non-LOCA Thermal-Hydraulic Safety Analysis," October 1999.

9.3-8 Westinghouse Documents WCAP-15644-P, Rev. 2 (Proprietary) and WCAP-15644-NP, Rev. 2 (Non-Proprietary), "AP1000 Code Applicability Report," March 2004.

9.3-9 Not Used.

9.3-10 Westinghouse Document UKP-GW-GLR-016, Rev. B, "Evaluation of ATWS Events for UK AP1000™ Pressurized Water Reactor," October 2010.

9.3-11 Not Used.

9.3-12 Westinghouse Document UKP-GW-GL-067, Rev. 1, "AP1000 Assessment of Diverse Mitigation of Frequent Faults for the UK," December 2011.

9.3-13 European Commission Report EUR 19841 EN, "Determination of the in-containment source term for a large-break loss of coolant accident," April 2001.

9.3-14 Westinghouse Report UKP-SSAR-GLR-001, Rev. 0, "UK Fault Studies Analysis Basis," August 2016.

Table 9.3-1. DBA Time Sequence Of Events For Incidents That Result In A Decrease In Reactor Coolant System Flow Rate

Accident	Event	Time (seconds)
Partial loss of forced reactor coolant flow		
– Loss of two pumps with four pumps running	Two pumps lose power and begin coasting down Low-flow reactor trip setpoint reached Rods begin to drop Minimum DNBR occurs	0.00 1.97 3.42 5.40
Complete loss of forced reactor coolant		
– Loss of four pumps with four pumps running (loss of voltage)	All pumps lose power and begin coasting down Reactor coolant pump under-speed trip setpoint reached Rods begin to drop Minimum DNBR occurs	0.00 0.50 1.15 3.00
Loss of four pumps with four pumps running (following an electrical grid frequency perturbation)	Grid frequency perturbation occurs * All pumps lose power and begin coasting down Reactor coolant pump under-speed trip setpoint reached Rods begin to drop Minimum DNBR occurs	*See Note* 0.0 0.49 1.14 3.50
Reactor coolant pump shaft seizure (locked rotor)		
– One locked rotor with four pumps running without offsite power available	Rotor on one pump locks Low-flow trip point reached Rods begin to drop Maximum reactor coolant system pressure occurs Maximum cladding temperature occurs	0.00 0.10 1.55 3.40 4.10

* Note: The times presented here do not include 88.7 seconds of the initial grid frequency perturbation transient. The reactor coolant pumps were modelled to begin coasting down at 88.7 seconds, the time at which core power reaches its most conservative value.

Table 9.3-2. DBA Summary Of Results For Locked Rotor Transients (Four Reactor Coolant Pumps Operating Initially)

	Without Offsite Power Available
Maximum reactor coolant system pressure	18.73 MPa abs (2716 psia)
Maximum cladding average temperature, core hot spot	1101°C (2014°F)
Zr-H_2O reaction, core hot spot (percentage by weight)	0.57

Table 9.3-3 (Sheet 1 of 2). DBA Parameters Used In Evaluating The Radiological Consequences Of A Locked Rotor Accident

Reactor coolant iodine activity	Equal to the operating limit for reactor coolant activity of 9.25E6 Bq/kg (0.25 μCi/g) dose equivalent I-131 (see Table 9A-1)
Reactor coolant noble gas activity	Equal to the operating limit for reactor coolant activity of 2.6E9 Bq/kg (70 μCi/g) dose equivalent Xe-133 (see Table 9A-1)
Reactor coolant alkali metal activity	Design basis activity (see Table 9A-1)
Secondary coolant initial iodine and alkali metal activity	10% of design basis reactor coolant concentrations at maximum equilibrium conditions
Fraction of fuel rods assumed to fail	0.10
Core activity	See Table 9A-3
Radial peaking factor (for determination of activity in failed fuel rods)	1.75
Fission product gap fractions Iodines Noble gases Alkali metals	 0.03 0.10 0.04
Reactor coolant mass	1.684E5 kg (3.713E5 lbm)
Condenser	Not available
Primary to secondary leak rate	0.79[(1)] kg/min (1.74 lbm/min)
Partition coefficient in steam generators Volatile (iodine) Particulates (iodine, alkali metals)	See Appendix 9A.4 1.0 0.0005
Accident scenario in which startup feedwater is not available Duration of accident Duration of flashing Steam release rate Minimum secondary coolant mass	 1.5 hr 1.5 hr 54.44 kg/sec (120 lbm/sec) 3,4E4 kg (7.5E4 lbm)

Table 9.3-3 (Sheet 2 of 2). DBA Parameters Used In Evaluating The Radiological Consequences Of A Locked Rotor Accident

Accident scenario in which startup feedwater is available	
Duration of accident	8.0
Duration of flashing	Not applicable
Steam release rate	27.22 kg/sec (60 lbm/sec)
Minimum secondary coolant mass	1.32E5 kg (2.92E5 lbm)
Volatile iodine fraction	See Appendix 9A.5.3
With primary-to-secondary flashing	0.002
Without primary-to-secondary flashing	0.001
Offsite atmospheric dispersion factors	See Table 9A-5
Control room modelling	See Appendix 9A

Notes:
1. Equivalent to 0.57 m^3 (150 gal) per day per SG cooled liquid at 1000 kg/m^3 (62.4 lbm/ft^3).

Table 9.3-4. Partial Loss Of Forced Reactor Coolant Flow Mitigation Features

Category A Safety Function	Provision	SSCs	Classification
Short-term reactivity control	Primary means	Reactor trip breakers (PMS)	1
	Diverse means	Motor-generator set field breakers (DAS)	2
Long-term reactivity control	Primary means	CMT recirculation	1
	Diverse means	Passive feed and bleed	1
Decay heat removal	Primary means	PRHR HX	1
	Diverse means	Passive feed and bleed	1
RCS pressure control	Primary means	Pressuriser safety valve	1
	Diverse means	Pressuriser volume	1
RCS inventory control	Primary means	CMTs	1
	Diverse means	Passive feed and bleed	1
Containment cooling	Primary means	PCS AOVs	1
	Diverse means	PCS MOVs	1

Table 9.3-5. Not Used

Table 9.3-6. Not Used

Table 9.3-7. Complete Loss Of Forced Reactor Coolant Flow Mitigation Features

Category A Safety Function	Provision	SSCs	Classification
Short-term reactivity control	Primary means	Reactor trip breakers (PMS)	1
	Diverse means	Motor-generator set field breakers (DAS)	2
Long-term reactivity control	Primary means	CMT recirculation	1
	Diverse means	Passive feed and bleed	1
Decay heat removal	Primary means	PRHR HX	1
	Diverse means	Passive feed and bleed	1
RCS pressure control	Primary means	Pressuriser safety valve	1
	Diverse means	Pressuriser volume	1
RCS inventory control	Primary means	CMTs	1
	Diverse means	Passive feed and bleed	1
Containment cooling	Primary means	PCS AOVs	1
	Diverse means	PCS MOVs	1

Table 9.3-8. Complete Loss Of Forced Reactor Coolant Flow Potential Operator Actions

Operator Action	Class
If PRHR fails, initiate the passive feed and bleed by manually activating ADS, recirculation and IRWST	1

Table 9.3-9. Not Used

Table 9.3-10. Not Used

Table 9.3-11. Not Used

Table 9.3-12. Locked Rotor Technical Specifications Used In Dose Analysis

Limit or Condition	Tech Spec Identification and Notes
Primary-to-secondary leakage rate	3.4.7 leak rate to be < 0.57 m^3 (150 gal) per day for any one SG
Primary coolant specific activity	3.4.10 dose equivalent specific activity to be < 9.25E6 Bq/kg (0.25 µCi/g) for I-131 and < 2.6E9 Bq/kg (70 µCi/g) for Xe-133
Secondary coolant specific activity	3.7.4 dose equivalent I-131 specific activity to be < 9.25E5 Bq/kg (0.025 µCi/g)

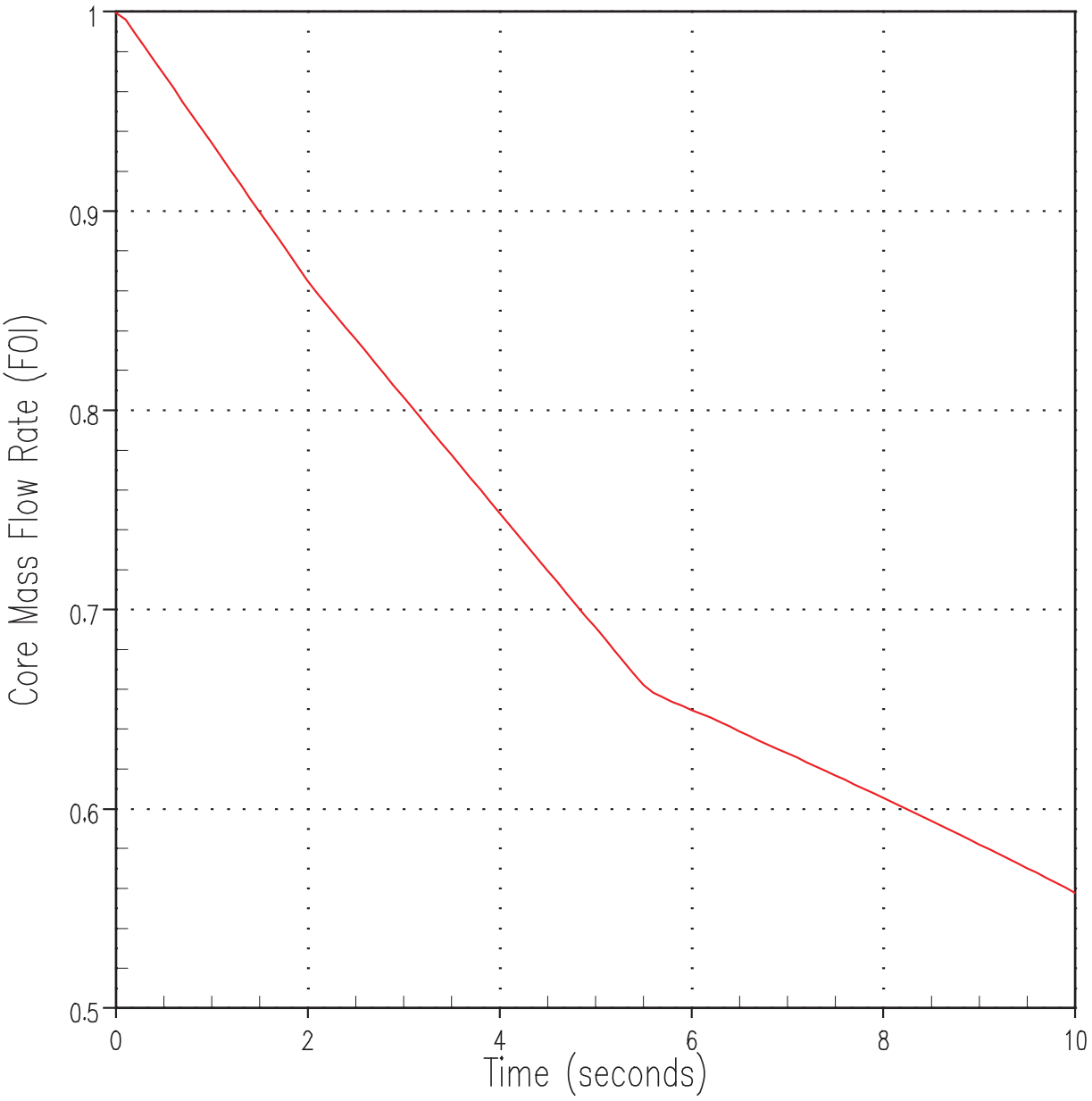


Figure 9.3.1-1. DBA Core Mass Flow Transient for 2 of 4 RCPs PLOF

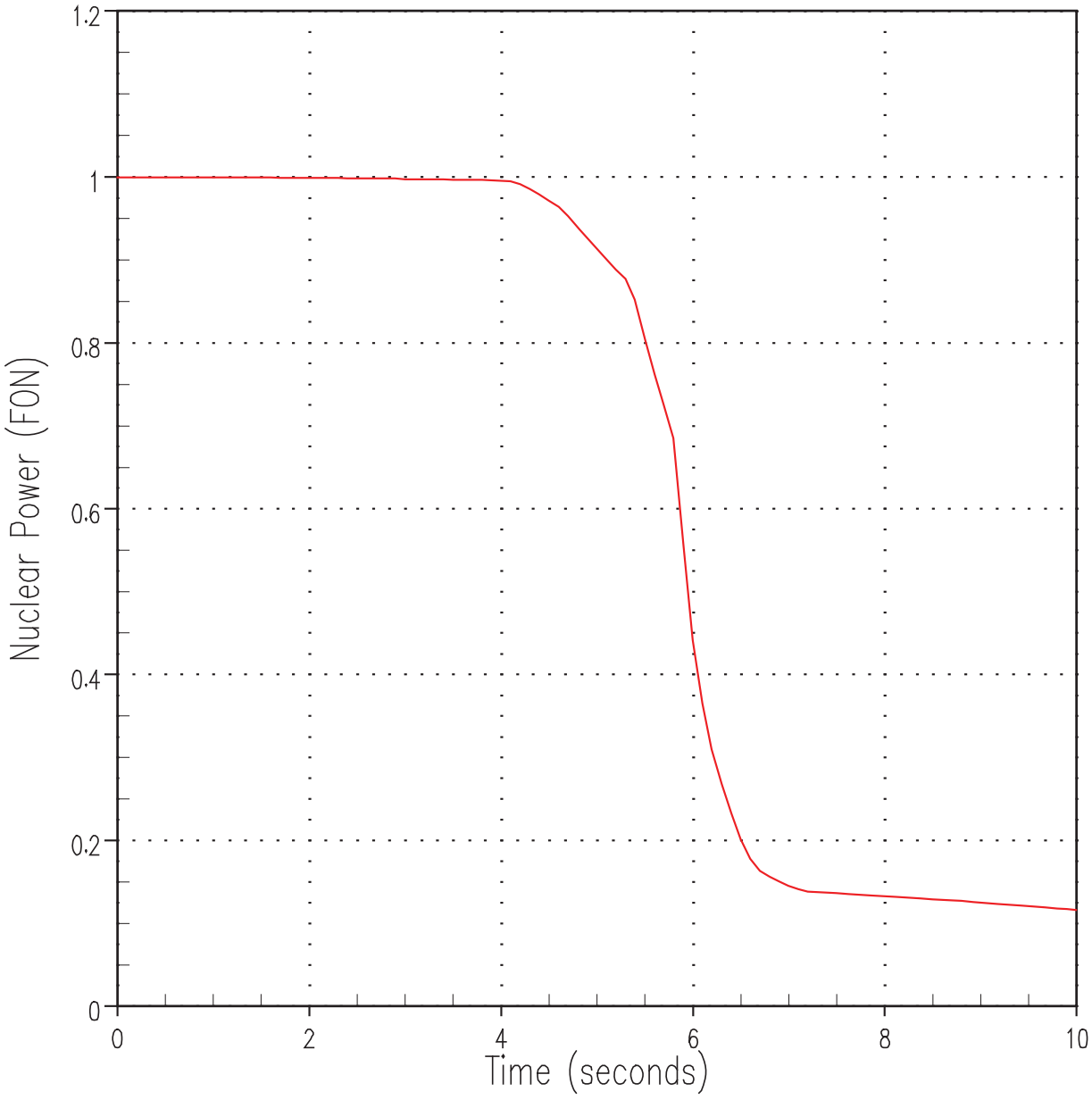


Figure 9.3.1-2. DBA Nuclear Power Transient for 2 of 4 RCPs PLOF

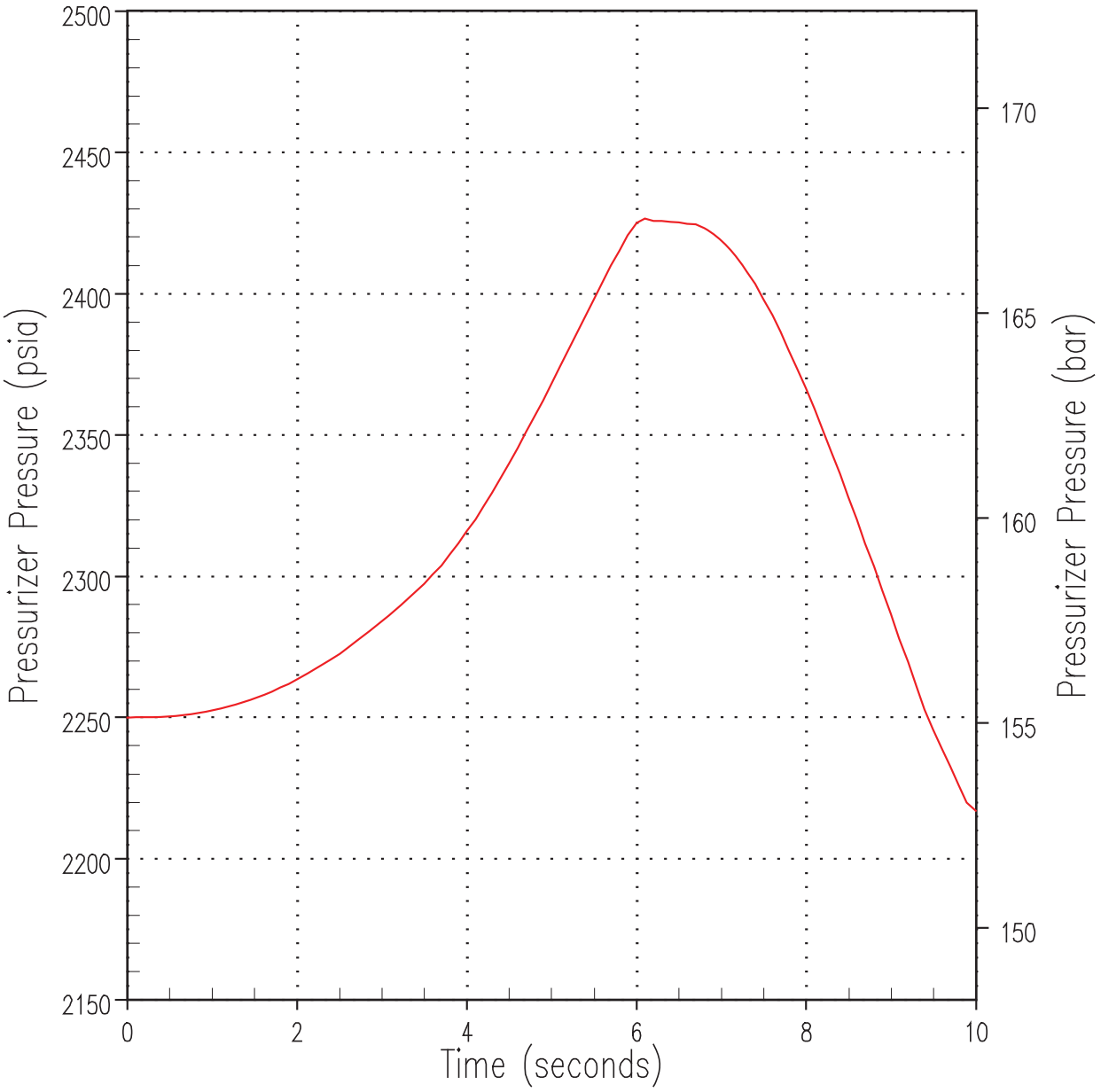


Figure 9.3.1-3. DBA Pressuriser Pressure Transient for 2 of 4 RCPs PLOF

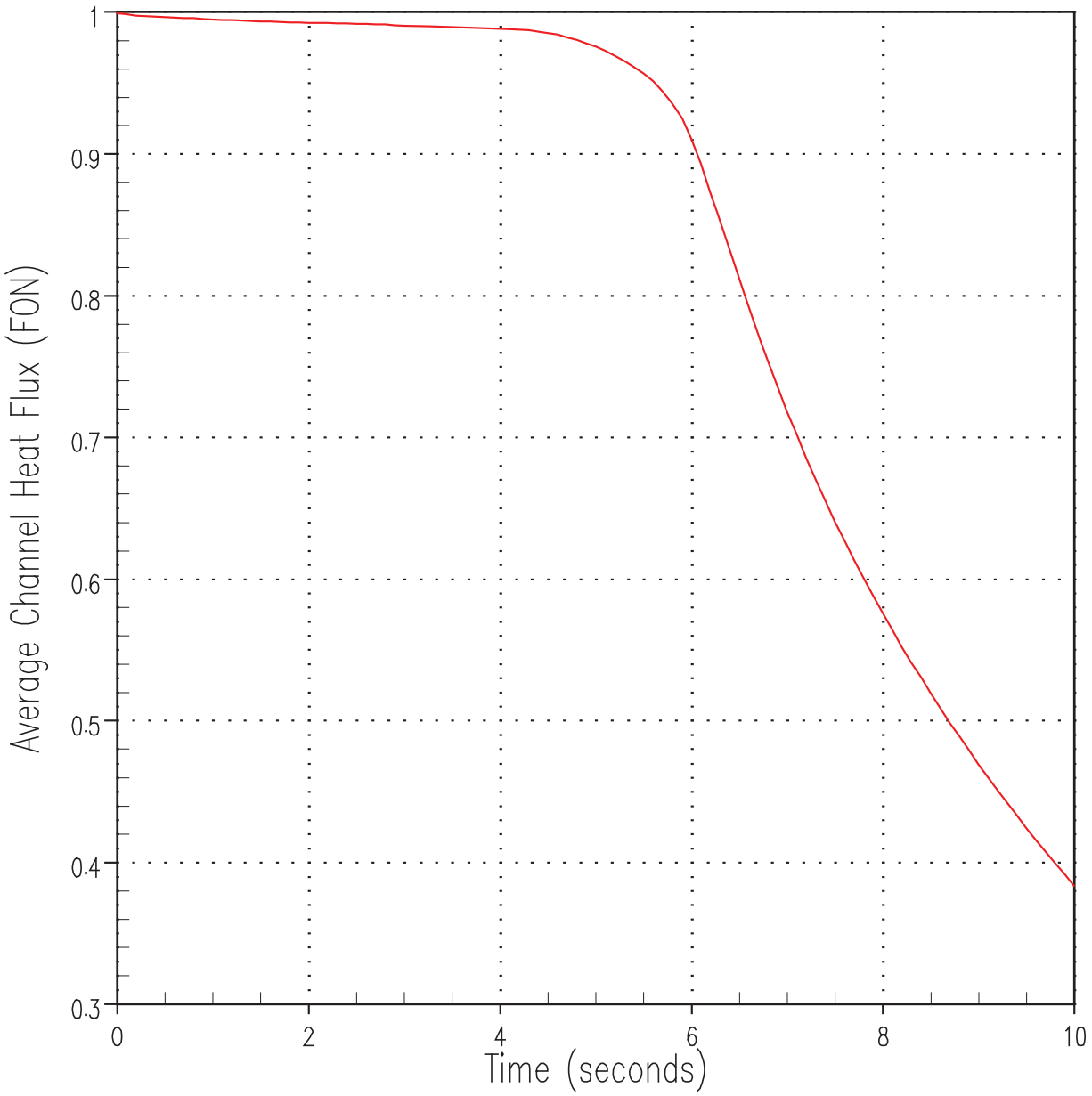


Figure 9.3.1-4. DBA Average Channel Heat Flux Transient for 2 of 4 RCPs PLOF

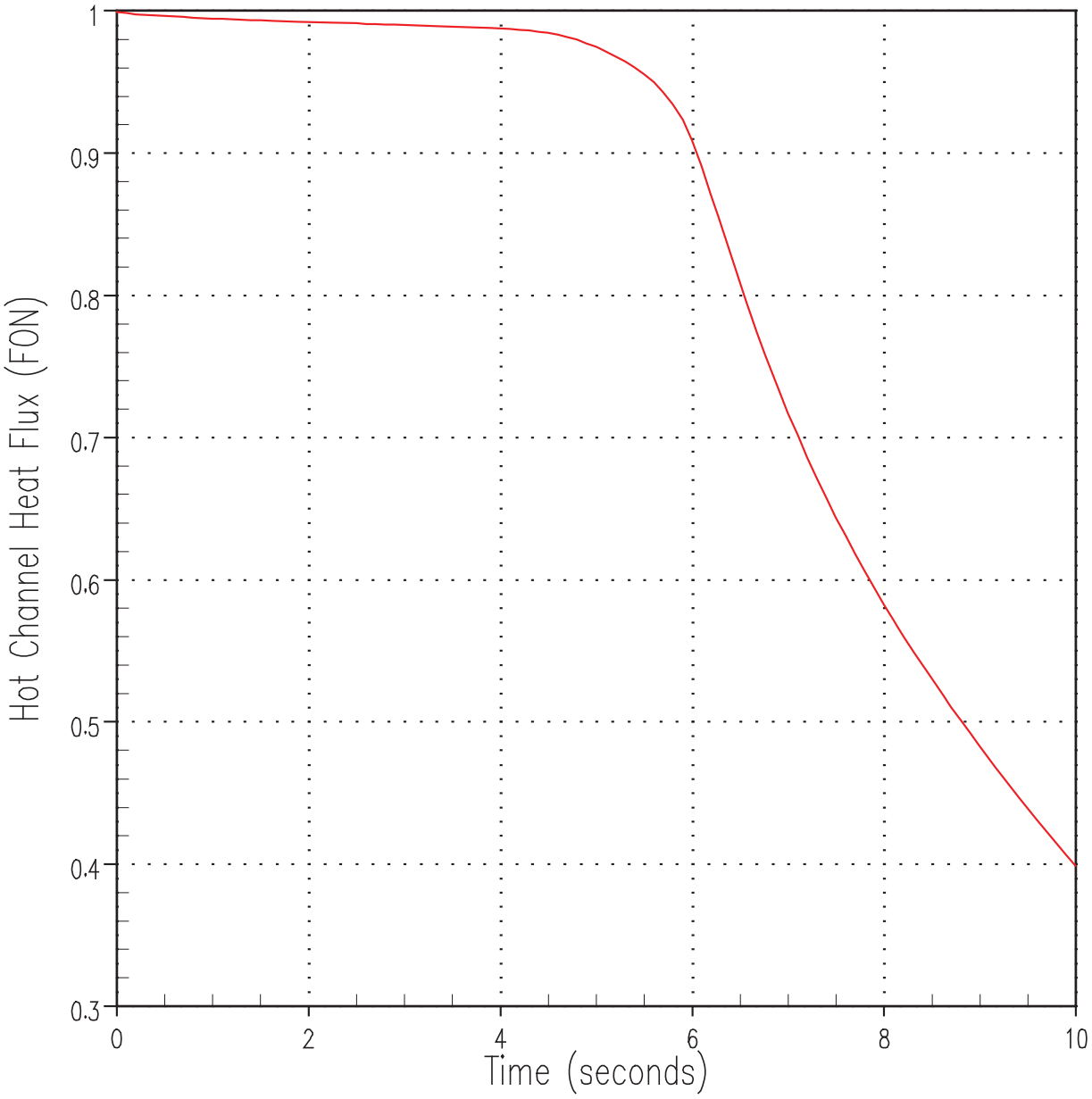


Figure 9.3.1-5. DBA Hot Channel Heat Flux Transient for 2 of 4 RCPs PLOF

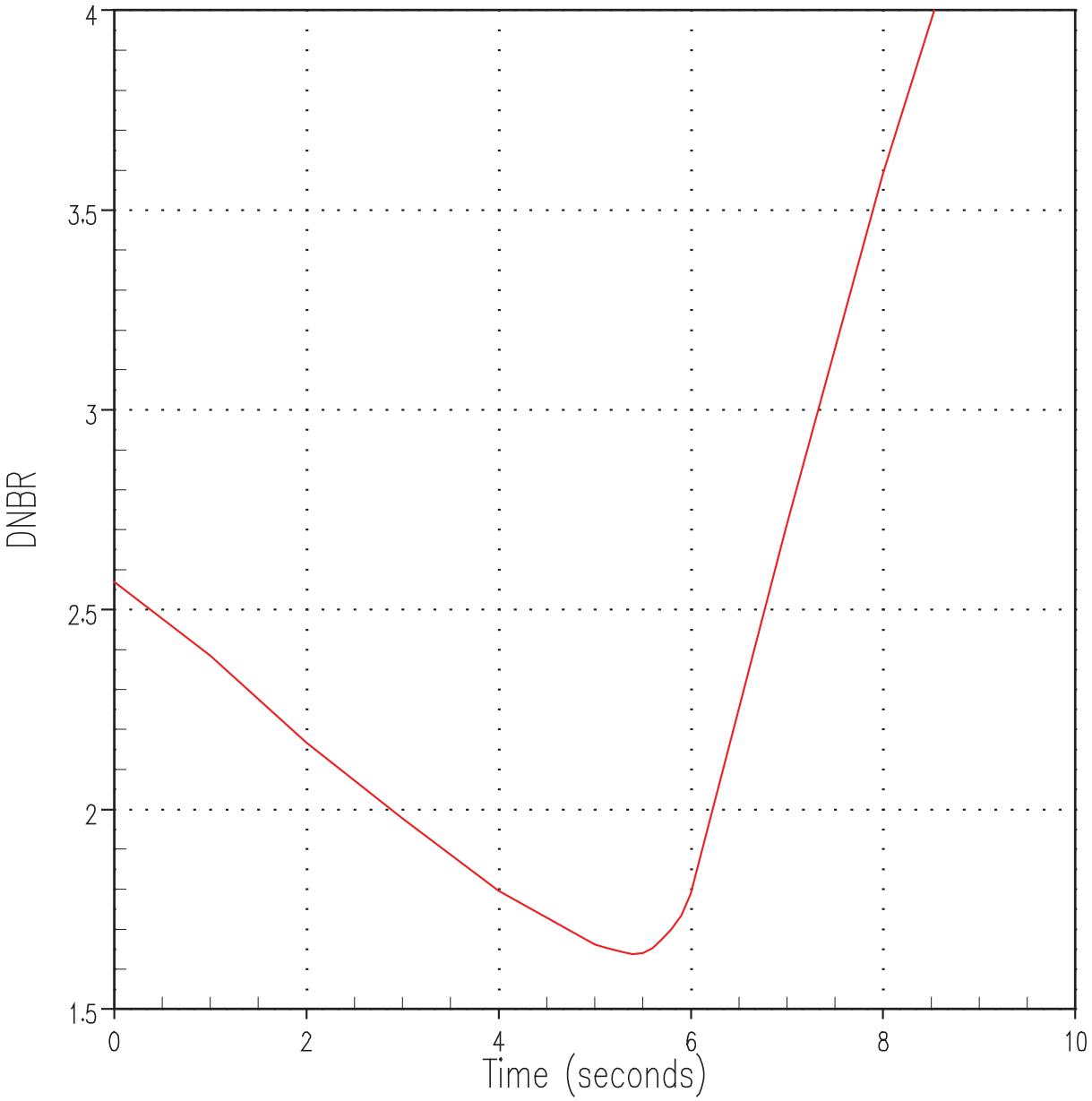


Figure 9.3.1-6. DBA DNBR Transient for 2 of 4 RCPs PLOF

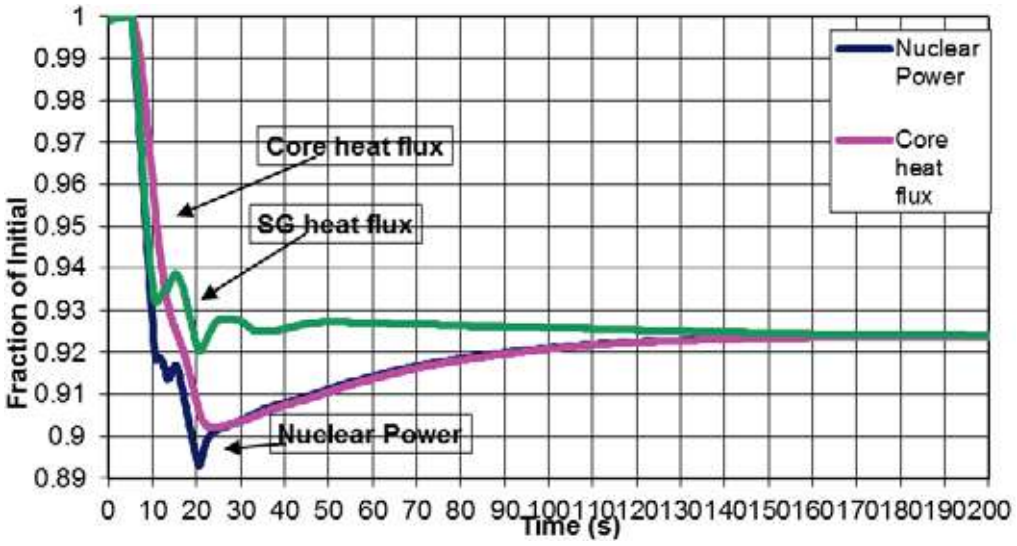


Figure 9.3.1-7. ATWT 1 of 4 RCPs PLOF with PMS CCF – Power and Heat Transfer

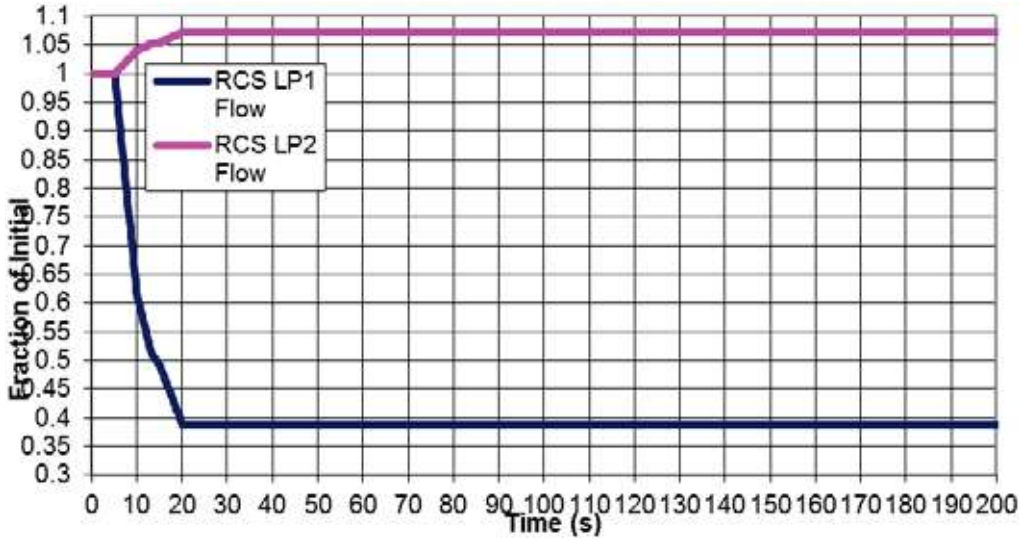


Figure 9.3.1-8. ATWT 1 of 4 RCPs PLOF with PMS CCF – RCS Loop Flow

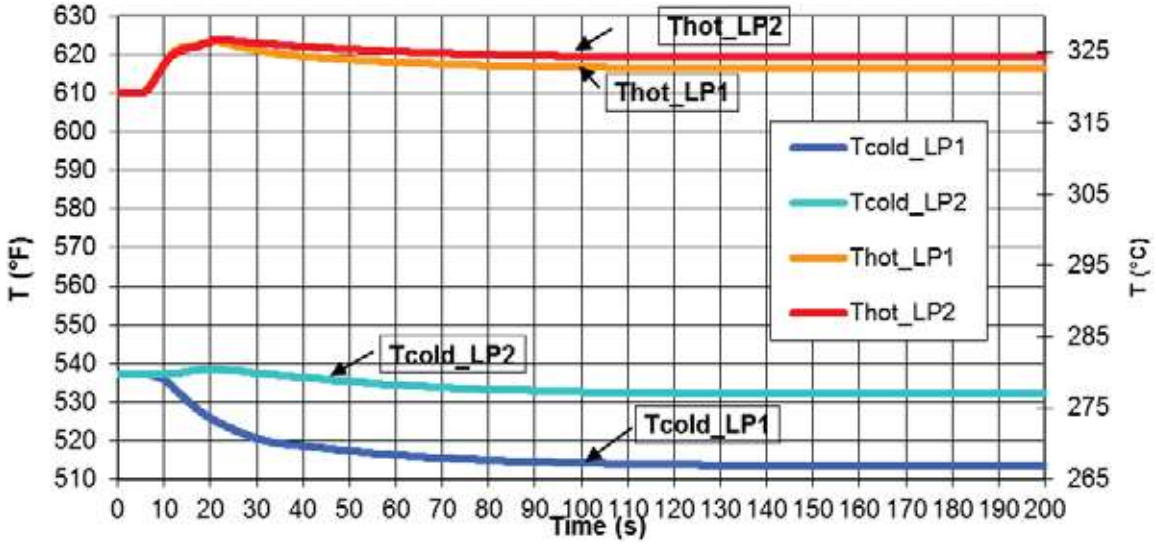


Figure 9.3.1-9. ATWT 1 of 4 RCPs PLOF with PMS CCF – Loop Coolant Temperature

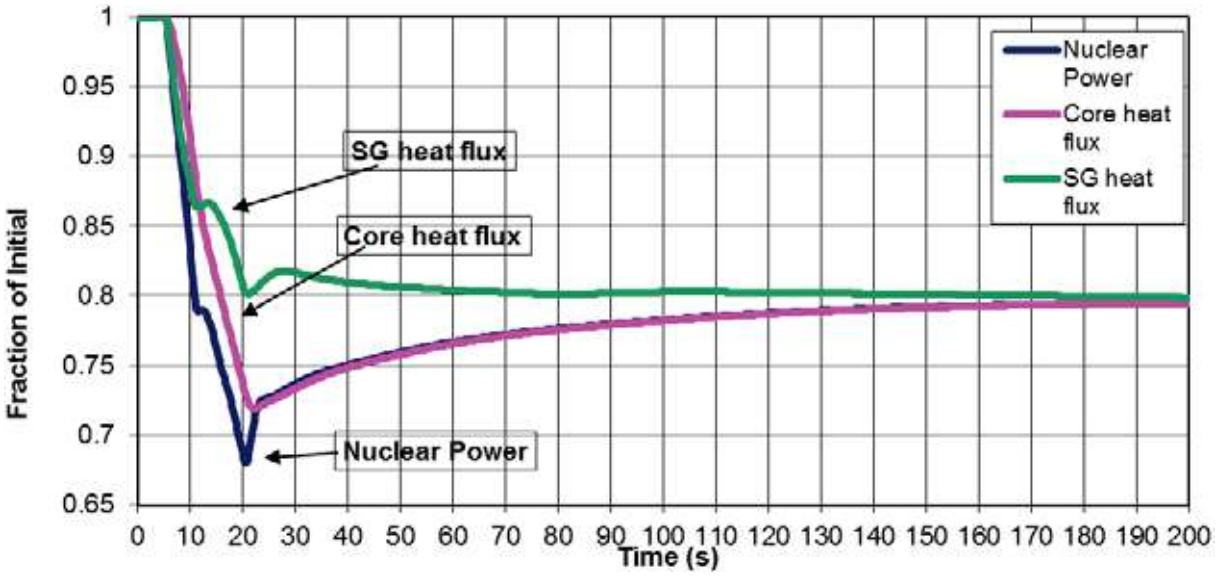


Figure 9.3.1-10. ATWT 2 of 4 RCPs PLOF with PMS CCF – Power and Heat Transfer

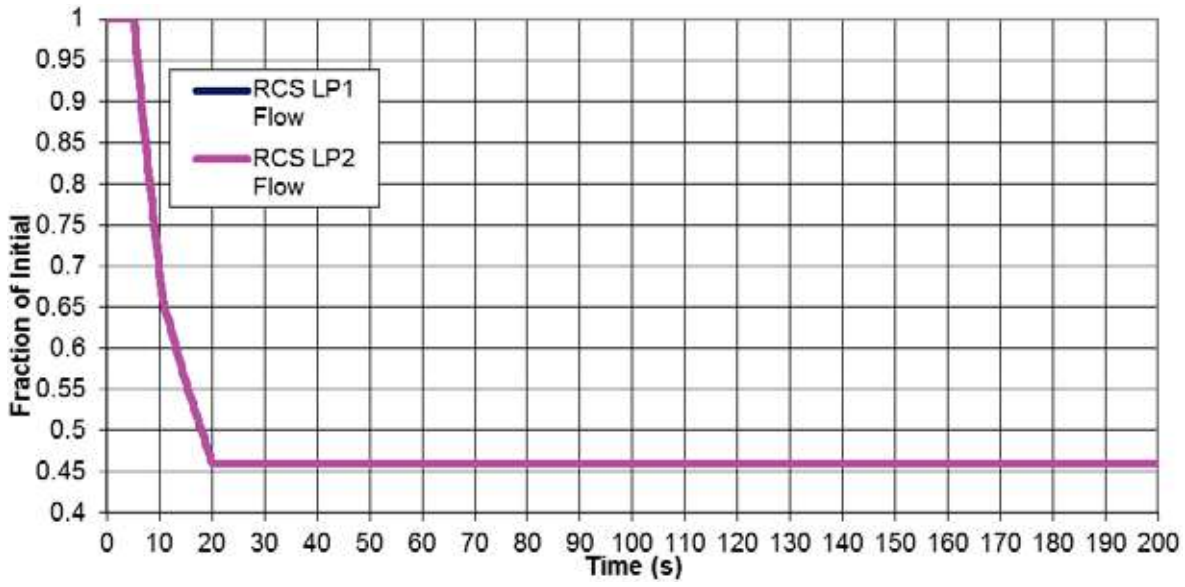


Figure 9.3.1-11. ATWT 2 of 4 RCPs PLOF with PMS CCF – RCS Loop Flow

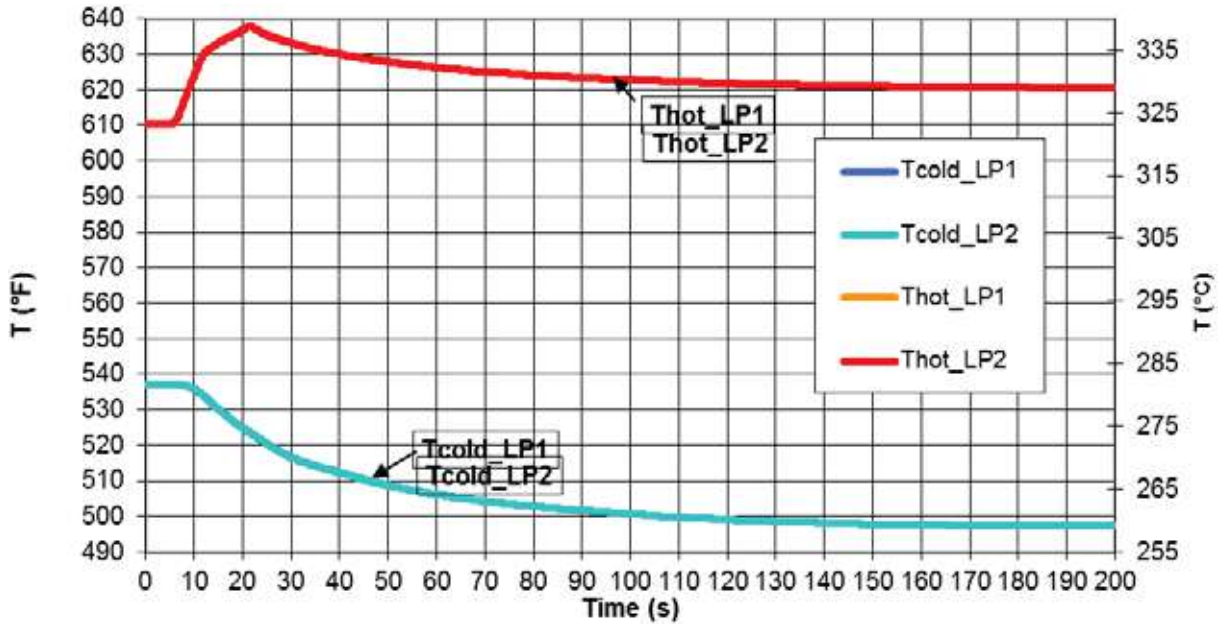


Figure 9.3.1-12. ATWT 2 of 4 RCPs PLOF with PMS CCF – Loop Coolant Temperature

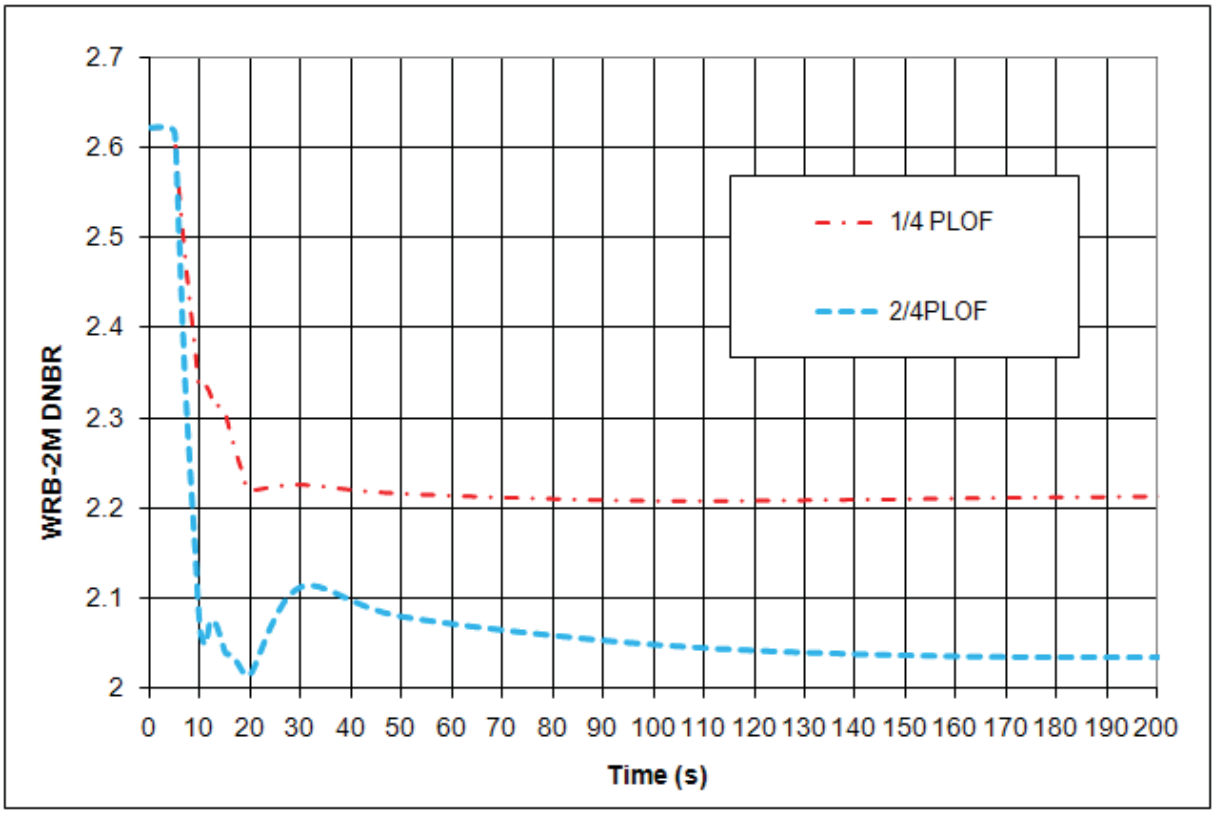


Figure 9.3.1-13. ATWT PLOF - WRB-2M DNBR

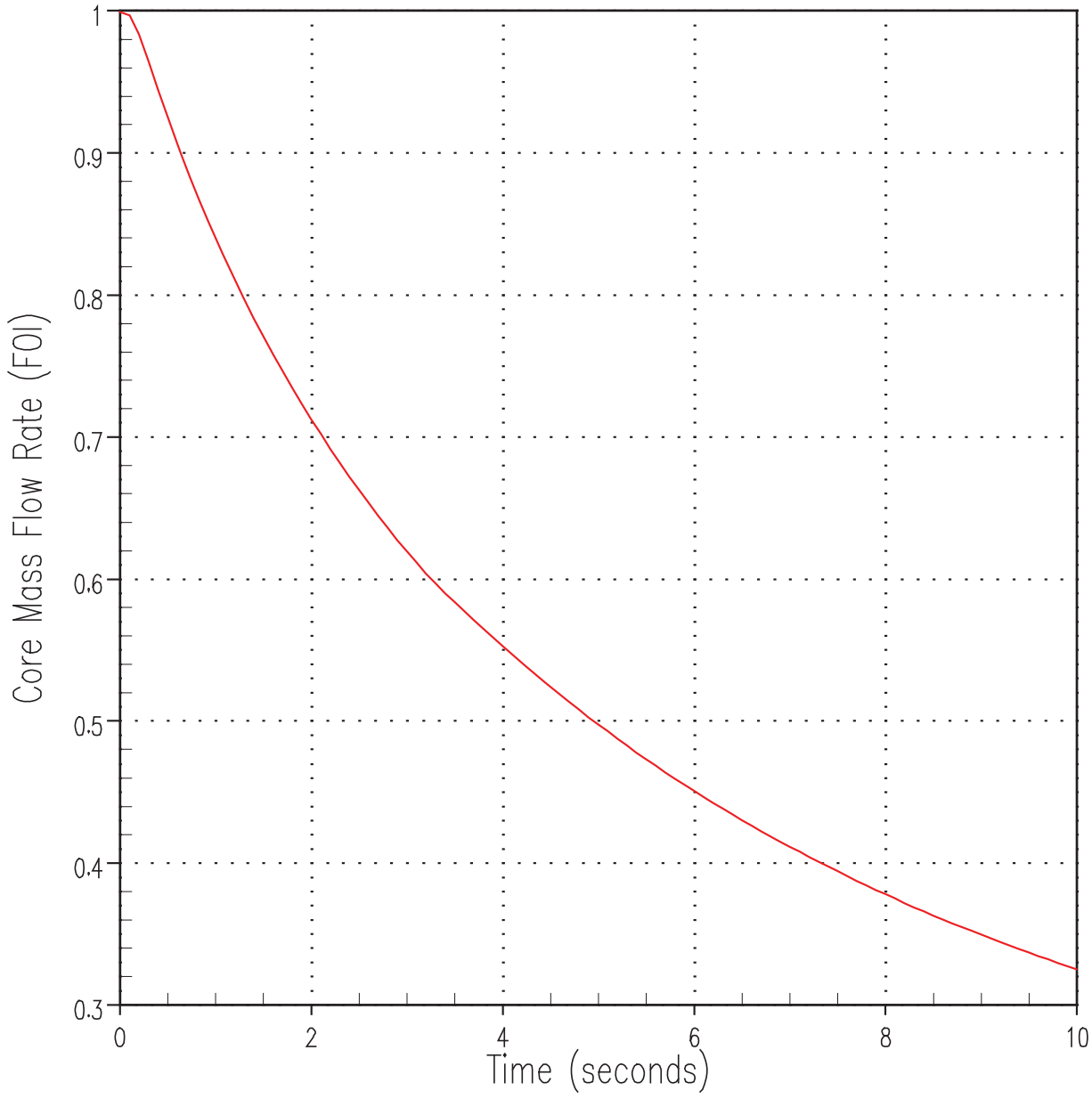


Figure 9.3.2-1. DBA Core Mass Flow Transient for 4 of 4 RCPs CLOF (Loss of Voltage)

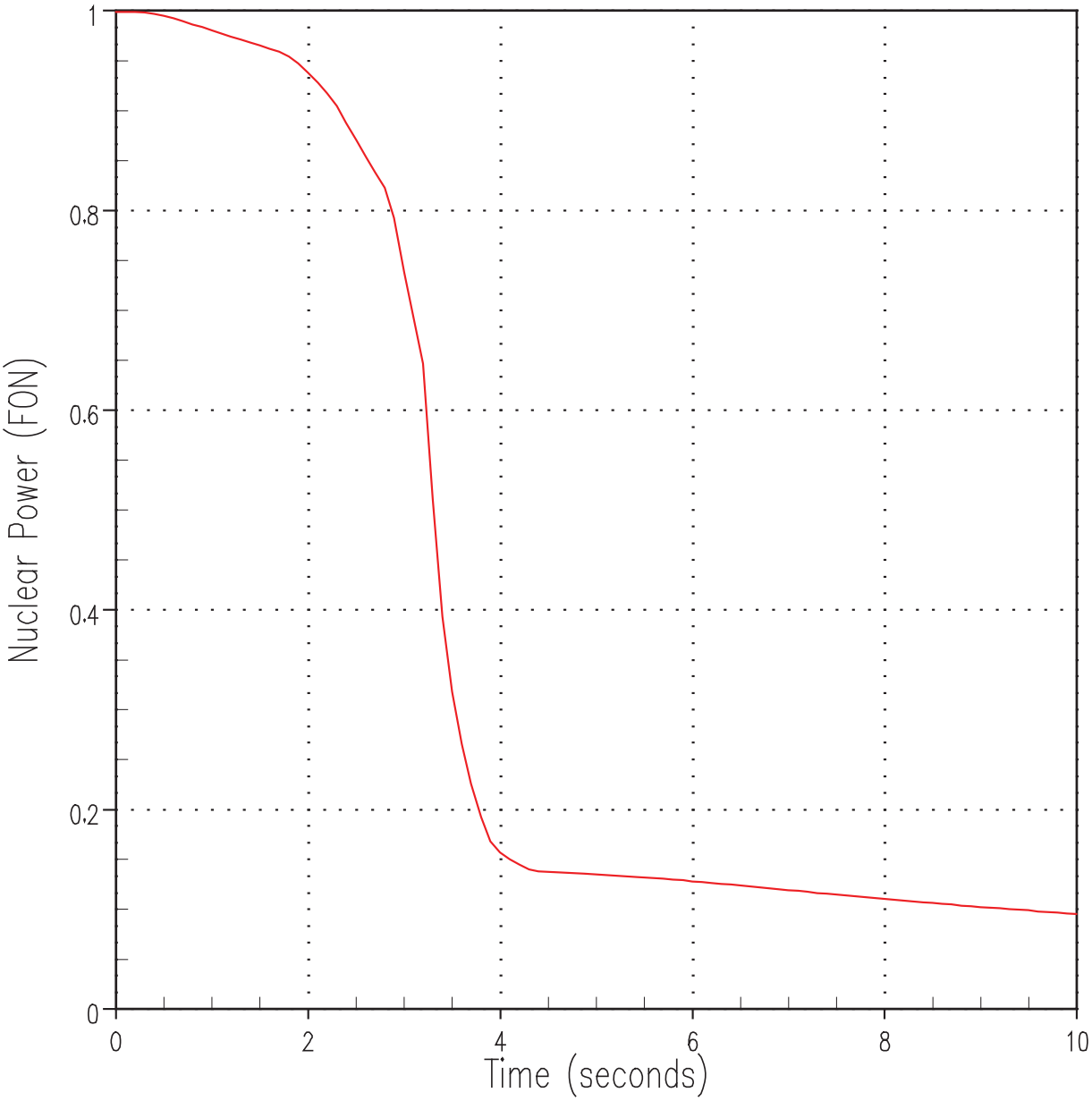


Figure 9.3.2-2. Nuclear Power Transient for 4 of 4 RCPs CLOF (Loss of Voltage)

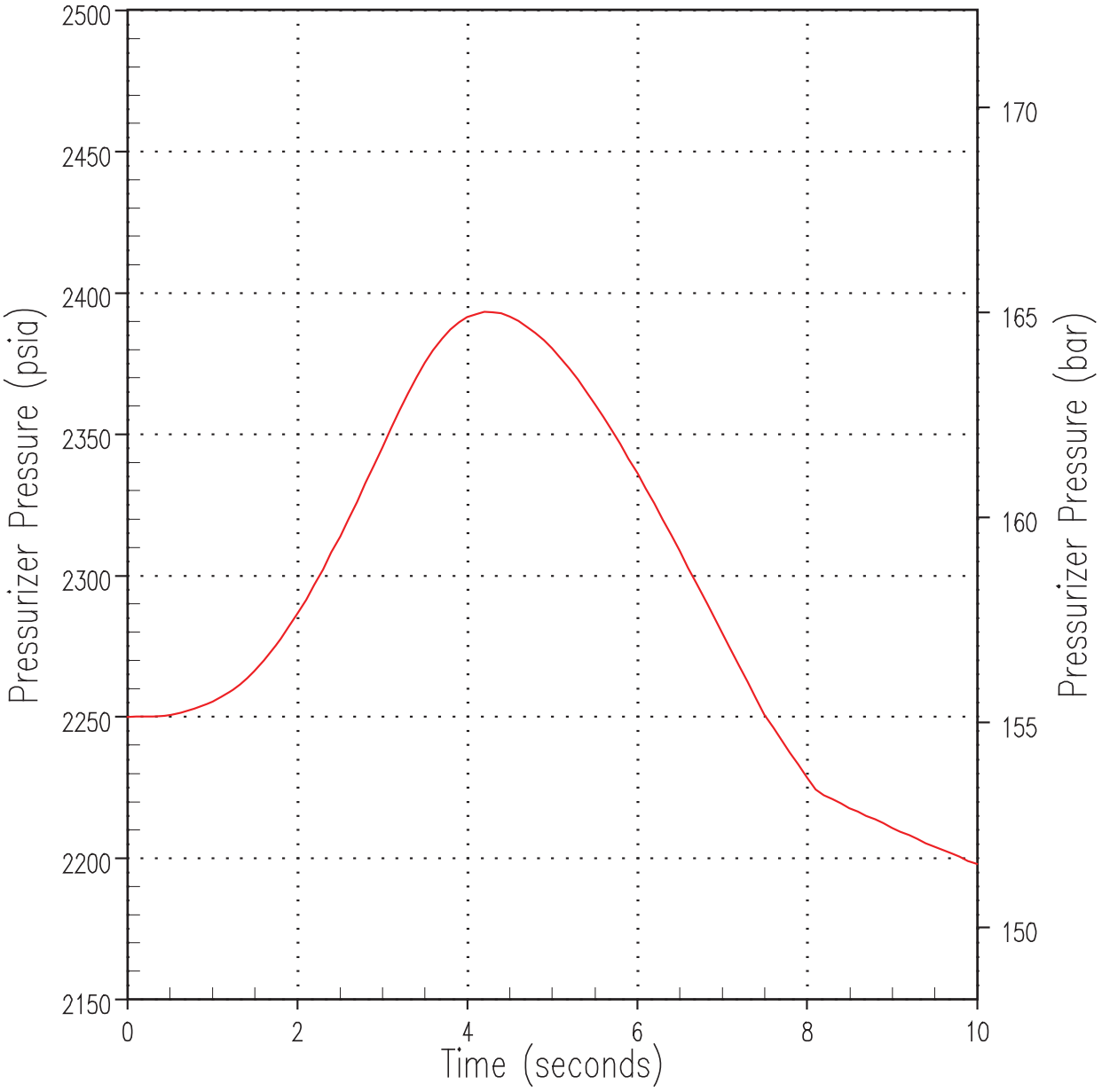


Figure 9.3.2-3. Pressuriser Pressure Transient for 4 of 4 RCPs CLOF (Loss of Voltage)

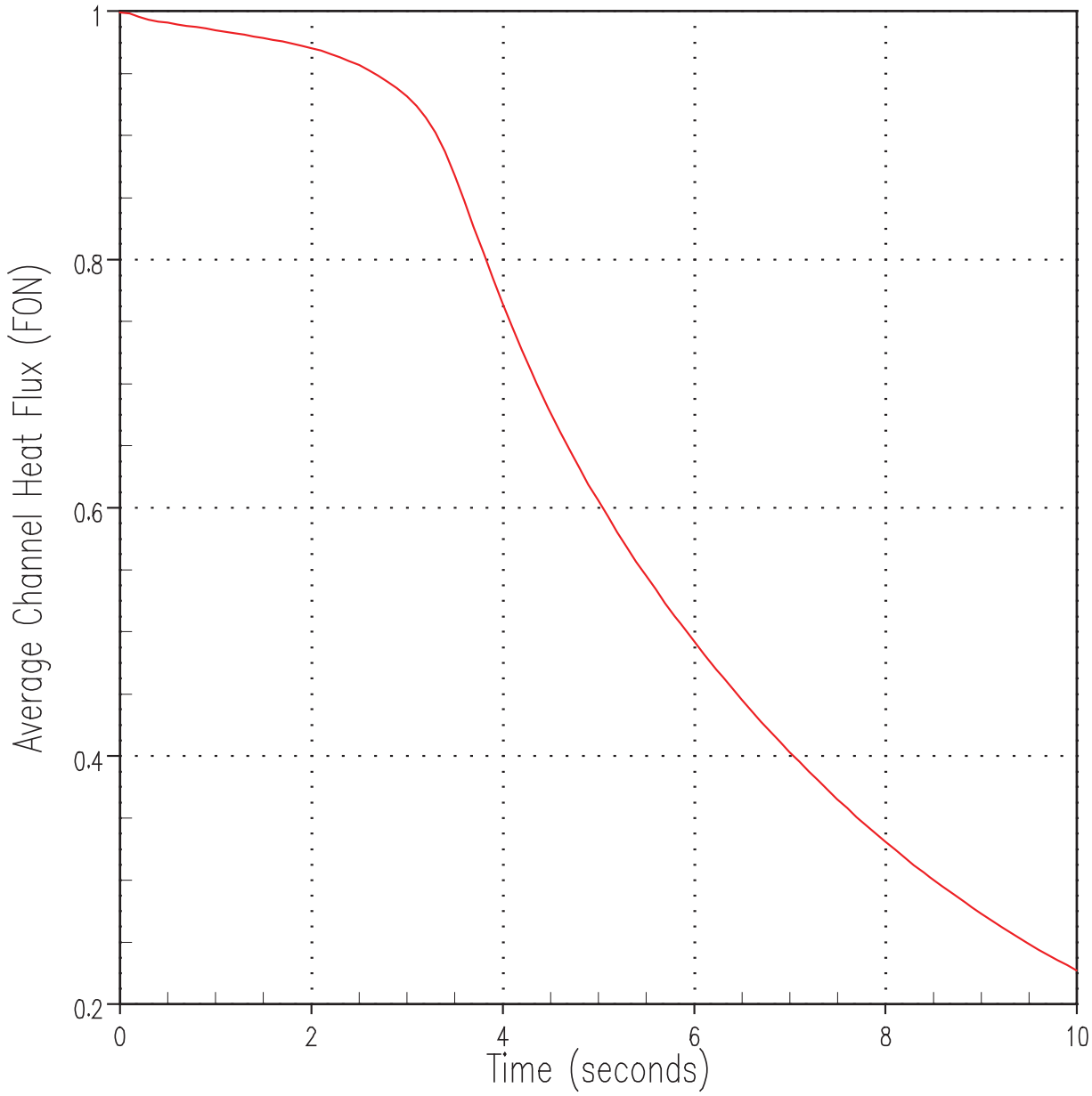


Figure 9.3.2-4. Average Channel Heat Flux Transient for 4 of 4 RCPs CLOF (Loss of Voltage)

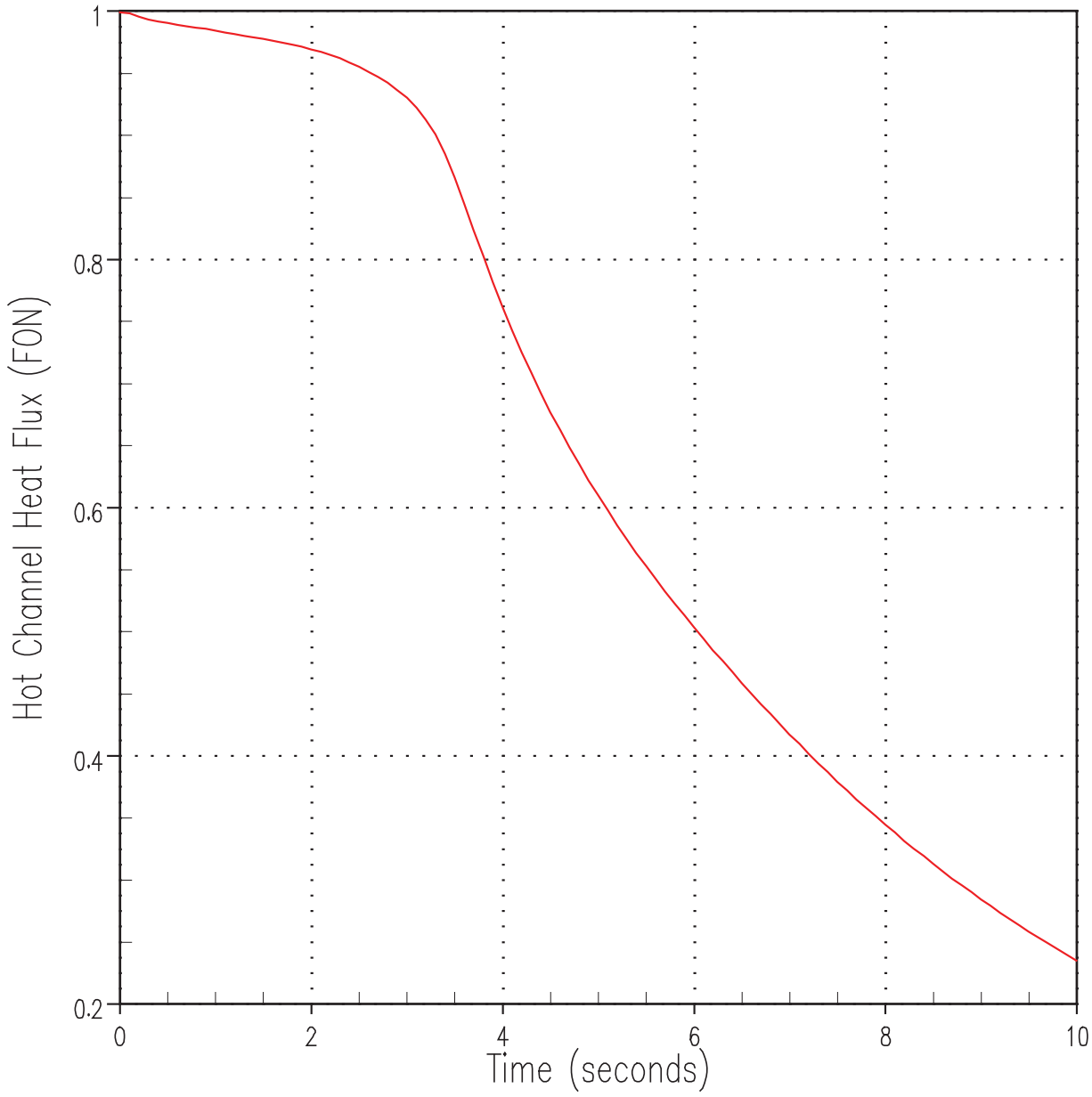


Figure 9.3.2-5. Hot Channel Heat Flux Transient for 4 of 4 RCPs CLOF (Loss of Voltage)

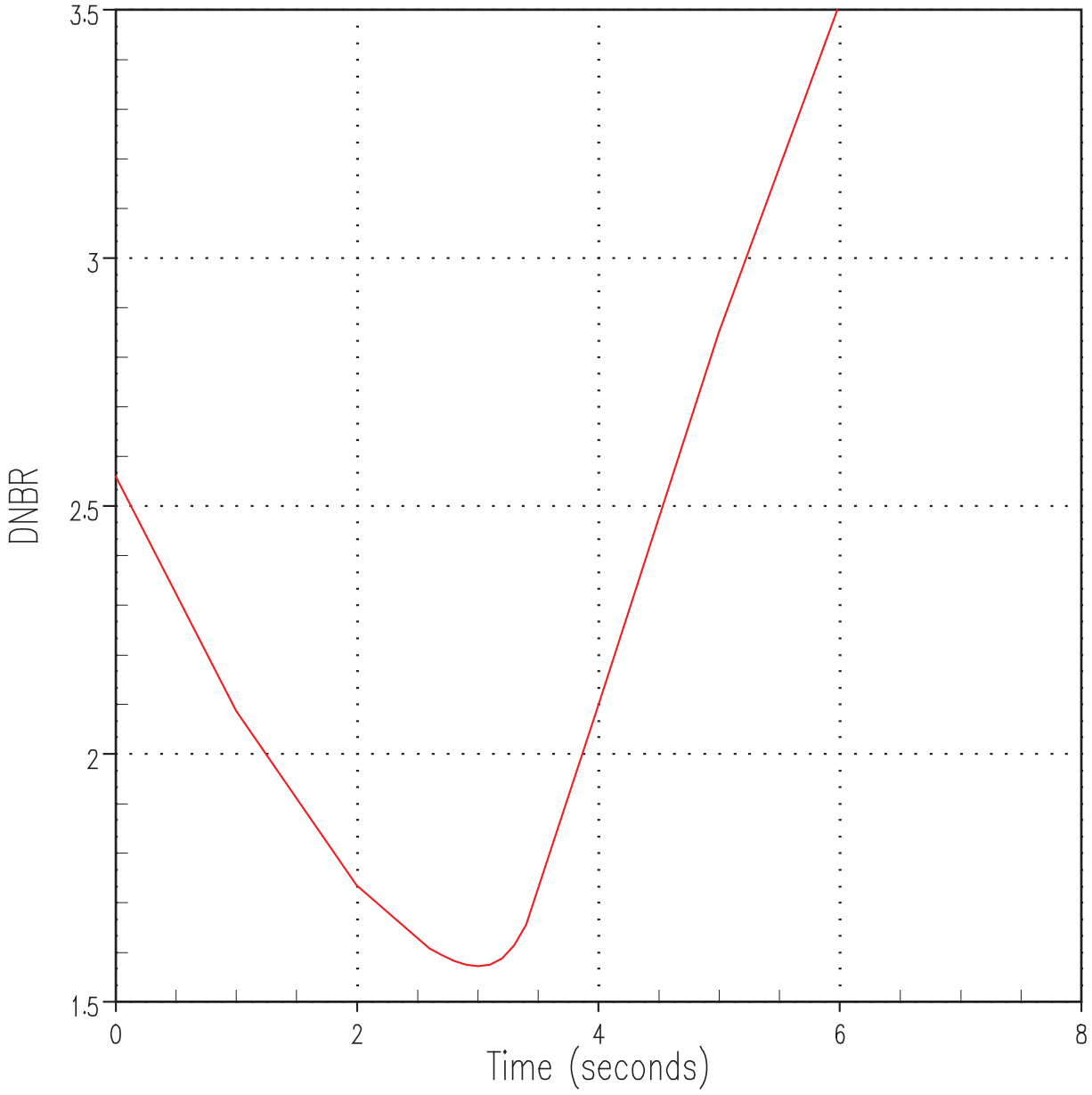


Figure 9.3.2-6. DNBR Transient for 4 of 4 RCPs CLOF (Loss of Voltage)

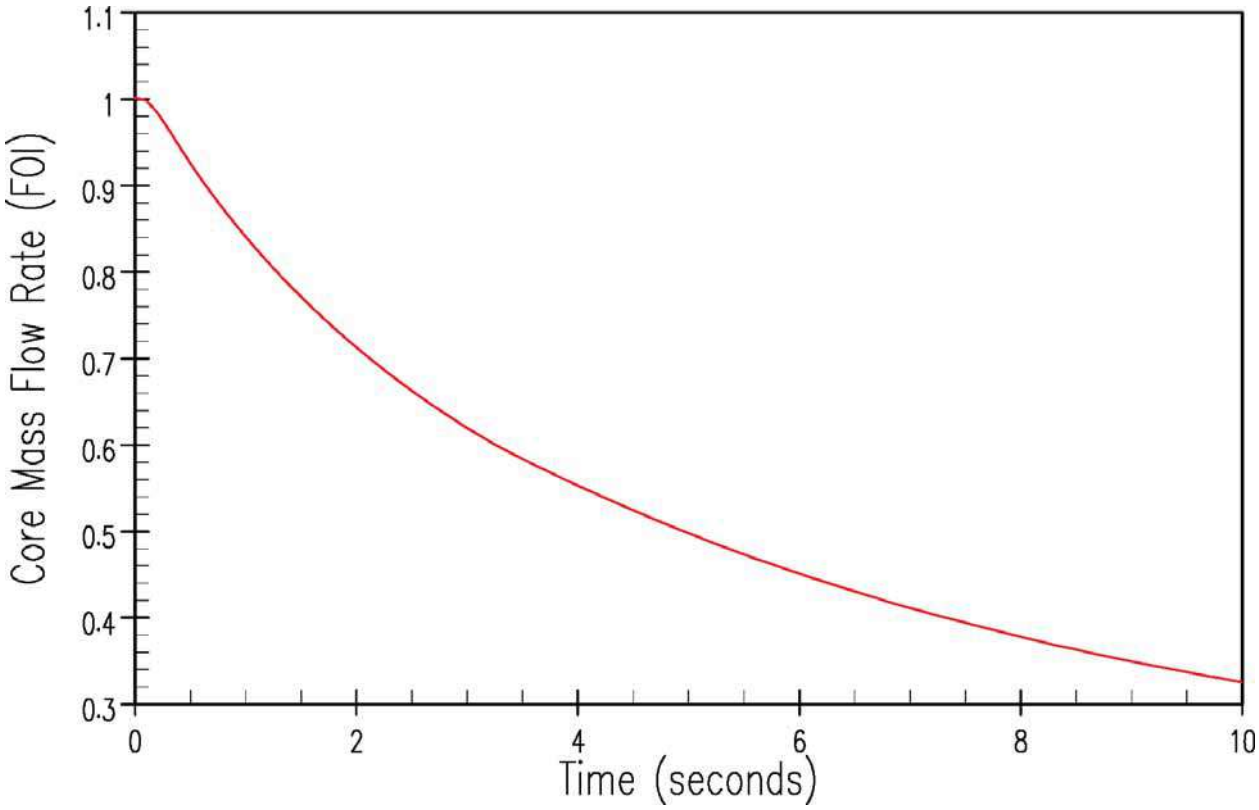


Figure 9.3.2-7. Core Mass Flow Transient for 4 of 4 RCPs CLOF (Grid Frequency Perturbation)

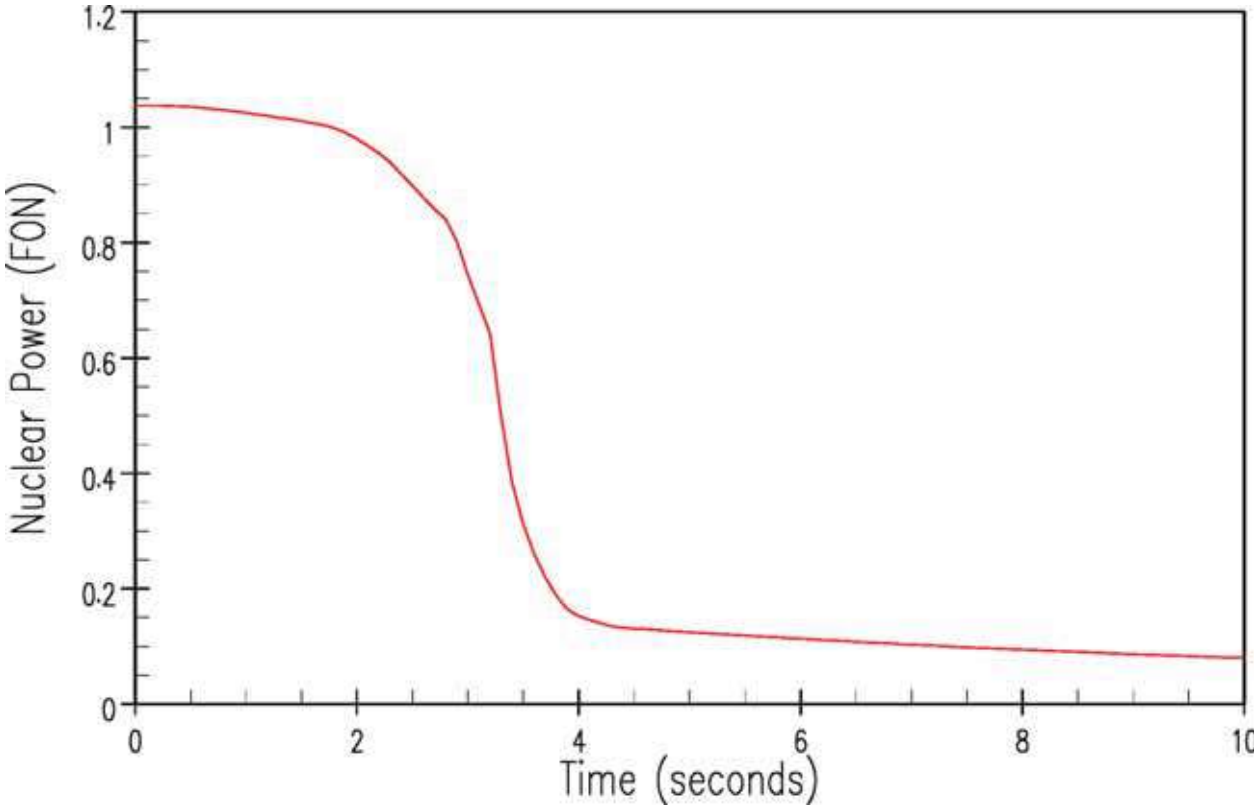


Figure 9.3.2-8. Nuclear Power Transient for 4 of 4 RCPs CLOF (Grid Frequency Perturbation)

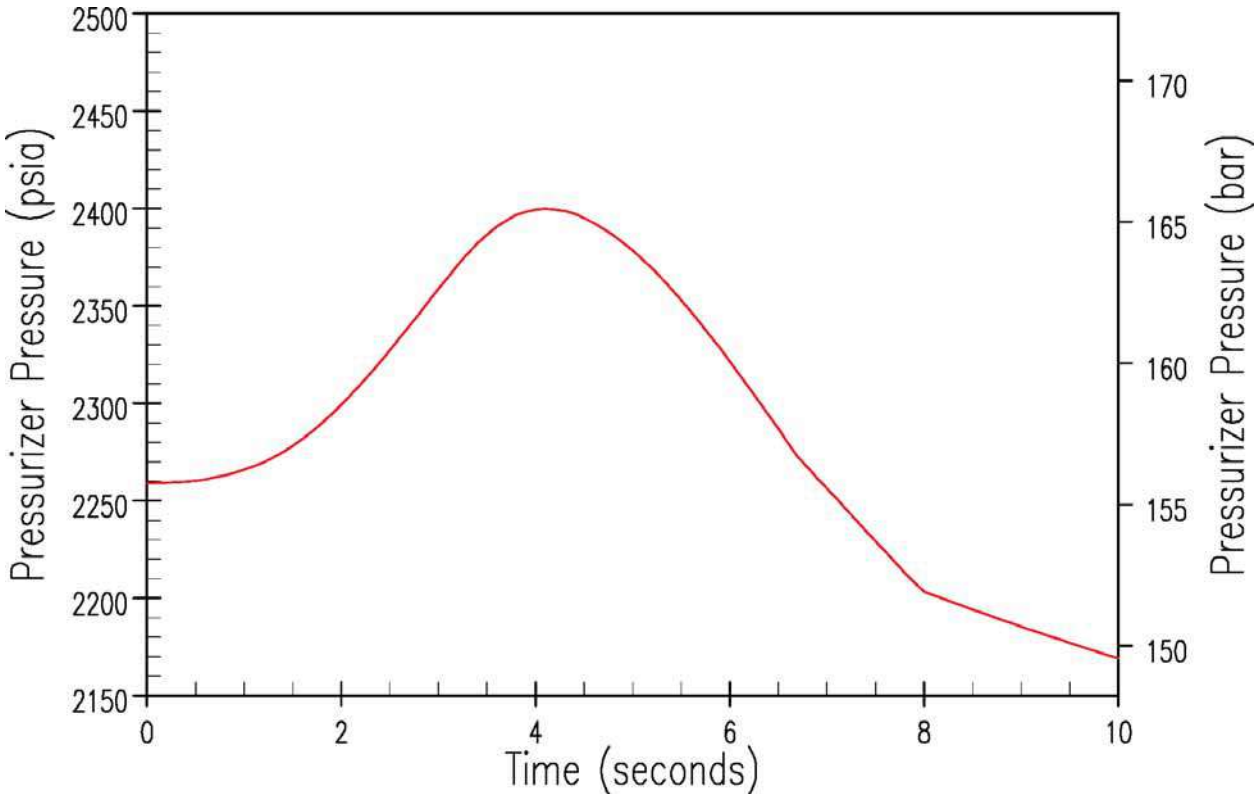


Figure 9.3.2-9. Pressuriser Pressure Transient for 4 of 4 RCPs CLOF (Grid Frequency Perturbation)

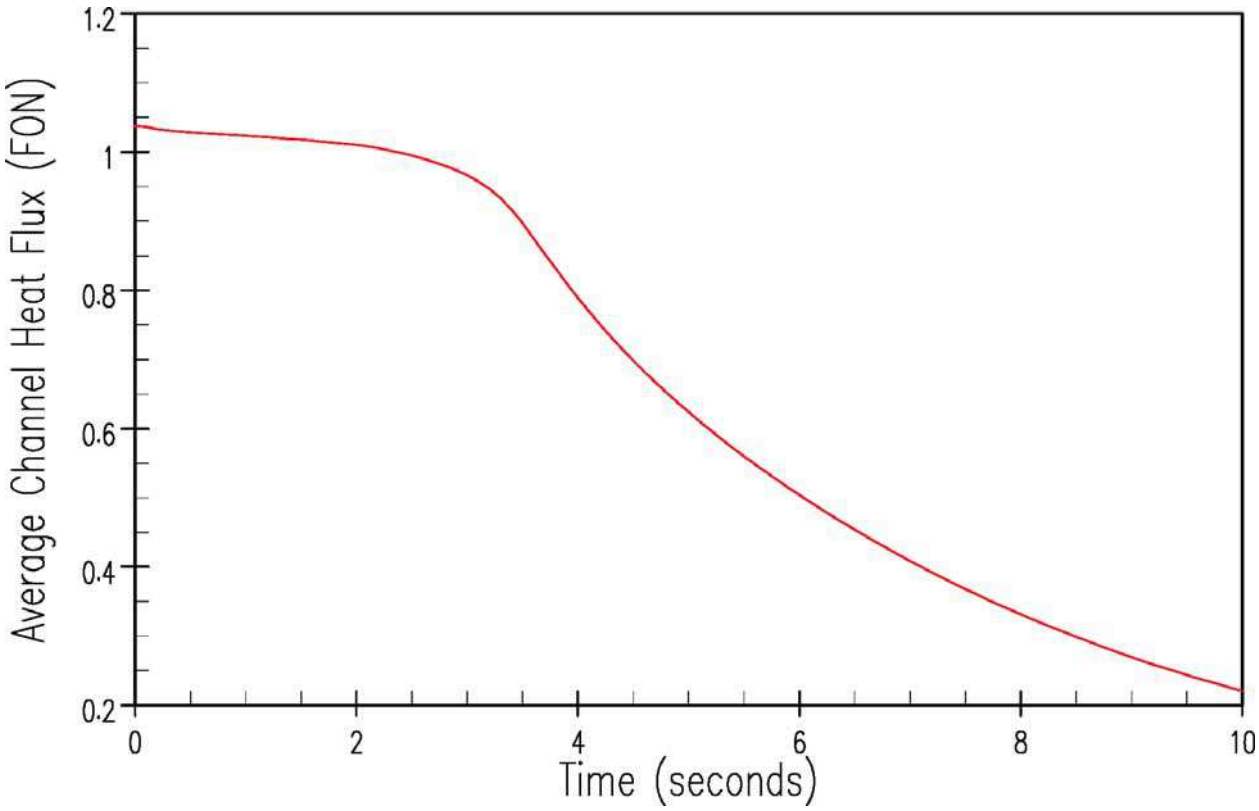


Figure 9.3.2-10. Average Channel Heat Flux Transient for 4 of 4 RCPs CLOF (Grid Frequency Perturbation)

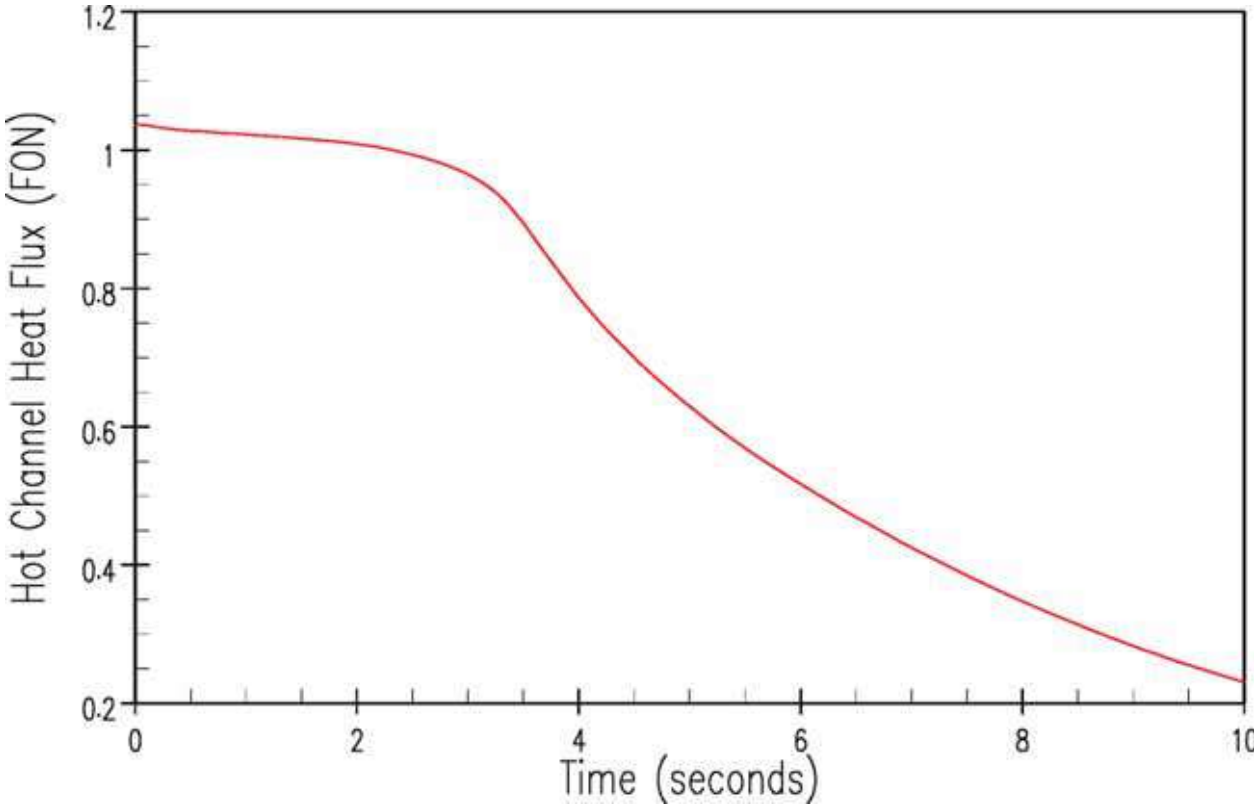


Figure 9.3.2-11. Hot Channel Heat Flux Transient for 4 of 4 RCPs CLOF (Grid Frequency Perturbation)

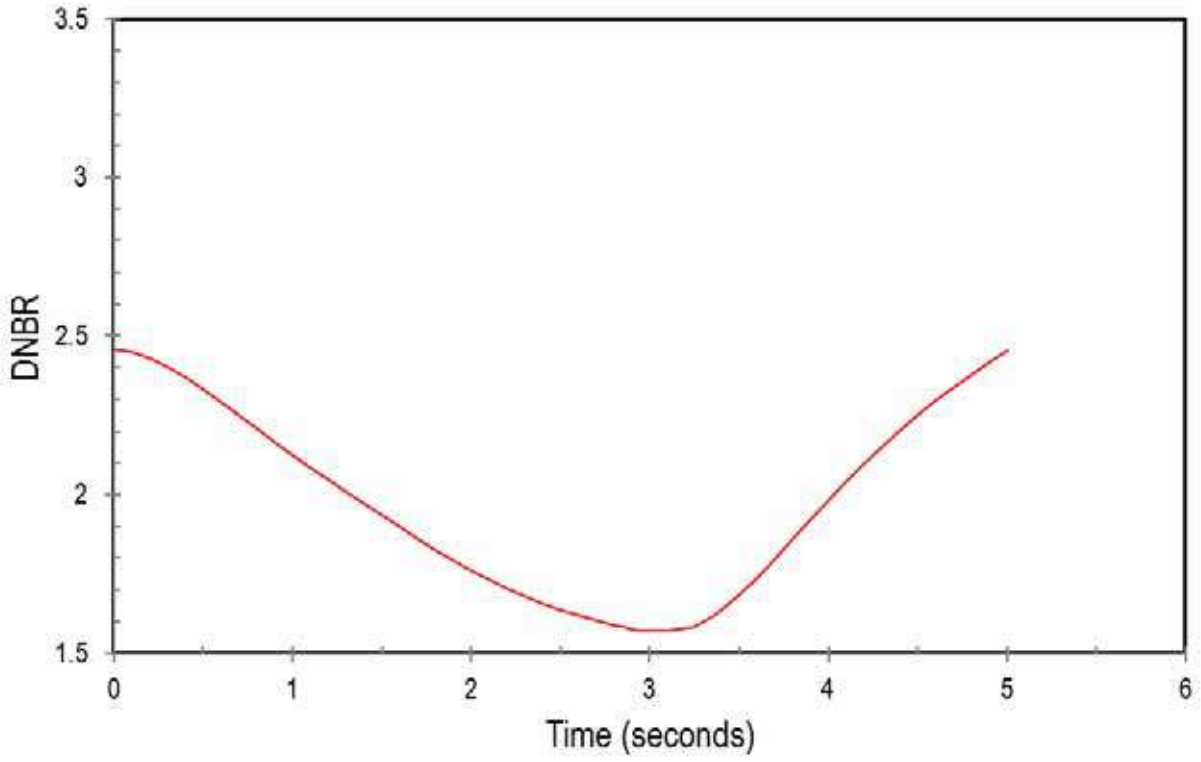


Figure 9.3.2-12. DNBR Transient for 4 of 4 RCPs CLOF (Grid Frequency Perturbation)

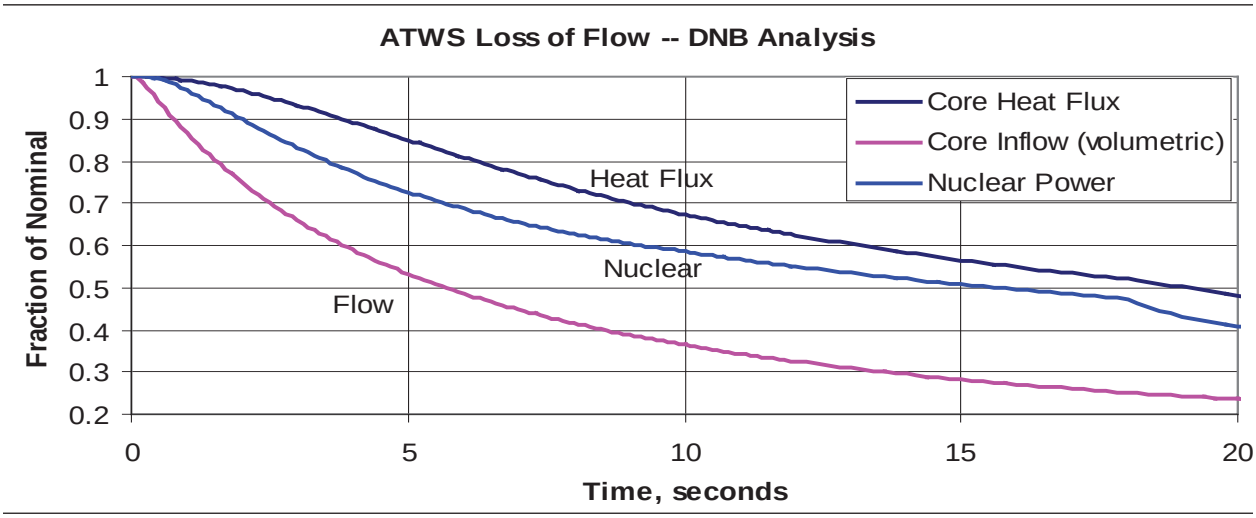


Figure 9.3.2-13. ATWT Limiting DNB 4 of 4 RCPs CLOF Case 1 – Core Power and Flow

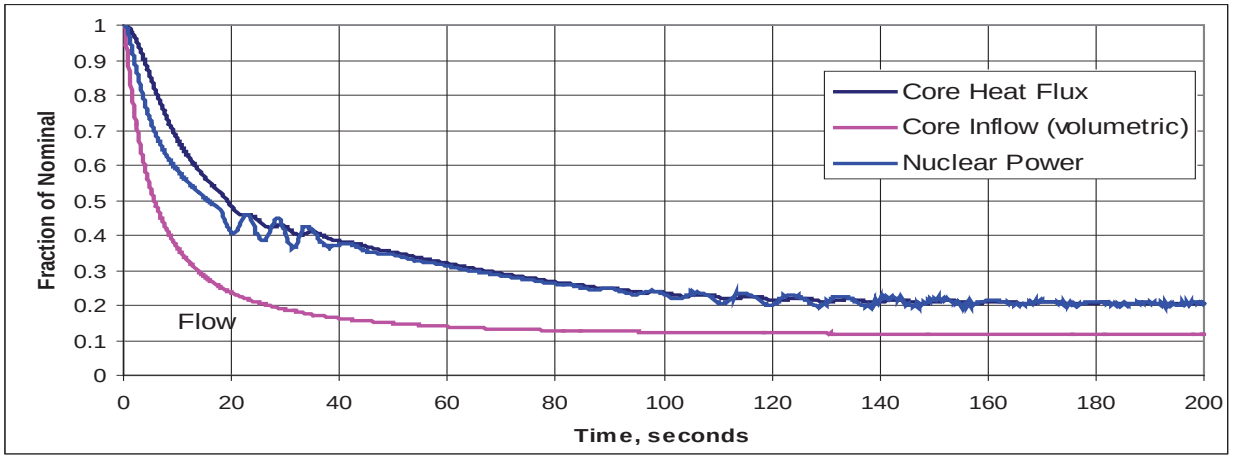


Figure 9.3.2-14. ATWT Limiting DNB 4 of 4 RCPs CLOF Case 1 – Core Power and Flow

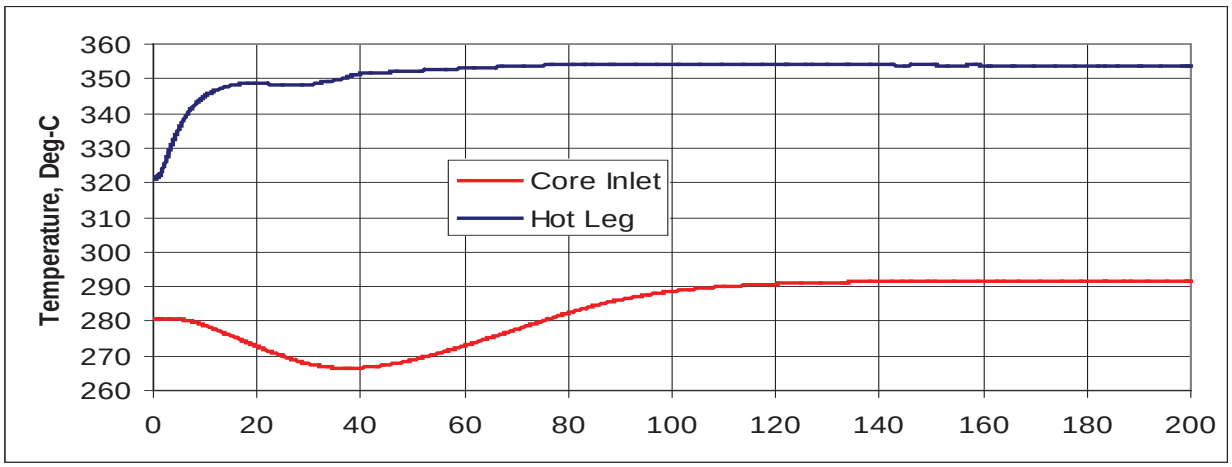


Figure 9.3.2-15. ATWT Limiting DNB 4 of 4 RCPs CLOF Case 1 – T_{HOT} and T_{COLD}

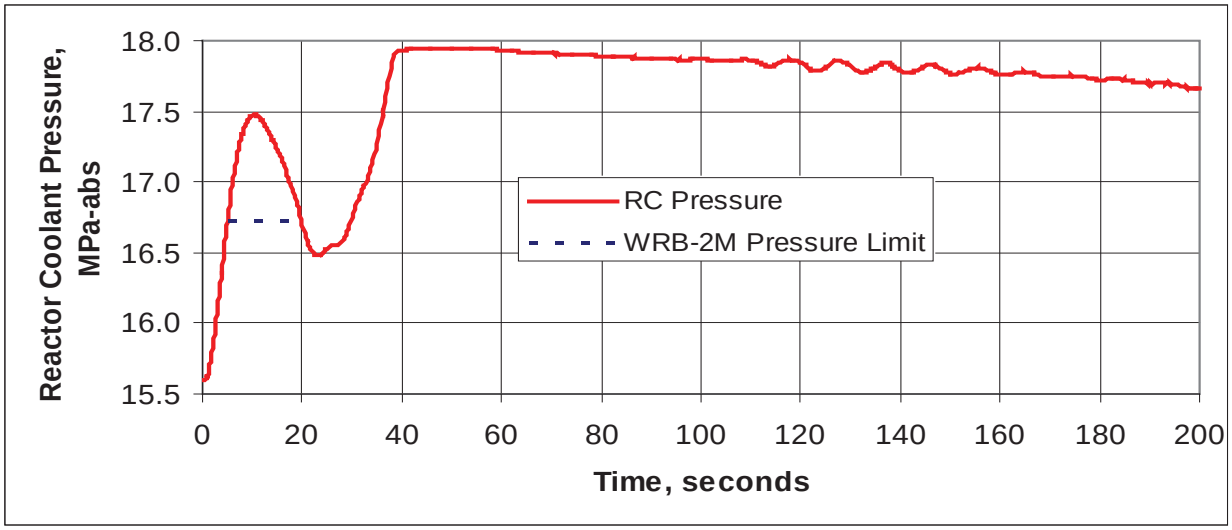


Figure 9.3.2-16. ATWT Limiting DNB 4 of 4 RCPs CLOF Case 1 – Core Pressure

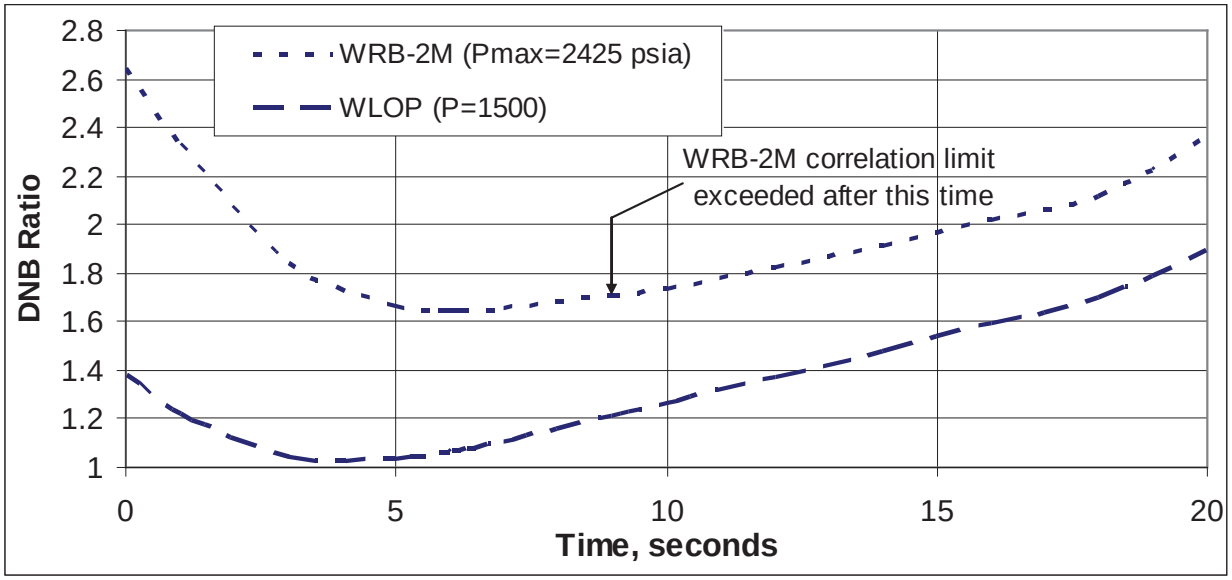


Figure 9.3.2-17. ATWT Limiting DNB 4 of 4 RCPs CLOF Case 1 – DNB Ratio

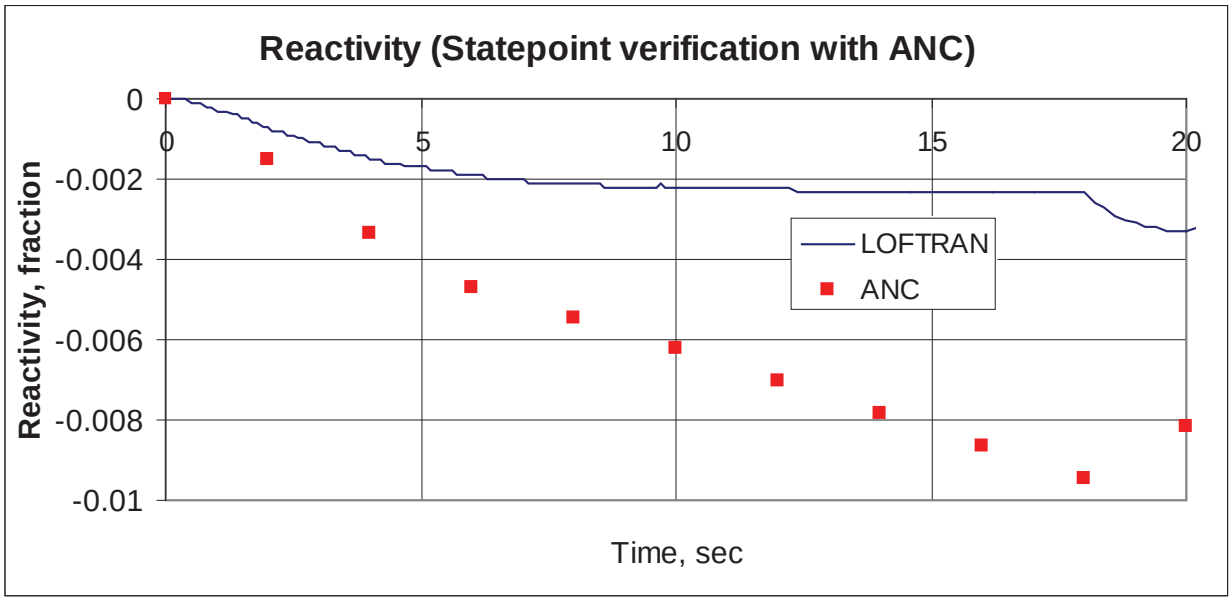


Figure 9.3.2-18. ATWT Limiting DNB 4 of 4 RCPs CLOF Case 1 – Reactivity

Figure 9.3.2-19. Not Used

Figure 9.3.2-20. Not Used

Figure 9.3.2-21. Not Used

Figure 9.3.2-22. Not Used

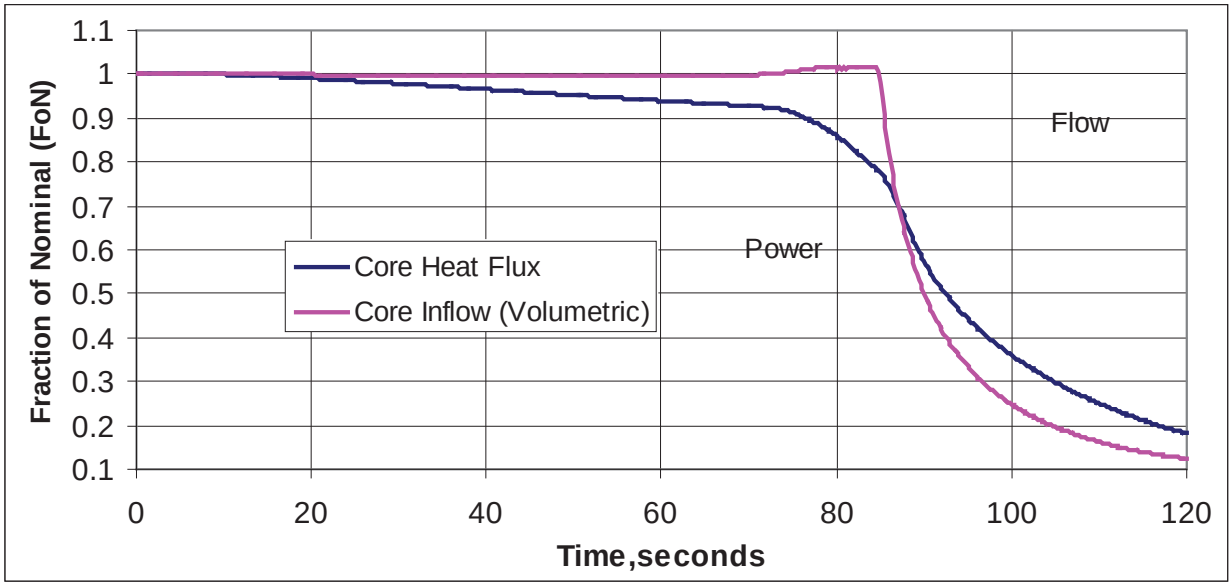


Figure 9.3.2-23. ATWT Limiting DNB 4 of 4 RCPs CLOF ATWT Case 2 – Core Power and Flow

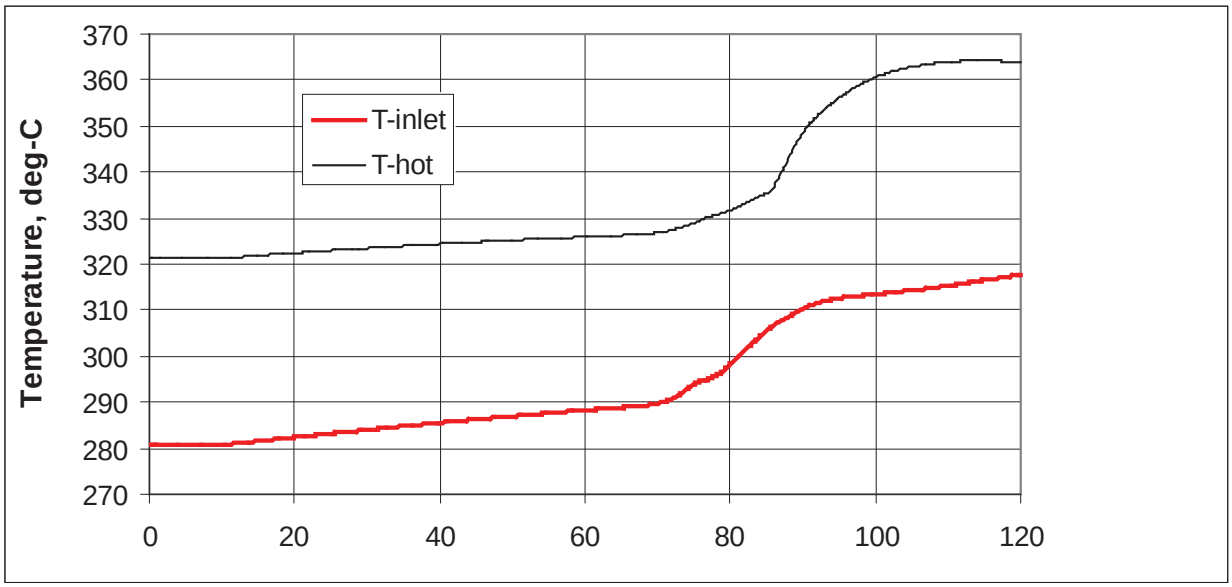


Figure 9.3.2-24. ATWT Limiting DNB 4 of 4 RCPs CLOF Case 2 – T_{HOT} and T_{COLD}

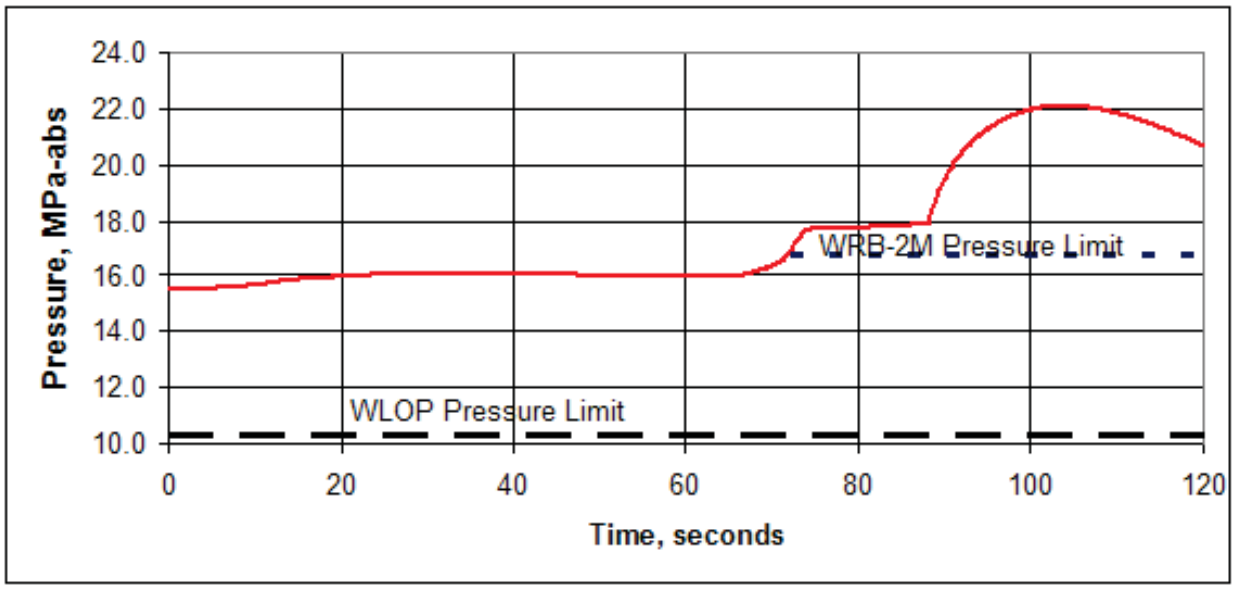


Figure 9.3.2-25. ATWT Limiting DNB 4 of 4 RCPs CLOF Case 2 – RCS Pressure

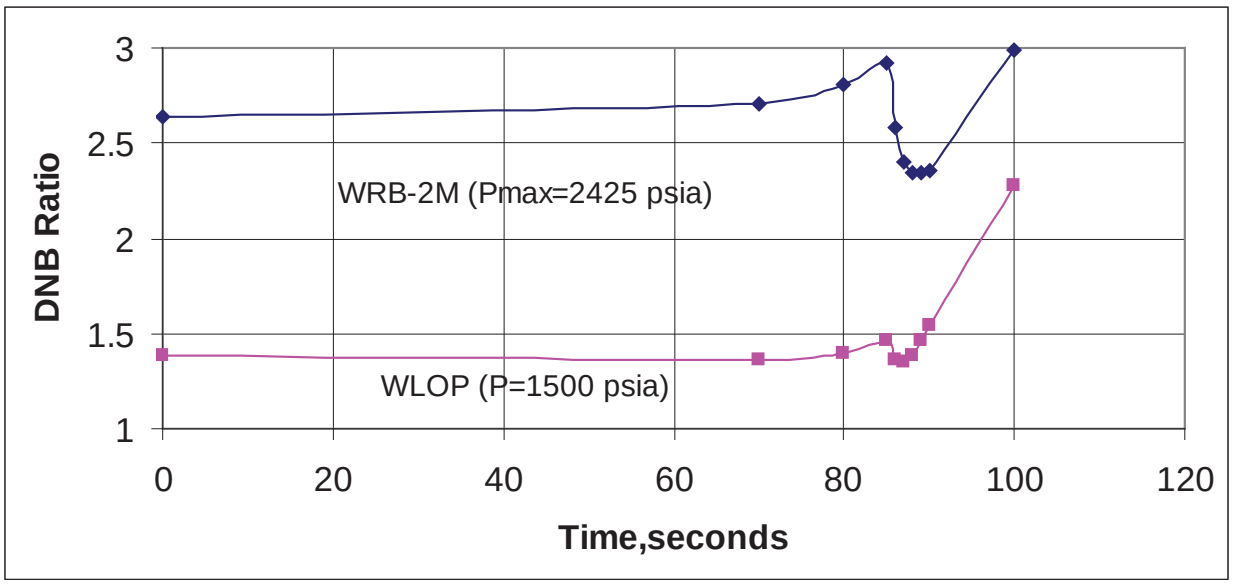


Figure 9.3.2-26. ATWT Limiting DNB 4 of 4 RCPs CLOF Case 2 – T_{HOT} and T_{COLD}

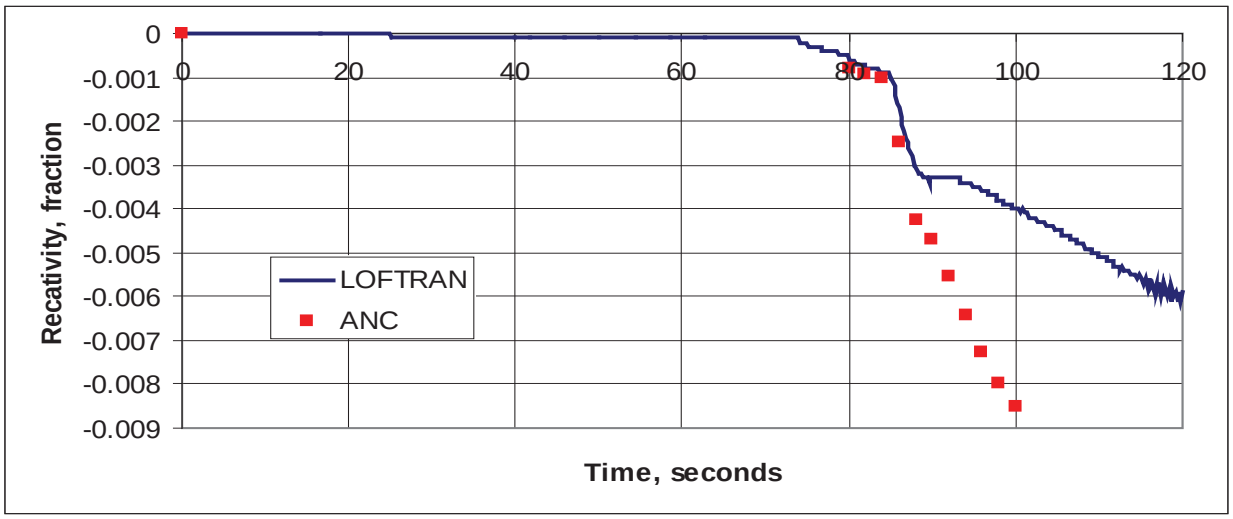


Figure 9.3.2-27. ATWT Limiting DNB 4 of 4 RCPs CLOF Case 2 – Reactivity

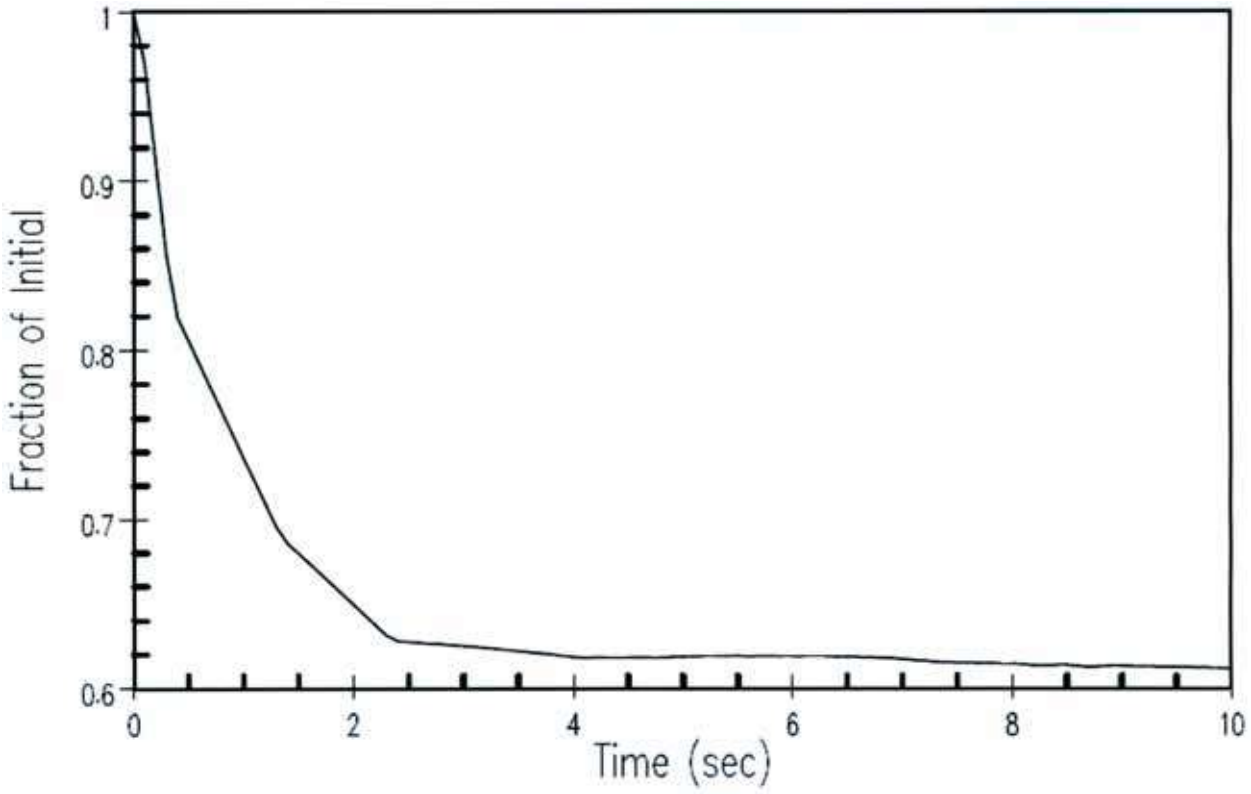


Figure 9.3.3-1. DBA Core Mass Flow Transient for 1 of 4 RCPs Locked Rotor

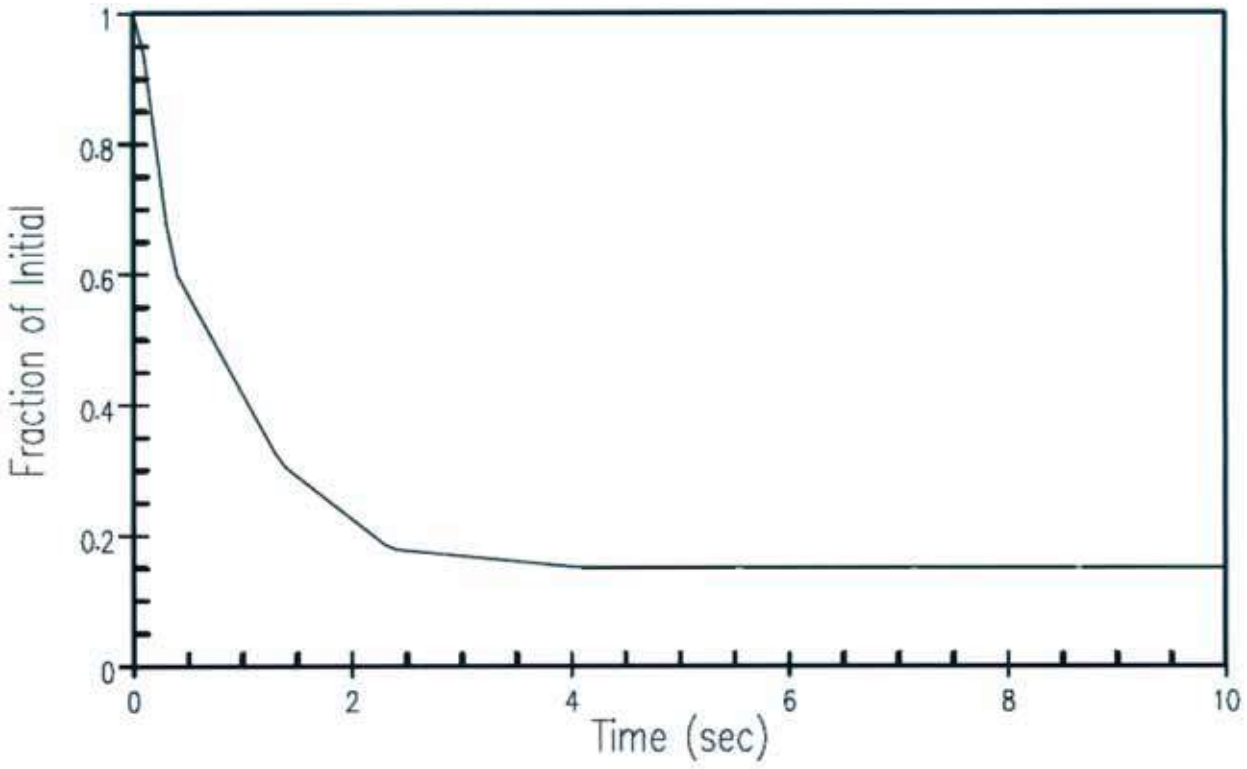


Figure 9.3.3-2. DBA Faulted Loop Volumetric Flow Transient for 1 of 4 RCPs Locked Rotor

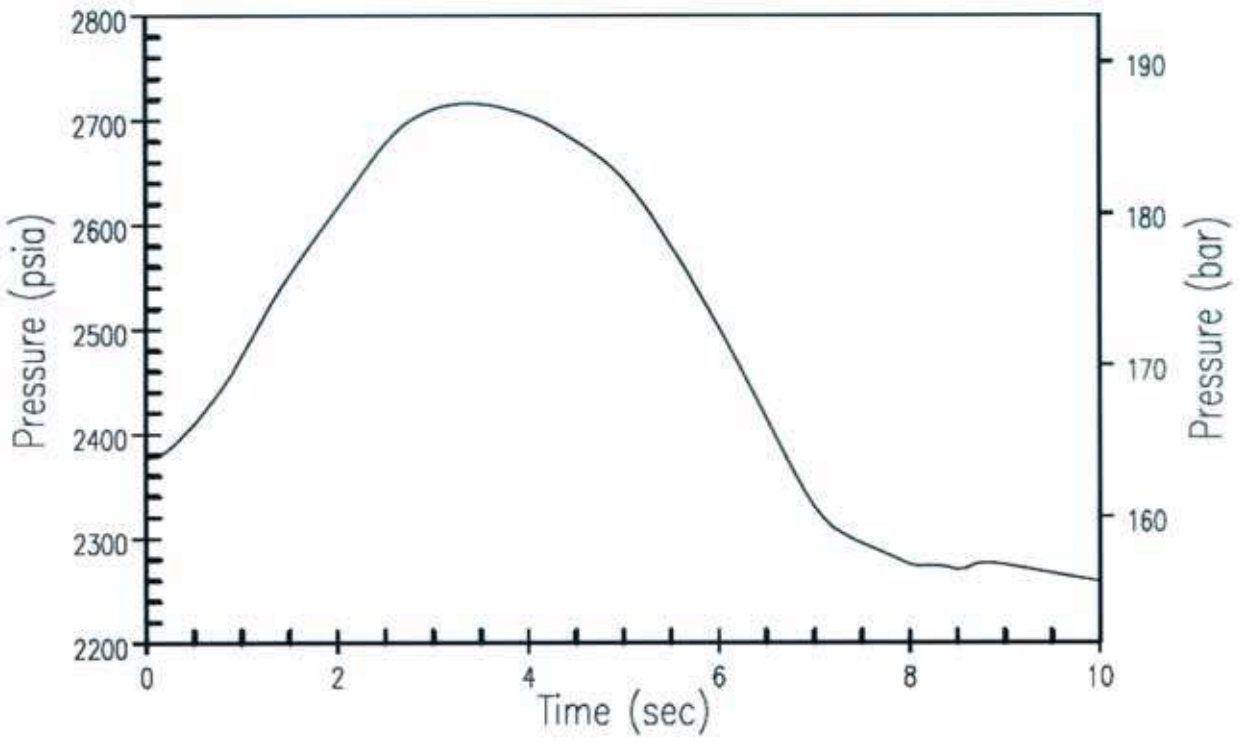


Figure 9.3.3-3. DBA Peak Reactor Coolant Pressure for 1 of 4 RCPs Locked Rotor

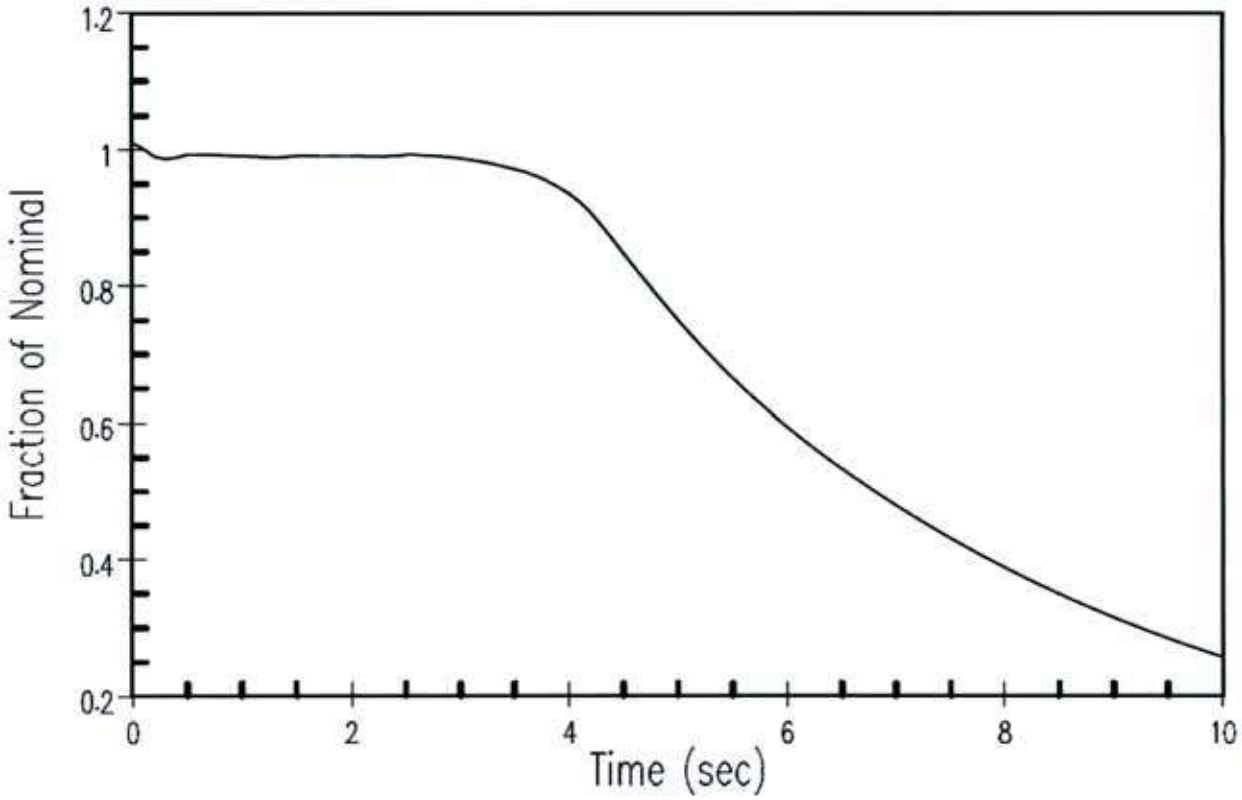


Figure 9.3.3-4. DBA Average Channel Heat Flux Transient for 1 of 4 RCPs Locked Rotor

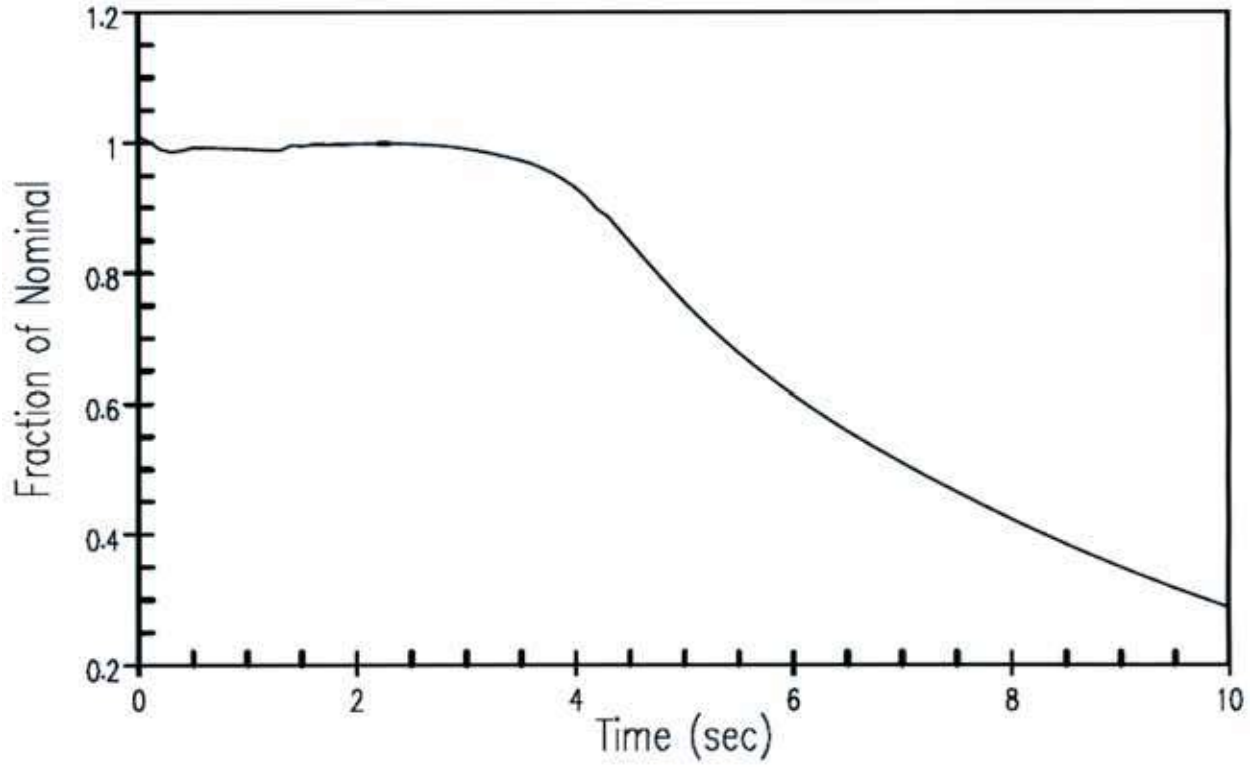


Figure 9.3.3-5. DBA Hot Channel Heat Flux Transient for 1 of 4 RCPs Locked Rotor

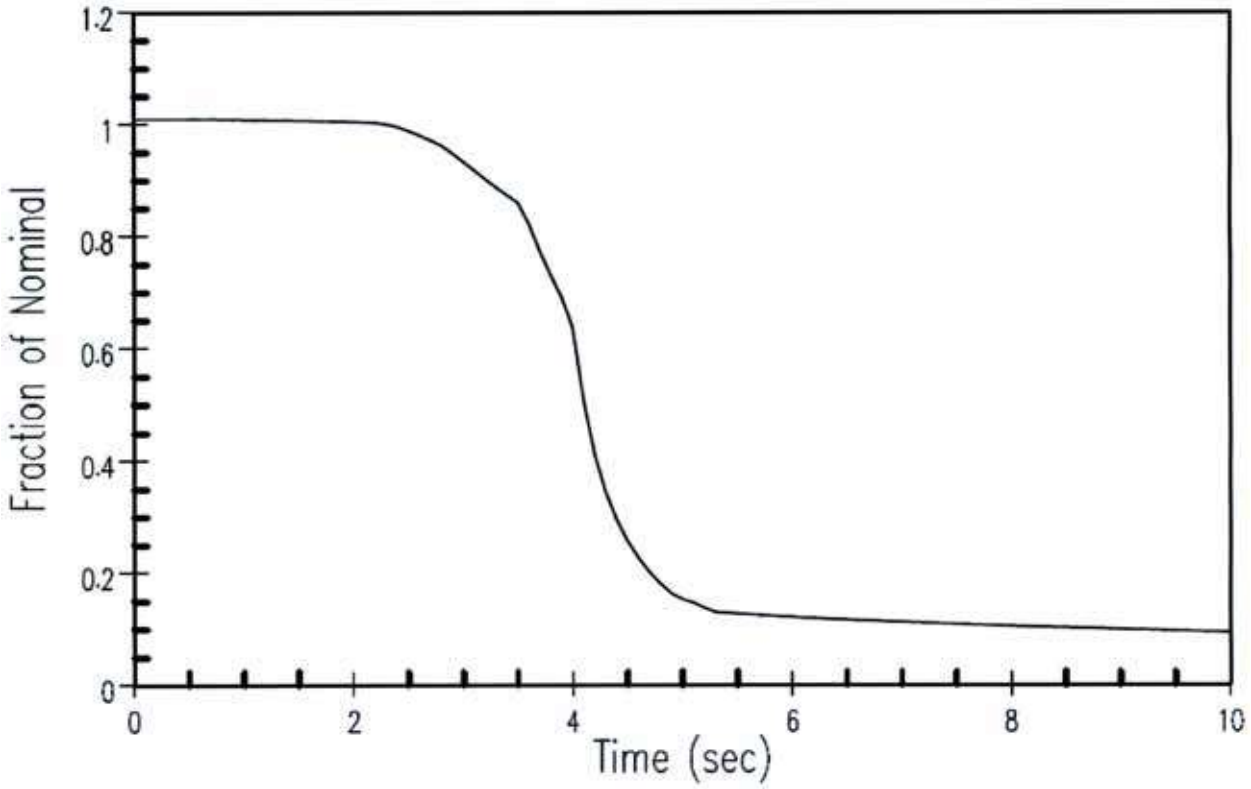


Figure 9.3.3-6. DBA Nuclear Power Transient for 1 of 4 RCPs Locked Rotor

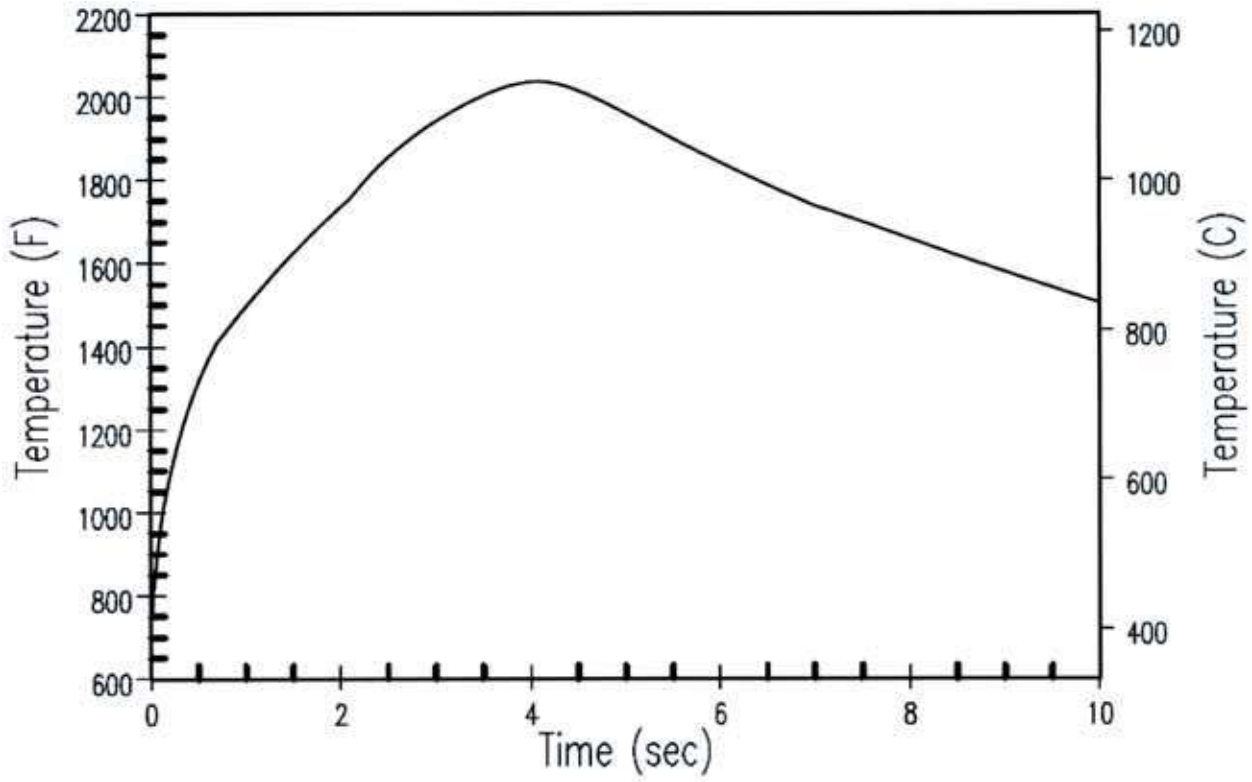


Figure 9.3.3-7. DBA Cladding Inside Temperature Transient for 1 of 4 RCPs Locked Rotor

9.4 Reactivity and Power Distribution Anomalies

A number of faults are postulated that result in reactivity and power distribution anomalies. Reactivity changes could be caused by control rod motion or ejection, boron concentration changes, or addition of cold water to the reactor coolant system. Power distribution changes could be caused by control rod motion, misalignment, or ejection, or by static means such as fuel assembly mislocation. These events are discussed in this section. Analyses are presented for the most limiting of these events.

9.4.0 Introduction and Overview of Faults

Reactivity changes can be caused by a number of initiating faults which are split into two parts:

- Reactivity and power distribution faults (excluding control rod ejection).
    - Uncontrolled rod cluster control assembly bank withdrawal from a subcritical or low-power startup condition
    - Uncontrolled rod cluster control assembly bank withdrawal at power
    - Rod cluster control assembly misalignment due to system malfunction or operator error
    - Inadvertent boron dilution due to controller, operator or mechanical failure of CVS
- Rod ejection faults.
    - Single rod cluster control assembly ejection fault

This section considers these faults in turn. Each fault is first described; the initial event frequency and the design basis class are provided and the bounding fault or faults are identified (if needed). The analysed faults are presented individually in Table 8A-2.

The analysed fault(s) are described in additional detail in the subsequent sections to complete the safety case for each fault, including:

- Identification of Causes and Accident Description
- Design Basis Analysis of Effects and Consequences
- Assessment of the Radiological Consequences for the DBA
- Diverse Mitigation and ATWT for Frequent Faults
- ALARP Assessment
- Conclusions

ATWT analyses presented herein are based on Reference 9.4-20 and supplemented by diversity cases for lower mode accidents from Reference 9.4-23.

9.4.0.1 Reactivity and Power Distribution Faults (Excluding Control Rod Ejection)

Description

A number of transients and accidents could result in an addition of reactivity to the core. These faults are shown below:

- Uncontrolled RCCA bank withdrawal from a subcritical or low-power startup condition (Fault 1.15.1)

- Uncontrolled RCCA bank withdrawal at power (Fault 1.15.4)

- RCCA misalignment as a result of one of the following (Faults 1.15.5, 1.15.5a, and 1.15.5b):

  – One or more dropped RCCAs within the same group
  – Statically misaligned RCCA
  – Uncontrolled withdrawal of a single RCCA

- CVS malfunctions that result in a decrease in the boron concentration in the reactor coolant (Fault 1.15.7)

- Inadvertent loading and operation of a fuel assembly in an improper position (Fault 1.15.10)

An uncontrolled addition of reactivity to the core results in a power excursion. Such a transient can be caused, for example, by a malfunction of the reactor control or rod control systems. This can occur with the reactor subcritical, at hot zero power (HZP), or at power.

Although the reactor is normally brought to power from a subcritical condition by RCCA withdrawal, initial startup procedures with a clean core use boron dilution. The maximum rate of reactivity increase in the case of boron dilution is less than that assumed for the transients caused by reactivity insertion by the control rods.

The neutron flux response to a continuous reactivity insertion is characterised by a fast rise terminated by the reactivity feedback effect of the negative Doppler coefficient. This self-limitation of the power excursion restricts the power during the delay time for protective action. Should a continuous addition of reactivity accident occur, the transient is terminated by the automatic features of the PMS.

RCCA ejection accidents also result in an addition of reactivity to the core but are considered separately, since they place significant demands on additional safety systems.

Initiating Event Frequency[1]

Appendix 8A gives frequencies for various reactivity and power distribution faults as less than 0.01/yr. All these frequencies are conservative for a range of reactivity insertion scenarios, but the one for single RCCA withdrawal is judged to be overly conservative, as it would require multiple failures (either electrical failures or operator errors) to occur. A more realistic frequency is less than 1E-04/yr.

The value of less than 1E-04/yr is estimated based on the following. The probability of open wire (or terminal) failure is 1.6E-08/hr in Reference 9.4-6. The resulting yearly frequency is 1.4E-04. These wire failures would also have to occur coincidently with either a breakdown or an operator disregard of the indications mentioned above, so the frequency is considered to be <1E-04.

[1] As discussed in Chapter 8, the frequency for initiating events from the PSA is used in both Chapters 8 and 9 with the sole purpose of supporting the categorisation of the fault to a specific DB category. As noted in Chapter 8, these probabilities should not be considered to be representative of actual frequency of the events, and for several events they can be significantly conservative. Detailed PSA results and their basis are discussed in Chapter 10.

Design Basis Class

The unmitigated consequences of reactivity faults are assumed to be greater than the Target 4 BSL for frequent faults (1 mSv offsite and 20 mSv onsite). Given the IEF above, the events are in the DB2 class.

9.4.0.2 Rod Ejection Faults

Description

This fault is the ejection of a single RCCA assembly from the reactor core (Fault 1.15.11).

This fault is defined as the mechanical failure of a control rod mechanism pressure housing resulting in the ejection of an RCCA from the core. This results in a rapid positive reactivity insertion with an adverse core power distribution.

In general, the reactor is operated with the RCCAs inserted only far enough to permit load following. This limits the size of the reactivity insertion caused by the RCCA ejection. The axial offset RCCAs are positioned so that the targeted axial offset can be met throughout core life. Reactivity changes caused by core depletion and xenon transients are compensated for by changes in the boron concentration of the primary coolant and mechanical shim rods. Therefore, should an RCCA be ejected from its normal position during high power operation, only a limited reactivity excursion would be expected to occur.

Occasionally, it might be desirable to operate with larger than normal insertions. For this reason, a power control and axial offset rod insertion limit is defined as a function of power level. Operation with the RCCAs above this limit provides adequate shutdown capability and an acceptable power distribution. The position of the RCCAs is continuously indicated in the main control room (MCR). An alarm occurs if a bank of RCCAs approaches its insertion limit or if one RCCA deviates from its bank. Operating instructions require boration at the low-level alarm and emergency boration at the low-low-level alarm.

Initiating Event Frequency

The AP1000 design PSA gives the frequency of control rod ejection events as less than 1.0E-04/yr (Table 8A-2), which makes the fault an infrequent fault.

Design Basis Class

The unmitigated consequences of a rod ejection are assumed to be greater than the Target 4 BSL for frequent faults (1 mSv offsite and 20 mSv onsite). Given the IEF above, the event is in the DB1 class.

9.4.1 Uncontrolled Rod Cluster Control Assembly Bank Withdrawal from a Subcritical or Low-Power Startup Condition (Fault 1.15.1)

9.4.1.1 Identification of Causes and Accident Description

An RCCA withdrawal accident is an uncontrolled addition of reactivity to the reactor core caused by the withdrawal of RCCAs which results in a power excursion. Such a transient can be caused by a malfunction of the reactor control or rod control systems. This can occur with the reactor subcritical, at hot zero power, or at power. The at-power case is discussed in Section 9.4.2.

The reactor may be brought to a critical condition by either RCCA withdrawal or boron dilution. The maximum rate of reactivity increase in the case of boron dilution is less than that assumed in this analysis (see Section 9.4.6).

The RCCA drive mechanisms are grouped into preselected bank configurations. These groups prevent the RCCAs from being automatically withdrawn in other than their respective banks. Power supplied to the banks is controlled such that no more than two banks are withdrawn at the same time and in their proper withdrawal sequence. The RCCA drive mechanisms are the magnetic latch type, and coil actuation is sequenced to provide variable speed travel. The maximum reactivity insertion rate analysed is that occurring with the simultaneous withdrawal of the combination of two sequential RCCA banks having the maximum combined worth at maximum speed.

The neutron flux response to a continuous reactivity insertion is characterized by a fast rise terminated by the reactivity feedback effect of the negative Doppler coefficient. This self-limitation of the power excursion limits the power during the delay time for protective action. Should a continuous RCCA withdrawal accident occur, the transient is terminated by the following automatic features of the protection and safety monitoring system:

- Source range high neutron flux reactor trip

  This trip function is actuated when two out of four independent source range channels indicate a neutron flux level above a preselected, manually adjustable setpoint. It may be manually bypassed only after an intermediate range flux channel indicates a flux level above a specified level. It is automatically reinstated when the coincident two out of four intermediate range channels indicate a flux level below a specified level.

- Intermediate range high neutron flux reactor trip

  This trip function is actuated when two out of four independent, intermediate range channels indicate a flux level above a preselected, manually adjustable setpoint. It may be manually bypassed only after two out of four power range channels are reading above approximately 10 percent of full power. It is automatically reinstated when the coincident two out of four channels indicate a power level below this value.

- Power range high neutron flux reactor trip (low setting)

  This trip function is actuated when two out of four power range channels indicate a power level above approximately 25 percent of full power. It may be manually bypassed when two out of four power range channels indicate a power level above approximately 10 percent of full power. It is automatically reinstated when the coincident two out of four channels indicate a power level below this value.

- Power range high neutron flux reactor trip (high setting)

  This trip function is actuated when two out of four power range channels indicate a power level above a preset setpoint. It is always active.

- High nuclear flux rate reactor trip

  This trip function is actuated when the positive rate of change of neutron flux on two out of four nuclear power range channels indicate a rate above a preset setpoint.

In addition, control rod stops on high intermediate range flux level (one out of two) and high power range flux level (one out of four) serve to discontinue rod withdrawal and prevent the need to actuate the intermediate range flux level trip and the power range flux level trip, respectively.

9.4.1.2 Design Basis Mitigation

Analysis is performed to demonstrate the adequacy of the PMS to detect and mitigate the fault and show that the safety analysis criteria are satisfied including:

- No fuel failures (confirmed using minimum DNBR and fuel melt criteria),
- The RCS pressure criterion is met,
- The MSS pressure criterion is met, and
- The pressuriser does not fill (which could result in a LOCA)

It is noted that this event is bounded by the Section 9.2.3 analysis with respect RCS/MSS pressure and pressuriser filling criteria, therefore, these limits are not explicitly confirmed for this event. Accordingly, fuel failure is the primary criterion for this event.

9.4.1.2.1 DBA Method of Analysis

The analysis of the uncontrolled RCCA bank withdrawal from subcritical accident is performed in three stages: first, an average core nuclear power transient calculation; then, an average core heat transfer calculation; and finally, the DNBR calculation. In the first stage, the average core nuclear calculation is performed using spatial neutron kinetics methods, using the code TWINKLE (Reference 9.4-1), to determine the average power generation with time, including the various total core feedback effects (Doppler reactivity and moderator reactivity).

In the second stage, the average heat flux and temperature transients are determined by performing a fuel rod transient heat transfer calculation in FACTRAN (Reference 9.4-2). In the final stage, the average heat flux is used in VIPRE-01 (described in Section 22.7.1.1) for the transient DNBR calculation.

Plant characteristics and initial conditions are discussed in Section 9.0.2. The following assumptions are made to give conservative results for a startup accident:

- Because the magnitude of the power peak reached during the initial part of the transient for any given rate of reactivity insertion is strongly dependent on the Doppler coefficient, conservatively low values, as a function of power, are used (see Table 9.0-6).

- Contribution of the moderator reactivity coefficient is negligible during the initial part of the transient because the heat transfer time between the fuel and the moderator is much longer than the neutron flux response time. After the initial neutron flux peak, the succeeding rate of power increase is affected by the moderator reactivity coefficient. A conservative value is used in the analysis to yield the maximum peak heat flux (see Table 9.0-6).

- The reactor is assumed to be at hot zero power. This assumption is more conservative than that of a lower initial system temperature. The higher initial system temperature yields a larger fuel-water heat transfer coefficient, larger specific heats, and a less negative (smaller absolute magnitude) Doppler coefficient, all of which tend to reduce the Doppler feedback effect and thereby increase the neutron flux peak. The initial effective multiplication factor (k_{eff}) is assumed to be 1.0 because this results in the worst nuclear power transient.

- Reactor trip is assumed to be initiated by the power range high neutron flux (low setting). The most adverse combination of instrument and setpoint errors, as well as delays for trip signal actuation and RCCA release, is taken into account. A 10-percent uncertainty increase is assumed for the power range flux trip setpoint, raising it to 35 percent from the nominal value of 25 percent.

  Because the rise in the neutron flux is so rapid, the effect of errors in the trip setpoint on the actual time at which the rods are released is negligible. In addition, the reactor trip insertion characteristic is based on the assumption that the highest worth RCCA is stuck in its fully withdrawn position. See Section 9.0.6 for RCCA insertion characteristics.

- The maximum positive reactivity insertion rate assumed is greater than that for the simultaneous withdrawal of the combination of the two sequential RCCA banks having the greatest combined worth at maximum speed (1.143 m [45 inches] per minute). Control rod drive mechanism design is discussed in Section 17.3.3.

- The most limiting axial and radial power shapes, associated with having the two highest combined worth banks in their high-worth position, are assumed in the DNB analysis.

- The initial power level is assumed to be below the power level expected for any shutdown condition (10^{-9} of nominal power). The combination of highest reactivity insertion rate and lowest initial power produces the highest peak heat flux.

- Four reactor coolant pumps are assumed to be in operation.

- Pressuriser pressure is assumed to be 0.345 MPa (50 psi) below nominal for steady-state fluctuations and measurement uncertainties.

Plant systems and equipment available to mitigate the effects of the accident are discussed in Section 9.0.4 and listed in Table 9.0-10. No single active failure in any of these systems or components adversely affects the consequences of the accident. A loss of offsite power as a consequence of a turbine trip disrupting the grid is not considered because the accident is initiated from a subcritical condition where the plant is not providing power to the grid.

9.4.1.2.2 DBA Credited SSCs

For the DB, all the claimed SSCs are Class 1. The claimed Class 1 SSCs are listed in Table 9.0-10. The presented DBA ends shortly after reactor trip; however, essential safety functions for the long term safe shutdown analysis (Appendix 9C) bound safe shutdown response for this event. The primary core cooling is provided by the PRHR and passive containment cooling. Other SSCs include the CMTs, containment isolation, steam line isolation valves and SG flow restrictors. The PMS provides the following:

- RT on power range high neutron flux (low setpoint)

- PRHR actuation on Low-2 SG NR level coincident with Low-2 SFW flow

- CMTs and containment isolation on Low-2 CL temperature

- PCS on High-2 containment pressure

9.4.1.2.3 DBA Results

Figures 9.4.1-1 through 9.4.1-4 show the transient behaviour for the uncontrolled RCCA bank withdrawal from subcritical incident. The accident is terminated by reactor trip at 35 percent of nominal power. The reactivity insertion rate used is greater than that calculated for the two highest-worth sequential rod cluster control banks, both assumed to be in their highest incremental worth region.

Figure 9.4.1-1 shows the average neutron flux transient. The energy release and the fuel temperature increases are relatively small. The heat flux response (of interest for DNB considerations) is also shown in Figure 9.4.1-2. The beneficial effect of the inherent thermal lag in the fuel is evidenced by a peak heat flux much less than the full-power nominal value. There is margin to DNB during the transient because the rod surface heat flux remains below the critical heat flux value, and there is a high degree of subcooling at all times in the core. Figures 9.4.1-3 and 9.4.1-4 show the response of the average fuel temperature and the inner cladding temperature, respectively. The minimum DNBR at all times remains above the design limit value (see Section 22.7.1.1).

The calculated sequence of events for this accident is shown in Table 9.4-1. With the reactor tripped, the plant returns to a stable condition. Subsequently, the plant may be cooled down further by following normal plant shutdown procedures.

9.4.1.3 Diverse Mitigation

The available diverse mitigation for this event is the same as for the RCCA misalignment faults (Section 9.4.3.3).

9.4.1.3.1 Diverse Mitigation for ATWT

As explained in section 9.4.2.3.1.3 considering an ATWT event, this fault is bounded by that of the uncontrolled RCCA withdrawal at-power fault. The bounding ATWT analysis for the at-power fault is in Section 9.4.2.3.1.

9.4.1.3.2 Diverse Mitigation for Core Cooling

The loss of normal feedwater diverse core cooling, as analysed in Section 9.2.7.3.2, was determined to be bounding of all non-LOCA events.

9.4.1.4 Radiological Consequences

The initiating event does not result in fuel damage and the primary and secondary circuits remain intact. Because offsite power remains available, there is no release of activity to the environment and the Target 4 BSOs (0.01 mSv offsite and 0.1 mSv onsite) are met.

9.4.1.5 As Low as Reasonably Practicable Assessment

The ALARP evaluation for this event is the same as for the RCCA misalignment fault (Section 9.4.3.5).

9.4.1.6 Conclusions

In the event of an RCCA withdrawal accident from the subcritical condition, the core and the reactor coolant system are not adversely affected because the combination of thermal power

and the coolant temperature results in a DNBR greater than the safety analysis limit value. Thus, no fuel or cladding damage is predicted as a result of DNB.

It has been shown that the AP1000 plant design includes adequate systems for the protection of this fault, which limit the radiological consequences such that they are compliant with the SAPs targets and the risks have been reduced to be ALARP.

9.4.2 Uncontrolled Rod Cluster Control Assembly Bank Withdrawal at Power (Fault 1.15.4)

9.4.2.1 Identification of Causes and Accident Description

An uncontrolled RCCA bank withdrawal at power results in an increase in the core heat flux. Because the heat extraction from the steam generator lags behind the core power generation until the steam generator pressure reaches the relief or safety valve setpoint, there is a net increase in the reactor coolant temperature. Unless terminated by manual or automatic action, the power mismatch and resultant coolant temperature rise could eventually result in a violation of the DNB design basis or excessive linear power. Therefore, to avert damage to the fuel cladding, the PMS is designed to terminate any such transient before the DNBR falls below the design limit (see Section 22.7.1.1) or the overpower limit is exceeded.

9.4.2.2 Design Basis Mitigation

Analysis is performed to demonstrate the adequacy of the PMS to detect and mitigate the fault and show that the safety analysis criteria are satisfied including:

- No fuel failures (confirmed using minimum DNBR and fuel melt criteria),
- The RCS pressure criterion is met,
- The MSS pressure criterion is met, and
- The pressuriser does not fill (which could result in a LOCA)

It is noted that this event is bounded by the Section 9.2.3 analysis with respect MSS pressure criteria, therefore, these limits are not explicitly confirmed for this event. Pressuriser filling is only a concern after reactor trip for this event of the high pressuriser water level reactor trip. For post-trip pressuriser filling, this event is bounded by Section 9.2.7 analysis.

9.4.2.2.1 DBA Method of Analysis

This transient is analysed using the LOFTRAN (References 9.4-3 and 9.4-11) code. This code simulates the neutron kinetics, reactor coolant system, pressuriser, pressuriser safety valves, pressuriser spray, steam generators, and steam generator safety valves. The code computes pertinent plant variables including temperatures, pressures, and power level. The core limits as illustrated in Figure 9.0-1 are used to define the inputs to LOFTRAN that determine the minimum DNBR during the transient.

Plant characteristics and initial conditions are discussed in Section 9.0.2. In performing a conservative analysis for an uncontrolled RCCA bank withdrawal at-power accident, the following assumptions are made:

- The nominal initial conditions are assumed in accordance with the revised thermal design procedure. Uncertainties in the initial conditions are included in the DNBR limit as described in WCAP-11397-P-A (Reference 9.4-9).

- Two sets of reactivity coefficients are considered:

Minimum reactivity feedback — A least-negative moderator temperature coefficient of reactivity is assumed, corresponding to the beginning of core life. A variable Doppler power coefficient with core power is used in the analysis. A conservatively small (in absolute magnitude) value is assumed (see Figure 9.0-3).

Maximum reactivity feedback — A conservatively large positive moderator density coefficient corresponding to the end of core life and a large (in absolute magnitude) negative Doppler power coefficient are assumed (see Figure 9.0-3).

- The high positive flux rate trip is assumed to be actuated when the power range neutron flux changes at a rate higher than 15% per second with a 60 second rate-lag time constant. The overpower ΔT and overtemperature ΔT trips include adverse instrumentation and setpoint uncertainties. The delays for trip actuation assumed are given in Table 9.0-8.

- The RCCA trip insertion characteristic is based on the assumption that the highest-worth assembly is stuck in its fully withdrawn position.

- A range of reactivity insertion rates is examined. The maximum positive reactivity insertion rate is greater than that for the simultaneous withdrawal of the combination of the two control banks having the maximum combined worth at maximum speed.

If RCCA movement were to cause an adverse effect on the axial core power distribution the overtemperature ΔT trip setpoint would be decreased as necessary to maintain margin to the DNBR design limit, and the overpower ΔT trip setpoint would be decreased as necessary to maintain margin to the overpower limit.

Plant systems and equipment available to mitigate the effects of the accident are discussed in Section 9.0.4 and listed in Table 9.0-10. No single active failure in these systems or equipment adversely affects the consequences of the accident.

9.4.2.2.2 DBA Credited SSCs

For the DB, all claimed SSCs are Class 1. The credited Class 1 systems are listed in Table 9.0-10. The presented DBA ends shortly after reactor trip; however, essential safety functions for the long term safe shutdown analysis (Appendix 9C) bound safe shutdown response for this event. The primary core cooling is provided by the PRHR and passive containment cooling. Other SSCs include the CMTs, containment isolation, pressuriser SVs and steam generator SVs. The PMS provides the following:

- RT on (dependent on reactivity insertion rate):
  - Power range high positive flux rate
  - Overtemperature ΔT
  - Overpower ΔT
- PRHR actuation on Low-2 SG NR level coincident with Low-2 SFW flow
- CMTs and containment isolation on Low-2 CL temperature
- PCS on High-2 containment pressure

9.4.2.2.3 DBA Results

Three reactor trip functions were credited in the analyses to provide protection over the entire range of reactivity insertion rates. These are the high positive flux rate, overtemperature ΔT, and overpower ΔT trips.

Figures 9.4.2-1 through 9.4.2-6 show the transient response for a representative rapid (80 pcm/s) RCCA withdrawal incident starting from full power. Reactor trip on high positive flux rate occurs shortly after the start of the transient. Because this is rapid with respect to the thermal time constants of the fuel, small changes in temperature and pressure result, and the DNB design basis described in Section 22.7.1.1 is met.

The transient response for a representative intermediate (34 pcm/s) RCCA withdrawal from full power is shown in Figures 9.4.2-7 through 9.4.2-12. Reactor trip on overpower ΔT occurs preventing the peak heat flux from exceeding 118%. The minimum DNBR is greater than the design limit described in Section 22.7.1.1

The transient response for a representative slow (5 pcm/s) RCCA withdrawal from full power is shown in Figures 9.4.2-13 through 9.4.2-18. Reactor trip on overtemperature ΔT occurs after a longer period. The rise in temperature and pressure is consequently larger than for rapid RCCA withdrawal. The DNB design basis described in Section 22.7.1.1 is met.

Figure 9.4.2-19 shows the minimum DNBR as a function of reactivity insertion rate from initial full-power operation for minimum and maximum reactivity feedback. Minimum DNBR occurs immediately after rod motion. The minimum DNBR is greater than the design limit value described in Section 22.7.1.1.

Figures 9.4.2-20 and 9.4.2-21 show the minimum DNBR as a function of reactivity insertion rate for RCCA withdrawal incidents for minimum and maximum reactivity feedback, starting at 60-percent and 10-percent power, respectively. Minimum DNBR occurs immediately after rod motion. In all cases, the DNBR is greater than the design limit value described in Section 22.7.1.1.

The shape of the curves of minimum DNBR versus reactivity insertion rate in the referenced figures is due both to reactor core and coolant system transient response and to PMS action in initiating a reactor trip.

Referring to Figure 9.4.2-19, for transients initiated from full power, it is noted that:

A. Three reactor trip functions provide the DNB and overpower protection over the range of reactivity insertion rates analysed. The overtemperature ΔT reactor trip provides DNB protection except for rapid power excursions. The overpower ΔT reactor trip provides protection for the slow to moderate power excursions. The high positive flux rate trip prevents both overpower and low DNBR for rapid power excursions.

B. For minimum reactivity feedback cases, the high positive flux rate trip provides protection for reactivity insertion rates between 110 pcm/s and 10 pcm/s. The overpower ΔT reactor trip provides protection for reactivity insertion rates between 5.0 pcm/s and 1.2 pcm/s and the overtemperature ΔT reactor trip provides protection for the reactivity insertion rates between 1.0 pcm/s and 0.5 pcm/s.

C. For maximum reactivity feedback cases, the high positive flux rate trip provides protection for reactivity insertion rates between 110 pcm/s and 50 pcm/s. The overpower

ΔT reactor trip provides for reactivity insertion rates between 40 pcm/s and 30 pcm/s and the overtemperature ΔT reactor trip provides protection for the reactivity insertion rates between 25 pcm/s and 0.6 pcm/s.

Steam generator safety valves never open before the reactor trip for transients initiated at full power.

Because the RCCA bank withdrawal at-power incident is an overpower transient, the fuel temperatures rise during the transient until after reactor trip occurs. For rapid power excursions, the overpower transient is fast with respect to the fuel rod thermal time constant and the core heat flux lags behind the neutron flux response. Taking into account the effect of the RCCA withdrawal on the axial core power distribution, the peak fuel centreline temperature still remains below the fuel melting temperature.

For slow to moderate power excursions, the core heat flux remains more nearly in equilibrium with the neutron flux. The overpower transient is terminated by either the overpower ΔT or overtemperature ΔT reactor trip before the DNB design basis is violated. Taking into account the effect of the RCCA withdrawal on the axial core power distribution, the peak centreline temperature remains below the fuel melting temperature.

The reactor is tripped during the RCCA bank withdrawal at-power transient such that the ability of the primary coolant to remove heat from the fuel rods is not reduced. Thus, the fuel cladding temperature does not rise significantly above its initial value during the transient.

The calculated sequence of events for this accident is shown in Table 9.4-1. With the reactor tripped, the plant returns to a stable condition. The plant may be cooled down further by following normal plant shutdown procedures.

Appendix 9C provides discussion and analysis of long term safe shutdown for non-LOCA events.

Overpressure Evaluation Results

In addition to the DNB cases discussed above, several cases are analysed to ensure that the maximum RCS pressure does not exceed 110% of the design pressure. The cases cover a range of reactivity insertion rates from less than 1 pcm/s to 110 pcm/s and power levels from 10% to 100% power. Initial condition uncertainties on power, pressure, and average temperature are conservatively included, and the thermal design flow rate is assumed. The most limiting case was for a reactivity insertion rate of 10 pcm/s and an initial power level of 65% power. The peak pressure calculated is 18.139 MPa abs (2630.8 psia), which is well below the limit of 18.950 MPa abs (2748.5 psia).

9.4.2.3 Diverse Mitigation

The available diverse protection for this event is the same as for the RCCA misalignment faults (Section 9.4.3.3).

9.4.2.3.1 Diverse Mitigation for ATWT

The AP1000 plant is designed with mechanical shim (control rod motion used for small burnup effects rather than boron changes), as well as automatic axial power control. These require deeper control rod insertion than operating Westinghouse pressurised water reactors (PWRs). In this assessment, an inserted worth of 1 percent (1000 pcm) is assumed at full

power for the M bank, and higher worth at lower power to compensate for the power defect. The Axial Offset bank has comparable reactivity (but does not increase at reduced power).

For the M bank, a realistic upper limit for incremental reactivity worth at hot zero power is 12 pcm per step (about 15 pcm/second at the maximum reactivity withdrawal rate of 72 steps/minute). During power operation, the comparable value is 3 pcm/second near full power and 12 pcm/second at low power. The axial offset bank has a higher maximum incremental worth (30 pcm/step) but is limited to 8 steps/minute (4 pcm/sec). The high rates at zero and low power occur over a short range of control rod travel (i.e., they cannot be sustained.) For the purpose of investigating limits, a preliminary hypothetical case was analysed assuming a sustained 15 pcm/second starting from full power. Results of more realistic cases with 4 pcm/second from full power are also shown.

Power distribution tends to improve with increasing power, and all inadvertent control rod withdrawal events of significance go to power levels above full power, so full-power design power distribution was used in the assessment. Thus, low initial power (or even initial sub-critical) events may be treated in the same way as an uncontrolled RCCA bank withdrawal from full power.

This analysis is performed to demonstrate the adequacy of the operable portions of the PMS (considering the impact of the CCF) as well as the DAS to detect and actuate mechanical SSCs to mitigate the fault. The following ATWT acceptance criteria are applicable to this event:

- The RCS does not overpressurise due to reactor coolant heatup. The ATWT pressure limit is 22.06 MPa-rel (3200 psig).

- There is no significant fuel damage.

- The rate and duration of energy release to containment is much less than for the design basis LOCA. This demonstrates that the containment does not overpressurise due to the energy release to the containment.

9.4.2.3.1.1 Diverse ATWT Method of Analysis

For this ATWT scenario, mechanical failure of the control rods to fall when de-energised is not considered. It is assumed that RCCAs that are able to step out during an uncontrolled withdrawal are not restricted from falling into the reactor on receipt of a trip signal. Therefore, only a PMS failure (including scram breaker failure) needs be addressed. The transient is terminated either when: (1) DAS reactor trip occurs on high T-hot; or (2) The control rods are fully withdraw (1 percent reactivity added for 100 percent initial power cases). The second case would be more likely later in core life with a strong reactivity feedback.

In addition to the preceding protective actions, the following rod control system interlocks are available to block RCCA withdrawal but are not credited for this analysis:

- High neutron flux (two out of four power range)
- Overpower ΔT (two out of four)
- Overtemperature ΔT (two out of four)

Analysis Assumptions

a. Plant initial conditions are assumed to be those of the nominal values consistent with Table 9.0-15.

b. Modelled reactivity coefficients are based on the reactivity coefficients discussed in Reference 9.4-20 for near the BOC.

c. Except for pressuriser sprays, the pressuriser pressure and level control system is not credited in the analyses.

d. The pressuriser safety valves are conservatively modelled to open at the maximum safety analysis setpoint 17.75 MPa abs (2575 psia).

e. The turbine bypass function is assumed to be operable and in pressure control mode. After a reactor trip signal is generated in PMS or DAS, the turbine bypass switches to pressure control automatically. Pressure setpoint for the turbine bypass system in pressure control mode is assumed to be the nominal no load secondary pressure (7.63 MPa abs [1106 psia]).

f. The turbine trip on reactor trip function is not modelled. However, the SG relief system is modelled consistent with the turbine bypass system following reactor trip. Therefore, turbine trip impact is included in the model.

g. The turbine control system is assumed to maintain initial steam flow throughout the transient.

h. Following protection functions are assumed available for this event:

- PMS Reactor Trip – None, all trip functions are set aside.

- DAS Reactor Trip – High Hot Leg Temperature in both hot legs.

Discussion of Cases Analysed

Cases modelling 100 percent, 60 percent, and 0 percent RTP were analysed. For 100 percent RTP, cases were run at the maximum hypothetical reactivity insertion (15 pcm/sec) and for a realistic reactivity insertion (4 pcm/sec). All reduced power analyses conservatively assumed the maximum hypothetical reactivity insertion (15 pcm/sec). For each case, the RCS pressure and DNBR margin have been assessed.

To determine the DNBR limit, a curve was developed based on the WRB-2M correlation which corresponds to the 95/95 DNBR limit for PWRs. This curve defines the DNBR limited core inlet temperature versus power for 100 percent of normal flow and an RCS pressure of [ ]. Next, the limiting core outlet temperature was calculated based on this inlet temperature limit and the specified core power (3400 MWt). Accordingly, the critical transient results for the core exit temperature (hot-leg inlet temperature) as a function nuclear power can be compared to determine whether the minimum DNBR exceeds the limit.

As expected, the setpoint temperature for the DAS high hot-leg trip is a significant parameter for this analysis. As this trip setpoint is increased, the peak reactor power (i.e., nuclear power just after the DAS rod insertion starts) increases. For this initial power, a sensitivity study was

run for three high hot-leg trip setpoints: 332.2°C (630°F), 335°C (635°F), and 337.8°C (640°F), as shown in Figure 9.4.2-22. As the trip setpoint was increased, the DNBR margin was reduced.

All transient results documented herein assume the high hot-leg trip setpoint is 335°C (635°F).

This event is less limiting for RCS overpressure than the loss of feedwater event as analysed in Section 9.2.7.5, is less limiting for core damage than the complete loss of RCS flow as analysed in Section 9.3.2.5. This event was explicitly analysed for the change in the current design reference point in the UK as described in Reference 9.4-12. The evaluation conducted to closeout FS-03 (Reference 9.4-13) demonstrated that there is little impact on the key analysis trends, results, and margin to the applicable acceptance criteria. Therefore, the change in design reference point would not invalidate the conclusions presented for this event.

9.4.2.3.1.2 Diverse ATWT Credited SSCs

For the diverse ATWT no Class 1 SSCs are claimed. The available SSCs are listed in Table 9.0-14. The DAS provides the following:

- RT on High hot leg temperature

9.4.2.3.1.3 Diverse ATWT Results

RCCA Withdrawal at Power from 100 Percent Power at Maximum Hypothetical Reactivity Insertion

For the 100-percent-power cases of RCCA withdrawal at power (RWAP), the event starts at nominal initial conditions with reactivity insertion at the start of the transient. Nuclear power increases initially and both the primary and secondary systems heat up. However, the rate of increase is limited by moderator temperature and power defect feedback. As the core power and RCS pressure increases, PMS trip setpoints for high neutron flux and high pressuriser pressure are reached; however, due to PMS CCF, no action is taken by the control system. PCS rod control system interlock setpoints for C-2 (high neutron flux) and C-3 (margin to overpower delta temperature (OPΔT) limit) would be reached, which would block further rod withdrawal and limit peak nuclear power. However, these interlocks are not modelled in the analyses presented.

Eventually, the high hot-leg temperature is reached, causing the DAS to shut down power to the diesel generator (DG), thereby releasing the latches on the trip scram control rods. After a 7 second delay, the control rods begin to move and insert negative reactivity into the core. Total reactivity turns negative almost immediately reducing core power. The steam generator continues to remove heat from the RCS, and the RCS coolant temperature gradually drops. Peak RCS pressure and DNBR margin are at a minimum at the peak power point.

If the turbine trip were to occur on reactor trip, the turbine bypass would switch to pressure control mode and maintain the heat sink as discussed previously.

Table 9.4.2-1 shows the sequence of events for the 100 percent initial power case with the high hot-leg trip setpoint of 335°C (635°F). Figures 9.4.2-22 to 9.4.2-26 show critical parameters for this transient.

RWAP from 100 Percent Power at Realistic Reactivity Insertion

The rod withdrawal from 100 percent power at realistic but bounding insertion rate (4 pcm/sec.) conditions produces results similar to the 100 percent power, maximum insertion case; however, the lower insertion rate produces a power excursion that is less severe. This results in higher loop temperature versus nuclear power; therefore, the DAS hot-leg trip occurs at much lower power. Since core peak heat flux is lower, DNB margin is improved as demonstrated in Figure 9.4.2-27.

RWAP from a Partial Power Condition

The cases modelling a rod withdrawal occurring from a partial power conditions produce results similar to the 100-percent-power case; however, these cases were found to be less limiting with respect to minimum DNBR. This is due to the DAS high hot-leg temperature trip of 335°C (635°F) being reached when the reactor has reached a lower core heat flux. While the cases initialised from a partial power condition result in a lower core heat flux, the partial power cases result in a higher secondary system pressure.

Figure 9.4.2-40 shows the margin to DNBR resulting from RWAP at reduced power.

Peak reactor power is significantly lower than for the 100 percent initial power case while peak hot-leg temperatures are similar for all cases. Based on the DNBR limits of Figure 9.4.2-22, it is clear that DNBR margin is greater for these cases than the 100-percent-power case.

Based on the previous discussion, uncontrolled RCCA withdrawal from lower sub-critical power would not result in a substantial risk provided the event starts from hot zero power loop temperature conditions.

9.4.2.3.2 Diverse Mitigation for Core Cooling

The loss of normal feedwater diverse core cooling, as analysed in Section 9.2.7.3.2, was determined to be bounding of all non-LOCA events.

9.4.2.4 Radiological Consequences

Design Basis

In the case where offsite power remains available, there is no release of activity to the environment and the Target 4 BSOs (0.01 mSv offsite and 0.1 mSv onsite) are met.

In the case where offsite power is lost, a small release of activity may occur as a result of steam dump to the atmosphere due to unavailability of the condensers. With no fuel damage and primary and secondary circuits intact, the initiating event has no impact on the doses. The doses are a consequence of the assumed loss of offsite power. Therefore, the loss of offsite power doses from Section 9.2.6.4 are presented. The calculated maximum doses for all relevant pathways (inhalation, cloudshine, and groundshine) are as follows:

- Offsite dose: 0.05 mSv Worker dose: 1.5 mSv

These doses are within the Target 4 BSL for frequent faults (1 mSv offsite and 20 mSv onsite).

Diverse Mitigation

Both the diverse ATWT and diverse core cooling scenarios demonstrate that the RCS does not overpressurise and there is no significant fuel damage. For a diverse mitigation radiological consequences analysis better estimate assumptions would be credited. This would include reactor coolant system activity levels significantly lower than those modelled for the DBA and better activity retention in containment and in the steam generators. In addition better estimate atmospheric dispersion factors would be used. Therefore, a diverse mitigation radiological consequences analysis would show that the doses for the diverse ATWT scenario would be less than those reported for the non-LOCA DBAs and doses for the diverse core cooling scenario would be much less than for the design basis LOCA. The diverse mitigation analyses would not have to meet the Target 4 BSL for frequent faults and would meet the Target 4 BSL for infrequent faults.

9.4.2.5 As Low as Reasonably Practicable Assessment

The ALARP evaluation for this event is the same as for the RCCA misalignment fault (Section 9.4.3.5).

9.4.2.6 Conclusions

The overpower ΔT, overtemperature ΔT, and high positive flux rate trip functions provide adequate protection over the entire range of possible reactivity insertion rates. The DNB and fuel melt design basis, as defined in Section 22.7.1.1, is met for all cases. The maximum reactor coolant system pressure remains below 110% of design.

This event has also been adequately assessed with respect to ATWT considerations.

Diverse core cooling capabilities have been demonstrated.

DBA radiological consequences are within the Target 4 BSL for frequent faults (1 mSv offsite and 20 mSv onsite). Thus, the identification of the Class 1 SSCs as protective functions is adequate to meet DB requirements.

It has been shown that the AP1000 plant design includes adequate systems for the protection of this fault, which limit the radiological consequences such that they are compliant with the SAPs targets and the risks have been reduced to be ALARP.

9.4.3 Rod Cluster Control Assembly Misalignment (System Malfunction or Operator Error) (Fault 1.15.5)

9.4.3.1 Identification of Causes and Accident Description

RCCA misoperation accidents include:

- One or more dropped RCCAs within the same group (Fault 1.15.5a)
- Statically misaligned RCCA (Fault 1.15.5)
- Withdrawal of a single RCCA (Fault 1.15.5b)

Each RCCA has a position indicator channel which displays the position of the assembly. The displays of assembly positions are grouped for the operator's convenience. Fully inserted assemblies are further indicated by a rod-at-bottom signal, which actuates a local alarm and a main control room annunciator. Group demand position is also indicated.

RCCAs are moved in preselected banks, and the banks are moved in a preselected sequence. Each bank of RCCAs is divided into one or two groups of four or five RCCAs each. The rods comprising a group operate in parallel. The two groups in a bank move sequentially such that the first group is always within one step of the second group in the bank. A definite schedule of actuation (or deactuation) of the stationary gripper, movable gripper, and lift coils of a mechanism is required to withdraw the RCCA attached to the mechanism. Because the stationary gripper, movable gripper, and lift coils associated with the RCCAs of a rod group are driven in parallel, any single failure which causes rod withdrawal affects the entire group. A single electrical or mechanical failure in the plant control system could, at most, result in dropping one or more RCCAs within the same group. Mechanical failures can cause either RCCA insertion or immobility, but not RCCA withdrawal.

No single electrical or mechanical failure in the rod control system could cause the accidental withdrawal of a single RCCA from the inserted bank at full-power operation. The operator could withdraw a single RCCA in the control bank because this feature is necessary to retrieve an assembly should one be accidentally dropped. The event analysed results from multiple wiring failures or multiple significant operator errors and subsequent and repeated operator disregard of event indication. The probability of such a combination of conditions is considered low such that the limiting consequences may include slight fuel damage.

It has been shown that single failures resulting in RCCA bank withdrawals do not violate specified fuel design limits. Moreover, no single malfunction can result in the withdrawal of a single RCCA. Thus, it is concluded that criterion established for the single rod withdrawal at power is appropriate.

A dropped RCCA or RCCA bank may be detected by one or more of the following:

- Sudden drop in the core power level as seen by the nuclear instrumentation system
- Asymmetric power distribution as seen by the incore or excore neutron detectors or core exit thermocouples, through online core monitoring
- Rod at bottom signal
- Rod deviation alarm
- Rod position indication

Misaligned RCCAs are detected by one or more of the following:

- Asymmetric power distribution as seen by the incore or excore neutron detectors or core exit thermocouples, through online core monitoring
- Rod deviation alarm
- Rod position indicators

The resolution of the rod position indicator channel is $\pm$5 percent span ($\pm$0.19 m [7.5 inches]). A deviation of any RCCA from its group by twice this distance (10 percent of span or 0.38 m [15 inches]) does not cause power distributions worse than the design limits. The deviation alarm alerts the operator to rod deviation with respect to the group position in excess of 5 percent of span.

If one or more of the rod position indicator channels is out of service, operating instructions are followed to verify the alignment of the nonindicated RCCAs. The operator also takes action as required by the Technical Specifications.

In the extremely unlikely event of multiple electrical failures that result in single RCCA withdrawal, rod deviation and rod control urgent failure are both displayed to the operator, and the rod position indicators indicate the relative positions of the assemblies in the bank. The urgent failure alarm also inhibits automatic rod motion in the group in which it occurs. Withdrawal of a single RCCA by operator action, whether deliberate or by a combination of errors, results in activation of the same alarm and the same visual indication. Withdrawal of a single RCCA results in both positive reactivity insertion tending to increase core power and an increase in local power density in the core area associated with the RCCA. Automatic protection for this event is provided by the overtemperature ΔT reactor trip. The evaluation criteria are met; however, due to the increase in local power density, the limits in Figure 9.0-1 may be exceeded.

Plant systems and equipment available to mitigate the effects of the various control rod misoperations are discussed in Section 9.0.4 and listed in Table 9.0-10. No single active failure in any of these systems or equipment adversely affects the consequences of the accident.

9.4.3.2 Design Basis Mitigation

Analysis is performed to demonstrate the adequacy of the PMS to detect and mitigate the fault and show that the safety analysis criteria are satisfied including:

- No fuel failures (confirmed using minimum DNBR and fuel melt criteria),
- The RCS pressure criterion is met,
- The MSS pressure criterion is met, and
- The pressuriser does not fill (which could result in a LOCA)

With respect to the RCS and MSS pressure criteria, the Dropped Rod event is bounded by the analysis presented in Section 9.2.3, and is not explicitly verified. In addition, pressuriser filling is not challenged in this event.

9.4.3.2.1 Dropped RCCAs, Dropped RCCA Bank, and Statically Misaligned RCCA

9.4.3.2.1.1 DBA Method of Analysis

- One or more dropped RCCAs from the same group

  A drop of one or more RCCAs from the same group results in an initial reduction in the core power and a perturbation in the core radial power distribution. Depending on the worth and position of the dropped rods, this may cause the allowable design power peaking factors to be exceeded. Following the drop, the reduced core power and continued steam demand to the turbine causes the reactor coolant temperature to decrease. In the manual control mode, the plant will establish a new equilibrium condition. The new equilibrium condition is reached through reactivity feedback. In the presence of a negative moderator temperature coefficient, the reactor power rises monotonically back to the initial power level at a reduced inlet temperature with no power overshoot. The absence of

any power overshoot establishes the automatic operating mode as a limiting case. If the reactor coolant system temperature reduction is very large, the turbine power may not be able to be maintained due to the reduction in the secondary-side steam pressure and the volumetric flow limit of the turbine system. In this case, the equilibrium power level is less than the initial power. In the automatic control mode, the plant control system detects the drop in core power and initiates withdrawal of a control bank. Power overshoot may occur, after which the control system will insert the control bank and return the plant to the initial power level. The magnitude of the power overshoot is a function of the plant control system characteristics, core reactivity coefficients, the dropped rod worth, and the available control bank worth.

For evaluation of the dropped RCCA event, the transient system response is calculated using the LOFTRAN code (References 9.4-3 and 9.4-11). The code simulates the neutron kinetics, reactor coolant system, pressuriser, pressuriser safety valves, pressuriser spray, steam generator and steam generator safety valves. The code computes pertinent plant variables, including temperatures, pressures and power level.

Steady-state nuclear models using the computer codes described in Section 22.7 are used to obtain a hot channel factor consistent with the primary system transient conditions and reactor power. By combining the transient primary conditions with the hot channel factor from the nuclear analysis, the departure from nucleate boiling design basis is shown to be met using the VIPRE-01 code (Reference 9.4-18).

- Statically misaligned RCCA

  Steady-state power distributions are analysed using the computer codes as described in Section 22.7. The peaking factors are then used as input to the VIPRE-01 code to calculate the DNBR.

9.4.3.2.1.2 DBA Credited SSCs

For the DB, all claimed SSCs are Class 1. The credited Class 1 SSCs are listed in Table 9.0-10. The presented DBA ends shortly after reactor trip; however, essential safety functions for the long term safe shutdown analysis (Appendix 9C) bound safe shutdown response for this event. The primary core cooling is provided by the PRHR and passive containment cooling. Other SSCs include the CMTs, containment isolation, and pressuriser SVs. For dropped RCCAs from the same group DB, the PMS provides the following:

- RT on Low-2 pressuriser pressure; however, the limiting dropped RCCA cases do not result in a reactor trip. Instead, the reactor will reach a new equilibrium power (see Section 9.4.3.2.1.3).

- PRHR actuation on Low-2 SG NR level coincident with Low-2 SFW flow

- CMTs and containment isolation on Low-2 CL temperature

- PCS on High-2 containment pressure

9.4.3.2.1.3 DBA Results

- One or more dropped RCCAs

  Figures 9.4.3-1 through 9.4.3-4 show the transient response of the reactor to a dropped rod (or rods) in automatic control. The nuclear power and heat flux drop to a minimum value and recover under the influence of both rod withdrawal and thermal feedback. The prompt decrease in power is governed by the dropped rod worth because the plant control system does not respond during the short rod drop time period. The plant control system detects the reduction in core power and initiates control bank withdrawal to restore the primary side power. Power overshoot occurs after which the core power is restored to the initial power level.

  The primary system conditions are combined with the hot channel factors from the nuclear analysis for the DNB evaluation. Uncertainties in the initial conditions are included in the DNB evaluation as discussed in Section 9.0.2.3. The calculated minimum DNBR for any single or multiple rod drop from the same group is greater than the design limit value described in Section 22.7.1.1. The sequence of events for a representative case is shown in Table 9.4-1.

  The analysis described previously includes consideration of drops of the RCCA groups which can be selected for insertion as part of the rapid power reduction system. This system is provided to allow the reactor to ride out a complete loss of load from full power without a reactor trip. If these RCCAs are inadvertently dropped (in the absence of a loss-of-load signal), the transient behaviour is the same as for the RCCA drop described. The evaluation showed that the DNBR remains above the design limit value as a result of the inadvertent actuation of the rapid power reduction system.

  The consequential loss of offsite power described in Section 9.0.12 is not limiting for the dropped RCCA event. Due to the delay from reactor trip until turbine trip and the rapid power reduction produced by the reactor trip, the minimum DNBR occurs before the reactor coolant pumps begin to coast down.

- Statically misaligned RCCA

  The most severe misalignment situations with respect to DNBR arise from cases in which one RCCA is fully inserted, or where the mechanical shim or axial offset rod banks are inserted up to their insertion limit with one RCCA fully withdrawn while the reactor is at full power. Multiple independent alarms, including a bank insertion limit or rod deviation alarm, alert the operator well before the postulated conditions are approached.

  For RCCA misalignments in which the mechanical shim or axial offset banks are inserted to their respective insertion limits, with any one RCCA fully withdrawn, the DNBR remains above the safety analysis limit value. This case is analysed assuming the initial reactor power, pressure, and reactor coolant system temperature are at their nominal values, but with the increased radial peaking factor associated with the misaligned RCCA. Uncertainties in the initial conditions are included in the DNB evaluation as described in Section 9.0.2.3.

  DNB does not occur for the RCCA misalignment incident, and thus the ability of the primary coolant to remove heat from the fuel rod is not reduced. The peak fuel temperature is that corresponding to a linear heat generation rate based on the radial peaking factor penalty associated with the misaligned RCCA and the design axial power

distribution. The resulting linear heat generation is well below that which causes fuel melting.

Following the identification of an RCCA group misalignment condition by the operator, the operator takes action as required by the plant Technical Specifications and operating instructions.

Appendix 9C provides discussion and analysis of long term safe shutdown for non-LOCA events.

9.4.3.2.2 Single Rod Cluster Control Assembly Withdrawal

9.4.3.2.2.1 DBA Method of Analysis

Power distributions within the core are calculated using the computer codes described in Section 22.7. The peaking factors are then used by VIPRE-01 to calculate the DNBR for the event. The case of the worst rod withdrawn from the mechanical shim or axial offset bank inserted at the insertion limit, with the reactor initially at full power, is analysed. This incident is assumed to occur at beginning of life because this results in the minimum value of moderator temperature coefficient. This assumption maximises the power rise and minimizes the tendency of increased moderator temperature to flatten the power distribution.

9.4.3.2.2.2 DBA Credited SSCs

The credited Class 1 SSCs are the same as those in Section 9.4.3.2.1.2 for Dropped RCCAs, Dropped RCCA bank, and Statically Misaligned RCCA faults. In addition, one PMS reactor trip is credited for the manual rod withdrawal case:

- RT on overtemperature ΔT

9.4.3.2.2.3 DBA Results

For the single rod withdrawal event, two cases are considered as follows:

A. If the reactor is in the manual control mode, continuous withdrawal of a single RCCA results in both an increase in core power and coolant temperature and an increase in the local hot channel factor in the area of the withdrawing RCCA. In the overall system response, this case is similar to those presented in Section 9.4.2. The increased local power peaking in the area of the withdrawn RCCA results in lower minimum DNBRs than for the withdrawn bank cases. Depending on initial bank insertion and location of the withdrawn RCCA, automatic reactor trip may not occur sufficiently fast to prevent the minimum DNBR from falling below the safety analysis limit value. Evaluation of this case at the power and coolant conditions at which the overtemperature ΔT trip is expected to trip the plant shows that an upper limit for the number of rods with a DNBR less than the safety analysis limit value is 5 percent.

B. If the reactor is in the automatic control mode, the multiple failures that result in the withdrawal of a single RCCA result in the immobility of the other RCCAs in the controlling bank. The transient then proceeds in the same manner as case A.

For such cases, a reactor trip ultimately occurs although not sufficiently fast in all cases to prevent a minimum DNBR in the core of less than the safety analysis limit value. Following reactor trip, normal shutdown procedures are followed.

The consequential loss of offsite power described in Section 9.0.12 is not limiting for the single RCCA withdrawal event. Due to the delay from reactor trip until turbine trip and the rapid power reduction produced by the reactor trip, the minimum DNBR, for rods where the DNBR did not fall below the design limit value (see Section 22.7.1.1) in the cases described, occurs before the reactor coolant pumps begin to coast down.

Appendix 9C provides discussion and analysis of long term safe shutdown for non-LOCA events.

9.4.3.3 Diverse Mitigation

In addition to the passive systems credited in the DBA, the plant also has a diverse mitigation capability that is able to supply the Category A safety functions for frequent faults. For this event the diverse features are also Class 1 except for the C&I, which is Class 2.

The diverse core cooling is provided by passive feed and bleed using PXS injection and ADS venting (Class 1). The DAS provides diverse reactor trip and safety system actuation (Class 2).

In this fault, the containment function is provided by the fuel cladding and by the RCS, neither of which is threatened in the DBA. The containment building provides diverse containment and is identified as a Class 1 system on that basis for this fault.

Table 9.4.3-1 summarizes the SSCs from this fault assessment. As this is a frequent fault, a diverse means of providing the Category A safety functions is provided. The information provided in Table 9.4.3-1 is from Reference 9.4-10, which documents the diversity for the frequent faults and provides additional information on the diverse mitigation functions. Table 9.4.3-2 provides the operator actions utilized in the diverse safety case.

9.4.3.3.1 Diverse Mitigation for ATWT

The primary protection for the dropped RCCA event is normally provided by the PMS low pressuriser pressure reactor trip function. This function provides a reactor trip for many of the larger dropped rod worth cases analysed due to the RCS pressure reduction caused by the drop of the RCCA(s). Cases that do not reach this reactor trip setpoint will reach a new equilibrium power level, with the possibility of a power overshoot. Some cases may actuate the P-17 permissive rod withdrawal block component of the rod control system. The P-17 is actuated as a result of a rapid reduction in neutron flux based on signals directly from the nuclear instrumentation system (NIS) and is independent of PMS comparators or logic. The P-17 function was included in the rod control system design in order to support operation of the Rapid Power Reduction System (RPRS), which allows the plant to sustain a full load rejection from full power without a reactor trip. The RPRS drops selected rod banks to reduce core power when steam dumps and normal rod control insertion cannot mitigate large load rejections. The P-17 function prevents the rod control system from unnecessarily increasing power following an RPRS actuation by blocking automatic rod withdrawal.

This analysis is performed to demonstrate the adequacy of the operable portions of the PMS (considering the impact of the CCF) as well as the DAS to detect and actuate mechanical SSCs to mitigate the fault. The following ATWT acceptance criteria are applicable to this event:

- The RCS does not overpressurise due to reactor coolant heatup. The ATWT pressure limit is 22.06 MPa-rel (3200 psig).

- There is no significant fuel damage.

- The rate and duration of energy release to containment is much less than for the design basis LOCA. This demonstrates that the containment does not overpressurise due to the energy release to the containment.

With respect to peak RCS overpressure criterion, this event is bounded by the Turbine Trip DB event (Section 9.2.3).

9.4.3.3.1.1 Diverse ATWT Method of Analysis

A bounding failure scenario was analysed for the dropped RCCA event ATWT diversity case. The scenario assumes simultaneous failures in both the PMS and the rod control system. It is assumed that the PMS low pressuriser pressure reactor trip function fails. As noted above, this trip provides protection for some large dropped rod worth cases, and was therefore assumed to fail. Also assumed to fail is the P-17 rod withdrawal block component of the rod control system. All other parts of the rod control system are assumed to function as designed. Since the P-17 function and the rod control system circuitry reside in a common logic cabinet, this type of failure is considered to be not credible. A credible failure would be the failure of all logic in a given cabinet, which in this case would disable both the P-17 function and the rod control system. This would eliminate the possibility of power overshoot from control rod withdrawal during a dropped rod event, and result in a less limiting scenario, as in the manual rod control scenario. However, for the purpose of demonstrating diversity the bounding case was analysed, in which only the P-17 portion of the rod control system is disabled.

The thermal-hydraulic conditions during the transient, namely core heat flux, RCS temperature, RCS pressure, and inserted reactivity were calculated using the LOFTRAN code for approximately 1100 cases (combinations of dropped rod worth, control bank worth, and MTC). These transient conditions were then used in the ANC and VIPRE-01 codes to calculate a maximum hot channel peaking factor ($F_{\Delta H}$) for each case for comparison to the $F_{\Delta H}$ corresponding to the DNBR limit. The WRB-2 DNBR correlation was used, consistent with the DBA analysis. Initial condition uncertainties on power, pressure, temperature, and flow were accounted for in the DNBR limit. For the frequent fault diversity analysis, some excess reserve margin was removed from the DNBR limit. The AP1000 plant is designed to have at least [ ] DNBR margin at startup for frequent fault analyses. For the purposes of defining a DNBR limit for use in the frequent fault diversity analysis, some of this reserve margin was used. However, the limit remains conservative relative to the correlation limit. The analysis confirmed that the limits are met for all cases.

9.4.3.3.1.2 Diverse ATWT Credited SSCs

For the diverse ATWT no SSCs are credited.

9.4.3.3.1.3 Diverse ATWT Results

Figures 9.4.3-5 through 9.4.3-8 show the transient response for several of the zero MTC 400 pcm control bank worth cases. The transient behaviour presented in these figures is typical of the results for other values of MTC, control bank worth, and dropped rod worth. The nuclear power and heat flux drop to a minimum value and recover under the influence of both rod withdrawal and thermal feedback. The prompt decrease in power is governed by the dropped rod worth because the plant control system does not respond during the short rod drop time period. The plant control system detects the reduction in core power and initiates control

bank withdrawal to restore the primary side power. Power overshoot occurs after which the core power is restored to the initial power level.

The analysis showed that the frequent fault DNBR limit was met, when a portion of the DNB margin typically reserved within the safety analysis limit for frequent faults was credited in the analysis. This is conservative compared to the correlation limit that is typically used for frequent fault diversity analyses. In addition, no fuel melting is predicted.

The analysis and results demonstrate that the AP1000 plant will remain safe with respect to the Dropped RCCA event if the reactor trip and P-17 rod withdrawal block functions are inoperable.

9.4.3.3.2 Diverse Mitigation for Core Cooling

The loss of normal feedwater diverse core cooling, as analysed in Section 9.2.7.3.2, was determined to be bounding of all non-LOCA events.

9.4.3.4 Radiological Consequences

9.4.3.4.1 Dropped RCCAs, Dropped RCCA Bank, and Statically Misaligned RCCA

Design Basis

In the case where offsite power remains available, there is no release of activity to the environment and the Target 4 BSOs (0.01 mSv offsite and 0.1 mSv onsite) are met.

In the case where offsite power is lost, a small release of activity may occur as a result of steam dump to the atmosphere due to unavailability of the condensers. With no fuel damage and primary and secondary circuits intact, the initiating event has no impact on the doses. The doses are a consequence of the assumed loss of offsite power. Therefore, the loss of offsite power doses from Section 9.2.6.4 are presented. The calculated maximum doses for all relevant pathways (inhalation, cloudshine, and groundshine) are as follows:

- Offsite dose: 0.05 mSv Worker dose: 1.5 mSv

These doses are within the Target 4 BSL for frequent faults (1 mSv offsite and 20 mSv onsite).

Diverse Mitigation

Both the diverse ATWT and diverse core cooling scenarios demonstrate that the RCS does not overpressurise and there is no significant fuel damage. For a diverse mitigation radiological consequences analysis better estimate assumptions would be credited. This would include reactor coolant system activity levels significantly lower than those modelled for the DBA and better activity retention in containment and in the steam generators. In addition better estimate atmospheric dispersion factors would be used. Therefore, a diverse mitigation radiological consequences analysis would show that the doses for the diverse ATWT scenario would be less than those reported for the non-LOCA DBAs and doses for the diverse core cooling scenario would be much less than for the design basis LOCA. The diverse mitigation analyses would not have to meet the Target 4 BSL for frequent faults and would meet the Target 4 BSL for infrequent faults.

9.4.3.4.2 Single Rod Cluster Control Assembly Withdrawal

Design Basis

In the case where offsite power remains available, there is no release of activity to the environment and the Target 4 BSOs (0.01 mSv offsite and 0.1 mSv onsite) are met.

In the case where offsite power is lost, a small release of activity may occur as a result of steam dump to the atmosphere due to unavailability of the condensers. The analysis results presented in Section 9.4.3.2.2.3 show that for this event, an upper bound of the number of fuel rods experiencing DNB is 5 percent of the total fuel rods in the core. The radiological consequences of the locked rotor accident presented in Section 9.3.3.4 assumed 10 percent of the fuel rods are damaged. Therefore, the locked rotor doses bound those of the single rod withdrawal event. The locked rotor doses from Section 9.3.3.4.5 are presented. The calculated maximum doses for all relevant pathways (inhalation, cloudshine, and groundshine) are as follows:

- Offsite dose: 2.8 mSv worker dose: 11 mSv

These doses are within the Target 4 BSL for infrequent faults (10 mSv offsite and 200 mSv onsite).

Thus, the identification of the Class 1 SSCs credited for protection is adequate to meet DB requirements.

9.4.3.5 As Low As Reasonably Practicable Assessment

For the this event, the identification of the primary safety functions as Class 1 SSCs has been shown to be adequate to meet DB requirements.

The diverse mitigation functions, including other Class 1 safety functions and the DAS function, which is Class 2, is also shown by analysis to meet the corresponding requirements for this event. See Reference 9.4-10 for additional discussions on these diverse mitigation features.

Additionally, the AP1000 plant design has a third level of redundancy provided by the DiD systems. The applicable DiD functions include:

- CVS boration for long-term reactivity control
- CVS make-up for RCS inventory control
- SFW with steam dump for short-term decay heat removal
- RNS cooling of the RCS for long-term decay heat removal. The RNS requires support from the CCS and SWS cooling water systems.
- Pressuriser spray and auxiliary spray for RCS pressure control
- Control by the PLS C&I

The characteristics of the above features were compared to improvements that were evaluated for the RNS for its mitigation of cliff edge small LOCAs. First it should be recognized that in this situation the RNS provides the second level of defence for this event and is therefore more important than the above DiD features which provide a 3rd level of defence. The RNS improvements included making the RNS alignment and acuation automatic, increasing the RNS pump head, and adding a RNS suction supply tank that is separate from the Class 1 system. None of these potential improvements were found to be ALARP (See Section 9.1.4.5).

However, the SFW and CVS already include characteristics similar to these proposed improvements. Another improvement that could be made to these DiD systems is to upgrade them to Class 1. This would be very expensive especially and would have wide reaching impacts to the design of SSCs; notable would be the impact on component and building design to address hazards including seismic and storm winds/missiles. Such a change would not be ALARP because the cost would be grossly disproportional to its benefit.

As discussed in Section 9.0.15, the AP1000 has incorporated ALARP thinking throughout its development. In addition, the current risk of a large radioactivity release is significantly less than the SAP Target 9 BSO (1E-7 pa). Considering the ALARP thinking that went into the AP1000 development, its low risk profile and the additional level of defence discussed above (including their performance characteristics), improving the Class 2 DiD to better remove decay heat or shutdown the reactor would be grossly disproportional to the risk reduction that might be achieved. As a result, the current design is considered ALARP.

9.4.3.6 Conclusions

For cases of dropped RCCAs or dropped banks, including inadvertent drops of the RCCAs in those groups selected to be inserted as part of the rapid power reduction system, it is shown that the DNBR remains greater than the safety analysis limit value and, therefore, the DNB design basis is met.

For cases of any one RCCA fully inserted, or the mechanical shim or axial offset banks inserted to their rod insertion limits with any single RCCA in one of those banks fully withdrawn (static misalignment), the DNBR remains greater than the safety analysis limit value (see Section 22.7.1.1).

For the case of the accidental withdrawal of a single RCCA, with the reactor in the automatic or manual control mode and initially operating at full power with the mechanical shim or axial offset banks at their insertion limits, an upper bound of the number of fuel rods experiencing DNB is 5 percent of the total fuel rods in the core.

This event has also been adequately assessed with respect to ATWT considerations.

Diverse core cooling capabilities have been demonstrated.

DBA radiological consequences for the dropped RCCAs or the statically misaligned RCCA are within the Target 4 BSL for frequent faults (1 mSv offsite and 20 mSv onsite). Thus, the identification of the Class 1 SSCs for event mitigation is adequate to meet DB requirements.

DBA radiological consequences for a single rod cluster control assembly withdrawal are within the Target 4 BSL for infrequent faults (10 mSv offsite and 200 mSv onsite). Thus, the identification of the Class 1 SSCs credited for protection is adequate to meet DB requirements.

It has been shown that the AP1000 plant design includes adequate systems for the protection of this fault, which limit the radiological consequences such that they are compliant with the SAPs targets and the risks have been reduced to be ALARP.

9.4.4 Startup of an Inactive Reactor Coolant Pump at an Incorrect Temperature (Fault 1.15.6)

The Technical Specifications require all RCPs to be operating while in Modes 1 and 2. The maximum initial core power level for the startup of an inactive loop transient is approximately

zero MWt. Furthermore, the reactor will initially be subcritical by the Technical Specification requirement. There will be no increase in core power, and no automatic or manual protective action is required.

9.4.5 Not Used

9.4.6 Chemical and Volume Control System Malfunction that Results in a Decrease in the Boron Concentration in the Reactor Coolant (Fault 1.15.7)

9.4.6.1 Identification of Causes and Accident Description

Other than control rod withdrawal, the principal means of positive reactivity insertion to the core is the addition of unborated, primary-grade water from the demineralized water transfer and storage system into the reactor coolant system through the reactor makeup portion of the chemical and volume control system. Normal boron dilution with these systems is manually initiated under strict administrative controls requiring close operator surveillance. Procedures limit the rate and duration of the dilution. A boric acid blend system is available to allow the operator to match the makeup water boron concentration to that of the reactor coolant system during normal charging.

An inadvertent boron dilution is caused by the failure of the demineralized water transfer and storage system or chemical and volume control system, either by controller, operator or mechanical failure. The chemical and volume control system and demineralized water transfer and storage system are designed to limit, even under various postulated failure modes, the potential rate of dilution to values that, with indication by alarms and instrumentation, allow sufficient time for automatic or operator response to terminate the dilution.

An inadvertent dilution from the demineralized water transfer and storage system through the chemical and volume control system may be terminated by isolating the makeup flow to the reactor coolant system, by isolating the makeup pump suction line to the demineralized water transfer and storage system storage tank, or by tripping the makeup pumps. Lost shutdown margin may be regained by adding borated water to the reactor coolant system from the boric acid tank.

Generally, to dilute, the operator would need to perform two actions:

- Switch control of the makeup from the automatic makeup mode to the dilute mode.
- Start the chemical and volume control system makeup pumps.

Failure to carry out either of those actions prevents initiation of dilution. Because the AP1000 chemical and volume control system makeup pumps do not run continuously (they are expected to be operated once per day to make up for reactor coolant system leakage), a makeup pump is started when the volume control system is placed into dilute mode.

The status of the reactor coolant system makeup is available to the operator by the following:

- Indication of the boric acid and blended flow rates
- Chemical and volume control system makeup pumps status
- Deviation alarms, if the boric acid or blended flow rates deviate by more than the specified tolerance from the preset values

- When reactor is subcritical:
  - High flux at shutdown alarm
  - Indicated source range neutron flux count rate
  - Audible source range neutron flux count rate
  - Source range neutron flux-multiplication alarm
- When the reactor is critical:
  - Axial flux difference alarm (reactor power ≥ 50 percent rated thermal power)
  - Control rod insertion limit low and low-low alarms
  - Overtemperature ΔT alarm (at power)
  - Overtemperature ΔT reactor trip
  - Power range neutron flux-high, both high and low setpoint reactor trips.

In addition, this section addresses concerns related to transient reactivity excursions associated with Xenon decay following a reactor trip from power, which was fully evaluated in Reference 9.4.27. The Xenon-induced reactivity excursion is relatively slow, and the CVS would normally maintain the required shutdown margin and reactivity control in this situation. In the event of CVS failure following reactor trip but before the Xenon level stabilizes, Reference 9.4.27 demonstrates that adequate diverse protection systems are available to control reactivity through RCS boration. Of particular concern for this scenario would be an uncontrolled return-to-power from Mode 2 or 3 due to Xenon decay. For this scenario, the CVS failure does not result in a reduction in boron; however, the Xenon-induced reactivity excursion produces a similar reactivity anomaly concern.

9.4.6.2 Design Basis Mitigation

Analysis is performed to demonstrate the adequacy of the PMS to detect and mitigate the fault and show that the safety analysis criteria are satisfied including:

- No fuel failures (confirmed using minimum DNBR and fuel melt criteria),
- The RCS pressure criterion is met,
- The MSS pressure criterion is met, and
- The pressuriser does not fill (which could result in a LOCA)

Analysis is performed to demonstrate the adequacy of the protection and safety monitoring system to detect and mitigate the fault and show no return to criticality (no complete loss of shutdown margin following a boron dilution).

Provided that the reactor core will not reach criticality, and the boron dilution transient is bounded by the other transients with respect to DNB, peak primary or secondary pressure, and pressuriser fill concerns.

9.4.6.2.1 DBA Method of Analysis

Boron dilutions during refuelling, cold shutdown, hot shutdown, hot standby, startup, and power modes of operation are considered in this analysis. Conservative values for critical/key parameters are used (high reactor coolant system critical boron concentrations, high boron worths, minimum shutdown margins, and lower-than-actual reactor coolant system volumes).

These assumptions (see Table 9.4-2) result in conservative determinations of the time available for operator or automatic system response after detection of a dilution transient in progress.

A loss of offsite power is considered for the boron dilution case initiated from the power mode of operation (Mode 1) with the reactor in manual control. This is the analysed Mode 1 boron dilution case that produces a reactor and turbine trip (Section 9.4.6.2.6). The loss of offsite power is assumed to occur as a direct result of a turbine trip that would disrupt the grid and produce a consequential loss of offsite ac power. As discussed in Section 9.0.12, that scenario can occur only with the plant at power and connected to the grid. Therefore, only a boron dilution case initiated from full power will be addressed with respect to the consequential loss of offsite power.

9.4.6.2.2 DBA Credited SSCs

For the DB, all of the claimed SSCs are Class 1. The credited Class 1 SSCs are listed in Table 9.0-10. The presented DBA ends shortly after reactor trip; however, essential safety functions for the long term safe shutdown analysis (Appendix 9C) bound safe shutdown response for this event. The primary core cooling is provided by the PRHR and passive containment cooling. Other SSCs include the CMTs, containment isolation, and pressuriser SVs. The PMS provides the following:

- RT on:
  - Overtemperature ΔT
  - Source range high flux
- Automatic isolation of dilution sources on:
  - Source range neutron flux-multiplication alarm prior to losing all shutdown margin when reactor is subcritical
  - Any reactor trip when reactor is critical
- PRHR actuation on Low-2 SG NR level coincident with Low-2 SFW flow
- CMTs and containment isolation on Low-2 CL temperature
- PCS on High-2 containment pressure

9.4.6.2.3 DBA Results

9.4.6.2.3.1 Dilution During Refuelling (Mode 6)

An uncontrolled boron dilution transient cannot occur during this mode of operation. Inadvertent dilution is prevented by administrative controls, which isolate the reactor coolant system from the potential source of unborated water by locking closed specified valves in the chemical and volume control system during refuelling operations. These valves block the flow paths that allow unborated makeup water to reach the reactor coolant system. Makeup which is required during refuelling uses water supplied from the boric acid tank (which contains borated water). This information is consistent with the boron dilution discussion provided in Section 9.8.4.4.5.

9.4.6.2.3.2 Dilution During Cold Shutdown (Mode 5)

The following conditions are assumed for inadvertent boron dilution while in this operating mode:

- A dilution flow of 39.75 m^3/hr (175 gpm) of unborated water exists. The dilution flow is assumed to be at 4.4°C and 0.101 MPa abs (40°F and 14.7 psia). The fluid conditions of the RCS are assumed to be 93.33°C and 0.101 MPa abs (200°F and 14.7 psia).

- The reactor coolant system volume is 73.86 m^3 (2608.2 ft^3). This is a conservative estimate of the minimum active volume of the reactor coolant system corresponding to the water level at mid-loop in the vessel while on normal residual heat removal. The assumed active volume does not include the volume of the reactor vessel upper head region.

- Control rods are fully inserted, which is the normal condition in cold shutdown, and the critical boron concentration is 1483 ppm. This is a conservative boron concentration with control rods inserted and accounts for the most reactive rod stuck in the fully withdrawn position.

- The shutdown margin is equal to 1.6-percent Δk/k, the minimum value identified by the Technical Specifications for the cold shutdown mode. Combined with the critical boron concentration identified above, this gives an initial boron concentration of 1675 ppm.

- At least one reactor coolant pump will be normally operating during plant operation in Mode 5. It may be possible under some conditions, however, to operate the plant in Mode 5 with no reactor coolant pumps operating. For this reason, the mixing volume assumed for the analysis in Mode 5 will include the reactor coolant loop and normal residual heat removal system volumes that are being actively mixed by the residual heat removal system pumps.

- A boron dilution protection system (BDPS) Safety Analysis Limit (SAL) flux multiplier setpoint of 3.0 is assumed.

In the event of an inadvertent boron dilution transient during cold shutdown, the source range nuclear instrumentation detects an increase in the neutron flux by comparing the current source range flux to that of about 50 minutes earlier. Upon detecting a sufficiently large flux increase, an alarm is sounded for the operator, and valves are actuated to terminate the dilution automatically.

Upon the actuation of a source range flux multiplier signal, the makeup flow to the reactor coolant system and the makeup pump suction line to the demineralized water transfer and storage system storage tank are isolated. This thereby terminates the dilution. In addition, the makeup pumps are tripped for equipment protection purposes.

No operator action is required to terminate this transient. The analysis demonstrates that the flux multiplier SAL will be reached 11.2 minutes after the dilution transient begins and that there is sufficient time at this point for the automatic protective features to terminate the dilution prior to losing all shutdown margin. After the automatic protection functions take place, the operator may take action to restore the Technical Specification shutdown margin.

9.4.6.2.3.3 Dilution During Safe Shutdown (Mode 4)

The following conditions are assumed for an inadvertent boron dilution while in this mode:

- A dilution flow of 39.75 m^3/hr (175 gpm) of unborated water exists. The dilution flow is assumed to be at 4.4°C and 0.101 MPa abs (40°F and 14.7 psia). The fluid conditions of the RCS are assumed to be 215.56°C and 2.765 MPa abs (420°F and 401 psia).

- The reactor coolant system volume is 215.38 m^3 (7605.9 ft^3). This is a conservative estimate of the minimum active volume of the reactor coolant system with the reactor coolant system filled and vented and one reactor coolant pump running. The assumed active volume does not include the volume of the reactor vessel upper head region.

- All control rods are fully inserted except the most reactive rod, which is assumed stuck in the fully withdrawn position. The critical boron concentration is 1449 ppm.

- The shutdown margin is equal to 1.6-percent $\Delta k/k$, the minimum value required by the Technical Specifications for the hot shutdown mode. Combined with the critical boron concentration given above, this gives an initial boron concentration of 1649 ppm.

- The reactor coolant system dilution volume is considered well-mixed. The Technical Specification 3.4.8 requires that at least one reactor coolant pump shall be operating with a flow of at least 3000 gpm (681.37 m^3/hr) when in Mode 4. This provides sufficient flow through the system to maintain the system well-mixed. If a reactor coolant pump is not operating, the demineralized water isolation valves are closed and an uncontrolled boron dilution transient cannot occur, as discussed in Section 9.4.6.2.1.

- A BDPS SAL setpoint of 3.0 is assumed.

In the event of an inadvertent boron dilution transient during safe shutdown, the source range nuclear instrumentation detects a sufficiently large increase in the neutron flux by comparing the current source range flux to that of about 50 minutes earlier, automatically initiates valve movement to terminate the dilution, and sounds an alarm.

Upon the actuation of a source range flux multiplier signal, the makeup flow to the reactor coolant system and the makeup pump suction line to the demineralized water transfer and storage system storage tank are isolated. This thereby terminates the dilution. Also, the makeup pumps are tripped for equipment protection purposes.

No operator action is required to terminate this transient. The analysis demonstrates that the flux multiplier SAL will be reached 28.83 minutes after the dilution transient begins and that there is sufficient time at this point for the automatic protective features to terminate the dilution prior to losing all shutdown margin. After the automatic protection functions take place, the operator may take action to restore the Technical Specification shutdown margin.

9.4.6.2.3.4 Dilution During Hot Standby (Mode 3)

The following conditions are assumed for an inadvertent boron dilution while in this mode:

- A dilution flow of 39.75 m^3/hr (175 gpm) of unborated water exists. The dilution flow is assumed to be at 4.4°C and 0.101 MPa abs (40°F and 14.7 psia). The fluid conditions of

the reactor coolant system are assumed to be 291.67°C and 15.513 MPa abs (557°F and 2250 psia).

- The reactor coolant system volume is 215.38 m^3 (7605.9 ft^3). This is a conservative estimate of the minimum active volume of the reactor coolant system with the reactor coolant system filled and vented and one reactor coolant pump running. The assumed active volume does not include the volume of the reactor vessel upper head region.

- Critical boron concentration is 1281 ppm. This is a conservative boron concentration assuming control rods are fully inserted minus the most reactive rod, which is assumed stuck in the fully withdrawn position.

- The shutdown margin is equal to 1.6-percent Δk/k, the minimum value required by the Technical Specifications for the hot standby mode. Combined with the critical boron concentration given above, this gives an initial boron concentration of 1509 ppm.

- The reactor coolant system dilution volume is considered well-mixed. The Technical Specification 3.4.8 requires that at least one reactor coolant pump shall be operating with a flow of at least 681.37 m^3/hr (3000 gpm) when in Mode 3. This provides sufficient flow through the system to maintain the system well mixed. If a reactor coolant pump is not operating, the demineralized water isolation valves are closed and an uncontrolled boron dilution transient cannot occur, as discussed in section 9.4.6.2.1.

In the event of an inadvertent boron dilution transient in hot standby, the source range nuclear instrumentation detects a sufficiently large increase in the neutron flux by comparing the current source range flux to that of about 50 minutes earlier, automatically initiates valve movement to terminate the dilution, and sounds an alarm. Upon the actuation of a source range flux multiplier signal, the makeup flow to the reactor coolant system and the makeup pump suction line to the demineralized water transfer and storage system storage tank are isolated. This thereby terminates the dilution. Also, the makeup pumps are tripped for equipment protection purposes.

No operator action is required to terminate this transient. The analysis demonstrates that the flux multiplier SAL will be reached 32.07 minutes after the dilution transient begins and that there is sufficient time at this point for the automatic protective features to terminate the dilution prior to losing all shutdown margin. After the automatic protection functions take place, the operator may take action to restore the Technical Specification shutdown margin.

9.4.6.2.3.5 Dilution During Startup (Mode 2)

The plant is in the startup mode only for startup testing at the beginning of each cycle. During this mode of operation, rod control is in manual. Normal actions taken to change power level, either up or down, require operator actuation. The Technical Specifications require an available shutdown margin of 1.6-percent Δk/k and four reactor coolant pumps operating. Other conditions assumed are the following:

- A dilution flow of 39.75 m^3/hr (175 gpm) of unborated water exists. The dilution flow is assumed to be at 4.4°C and 0.101 MPa abs (40°F and 14.7 psia). The fluid conditions of the reactor coolant system are assumed to be at the 5-percent power, 296.57°C and 15.513 MPa abs (565.83°F and 2250 psia).

- Minimum reactor coolant system water volume is 238.58 m^3 (8425.5 ft^3). This is a very conservative estimate of the active reactor coolant system volume, minus the pressuriser volume.

- The initial maximum critical boron concentration, corresponding to the rods inserted to the insertion limits, is 2031 ppm. The minimum change in boron concentration from this initial condition to a hot zero power critical condition with all rods inserted is 1097 ppm, which gives a critical boron concentration of 934 ppm.

This mode of operation is a transitory operational mode in which the operator intentionally dilutes and withdraws control rods to take the plant critical. During this mode, the plant is in manual control. For a normal approach to criticality, the operator manually withdraws control rods and dilutes the reactor coolant with unborated water at controlled rates until criticality is achieved. Once critical, the power escalation is slow enough to allow the operator to manually block the source range reactor trip after receiving the P-6 permissive signal from the intermediate range detectors (nominally at 10^5 cps). Too fast a power escalation (due to an unknown dilution) would result in reaching P-6 unexpectedly, leaving insufficient time to manually block the source range reactor trip. Failure to perform this manual action results in a reactor trip and immediate shutdown of the reactor.

Upon any reactor trip signal, or low input voltage to the Class 1E DC and uninterruptable power supply system battery chargers, a Class 1 function automatically isolates the potentially unborated water from the demineralized water transfer and storage system and thereby terminates the dilution. Additionally, the suction lines for the chemical and volume control system pumps are automatically realigned to draw borated water from the chemical and volume control system boric acid tank.

After reactor trip, the dilution would have to continue for approximately 205 minutes to overcome the available shutdown margin.

9.4.6.2.3.6 Dilution During Full Power Operation (Mode 1)

The plant may be operated at power two ways: automatic T_{avg}/rod control and under operator control. The Technical Specifications require an available shutdown margin of 1.6-percent $\Delta k/k$ and four reactor coolant pumps operating. With the plant at power and the reactor coolant system at pressure, the dilution rate is limited by the capacity of the chemical and volume control system makeup pumps. The analysis is performed assuming two chemical and volume control system pumps are in operation, even though normal operation is with one pump. Conditions assumed for a dilution in this mode are the following:

- A dilution flow of 39.75 m^3/hr (175 gpm) of unborated water exists. The dilution flow is assumed to be at 4.4°C and 0.101 MPa abs (40°F and 14.7 psia). The fluid conditions of the RCS are assumed to be at full power, 305.33°C and 15.513 MPa abs (581.6°F and 2250 psia).

- Minimum reactor coolant system water volume is 238.58 m^3 (8425.5 ft^3). This is a very conservative estimate of the active reactor coolant system volume, minus the pressuriser volume.

- An initial maximum boron concentration, corresponding to the rods inserted to the insertion limits, is 1811 ppm. The minimum change in boron concentration from this initial condition to a hot zero power critical condition with all rods inserted is 877 ppm,

which gives a critical boron concentration of 934 ppm. Full rod insertion, minus the most reactive stuck rod, occurs due to reactor trip.

With the reactor in automatic rod control, the pressuriser level controller limits the dilution flow rate to the maximum letdown rate. If a dilution rate in excess of the letdown rate is present, the pressuriser level controller throttles charging flow down to match letdown rate. For the safety analysis, a conservative dilution flow rate of 39.75 m^3/hr (175 gpm) is assumed. With the reactor in automatic rod control, a boron dilution results in a power and temperature increase in such a way that the rod controller attempts to compensate by slow insertion of the control rods. This action by the controller results in at least three alarms to the operator:

A. Rod insertion limit – low level alarm
B. Rod insertion limit – low-low level alarm if insertion continues
C. Axial flux difference alarm (ΔI outside of the target band)

Given the many alarms, indications, and inherent slow process of dilution at power, the operator has sufficient time for action. The operator has at least 170.6 minutes from the rod insertion limit low-low alarm until shutdown margin is lost at beginning of cycle. The time is significantly longer at the end of the cycle because of the lower initial and critical boron concentrations.

Because the analysis for the boron dilution event with the reactor in automatic rod control does not predict a reactor and turbine trip, considering the consequential loss of offsite power for this case is not needed.

With the reactor in manual control and no operator action taken to terminate the transient, the power and temperature would rise and cause the reactor to reach the overtemperature ΔT trip setpoint resulting in a reactor trip. Upon any reactor trip signal, a Class 1 function automatically isolates the unborated water from the demineralized water transfer and storage system and thereby terminates the dilution. Additionally, the suction lines for the chemical and volume control system pumps are automatically realigned to draw borated water from the chemical and volume control system boric acid tank.

The boron dilution transient in this case is essentially equivalent to an uncontrolled rod withdrawal at power (see Section 9.4.2). The maximum reactivity insertion rate for a boron dilution transient is conservatively estimated to be approximately 0.5 pcm/s and is within the range of insertion rates analysed for uncontrolled rod withdrawal at power. Before reaching the overtemperature ΔT reactor trip, the operator receives an alarm overtemperature ΔT and an overtemperature ΔT turbine runback.

Should a consequential loss of offsite power occur after reactor and turbine trip, it does not alter the fact that the dilution event has been terminated by automatic protection features. As indicated previously, the reactor trip signal that occurs in parallel with the turbine trip will actuate a Class 1 function that automatically isolates the unborated water from the demineralized water system and thereby terminates the dilution. A subsequent loss of offsite power will cause the chemical and volume control system pumps to shut down.

After reactor trip, the automatic termination of the dilution flow from the demineralized water transfer and storage system precludes a post-trip return to criticality.

9.4.6.3 Diverse Mitigation

The available diverse protection for the Mode 1 and Mode 2 scenarios of this event is the same as for the RCCA misalignment faults (Section 9.4.3.3).

Section 9.4.6.3.1 provides a discussion of the ATWT evaluation for this event that is divided into two parts. The first evaluation addresses ATWT initiated from Mode 1 and Mode 2. The second evaluation addresses inadvertent boron dilution event initiated from the lower modes of operation with control rods already inserted. As such, this second evaluation is not technically an ATWT event. The second evaluation relies on a DAS signal as follows.

The boron dilution event at shutdown conditions is characterized by a slow increase in nuclear power from very low power levels. As a result of the increase in nuclear power the source range alarm would be generated; however this alarm is assumed to not be created in the PMS due to the common cause failure and is not credited in the analysis. The slow nuclear power increase eventually results in criticality.

As the source range nuclear instrumentation is considered the primary protection for the inadvertent boron dilution event at lower modes, a new DAS actuation based on the intermediate range nuclear instrumentation (IRNI) is credited for boron dilution at shutdown conditions. The DAS actuation logic is "ARMED" when the reactor trip breakers are open and IRNI indicates < [ ] FON power. The arming signal is retained even if the IRNI signal goes above the nominal setpoint of [ ] fraction of nominal (FON) power. The arming signal is removed if either the reactor trip breakers are "NOT" open or a demineralised water storage tank (DWST) isolation signal has been generated.

The DAS IRNI actuation signal results in trip of the RCPs and RNS pumps, isolation of the boron dilution sources (i.e., makeup flow to the RCS and the makeup pump suction line to the DWST), and CMT actuation. Boron addition to the core following the CMT actuation results in a negative reactivity addition and terminates the event. The rate of increase in the nuclear power level on the intermediate range detector scale from the DAS actuation setpoint of [ ] FON to the point of adding heat ([ ] FON) is slow enough that the required DAS functionality can be carried out in a timely manner to automatically terminate the event.

9.4.6.3.1 Diverse Mitigation for ATWT

One of the two principal means of positive reactivity insertion to the core is the addition of unborated, primary-grade water from the demineralised water into the RCS through the reactor makeup portion of the CVS. Normal boron dilution with these systems is manually initiated under strict administrative controls requiring close operator surveillance.

An inadvertent boron dilution is postulated to be caused by the failure of the CVS by the controller, mechanical failure, or operator. Two diversity scenarios are evaluated: inadvertent boron dilution from Modes 1 or 2 (ATWT) and inadvertent boron dilution from lower modes.

An inadvertent boron dilution results in a slow addition of positive reactivity. If the reactor is in Mode 1 or Mode 2, an uncontrolled boron dilution causes a slow increase in core power.

If the event is initiated at lower modes, multiple alarms are available to alert the operator of a dilution event including displayed / audible source range neutron flux count rates, and the source range neutron flux-multiplication alarm. The probability that a problem occurs in the source range neutron flux monitoring system with a simultaneous independent failure would cause a boron dilution event is extremely remote. However, boron dilution diversity analysis

at lower modes is completed to demonstrate that the DAS IRNI function would protect the plant in this scenario.

This analysis is performed to demonstrate the adequacy of the operable portions of the PMS (considering the impact of the CCF) as well as the DAS to detect and actuate mechanical SSCs to mitigate the fault. The following ATWT acceptance criteria are applicable to this event:

- The RCS does not overpressurise due to reactor coolant heatup. The ATWT pressure limit is 22.06 MPa-rel (3200 psig).
- There is no significant fuel damage.
- The rate and duration of energy release to containment is much less than for the design basis LOCA. This demonstrates that the containment does not overpressurise due to the energy release to the containment.

For the lower modes of operation, a conservative acceptance criterion is used that the point of adding heat is not reached, which ensures that the previous ATWT criteria are met.

9.4.6.3.1.1 Diverse ATWT Method of Analysis

Analysis Assumptions

The assumptions used for the ATWT Boron Dilution in Mode 1 and 2 are discussed below. No measurement/instrumentation errors are assumed.

a. Initial conditions are assumed at the nominal full power values. If the event is initiated at a lower power level, the first part of event will be dominated by a power increase. After reaching full power, the rest of the event will be essentially the same as a boron dilution event initiated at full power.

b. The initial boron concentration and core kinetics parameters are assumed to be at their BOC values. Refer to Reference 9.4-20 for core neutronics discussion.

c. Modelled reactivity coefficients are more conservative than the reactivity coefficients discussed in Reference 9.4-20. Also, to model power increase due to boron dilution, boron coefficient was set equal to -9.7, -9.3, -8.9 pcm/ppm for boron concentrations 600, 900, 1200 ppm.

d. The pressuriser pressure control system, including heaters and sprays, are assumed to be operable and function normally.

e. It is assumed that the pressuriser level control system maintains pressuriser level. The normal makeup flow when one pump is running is 0.0063 m^3/s (100 gpm) is assumed because no single failure could cause inadvertent makeup and simultaneous inadvertent wrong blending.

f. The minimum reactor coolant system water volume used for the boron concentration calculation was assumed to be 230 m^3 (8126 ft^3). The fluid density was calculated assuming an RCS pressure of 15.513 MPa abs (2250 psia) and a temperature of 316°C (600°F). The initial boron concentration is assumed to be 1050 ppm, and the dilution flow rate is assumed to be 8.6 kg/s (19 lbm/s) with a boron concentration of 0 ppm.

g. The turbine trip on reactor trip function is assumed to be operable. Turbine trip is assumed to occur 7 seconds after reaching the reactor trip setpoint. This delay includes 2 seconds for PMS/DAS logic to evaluate the setpoint and a 5 second programmed turbine trip delay from the expected time of reactor trip, which is specified in PMS and DAS.

h. The SG PORVs are assumed to be operable for all cases in which offsite power is available. A set pressure of 7.85 MPa abs (1138 psia) is assumed.

i. The turbine bypass system is assumed to be operable and the turbine is assumed to operate such that the initial steam flow is maintained.

j. The following protection functions are available for this event:

- PMS reactor trip and turbine trip and demineralised water tank line isolation on OTΔT, OPΔT or high neutron flux
- DAS reactor trip and turbine trip – High Hot Leg Temperature in both hot legs
- DAS ESF – PRHR on High Hot Leg Temperature in both hot legs (High Hot Leg Temperature Setpoint is assumed to be 343.3°C (650°F))

k. Prior to reaching PMS reactor trip setpoints, some of the PLS low margin to setpoints alarms may be actuated. The high flux power range above setpoint (C-2), the Low Margin to OTΔT (C-3) and OPΔT (C-4) rod control system power control subsystem interlocks will actuate an alarm, along with blocking automatic and manual withdrawal of control rods, and will actuate turbine runback. The deviation (above or below) of the TAVG/TREF mismatch error signal and deviation of the QN/PTU mismatch error signal will also generate an alarm. Although it is expected that these alarms would alert the operator to manually terminate the dilution and trip the reactor (for cases without RCCA CCF), these alarms are not credited in these analyses.

l. Only cases with continuing ac power supply to plant are presented due to following reasons:

- Assuming a loss of offsite power would mean assuming another independent failure.
- On a loss of ac power signal, the CVS makeup pumps are not automatically sequenced onto the diesel generator. They must be sequenced manually, and DWST must be isolated when the makeup pumps are started. Additionally, the DWST pumps (which provide demineralised water to the makeup pump suction) are not sequenced onto the diesel, providing additional protection against unwanted dilution.
- For the cases with PMS operable, the DWST is automatically isolated on low input voltage to the Class 1 IDS battery chargers.

The assumptions used in the boron dilution diversity analysis from the lower modes of operation are discussed below.

a. Modes of Operation: The lower mode boron dilution events are only considered for Mode 3 (Hot Standby), Mode 4 (Hot Shutdown) and Mode 5 (Cold Shutdown). As discussed in Section 9.4.6.2.3.1, an uncontrolled boron dilution transient cannot occur during Mode 6; therefore, no evaluation was required for this mode.

b. Minimum Dilution Volume: The active RCS volume determines the minimum dilution volume, which is a critical parameter for a dilution event. Cases both with and without RCPs operating are considered, as this assumption significantly changes the active RCS volume. For these shutdown mode analyses, three general conditions were considered:

- Cases where at least one RCP is operating and providing core cooling (Mode 3, 4, or 5). For these cases, the minimum dilution volume is 215.4 m^3 (7605.9 ft^3).
- A Mode 5 case with the RCS drained to the mid-plane of the hot legs and the RNS pumps operating and providing core cooling. For this case, the minimum dilution volume is 73.9 m^3 (2608.2 ft^3).
- Cases where both the RCPs and RNS pumps are operating. For these cases, the minimum dilution volume would be larger than either of the cases described above, and therefore would not be limiting from a boron dilution standpoint.

c. Credible Dilution Flow Rate:

- A dilution flow rate of 22.71 m^3/hr (100 gallons per minute (gpm)) is used, corresponding to a nominal CVS makeup flow from one makeup pump (normal operation). Two makeup pumps would not be operating under normal conditions.
- For conditions where the normal makeup dilution path is isolated, e.g., per Technical Specifications, a dilution path from the CVS chemical mixing tank is still possible, but the flow from this tank is limited to a maximum of 0.45 m^3/hr (2 gpm) by the chemical mixing tank demineralised water inlet flow orifice. A bounding flow of 0.68 m^3/hr (3 gpm) is conservatively considered in the analysis.

d. Initial RCS Temperature: Maximum RCS temperatures are conservatively modelled for each mode. Minimum RCS temperatures are not expected to be limiting for the boron dilution event since the increased density of the water limits the effectiveness of the dilution process. However, the effects of the higher density water on the IRNI indication (limiting the transport of fission neutrons to the detector) must be considered for the DAS actuations that are required.

- For RCP operation in Mode 3, the modelled RCS temperature is 291.7°C (557°F).
- For RCP operation in Mode 4, the modelled RCS temperature is 215.6°C (420°F).
- For Mode 4 RNS pump operation, the modelled RCS temperature is 176.7°C (350°F).
- For Mode 5 RNS pump operation, the modelled RCS temperature is 93.3°C (200°F).

e. Credible Cases: Based on the descriptions of the conditions and limitations of the analysis, the following two credible boron dilution scenarios exist:

- Dilution flow of 22.71 m^3/hr (100 gpm) with at least one RCP in operation (Modes 3 and 4).
- Dilution flow of 22.71 m^3/hr (100 gpm) for one hour with only RNS pumps in operation followed by a maximum dilution rate of 0.68 m^3/hr (3 gpm) (Modes 4 and 5).

f. Accident Scenario: For the credible cases, accident scenario evaluated in the analysis is as follows.

- Initial subcritical conditions with all control rods inserted and the core borated to the minimum shutdown margin or maintain the hot full power (HFP) critical boron concentration prior to trip.
- Simple boron concentration vs. time for dilution until the IRNI setpoint is reached. A conservative safety analysis setpoint power level for the DAS activation is [ ] FON.
- Upon DAS IRNI signal, the following actions are credited:
  - Isolate dilution sources
  - Trip RNS pumps and RCPs
  - Actuate CMTs (with a conservative [ ] second delay)
- To ensure that the ATWT criteria are met, a conservative acceptance criterion used, requiring that the point of adding heat is not reached. For practical purposes, the point of adding heat is assumed to be [ ] RTP.

9.4.6.3.1.2 Diverse ATWT Credited SSCs

For the diverse ATWT all of the claimed SSCs are Class 1 except for the DAS. The available Class 1 SSCs are listed in Table 9.0-14.

For Modes 1 2, the following actuations are provided:

- PMS Automatic isolation of dilution sources on OTΔT reactor trip signal (not credited for PMS CCF case)
- DAS PRHR on High hot leg temperature in both loops

For Modes 3-5, the DAS provides the following:

- Isolation of dilution sources, RCP trip, CMTs, and containment isolation on High intermediate range nuclear power
- Termination of RNS flow on High intermediate range nuclear power (either by RNS pump trip or RNS isolation)

9.4.6.3.1.3 Diverse ATWT Results

9.4.6.3.1.3.1 Mode 1 and Mode 2 Diverse ATWT Boron Dilution

ATWT analyses evaluated scenarios for PMS CCF, Reactor Trip Breaker CCF, and RCCA mechanical CCF. Two limiting cases are presented for this accident group: boron dilution with a PMS CCF in manual rod control and boron dilution with a RCCA mechanical CCF dilution in manual rod control. Although both automatic and manual rod control case were considered, the manual rod control cases are presented. The automatic rod control cases would compensate for a boron dilution by inserting the RCCAs during the initial portion of the transient. This would result in additional indications to alert the operator to the dilution event.

Eventually, the rod control limits would be reached and the remainder of the transient would look the same as the manual rod control scenario.

Boron Dilution with PMS CCF in Manual Rod Control

Table 9.4.6-1 shows the sequence of events for a boron dilution with a CCF of the PMS in manual rod control.

This event is characterised by a slow increase in nuclear power, which results in a primary to secondary side power mismatch due to the fact that turbine is assumed to keep initial steam flow. Secondary pressure increases, which results in an increase in RCS temperature, resulting in a negative reactivity feedback. The increase in nuclear power is slow enough that the core power reaches equilibrium with steam load. As the secondary pressure reaches the SG PORV opening pressure, the opening of SG PORV provides additional steam load. The additional load results in a further increase in the nuclear power. As a result in the increase in nuclear power, the PMS OTΔT reactor trip setpoint is reached; however, a reactor trip signal is not created in the PMS due to the CCF.

Power continues to increase until the DAS High Hot Leg Temperature setpoint of 343.3°C (650°F) is reached.

The DAS High Hot Leg Temperature signal results in a reactor trip, turbine trip, and PRHR actuation. The core power reaches maximum power of 107.5 percent at the time that the High Hot Leg Temperature signal is reached. The PMS OTΔT reactor trip typically results in an isolation of dilution paths; however, due to the failure of the PMS, the automatic isolation of the dilutions does not occur (the DAS High Hot Leg Temperature signal does not result in an automatic isolation of the dilution sources). A manual operator action is required to terminate the dilution and initiate boration of RCS.

As stated in Section 9.4.6.2.3.6, the conservatively minimised boron concentration difference between full power with rods inserted to the insertion limits and hot zero power critical condition with all rods inserted is 877 ppm. If the boron dilution continues from the beginning of the event, such dilution will be require up to approximately 500 minutes of dilution time.

Assuming that operator is not alerted to the transient until after the DAS reactor trip has occurred at 1094 seconds (18 minutes), and assuming 30 minutes for operator action, the operator would be able to act around 2894 seconds (48 minutes) after the beginning of dilution. At that time, the boron concentration will be diluted by 150 ppm from the initial boron concentration.

Boron Dilution with a RCCA Mechanical CCF in Manual Rod Control

Table 9.4.6-2 shows the sequence of events for a boron dilution with a CCF that prevents the RCCAs from inserting in manual rod control. Transient response of this event is shown in Figures 9.4.6-1 to 9.4.6-3.

This event is characterised by a slow increase in nuclear power, which results in a primary to secondary side power mismatch due to the fact that turbine is assumed to keep initial steam flow. Secondary pressure increases, which results in an increase in RCS temperature, resulting in a negative reactivity feedback. The increase in nuclear power is slow enough that the core power reaches equilibrium with steam load. As the secondary pressure reaches the SG PORV opening pressure, the opening of SG PORV provides additional steam load. The additional load results in a further increase in the nuclear power. As a result in the increase in nuclear

power, the PMS OTΔT reactor trip setpoint is reached; however, RCCAs are not inserted into the core due to a reactor trip breaker CCF. Due to the generation of the reactor trip signal in the PMS, the following actions will be taken by the PMS:

- The DWST will be isolated, and blend valve will be aligned to the boric acid storage tank only. This would result in the injection of a highly borated solution at 4375 ppm. If the blending valve is assumed to fail, the dilution will still be terminated.

- The turbine will trip.

- The turbine bypass system will be unblocked, and turbine bypass operation will be initiated in pressure control mode.

After the turbine trips, secondary pressure starts to increase sharply as SG PORVs and the turbine bypass will not be able to take the entire steam load. The secondary side pressure will continue to increase until the steam generator safety valve opening pressure is reached. This increase in secondary pressure will also results in the increase of primary temperature. The DAS High Hot Leg Temperature setpoint of 343.3°C (650°F) will eventually be reached, which actuates the PRHR system.

The core power reaches equilibrium conditions at 102 percent power level.

After that, manual operator action will be necessary to shut down reactor via boration of the RCS.

Boron Dilution with a Reactor Trip Breaker CCF in Manual Rod Control

This scenario is identical to the manual rod control RCCA CCF scenario, until the time when the first reactor trip setpoint in DAS is reached. At that time, RCCA will be dropped from DAS reactor trip signal and terminate the event (the dilution flow will be already terminated from PMS reactor trip signal on OTΔT).

9.4.6.3.1.3.2 Diverse Boron Dilution in Lower Modes

For the credible cases, simplified boron dilution calculations have shown that the second scenario, the cases with only RNS pumps operating, is not as challenging as the first scenario with the RCPs running. For the second scenario, the boron concentration decreases rapidly for the first hour (60 minutes) because of a lower active dilution volume compared to the cases with at least one RCP operating. Thereafter, the boron dilution is attenuated significantly as a result of the dilution flow change to only 0.68 m^3/hr (3 gpm). In the first hour, the boron concentration for all of the RNS-only cases does not decrease below the critical boron concentration. As the boron dilution rate significantly reduces after the CVS isolation within one hour it provides a slower transition through the neutron flux levels for the DAS actuation compared to the first scenario with the RCP(s) operating. Therefore, the scenario with RCP(s) operating is the limiting credible scenario for this event. The results and discussions provided below are based on this limiting scenario.

For the dilution event, the reactor was initially assumed to be critical at HFP with all control rods withdrawn and at equilibrium xenon conditions, followed by a reactor trip and an extended shutdown such that all xenon has decayed. The HFP critical boron concentration at the initial condition is more than sufficient to meet the shutdown margin requirements after reactor trip. Therefore, the initial condition for the transient simulation is HZP temperature

with all control rods inserted and the initial HFP boron concentration. As the dilution progresses, the core becomes nearly critical. The calculations after this point were carried out using both a static solution in ANC and a kinetic solution in SPNOVA.

The dilution event was first simulated for a typical reload cycle without the DAS activation (no boron injection from the CMTs and isolation of the dilution sources) to calculate the time it takes to increase the nuclear power from the IRNI safety analysis setpoint of [ ] FON to the point of adding detectable nuclear heat (assumed to be [ ] FON). A sensitivity study was performed and all cases demonstrated that CMT injection would terminate the transient before the point of adding heat is reached. The most conservative sensitivity is discussed in the following.

The beginning of Cycle 1 was also examined since it is the special case of a "clean" core with the only neutron source being the installed primary source rods. However, it was found that the Cycle 1 core has sufficient control rod worth at BOC such that the core remains subcritical at no-load temperature conditions with all control rods inserted and no soluble boron in the core. To create a more limiting case, it was assumed that the operation staff was in the process of bringing the reactor critical for the first time, and then paused with all shutdown banks withdrawn. An undetected boron dilution is then assumed to start from this condition. For this very conservative case, without any boron injection from the CMTs, the time from [ ] FON to [ ] FON is approximately [ ] from the static solution and [ ] from the kinetic solution. This conservatively calculated time [ ] is greater than the time from the IRNI safety analysis setpoint reached to the conservative time for the CMT injection start [ ]. Therefore, CMT injection will terminate the transient before the generation of detectable nuclear heat occurs.

To demonstrate this assertion, the nuclear power transients for the boron dilution cases with and without CMT injection are shown in Figure 9.4.6-4. As can be seen in these results, the injection of boron into the core terminates the power increase very rapidly. The peak nuclear power of approximately [ ] FON is reached [ ] after the initiation of CMT injection, after which power decreases rapidly as more boron is injected into the core. Therefore, demonstrating that the CMT injection will terminate the transient before the generation of detectable nuclear heat occurs.

9.4.6.3.2 Diverse Mitigation for Core Cooling

The loss of normal feedwater diverse core cooling, as analysed in Section 9.2.7.3.2, was determined to be bounding of all non-LOCA events.

9.4.6.3.3 Diverse Mitigation for Post-Reactor Trip Xenon-Induced Reactivity Excursion

Reference 9.4.27 provides ALARP and diversity studies to address a potential post-reactor trip Xenon-induced reactivity excursion assuming failure of CVS. Key results of Reference 9.4.27 are:

- For all frequent fault scenarios (determined to be those events that could occur when the reactor trip breakers are open) two diverse means of protection to mitigate effects of the xenon transient. The primary protection would come from PMS – Source Range High Neutron Flux signal, which would alert operators to the reactivity excursion. Based on this alarm, operators would manually open the ADS stage 1 valves to reduce RCS pressure, which would allow borated water to inject from the accumulators. The diverse protection would be provided by DAS – High Intermediate Range Power signal. Upon reaching the DAS setpoint ([ ] fraction of nominal power), DAS will

automatically actuate the CMTs. Both of these mitigation options are sufficient to protect against the effects of the Xenon induced reactivity excursion.

- For all infrequent fault scenarios (determined to be those events that could occur when the reactor trip breakers are closed), the diverse protection is provided by PMS indications from the ex-core source range detectors that reactivity in the core is increasing. In this scenario, operators will have ample time to manually actuate the CMTs to borate the core. Although not required, a second diverse system is available to provide boration should CMTs be unavailable. Specifically, operators could initiate passive feed and bleed using ADS, Accumulators, and the IRWST to provide RCS boration.

- The ALARP assessment concludes that providing automatic actuation of existing Class 1 components for boration provides the best alternative for this concern. Specifically, the intermediate range excore detector input has been added to the DAS to provide the diverse frequent fault protection.

9.4.6.4 Radiological Consequences

Design Basis

In the case where offsite power remains available, there is no release of activity to the environment and the Target 4 BSOs (0.01 mSv offsite and 0.1 mSv onsite) are met.

In the case where offsite power is lost, a small release of activity may occur as a result of steam dump to the atmosphere due to unavailability of the condensers. With no fuel damage and primary and secondary circuits intact, the initiating event has no impact on the doses. The doses are a consequence of the assumed loss of offsite power. Therefore, the loss of offsite power doses from Section 9.2.6.4 are presented. The calculated maximum doses for all relevant pathways (inhalation, cloudshine, and groundshine) are as follows:

- Offsite dose: 0.05 mSv Worker dose: 1.5 mSv

These doses are within the Target 4 BSL for frequent faults (1 mSv offsite and 20 mSv onsite).

Diverse Mitigation

Both the diverse ATWT and diverse core cooling scenarios demonstrate that the RCS does not overpressurise and there is no significant fuel damage. For a diverse mitigation radiological consequences analysis better estimate assumptions would be credited. This would include reactor coolant system activity levels significantly lower than those modelled for the DBA and better activity retention in containment and in the steam generators. In addition better estimate atmospheric dispersion factors would be used. Therefore, a diverse mitigation radiological consequences analysis would show that the doses for the diverse ATWT scenario would be less than those reported for the non-LOCA DBAs and doses for the diverse core cooling scenario would be much less than for the design basis LOCA. The diverse mitigation analyses would not have to meet the Target 4 BSL for frequent faults and would meet the Target 4 BSL for infrequent faults.

9.4.6.5 As Low as Reasonably Practicable Assessment

The ALARP evaluation for this event is the same as for the RCCA misalignment fault (Section 9.4.3.5).

It is noted that the recently-implemented DAS function that monitors the IRNI signal and, upon actuation, trips the RCPs and RNS pumps (or RNS isolation), isolates the boron dilution sources, and actuates CMT, follows the ALARP principles. This function provides the diverse protection for boron dilution events initiated from subcritical conditions (Section 9.4.6.3). Additional information is provided in Reference 9.4-23.

9.4.6.6 Conclusions

Inadvertent boron dilution events are administratively prevented by the Technical Specifications during refuelling (Mode 6) and automatically terminated during cold shutdown (Mode 5), safe shutdown (Mode 4), and hot standby (Mode 3) modes. Inadvertent boron dilution events during startup (Mode 2) or power operation (Mode 1), if not detected and terminated by the operators, result in an automatic reactor trip. Following reactor trip, automatic termination of the dilution occurs and post-trip return to criticality is prevented.

The preceding results demonstrate that in all modes of operation, an inadvertent boron dilution is prevented or responded to by automatic functions, or sufficient time is available for operator action to terminate the transient. Following termination of the dilution flow and initiation of boration, the reactor is in a stable condition.

This event has also been adequately assessed with respect to ATWT considerations. Additionally, diverse core cooling capabilities have been demonstrated.

DBA radiological consequences are within the Target 4 BSL for frequent faults (1 mSv offsite and 20 mSv onsite). Thus, the identification of the Class 1 SSCs credited for protection is adequate to meet DB requirements.

It has been shown that the AP1000 plant design includes adequate systems for the protection of this fault, which limit the radiological consequences such that they are compliant with the SAPs targets and the risks have been reduced to be ALARP.

9.4.7 Inadvertent Loading and Operation of a Fuel Assembly in an Improper Position (Fault 1.15.10)

9.4.7.1 Identification of Causes and Accident Description

The Inadvertent Loading Event comprises core misloading scenarios such as the loading of:

- one or more fuel assemblies into improper positions
- a fuel rod during manufacture with one or more pellets of the wrong enrichment
- a full fuel assembly during manufacture with pellets of the wrong enrichment

In addition to these scenarios, misloading events involving burnable absorbers and control rods are theoretically possible. For example, scenarios such as the placement of a cluster of 8 discrete burnable absorbers into a core location intended to have 12 discrete burnable absorbers are feasible. Also, a swap of grey rod control assembly (GRCA) and an RCCA is possible for the AP1000 plant. All of these misloading scenarios potentially result in a core reactivity distribution that differs from the intended core reactivity distribution. As a result, the core power distribution and peaking factors may differ from predictions. Specifically, misloading errors can lead to increased local power peaking at the location of the misloading if the misloading results in a local reactivity increase relative to the intended pattern. Sufficiently large local power increases can lead to fuel failure at normal operation conditions

if the power distribution increase is undetected. If the misloading results in a local reactivity decrease, power peaking increases far away from the location of the misloading are possible due to unintended power tilts. These kinds of increases, however, are generally distributed over a large core volume and are small relative to those where the local reactivity is increased. In such cases, fuel failure is unlikely even if the anomaly goes undetected.

Fuel misloads are prevented by the manufacturing controls employed to build the fuel and the core loading controls used to assemble the core. The manufacturing controls include checks on fuel rod weight to confirm the uranium loading in the fuel rod, active and passive gamma scans of individual fuel rods to confirm fuel enrichments, pellet stack lengths, pellet types, and the absence of pellet gaps during fuel manufacturing, and bar coding of each fuel rod to confirm its proper placement in the fuel assembly.

To reduce the probability of core loading errors during fuel loading, each fuel assembly and core component is marked with an identification number and loaded in accordance with a core loading diagram. During core loading, the identification numbers are checked before each assembly is moved into the core. Identification numbers read during fuel movement are subsequently recorded on the loading diagram as a further check on proper placement after the loading is completed. These procedures make the likelihood of core misloadings very small.

The severity and detectability of fuel misloads are influenced by several factors: the local reactivity perturbation relative to the intended core loading pattern, the core position of the misload, the local environment of the misloaded fuel assembly, and the number of operable fixed incore detector locations and their proximity to the misload location. Should misloadings occur, the system of fixed incore detectors, which is used to verify power distributions during startup and throughout the operating cycle, is capable of revealing enrichment errors or misloadings which would cause the kind of substantial power distribution perturbation that would be necessary to induce large numbers of fuel rod failures. In addition, thermocouples and excore detectors can provide additional indications of power distribution anomalies. This instrumentation, along with the startup testing performed each cycle, make the detection of severe misloadings highly likely.

Fuel misloads involving a single fuel rod or fuel pellet were not evaluated as part of this analysis. Such misloads, in general, will not be detectable using the fixed incore detector system due to their localized power distribution perturbations. In terms of increased peaking factors and reduced DNBR values, however, the consequences of such misloads will be very small and limited to the affected fuel rod and the immediately adjacent fuel rods.

9.4.7.2 Design Basis Mitigation

Plant operating procedures should include a provision requiring that reactor instrumentation be used to search for potential fuel loading errors after fueling operations. In the event the error is not detectable by the instrumentation system and fuel rod failure limits could be exceeded during normal operation, the acceptability of any fuel damage is judged by the radiological consequences.

9.4.7.2.1 DBA Method of Analysis

The fuel misload event is different than most other analysed events in several respects. First, the fuel misload event is not a transient; it is not the result of a system failure that causes a

dynamic reactor response. The context of the event is normal operation, i.e., there is no overpower condition. Second, it is unlike most other accident scenarios in that a bounding scenario is not obvious. For a fuel misload, the bounding scenario is not necessarily the fuel misload that results in the largest perturbation. Fuel misloads with very large power distribution perturbations tend to be very easy to detect. Rather, a bounding scenario would be an "undetectable" fuel misload case that causes the largest possible census of fuel rods to exceed the limit for fuel failure. Third, while most accident analyses can be limited to a small number of scenarios, the number of ways in theory to misload a reactor core is virtually infinite. In any analysis of fuel misload scenarios, therefore, one has to choose a limited set of specific scenarios for analysis which must then be used to make judgments concerning the general ability of the core monitoring system to resolve the misload power distributions and detect those cases that could lead to fuel failure.

The general method employed in this analysis involved modelling a range of fuel misload scenarios and then determining whether or not those misload scenarios would be detectable during the startup power distribution measurements given the resulting power distribution perturbations and defined detectability criteria. The misload scenarios specifically modelled comprised a wide range of reactivity perturbations leading to a wide range of power distribution perturbations. Misload scenarios were modelled in various core positions relative to the detector pattern. The objective of the analysis was to ascertain the ability of the fixed incore detector (FID) system to resolve the power distributions for these scenarios. In this way, the threshold for detectability was determined. If the FID system can detect misloads that could fail fuel during normal operation with high confidence, then no fuel failure would be expected for this event since the core power distribution is monitored continuously once the minimum power level for the [ ] detectors is reached (~25% power). .

The fuel failure limit for this event is the $F_{\Delta H}$ limit for DNB at normal operation conditions. The $F_{\Delta H}$ limit for DNB is approached before any fuel melt limits are reached in any non-overpower event. This is the same effective limit used in analysing the static rod cluster control assembly misalignment event. The static rod misalignment event is very analogous to the fuel misload event in that both are conditions of normal operation, both are static as opposed to dynamic events, and both are caused by deviations with respect to the intended core reactivity distribution. In the case of the static rod misalignment, the reactivity deviation is caused by the mispositioning of a control rod. In the case of a fuel misload, the reactivity deviation is caused by the mispositioning or mismanufacture of one or more fuel assemblies. For the AP1000 reactor, the $F_{\Delta H}$ limit for DNB at normal operation conditions is 1.99 on a best estimate basis. This is the largest $F_{\Delta H}$ value that could occur at normal operation conditions without exceeding the DNBR limit. (Note that this value is larger than the Technical Specification $F_{\Delta H}$ limit because the Technical Specification limit protects against overpower transient events.) Therefore, misloads which could cause the HFP hot rod relative power to exceed 1.99 on a best estimate basis have the potential for fuel failure during normal operation if they remain undetected.

In the analysis presented here, misload cases were modelled for the first cycle core design. Analysis was also performed for a representative equilibrium cycle reload core design, and the results were comparable to the results presented here for the first core. The misload scenarios comprised a range of reactivity perturbations, core positions, and misload positions relative to the detector pattern. The majority of these scenarios had power distribution perturbations which were not quite severe enough to fail fuel at normal operation conditions. If the FID system can detect these scenarios, then scenarios with larger perturbations that could cause fuel failure are even more likely to be detected. The scenarios chosen were a combination of

assembly swaps and single assembly misloads. As mentioned above, it is not feasible to model all possible misload scenarios. Rather, the objective was to model a range of scenarios of various reactivity perturbations to characterize the threshold for detectability relative to the fuel failure limit.

The AP1000 FID pattern has quarter-core reflective symmetry and a highly regular pattern of detectors such that each fuel assembly is either in a detector location or very close to a detector location. For this detector pattern, a misloaded assembly has one of three possible orientations with respect to the detector pattern. These orientations are described as Types A, B, and C:

Type A: Misloaded assembly is in a detector location

Type B: Misloaded assembly is face adjacent to one or more detector locations

Type C: Misloaded assembly is diagonally adjacent to one or more detector locations

A number of misloads of each of these types were modelled in this analysis using the first cycle core model. A total of 25 misload scenarios were modelled. Cycle depletions at hot full power were performed for each scenario, and the depletion maximum $F_{\Delta H}$ was determined. This depletion maximum $F_{\Delta H}$ value was used to characterize the severity of the misload scenario relative to the 1.99 best estimate $F_{\Delta H}$ fuel failure limit.

For each misload scenario, the "measured" power distribution at the 30% power startup condition was simulated using the same algorithm employed by the online power distribution monitoring system. Simulated detector signals were generated using the misload core model and used as inputs to the algorithm. For each misload scenario, a total of 400 simulated measured power distributions were generated reflecting different patterns of operable fixed incore detectors. For the initial power distribution assessment at the start of the operating cycle, at least 75% of the detectors must be operable. Each of the 400 simulated measured power distributions, therefore, assumed 75% of the detectors to be operable. In addition, a detector signal variability of 1% on a 1σ basis was assumed.

Detectability assessments were then performed for each measured power distribution of each misload scenario. Since 25 misload scenarios were modelled and 400 measured power distributions were simulated for each misload scenario, a total 10,000 detectability assessments were performed. Two different detectability criteria were employed in these assessments.

The first criterion was the measured versus predicted assembly average power criterion. For this criterion, the simulated measured misload startup power distributions (at 30% power) were compared to the reference startup power distribution (i.e., the predicted or expected startup power distribution). Each measured assembly power was compared to its reference power distribution counterpart. Detection of a particular misload scenario was assumed if, on a 95/95 basis, deviations of 10% or greater between the measured and predicted assembly powers in a core location were observed over the 400 simulated measured power distributions. The measured versus predicted detectability assessment was limited to core locations where the reference relative power was 0.8 or greater.

The second detectability criterion was a symmetry criterion for the measured power distributions. For this criterion, the measured relative power of each assembly was compared to the relative powers of each of its three symmetric counterparts (assuming quarter-core, cyclic symmetry) for a given simulated measured power distribution. The symmetry percent difference value was determined by taking the maximum difference between the symmetric

assembly powers and then dividing it by the average power of the four assemblies in the symmetry group. The result was then multiplied by 100%. Detection of a particular misload scenario was assumed if, on a 95/95 basis, a symmetry difference of 10% or greater was observed for a core location over the 400 simulated measured power distributions. The symmetry detectability assessment was limited to core locations where the relative power was 0.8 or greater.

For each core loading error case analysed, the percent deviations from detector readings for a normally loaded core are shown in the incore detector locations. (See Figures 9.4.7-1 through 9.4.7-4.)

9.4.7.2.2 DBA Credited SSCs

The available Class 1 systems for this fault are the same as those in Section 9.4.3.2.1.2 for Dropped RCCAs, Dropped RCCA bank, and Statically Misaligned RCCA faults.

9.4.7.2.3 DBA Results

The fixed incore detector system is used to search for potential fuel misloads at the start of each operating cycle. Following fuel loading and low power physics testing, an initial core power distribution measurement is made. The core power level of this initial measurement is ~30% of rated thermal power. The [ ] fixed incore detectors used in the AP1000 become effective for power distribution measurements at approximately [ ] power. This initial power distribution measurement is used to confirm that the measured power distribution is consistent with the predicted power distribution. At least [ ] of the fixed incore detectors are required to be operable for this initial measurement. Observed power distribution deviations in excess of the review criteria (see Table 9.4.7-1) would prompt an investigation of a possible core anomaly.

The detectability assessments performed in this analysis confirm that the fixed incore detector system can reliably detect fuel misloads that could fail fuel during normal operation when the Table 9.4.7-1 review criteria are employed for the initial power distribution assessment (≥ [ ] of detectors operable). Figure 9.4.7-1 gives the 95/95 detectability assessment value as a function of the best estimate misload depletion maximum $F_{\Delta H}$ value. The maximum difference of the measured versus predicted or symmetry assessments was plotted. This figure demonstrates that detection is expected for fuel misloads with power distribution perturbations severe enough to cause fuel failure at normal operation conditions. All of the misload cases that exceeded the fuel failure limit were easily detectable, i.e., the measured versus predicted or symmetry assessments showed differences far in excess of the 10% review criterion. Misload cases with much smaller perturbations were detectable as well. Figure 9.4.7-1 suggests that the threshold for misload detectability is in the range of a maximum depletion $F_{\Delta H}$ value of approximately 1.80 to 1.85. In other words, misloads that could lead to depletion $F_{\Delta H}$ values above this threshold are very likely to be detected. This threshold is well below the failure limit of 1.99. Consequently, detection of any misload that could fail fuel at normal operation conditions is expected with high confidence. Therefore, no fuel failure would be expected for this event.

Figures 9.4.7-2 through 9.4.7-4 provide examples of the three types of misload cases for the first core. Figure 9.4.7-2 illustrates a Type A swap misload where two fuel assemblies, Region D and E assemblies, have been interchanged. In this case, each of the swapped assemblies is in a FID location. The core diagram gives the difference between the mean measured power distribution and the expected power distribution for the 30% power startup condition. The mean measured power distribution represents the average power distribution

over the 400 simulated measured power distributions. As the figure shows, the mean measured versus predicted differences are quite large even though the power distribution perturbation was not severe enough to cause fuel failure; the depletion maximum $F_{\Delta H}$ for this case was 1.882, less than the limit for fuel failure at normal operation conditions. Consequently, this particular misload is easily detectable. Figure 9.4.7-2 also provides the maximum 95/95 measured versus predicted and symmetry differences. The 95/95 measured versus predicted difference was 25.2%, much larger than the 10% review criterion. This difference occurred in location G-8. Note that the mean difference in this location is 28.7%. The 25.2% 95/95 difference means that there is 95% confidence that at least 95% of the operable detector patterns would result in a measured versus predicted difference of ≥25.2% in location G-8. Similarly, the 95/95 symmetry difference was 26.0%, which came from the symmetry group G-14, B-7, J-2, and P-9. These large differences indicate that there is high confidence that this misload is detectable.

Figure 9.4.7-3 illustrates another swap misload. In this case, however, the misload locations are Type B, i.e., face adjacent to FID positions. For this scenario, Region B and E assemblies were interchanged. As in the previous case, the 95/95 measured versus predicted and symmetry errors are quite large, 22.7% and 25.0%, respectively, indicating that this misload would be readily detectable despite the fact that this misload is not quite severe enough to fail. The depletion maximum $F_{\Delta H}$ for this case was 1.987, which is just under the fuel failure limit.

Figure 9.4.7-4 illustrates a single assembly misload of Type C, where the misloaded assembly is diagonally adjacent to FID positions. In this scenario, a Region E assembly was loaded into position H-9 where a Region D assembly was intended. As the measured versus predicted percent difference distribution shows, this misload resulted in a much smaller power distribution perturbation than the other two cases. However, the 95/95 measured versus predicted difference was 10.3%; thus, this misload was detectable even though the depletion maximum $F_{\Delta H}$ was 1.865, well below the limit for fuel failure. The 95/95 symmetry difference was only 6.5%. Misload cases where the power distribution perturbation is at or near the center of the core do not cause large symmetry differences since the quadrant tilts in such cases are minimal. This and the fact that this misload is not in a FID location make it somewhat more difficult to detect.

Figures 9.4.7-1 through 9.4.7-4 indicate that misloads of Types A, B, or C that can lead to fuel failure will be detectable with high confidence at the 30% power startup condition when ≥ [ ] of the FIDs are operable and the 10% review criteria for symmetry and measured versus predicted are used. Given that detection of misloads severe enough to fail fuel is expected using these review criteria, a radiological consequences analysis is deemed unnecessary. In the unlikely event, however, that a misload that could fail fuel remains undetected, the radiological consequences would be acceptable as presented in Section 9.4.7.4.

Following startup, at least [ ] of the FIDs must be operable. If the number of operable detectors decreases to less than [ ] of the total number of detectors, then Table 9.4.7-1 recommends slightly tighter review criteria, [ ] for both the measured versus predicted and symmetry assessments. This is judged to be a prudent measure to ensure that any significant core anomalies that develop following startup are investigated in light of the reduced incore detector instrumentation.

The primary consideration with respect to misload detection is detector density, not the core loading pattern. Since the FID locations are fixed from cycle to cycle, one would expect power distribution perturbations of comparable magnitudes to be detectable from cycle to cycle. Furthermore, reload loading patterns tend to be designed with similar power distributions and margins to peaking factor limits. Reload core designs would be expected to

have similar peaking factor values and, therefore, comparable margins to fuel failure limits. In other words, the required perturbation to reach fuel failure limits will be similar from cycle to cycle and the ability to detect that perturbation will be similar from cycle to cycle since it is primarily dependent on the FID pattern. Furthermore, the above detectability analysis indicates that the FID system is capable of detecting power distribution perturbations which are significantly smaller than the perturbations required for fuel failure. Consequently, the ability to detect misloads that could fail fuel during normal operation should be insensitive to the details of individual reload cycle loading patterns. As such, it is judged that cycle specific misload analyses are unnecessary.

With respect to misloads of control rods, misloads of GRCAs and RCCAs are prevented by the core loading controls used to assemble the core. Each RCCA and GRCA component will have a unique engraved identification number. The identification (ID) number can be compared to the core loading diagram to confirm proper loading.

A [ ] will also provide visual differentiation between a GRCA and an RCCA. This identifying feature, along with the engraved ID, will make a GRCA/RCCA misload very unlikely to occur.

In the unlikely event of a misload of an RCCA in a GRCA position, detection of the misload is expected. Rod worth measurements and power distribution monitoring during startup and subsequent operation can detect scenarios where an RCCA is inadvertently loaded into a grey bank position.

If a GRCA is inadvertently placed in an RCCA position, the primary consequence is potentially larger peaking factors during normal operation if the black bank is deeply inserted (e.g., the axial offset (AO) bank). This scenario, however, is bounded by analyses of static rod misalignments routinely performed for each operating cycle, which assume complete withdrawal of a single RCCA. This represents a larger local reactivity perturbation than a misload of a GRCA in an RCCA position. Consequently, the current safety evaluation ensures fuel integrity during normal operation for this kind of event.

9.4.7.3 Diverse Mitigation

As this is an infrequent fault, diverse mitigation is not required.

9.4.7.4 Radiological Consequences

An undetected misload is unlikely to lead to fuel damage. With no fuel damage, the primary and secondary circuits intact, and with offsite power remaining available, there is no release of activity to the environment and the Target 4 BSOs (0.01 mSv offsite and 0.1 mSv onsite) are met.

In the unlikely event that a misload that could fail fuel remains undetected, the Target 4 BSOs will still be met. In such a case, fuel failures in fresh fuel during startup would have negligible radiological consequences since there would be only a small fission product inventory. Following startup, any fuel rod failures would occur gradually and would be detected by coolant activity monitoring. Since the number of potential fuel rod failures due to a core misload would be small and such failures would occur gradually, any coolant activity releases would initially be well within the cleanup capacity of the plant and operations would be maintained within Technical Specification coolant activity guidelines. Any trend in increased coolant activity would warrant further investigation and evaluation.

9.4.7.5 As Low as Reasonably Practicable Assessment

The ALARP evaluation for this event is the same as for the RCCA misalignment fault (Section 9.4.3.5), with the exception of this being an infrequent fault. Therefore, although diverse mitigation is not required, it is still available.

9.4.7.6 Conclusions

Fuel assembly enrichment errors are prevented by administrative procedures implemented in fabrication.

In the event that a single pin or pellet has a higher enrichment than the nominal value, the consequences in terms of reduced DNBR and increased fuel and cladding temperatures are limited to the incorrectly loaded pin or pins and perhaps the immediately adjacent pins.

Fuel misloads are prevented by manufacturing controls and core loading controls. In the unlikely event that a fuel misload should occur, the fixed incore detector system is capable of reliably detecting misloads that could fail fuel at normal operation conditions. Exceeding the review criteria herein would initiate an investigation to identify potential core anomalies. It is expected that any misload with the potential to fail fuel would be detected. However, any fuel failures associated with an undetected fuel misload would be gradual and detectable. Consequently, plant operations would always be maintained within Technical Specification coolant activity guidelines.

It has been shown that the AP1000 plant design includes adequate systems for the protection of this fault, which limit the radiological consequences such that they are compliant with the SAPs targets and the risks have been reduced to be ALARP.

9.4.8 Spectrum of Rod Cluster Control Assembly Ejection Accidents (Fault 1.15.11)

9.4.8.1 Identification of Causes and Accident Description

This accident is defined as the mechanical failure of a control rod mechanism pressure housing, resulting in the ejection of an RCCA and drive shaft. The consequence of this mechanical failure is a rapid positive reactivity insertion together with an adverse core power distribution, possibly leading to localized fuel rod damage.

9.4.8.1.1 Design Precautions and Protection

9.4.8.1.1.1 Mechanical Design

The mechanical design is discussed in Section 22.8. Mechanical design and quality control procedures intended to prevent the possibility of an RCCA drive mechanism housing failure are listed below:

- Each control rod drive mechanism housing is completely assembled and shop tested at a minimum of 125 percent of system design pressure.

- The mechanism housings are hydrotested after they are attached to the reactor vessel head. The hydrostatic test of the connection between the rod travel housing and the latch housing is done as part of the system hydrostatic test.

- The allowable stress levels in the mechanism are not exceeded due to system thermal transients at power or by the thermal movement of the coolant loops. Moments induced by the safe shutdown earthquake can be accepted within the allowable primary working stress range specified for Class 1 components.

- The latch mechanism housing and rod travel housing are each a single length of forged stainless steel. This material exhibits excellent notch toughness at temperatures that are encountered.

A significant margin of strength in the elastic range together with the large energy absorption capability in the plastic range gives additional confidence that gross failure of the housing does not occur. The joint between the latch housing and latch housing nozzle is a full penetration bi-metallic weld, and the joint between the latch housing and rod travel housing is a threaded joint with a canopy seal weld.

9.4.8.1.1.2 Nuclear Design

If a rupture of an RCCA drive mechanism housing is postulated, the operation using chemical shim is such that the severity of an ejected RCCA is inherently limited. In general, the reactor is operated with the power control (or mechanical shim) RCCAs inserted only far enough to permit load follow. The axial offset RCCAs are positioned so that the targeted axial offset can be met throughout core life. Reactivity changes caused by core depletion and xenon transients are normally compensated for by boron changes and the mechanical shim banks, respectively. Further, the location and grouping of the power control and axial offset RCCAs are selected with consideration for an RCCA ejection accident. Therefore, should an RCCA be ejected from its normal position during full-power operation, a less severe reactivity excursion than analysed is expected.

It may occasionally be desirable to operate with larger than normal insertions. For this reason, a power control and axial offset rod insertion limit is defined as a function of power level. Operation with the RCCAs above this limit provides adequate shutdown capability and an acceptable power distribution. The position of the RCCAs is continuously indicated in the main control room. An alarm occurs if a bank of RCCAs approaches its insertion limit or if one RCCA deviates from its bank. Operating instructions require boration at the low level alarm and emergency boration at the low-low level alarm.

9.4.8.1.1.3 Reactor Protection

The reactor protection in the event of a rod ejection accident is described in WCAP-15806-P-A (Reference 9.4-4). The protection for this accident is provided by the high neutron flux trip (high and low setting) and the high rate of neutron flux increase trip. These protection functions are described in Section 19.2.

9.4.8.1.1.4 Effects on Adjacent Housings

Failures of an RCCA mechanism housing, due to either longitudinal or circumferential cracking, does not cause damage to adjacent housings. The control rod drive mechanism is described in Section 6.2.1.6.

9.4.8.1.1.5 Consequences

The probability of damage to an adjacent housing is considered remote. If damage is postulated, it is not expected to lead to a more severe transient because RCCAs are inserted in

the core in symmetric patterns and control rods immediately adjacent to worst ejected rods are not in the core when the reactor is critical. Damage to an adjacent housing could, at worst, cause that RCCA not to fall on receiving a trip signal. This is already taken into account in the analysis by assuming a stuck rod adjacent to the ejected rod.

9.4.8.1.1.6 Summary

Failure of a control rod housing does not cause damage to adjacent housings that increase the severity of the initial accident.

9.4.8.2 Design Basis Mitigation

Analysis is performed to demonstrate the adequacy of the protection and safety monitoring system to detect and mitigate the fault and show that the applicable safety criteria are satisfied.

Because of the extremely low probability of an RCCA ejection accident, some fuel damage is considered an acceptable consequence.

Criteria are applied to provide confidence that there is little or no possibility of fuel dispersal in the coolant, gross lattice distortion, or severe shock waves. These criteria are the following:

- The pellet clad mechanical interaction (PCMI) failure criteria is a change in radial average fuel enthalpy greater than the corrosion-dependent limit depicted in Figure B-1 of SRP 4.2, Revision 3, Appendix B (Reference 9.4-24).

- The high cladding temperature failure criteria for zero-power conditions is a peak radial average fuel enthalpy greater than 170 cal/g (300 Btu/lb) for fuel rods with an internal rod pressure at or below system pressure and 150 cal/g (270 Btu/lb) for fuel rods with an internal rod pressure exceeding system pressure.

- For intermediate (greater than 5% rated thermal power) and full-power conditions, fuel cladding is presumed to fail if local heat flux exceeds thermal design limits (e.g., DNBR).

- For core coolability, it is conservatively assumed that the average fuel pellet enthalpy at the hot spot remains below 200 cal/g (360 Btu/lb) for irradiated fuel. This bounds non-irradiated fuel, which has a slightly higher enthalpy limit.

- For core coolability, the peak fuel temperature must remain below incipient fuel melting conditions.

- Mechanical energy generated as a result of (1) non-molten fuel-to-coolant interaction and (2) fuel rod burst must be addressed with respect to reactor pressure boundary, reactor internals, and fuel assembly structural integrity.

- No loss of coolable geometry due to (1) fuel pellet and cladding fragmentation and dispersal and (2) fuel rod ballooning.

- Peak reactor coolant system pressure is less than that which could cause stresses to exceed the “Service Limit C” as defined in the ASME code.

9.4.8.2.1 DBA Method of Analysis

The calculation of the RCCA ejection transients is performed in two stages: first, an average core calculation and then, a hot rod calculation. The average core calculation is performed using spatial neutron kinetics methods to determine the average power generation with time, including the various total core feedback effects (Doppler reactivity and moderator reactivity). Enthalpy, fuel temperature, and DNB transients are then determined by performing a conservative fuel rod transient heat transfer calculation.

A discussion of the method of analysis appears in WCAP-15806-P-A (Reference 9.4-4).

Average Core Analysis

The three-dimensional nodal code ANC (References 9.4-7, 9.4-14, 9.4-15, 9.4-16, 9.4-17, 9.4-21, 9.4-22, and 9.4-8) is used for the average core transient analysis. This code solves the two-group neutron diffusion theory kinetic equation in three spatial dimensions (rectangular coordinates) for six delayed neutron groups. The core moderator and fuel temperature feedbacks are based on the U.S. Nuclear Regulatory Commission (NRC)-approved Westinghouse version of the VIPRE-01 code and methods (References 9.4-18 and 9.4-19).

Hot Rod Analysis

The hot fuel rod models are based on the Westinghouse VIPRE models described in WCAP-15806-P-A (Reference 9.4-4). The hot rod model represents the hottest fuel rod from any channel in the core. VIPRE performs the hot rod transients for fuel enthalpy, temperature, and DNBR using as input the time-dependent nuclear core power and power distribution from the core average analysis. A description of the VIPRE code is provided in Reference 9.4-18.

System Overpressure Analysis

If the fuel coolability limits are not exceeded, the fuel dispersal into the coolant or a sudden pressure increase from thermal to kinetic energy conversion is not needed to be considered in the overpressure analysis. Therefore, the overpressure condition may be calculated on the basis of conventional fuel rod to coolant heat transfer and the prompt heat generation in the coolant. The system overpressure analysis is conducted by first performing the core power response analysis to obtain the nuclear power transient (versus time) data. The nuclear power data is then used as input to a plant transient computer code to calculate the peak reactor coolant system pressure. This code calculates the pressure transient, taking into account fluid transport in the reactor coolant system and heat transfer to the steam generators. For conservatism, no credit is taken for the possible pressure reduction caused by the assumed failure of the control rod pressure housing.

9.4.8.2.1.1 Calculation of Basic Parameters

Input parameters for the analysis are conservatively selected as described in Reference 9.4-4.

Ejected Rod Worths and Hot Channel Factors

The values for ejected rod worths and hot channel factors are calculated using three-dimensional static methods. Standard nuclear design codes are used in the analysis. The calculation is performed for the maximum allowed bank insertion at a given power level, as determined by the rod insertion limits. Adverse xenon distributions are considered in the calculation.

Appropriate safety analysis allowances are added to the ejected rod worth and hot channel factors to account for calculational uncertainties, including an allowance for nuclear peaking due to densification as discussed in Reference 9.4-4.

Moderator and Doppler Coefficients

The critical boron concentration is adjusted in the nuclear code to obtain a moderator temperature coefficient that is conservative compared to actual design conditions for the plant consistent with Reference 9.4-4. The fuel temperature feedback in the neutronics code is reduced consistent with Reference 9.4-4 requirements.

Delayed Neutron Fraction, β_{eff}

Calculations of the effective delayed neutron fraction (β_{eff}) typically yield values no less than 0.50 percent at the end of cycle. The accident is sensitive to β_{eff} if the ejected rod worth is equal to or greater than β_{eff}. To allow for future cycles, a pessimistic estimate of β_{eff} of [ ] percent is used in the analysis.

Trip Reactivity Insertion

The trip reactivity insertion accounts for the effect of the ejected rod and one adjacent stuck rod. The trip reactivity is simulated by dropping a limited set of rods of the required worth into the core. The start of rod motion occurs [ ] second after the high neutron flux trip setpoint is reached. This delay is assumed to consist of [ ] second for the instrument channel to produce a signal, [ ]second for the trip breakers to open, and [ ] second for the coil to release the rods. A curve of trip rod insertion versus time is used, which assumes that insertion to the dashpot does not occur until 2.7 seconds after the start of fall. The choice of such a conservative insertion rate means that there is over [ ] after the trip setpoint is reached before significant shutdown reactivity is inserted into the core. This conservatism is important for the hot full power accidents.

The minimum design shutdown margin available at hot zero power may be reached only at end of life in the equilibrium cycle. This value includes an allowance for the worst stuck rod, adverse xenon distribution, conservative Doppler and moderator defects, and an allowance for calculational uncertainties. Calculations show that the effect of two stuck RCCAs (one of which is the worst ejected rod) is to reduce the shutdown by about an additional 1-percent Δk. Therefore, following a reactor trip resulting from an RCCA ejection accident, the reactor is subcritical when the core returns to hot zero power.

9.4.8.2.2 DBA Credited SSCs

Reactor protection for a rod ejection is discussed in Section 9.4.8.1.1.3. For the DB, all claimed SSCs are Class 1. The credited Class 1 SSCs are listed in Table 9.0-10. The presented DBA ends shortly after reactor trip; however, essential safety functions for the long term safe shutdown analysis (Appendix 9C) bound safe shutdown response for this event. The primary core cooling is provided by the PRHR and passive containment cooling. Other SSCs include the CMTs, containment isolation, and pressuriser SVs. Although not credited in the limiting analysis presented, the accumulators, IRWST injection, containment recirculation, and ADS are available to mitigate the resultant LOCA (See Section 9.6 for loss of inventory events). The PMS provides the following:

- RT on power range high positive flux rate

- PRHR actuation on Low-2 SG NR level coincident with Low-2 SFW flow
- CMTs and containment isolation on Low-2 CL temperature
- PCS on High-2 containment pressure

9.4.8.2.3 DBA Results

For all cases, the core is preconditioned by assuming a fuel cycle depletion with control rod insertion that is conservative relative to expected baseload operation. All cases assume that the mechanical shim and axial offset control RCCAs are inserted to their insertion limits before the event and xenon is skewed to yield a conservative initial axial power shape. The limiting RCCA ejection cases for a typical cycle are summarised following the criteria outlined in Section 9.4.8.2.

- PCMI and high cladding temperature (hot zero power)

  The resulting maximum fuel average enthalpy rise and maximum fuel average enthalpy are less than the criteria given in Section 9.4.8.2.

- High cladding temperature (≥ 5% rated thermal power)

  The fraction of the core calculated to have a DNBR less than the safety analysis limit is less than the amount of failed fuel assumed in the dose analysis described in Section 9.4.8.4.

- Core coolability

  The resulting maximum fuel average enthalpy is less than the criterion given in Section 9.4.8.2. Fuel melting is not predicted to occur at the hot spot.

There are no fuel failures due to the fuel enthalpy deposition, i.e., both fuel and cladding enthalpy limits were met. Additionally, the coolability criteria for peak fuel enthalpy and the fuel melting criteria were met. Therefore, the fuel dispersal into the coolant, a sudden pressure increase from thermal to kinetic energy conversion, gross lattice distortion, or severe shock waves are precluded.

The nuclear power transients for the limiting cases are presented in Figures 9.4.8-1 through 9.4.8-3.

The calculated sequence of events for the limiting cases is presented in Table 9.4-1. Reactor trip occurs early in the transients, after which the nuclear power excursion is terminated.

The ejection of an RCCA constitutes a break in the reactor coolant system, located in the reactor pressure vessel head. The effects and consequences of LOCAs are discussed in Section 9.6. Following the RCCA ejection, the plant response is the same as a LOCA.

The consequential loss of offsite power described in Section 9.0.12 is not limiting for the enthalpy and temperature transients resulting from an RCCA ejection accident. Due to the delay from reactor trip until turbine trip and the rapid power reduction produced by the reactor trip, the peak fuel and cladding temperatures occur before the reactor coolant pumps begin to coast down.

Appendix 9C provides discussion and analysis of long term safe shutdown for non-LOCA events.

9.4.8.2.3.1 Rods in DNB

In the cases considered, less than 10 percent of the rods are assumed to enter DNB based on a detailed three-dimensional kinetics and hot rod analysis.

The consequential loss of offsite power described in section 9.0.12 is not limiting for the calculation of the number of rods assumed to enter DNB for the RCCA ejection accident. Due to the delay from reactor trip until turbine trip and the rapid power reduction produced by the reactor trip, the minimum DNBR, for rods where the DNBR did not fall below the design limit (see Section 22.7.1.1) in the cases described, occurs before the reactor coolant pumps begin to coast down.

9.4.8.2.3.2 Peak RCS Pressure

Calculations of the peak reactor coolant system pressure demonstrate that the peak pressure does not exceed that which would cause the stress to exceed the Service Level C Limit as described in the ASME Code, Section III. Therefore, the accident for this plant does not result in an excessive pressure rise or further damage to the reactor coolant system.

The consequential loss of offsite power described in Section 9.0.12 is not limiting for the pressure surge transient resulting from an RCCA ejection accident. Due to the delay from reactor trip until turbine trip and the rapid power reduction produced by the reactor trip, the peak system pressure occurs before the reactor coolant pumps begin to coast down.

9.4.8.2.3.3 Lattice Deformations

A large temperature gradient exists in the region of the hot spot. Because the fuel rods are free to move in the vertical direction, differential expansion between separate rods cannot produce distortion. However, the temperature gradients across individual rods may produce a differential expansion, tending to bow the midpoint of the rods toward the hotter side of the rod.

Calculations indicate that this bowing results in a negative reactivity effect at the hot spot because the core is undermoderated, and bowing tends to increase the undermoderation at the hot spot. In practice, no significant bowing is anticipated because the structural rigidity of the core is sufficient to withstand the forces produced.

Boiling in the hot spot region would produce a net flow away from that region. However, the heat from the fuel is released to the water relatively slowly, and it is considered inconceivable that crossflow is sufficient to produce lattice deformation. Even if massive and rapid boiling, sufficient to distort the lattices, is hypothetically postulated, the large void fraction in the hot spot region produces a reduction in the total core moderator to fuel ratio and a large reduction in this ratio at the hot spot. The net effect is therefore a negative feedback.

In conclusion, no credible mechanism exists for a net positive feedback resulting from lattice deformation. In fact, a small negative feedback may result. The effect is conservatively ignored in the analysis.

9.4.8.3 Diverse Protection Systems

As this is an infrequent fault (DB1), a diverse protection assessment is not required.

9.4.8.4 Radiological Consequences

The evaluation of the radiological consequences of a postulated rod ejection accident assumes that as a result of the accident, 10 percent of the fuel rods are damaged such that the activity contained in the fuel-cladding gap is released to the reactor coolant. Activity is released to the containment via the spill from the reactor vessel head and is assumed to be available for release to the environment via containment leakage.

9.4.8.4.1 Source Term

The significant radionuclide releases from the fuel due to the rod ejection accident are the iodines, alkali metals (caesiums, rubidiums) and noble gases. All activity in the fuel rod gap of the damaged fuel is assumed to be released to the coolant. Based on Table 7.3 of Reference 9.4-5, the gap fraction is assumed to be 3 percent of the core inventory for iodines, 10 percent for noble gases, and 4 percent for alkali metals. It is also assumed that a limited amount of fuel centreline melt occurs, equivalent to 0.25% of the core.

To address the fact that the failed fuel rods may have been operating at power levels above the core average, the source term is increased by a lead rod radial peaking factor of 1.75 which bounds the COLR limit of 1.72.

All gap activity in the damaged fuel rods is assumed to be immediately released to the primary coolant. For the fuel that is modelled as melting, it is assumed that all of the noble gas, iodine, and alkali metals activity is released to the primary coolant.

Noble gas releases from the primary coolant to the containment atmosphere would occur quickly.

The iodine activity is all assumed to enter into solution with 60 percent of the iodine assumed to convert to the elemental form and then enter the containment atmosphere, consistent with Section 2.2.1 of Chapter IX of Reference 9.4-5. It is assumed that 1% of the iodine released converts to the organic form while the other 99% stays in the elemental form. In practice, the iodine activity released from the fuel would initially enter into solution and is anticipated to be gradually released to the containment atmosphere over an indefinite period of time. However, it is conservatively assumed that all of the iodine releases to the containment atmosphere occur immediately. This assumption makes the activity quickly available for release to the environment by way of containment leakage.

The alkali metals activity is assumed to be retained in the primary coolant and none of it is assumed to enter the containment atmosphere.

Initial reactor coolant activities are of secondary importance compared to the release of the gap inventory of fission products from the portion of the core assumed to fail because of the accident.

9.4.8.4.2 Release Pathways

Activity from the reactor coolant system and the core is released to the containment atmosphere and is available for leakage to the environment through the assumed design basis

containment leakage. The leakage rate is modelled at the technical specification leakage rate until 24 hours and at half that rate after 24 hours.

9.4.8.4.3 Dose Calculation Models

The models used to calculate doses are provided in Appendix 9A.

9.4.8.4.4 Analytical Assumptions and Parameters

The assumptions and parameters used in the analysis are listed in Table 9.4-3.

9.4.8.4.5 Doses

The calculated maximum doses for all relevant pathways (inhalation, cloudshine, and groundshine) are as follows:

- Offsite dose: 5.5 mSv Worker dose: 8.4 mSv

These doses are within the Target 4 BSL for infrequent faults (10 mSv offsite and 200 mSv onsite).

The limiting conditions for operation of the Technical Specifications used in the dose assessment are provided in Table 9.4-4. The Table 9.4-4 values ensure the Target 4 BSLs are met.

9.4.8.5 As Low As Reasonably Practicable Assessment

For this fault, the identification of the primary safety functions (see Table 9.4.8-1) as Class 1 SSCs has been shown to be adequate to meet DB requirements.

Although not required, diverse mitigation for the RCCA misalignment faults (Section 9.4.3.4) is available.

Additionally, the AP1000 plant design has a third level of redundancy provided by the DiD systems. The applicable DiD functions include:

- CVS boration for long-term reactivity control
- SFW with steam dump for decay heat removal
- Pressuriser spray and auxiliary spray for RCS pressure control
- CVS make-up for RCS inventory control
- RNS cooling of the IRWST and SFW with steam dump via DAS for containment cooling

Providing further means of removing decay heat or tripping the reactor in addition to these functions would not significantly reduce the PSA risk for this event.

9.4.8.6 Conclusions

The analysis shows that the criterion stated in this subsection is satisfied.

Radiological consequences are within the Target 4 BSL for infrequent faults (10 mSv offsite and 200 mSv onsite).

It has been shown that the AP1000 plant design includes adequate systems for the protection of this fault, which limit the radiological consequences such that they are compliant with the SAPs targets and the risks have been reduced to be ALARP.

9.4.9 References

9.4-1 Westinghouse Documents WCAP-7979-P-A, Rev. 0 (Proprietary) and WCAP-8028-A, Rev. 0 (Non-Proprietary), "TWINKLE - A Multi-Dimensional Neutron Kinetics Computer Code," January 1975.

9.4-2 Westinghouse Document WCAP-7908-A (Non-Proprietary), "FACTRAN A FORTRAN-IV Code for Thermal Transients in a UO_2 Fuel Rod," December 1989.

9.4-3 Westinghouse Documents WCAP-7907-P-A, Rev. 0 (Proprietary) and WCAP-7907-A, Rev. 0 (Non-Proprietary), "LOFTRAN Code Description," April 1984.

9.4-4 Westinghouse Documents WCAP-15806-P-A, Rev. 0 (Proprietary) and WCAP-15807-NP-A, Rev. 0 (Non-Proprietary), "Westinghouse Control Rod Ejection Accident Analysis Methodology Using Multi-Dimensional Kinetics,", November 2003.

9.4-5 European Commission Report EUR 19841 EN, "Determination of the in-containment source term for a large-break loss of coolant accident," April 2001.

9.4-6 MIL-HDBK-217F, "Military Handbook Reliability Prediction of Electronic Equipment," Department of Defence, December 1991.

9.4-7 Westinghouse Documents WCAP-10965-P-A (Proprietary) and WCAP-10966-A (Non-Proprietary), "ANC: A Westinghouse Advanced Nodal Computer Code," September 1986.

9.4-8 Westinghouse Letter NSD-NRC-96-4679, "Process Improvement to the Westinghouse Neutronics Code System," March 1996.

9.4-9 Westinghouse Documents WCAP-11397-P-A (Proprietary) and WCAP-11397-A (Non-Proprietary), "Revised Thermal Design Procedure," April 1989.

9.4-10 Westinghouse Report UKP-GW-GL-067, Rev. 1, "AP1000 Assessment of Diverse Mitigation of Frequent Faults for the UK," December 2011.

9.4-11 Westinghouse Documents WCAP-15644-P, Rev. 2 (Proprietary) and WCAP-15644-NP, Rev. 2 (Non-Proprietary), "AP1000 Code Applicability Report," March 2004.

9.4-12 Westinghouse Report UKP-SSAR-GLR-001, Rev. 0, "UK Fault Studies Analysis Basis," August 2016.

9.4-13 Westinghouse Report UKP-SSAR-GLR-002, Rev. 0, "UK AP1000® Plant: Summary Report Supporting the Closure of Fault Studies Issue 03," May 2016.

9.4-14 Westinghouse Documents WCAP-11596-P-A (Proprietary) and WCAP-11597-A (Non-Proprietary), "Qualification of the PHOENIX-P/ANC Nuclear Design System for Pressurized Water Reactor Cores," June 1988.

9.4-15 Westinghouse Documents WCAP-16045-P-A, Rev. 0 (Proprietary) and WCAP-16045-NP-A, Rev. 0 (Non-Proprietary), "Qualification of the Two-Dimensional Transport Code PARAGON," August 2004.

9.4-16 Westinghouse Documents WCAP-10965-P-A, Addendum 1 (Proprietary) and WCAP-10966-A Addendum 1 (Non-Proprietary), "ANC: A Westinghouse Advanced Nodal Computer Code; Enhancements to ANC Rod Power Recovery," April 1989.

9.4-17 Westinghouse Letter NTD-NRC-95-4533, "Notification to the NRC Regarding Improvements to the Nodal Expansion Method Used in the Westinghouse Advanced Nodal Code (ANC)," August 1995.

9.4-18 Westinghouse Documents, WCAP-14565-P-A, Rev. 0 (Proprietary) and WCAP-15306-NP-A, Rev. 0 (Non-Proprietary), "VIPRE-01 Modeling and Qualification for Pressurized Water Reactor Non-LOCA Thermal-Hydraulic Safety Analysis," October 1999.

9.4-19 NP-2511-CCM-A, "VIPRE-01: A Thermal-Hydraulic Code for Reactor Core," Volume 1-3 (Revision 3, August 1989), Volume 4 (April 1987), Electric Power Research Institute, Stewart, C. W., et al.

9.4-20 Westinghouse Document UKP-GW-GLR-016, Rev. B, "Evaluation of ATWS Events for UK AP1000™ Pressurized Water Reactor," October 2010,.

9.4-21 Westinghouse Documents WCAP-16045-P-A, Addendum 1-A, Rev. 0 (Proprietary) and WCAP-16045-NP-A, Addendum 1-A, Rev. 0, (Non-Proprietary), "Qualification of the NEXUS Nuclear Data Methodology," August 2007.

9.4-22 Westinghouse Document WCAP-10965-P-A, Addendum 2-A, Rev. 0 (Proprietary), "Qualification of the New Pin Power Recovery Methodology," September 2010.

9.4-23 Westinghouse Report UKP-GW-GL-083, Rev. 0, "AP1000® Flux Protection and Diversity for Frequent Faults," June 2016.

9.4-24 NUREG-0800, Standard Review Plan, Section 4.2, Revision 3, "Fuel System Design," Appendix B, "Interim Acceptance Criteria and Guidance for the Reactivity Initiated Accidents," U. S. Nuclear Regulatory Commission, March 2007.

9.4-25 NUREG/CR-6928, "Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants," Nuclear Regulatory Commission, February 2007.

Table 9.4-1 (Sheet 1 of 3). DBA Time Sequence Of Events For Incidents Which Result In Reactivity And Power Distribution Anomalies

Accident	Event	Time (seconds)
Uncontrolled RCCA bank withdrawal from a subcritical or low-power startup condition	Initiation of uncontrolled rod withdrawal from 10^{-9} of nominal power	0.0
	Power range high neutron flux (low setting) setpoint reached	10.4
	Peak nuclear power occurs	10.6
	Rods begin to fall into core	11.3
	Peak heat flux occurs	12.9
	Minimum DNBR occurs	12.9
	Peak average clad temperature occurs	13.5
	Peak average fuel temperature occurs	13.7
One or more dropped RCCAs	Rods drop	0.0
	Control system initiates control bank withdrawal	0.4
	Peak nuclear power occurs	21.7
	Peak core heat flux occurs	24.2
Uncontrolled RCCA bank withdrawal at power		
1. Case A – Full power with Maximum Reactivity Feedback	Initiation of uncontrolled RCCA withdrawal at a fast reactivity insertion rate (80 pcm/s)	0.0
	High positive flux rate trip setpoint reached	5.2
	Rods begin to fall into core	6.1
	Minimum DNBR occurs	6.4
2. Case B – Full power with Maximum Reactivity Feedback	Initiation of uncontrolled RCCA withdrawal at an intermediate reactivity insertion rate (34 pcm/s)	0.0
	Overpower ΔT setpoint reached	18.0
	Rods begin to fall into core	19.9
	Minimum DNBR occurs	20.1
3. Case C – Full power with Maximum Reactivity Feedback	Initiation of uncontrolled RCCA withdrawal at a slow reactivity insertion rate (5 pcm/s)	0.0
	Overtemperature ΔT setpoint reached	568.3
	Rods begin to fall into core	570.3
	Minimum DNBR occurs	570.4

Table 9.4-1 (Sheet 2 of 3). DBA Time Sequence Of Events For Incidents Which Result In Reactivity And Power Distribution Anomalies

Accident	Event	Time (minutes)
Chemical and volume control system malfunction that results in a decrease in the boron concentration in the reactor coolant		
1. Dilution during power operation (Mode 1)		
a. Automatic reactor control	Operator receives low-low rod insertion limit alarm due to dilution	0.0
	Shutdown margin lost	170.6
b. Manual reactor control	Dilution initiated	0.0
	Reactor trip on overtemperature ΔT due to dilution	3.3
	Dilution automatically terminated by demineralized water transfer and storage system isolation	3.8
2. Dilution during startup (Mode 2)	Power range high neutron flux-low setpoint reactor trip due to dilution	0.0
	Shutdown margin lost	205.3
3. Dilution during hot standby (Mode 3)	Dilution initiated	0.0
	Boron Dilution Protection System setpoint reached, which initiates isolation of the dilution source	32.1
	Shutdown margin lost	39.6
4. Dilution during safe shutdown (Mode 4)	Dilution initiated	0.0
	Boron Dilution Protection System setpoint reached, which initiates isolation of the dilution source	28.8
	Shutdown margin lost	35.6
5. Dilution during cold shutdown (Mode 5)	Dilution initiated	0.0
	Boron Dilution Protection System setpoint reached, which initiates isolation of the dilution source	11.2
	Shutdown margin lost	13.1

Table 9.4-1 (Sheet 3 of 3). DBA Time Sequence Of Events For Incidents Which Result In Reactivity And Power Distribution Anomalies

Accident	Event	Time (seconds)
RCCA ejection accident		
1. PCMI limiting event	Initiation of rod ejection	0.00
	Peak nuclear power occurs	0.14
	Reactor trip setpoint reached	<0.30
	Peak cladding temperature occurs	0.36
	Peak enthalpy deposition occurs	0.44
	Rods begin to fall into core	1.20
2. Peak cladding temperature limiting event	Initiation of rod ejection	0.00
	Peak nuclear power occurs	0.08
	Minimum DNBR occurs	0.11
	Peak cladding temperature occurs	0.11
	Reactor trip setpoint reached	<0.30
	Rods begin to fall into core	1.20
3. Peak enthalpy/peak fuel centreline temperature event	Initiation of rod ejection	0.00
	Peak nuclear power occurs	0.06
	Reactor trip setpoint reached	<0.30
	Rods begin to fall into core	1.20
	Peak fuel centre temperature occurs	2.50
	Peak cladding temperature occurs	2.80

Table 9.4-2. DBA Key Input Parameters For Boron Dilution

Dilution Flow Rates		
Mode	**Flow Rate (gal/min)**	**Flow Rate (m^3/hr)**
1 through 5	175	39.75
Active RCS Volume		
Mode	**Volume (ft^3)**	**Volume (m^3)**
1 and 2	8425.5	238.58
3 and 4	7605.9	215.38
5	2608.2	73.86
Boron Concentration		
Mode	**Initial Concentration (ppm)**	**Critical Concentration (ppm)**
1	1811	934
2	2031	934
3	1509	1281
4	1649	1449
5	1675	1483

Table 9.4-3. DBA Parameters Used In Evaluating The Radiological Consequences Of A Rod Ejection Accident

Reactor coolant iodine activity	Equal to the operating limit for reactor coolant activity of 9.25E6 Bq/kg (0.25 µCi/g) dose equivalent I-131 (see Table 9A-1)
Reactor coolant noble gas activity	Equal to the operating limit for reactor coolant activity of 2.6E9 Bq/kg (70 µCi/g) dose equivalent Xe-133 (see Table 9A-1)
Reactor coolant alkali metal activity	Design basis activity (see Table 9A-1)
Fraction of fuel rods assumed to fail	0.10
Fraction of fuel assumed to melt	0.0025
Core activity	See Table 9A-3
Radial peaking factor (for determination of activity in failed fuel rods)	1.75
Fission product gap fractions Iodines Noble gases Alkali metals	 0.03 0.10 0.04
Fraction of activity released from fuel becoming airborne in containment Iodines Noble gases Alkali metals	 0.6 1.0 0.0
Airborne Iodine Chemical Fractions Elemental Iodine Organic Iodine	 0.99 0.01
Iodine Removal Coefficients[(a)] Elemental Iodine Organic Iodine	 1.7 (hr^{-1}) 0.0 (hr^{-1})
Containment Leakage Rate 0-24 hours 24-720 hours	 0.1 (%/day) 0.05 (%/day)
Offsite atmospheric dispersion factors	See Table 9A-5
Control room modelling	See Appendix 9A

Note:
1. Elemental iodine removal is modelled until a decontamination factor (DF) of 200 is reached.

Table 9.4-4. Rod Ejection Accident Technical Specifications Used In Dose Analysis

Limit or Condition	Tech Spec Identification and Notes
Primary Containment Leakage Rate	3.6.1 (SR 3.6.1.1) within containment leakage acceptance criteria. 5.5.8 (Containment leakage rate testing program) defines maximum allowable primary containment leak rate to be less than or equal to 0.1 weight-% per day at the calculated peak containment internal pressure for the design basis LOCA.
Primary coolant specific activity	3.4.10 dose equivalent specific activity to be < 9.25E6 Bq/kg (0.25 μCi/g) for I-131 and < 2.6E9 Bq/kg (70 μCi/g) for Xe-133

Table 9.4.2-1. ATWT Uncontrolled RCCA Withdrawal from 100 Percent Power

Event	Time (Sec)
Initiate Rod Withdrawal from 100 percent power (15 pcm/sec reactivity insertion rate)	0.0
High Neutron Flux Rod Control System Interlock C-2 reached. Rod withdrawal blocked.	not credited
High Neutron Flux trip setpoint reached (PMS trip blocked)	8.8
High Pressuriser Pressure setpoint reached (PMS trip blocked)	23.1
High Pressuriser level setpoint reached (PMS trip blocked)	28.5
Margin to OPΔT Rod Control System Interlock C-3 reached. Rod withdrawal blocked and turbine runback initiated.	not credited
High Hot Leg Temperature setpoint (335°C [635°F]) reached (DAS trip)	35.6
Control Rod Motion starts	42.6
Peak Nuclear Power (1.312 FON) reached	43.0
Peak RCS pressure (18.5 MPa [2679 psia])	43.5

Table 9.4.3-1. RCCA Misalignment Faults Mitigation Features

Category A Safety Function	Provision	SSCs	Classification
Short-term reactivity control	Primary means	Reactor trip Breakers (PMS)	1
	Diverse means	Motor-generator set field breakers (DAS)	2
Long-term reactivity control	Primary means	CMT Recirculation	1
	Diverse means	Passive feed and bleed	1
Decay heat removal	Primary means	PRHR HX	1
	Diverse means	Passive feed and bleed	1
RCS pressure control	Primary means	Pressuriser safety valve	1
	Diverse means	Pressuriser	1
RCS inventory control	Primary means	CMTs	1
	Diverse means	Passive feed and bleed	1
Containment cooling	Primary means	PCS AOVs	1
	Diverse means	PCS MOVs	1

Table 9.4.3-2. RCCA Misalignment Faults Potential Operator Actions

Operator Action	Class
On failure of automatic shutdown, initiate shutdown manually using DAS.	1
On failure of shutdown rods to insert, initiate RCP trip and actuation of CMTs to achieve shutdown by boration of the primary circuit	1
If PRHR fails, activate ADS to allow automatic actuation of recirculation RHR via the IRWST.	1

Table 9.4.6-1. ATWT Boron Dilution with a PMS CCF in Manual Rod Control

Event	Time (Sec)
Start of dilution	0
SG PORVs open in Loops 1 and 2	701
PLS Margin to OTΔT setpoint C-4 reached (alarm, blocks rod withdrawal and actuates turbine runback)	not credited
PMS OTΔT setpoint reached – no action due to PMS CCF	869
High Hot Leg Temperature = 343.3°C (650°F) in both loops reached, DAS signal generated 2 sec later	1094
RCCA starts to fall into the core (5 sec delay for M-G sets)	1101
Turbine is tripped (5 sec delay from reactor trip signal)	1101
Turbine bypass start to open in Pressure control mode	1101
SG safety valves open in Loops 1 and 2	1103
PRHR valves full flow on DAS High Hot Leg Temperature (delay 5 sec +7.5 sec)	1109

Table 9.4.6-2. ATWT Boron Dilution with a RCCA Mechanical CCF in Manual Rod Control

Event	Time (Sec)
Start of dilution	0
SG PORVs open in Loops 1 and 2	701
PLS Margin to OTΔT setpoint C-4 reached (alarm, blocks rod withdrawal and actuates turbine runback)	not credited
PMS OTΔT setpoint reached, reactor trip signal generated with 2 sec delay	869
Turbine is tripped (5 sec . delay from reactor trip signal)	876
Turbine bypass system starts to open in Pressure control mode	876
SG Safety Valves open in Loops 1 and 2	879
High Hot Leg Temperature = 343.3°C (650°F) in both loops reached, DAS signal generated 2 sec later	888
Line from the demineralised water tank is isolated (assumed 30 sec delay from PMS reactor trip signal) In this time, primary is diluted -50 ppm from initial 1050 ppm	900
PRHR valves full flow on DAS High Hot Leg Temperature (delay 5 sec + 7.5 sec)	902.5

Table 9.4.7-1. Fuel Misload Detectability Review Criteria

Available Detector Locations	Measured vs. Predicted Assembly Power*	Symmetric Assembly Measured Power Comparison+
≥ 75%	10%	10%
≥ 40% but < 75%	7%	7%

*Applicable to core locations with predicted assembly relative powers above 0.8.

+Applicable to core locations with assembly relative powers above 0.8. The review criterion is relative to the expected symmetric assembly measured power difference.

Table 9.4.8-1. Spectrum of RCCA Ejection Events Mitigation Features

Category A Safety Function	Provision	SSCs	Classification
Short-term reactivity control	Primary means	Reactor trip Breakers (PMS)	1
Long-term reactivity control	Primary means	CMT Recirculation	1
Decay heat removal	Primary means	PRHR HX	1
RCS pressure control	Primary means	Pressuriser safety valve	1
RCS inventory control	Primary means	CMTs, accumulators, IRWST	1
Containment cooling	Primary means	PCS AOVs	1

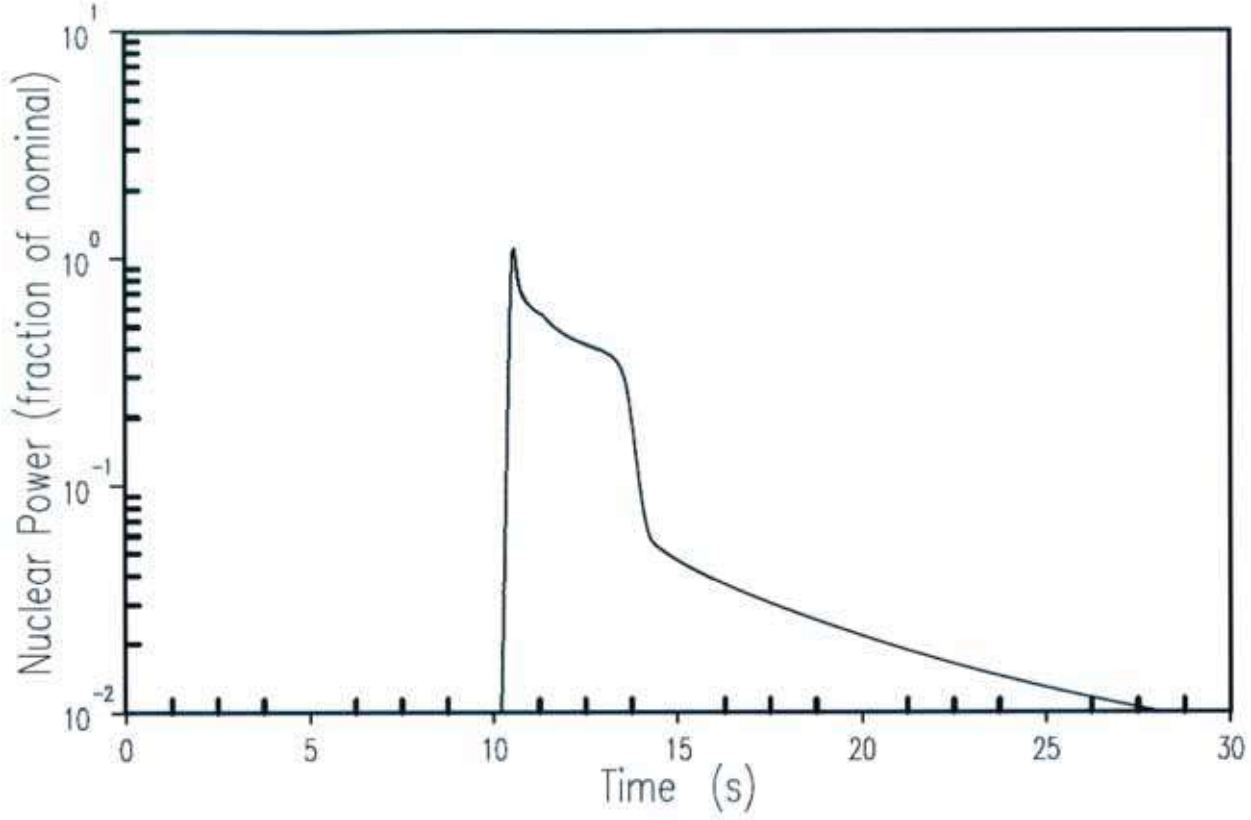


Figure 9.4.1-1. DBA RCCA Withdrawal from Subcritical Nuclear Power

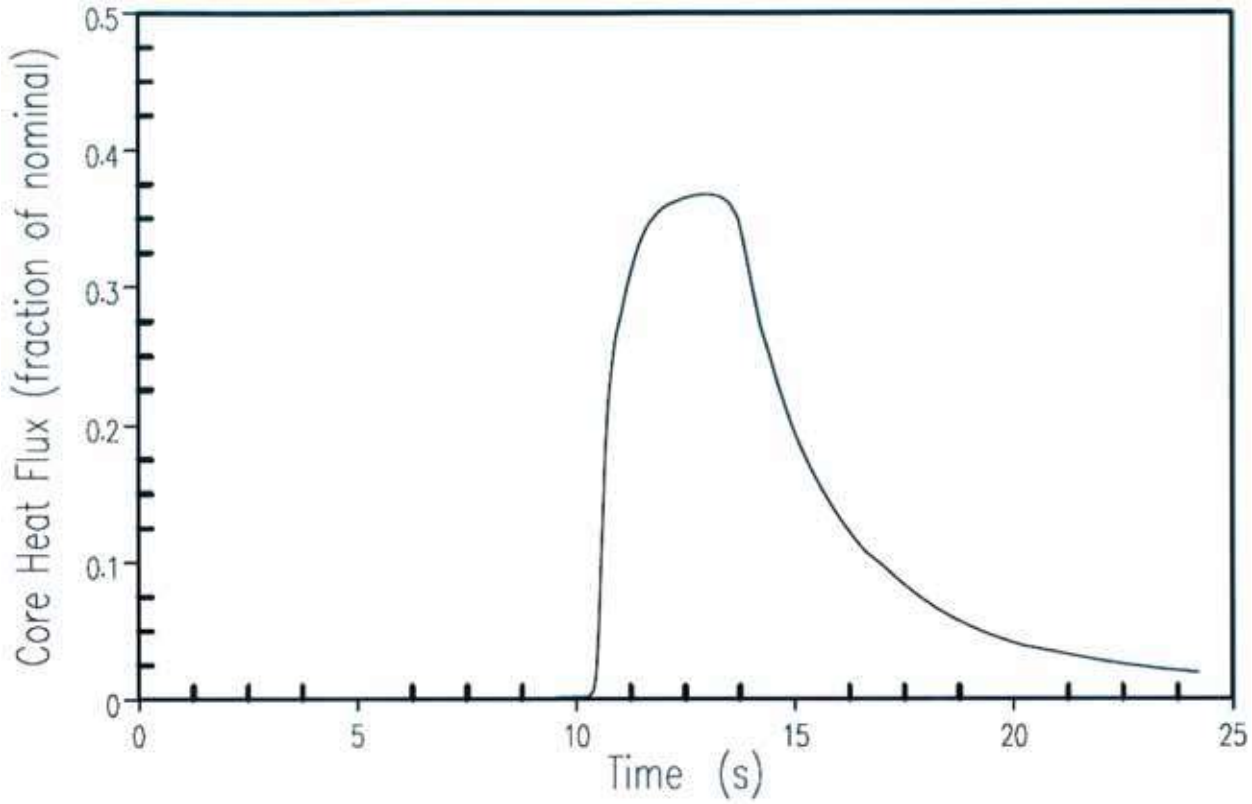


Figure 9.4.1-2. DBA RCCA Withdrawal from Subcritical Average Channel Core Heat Flux

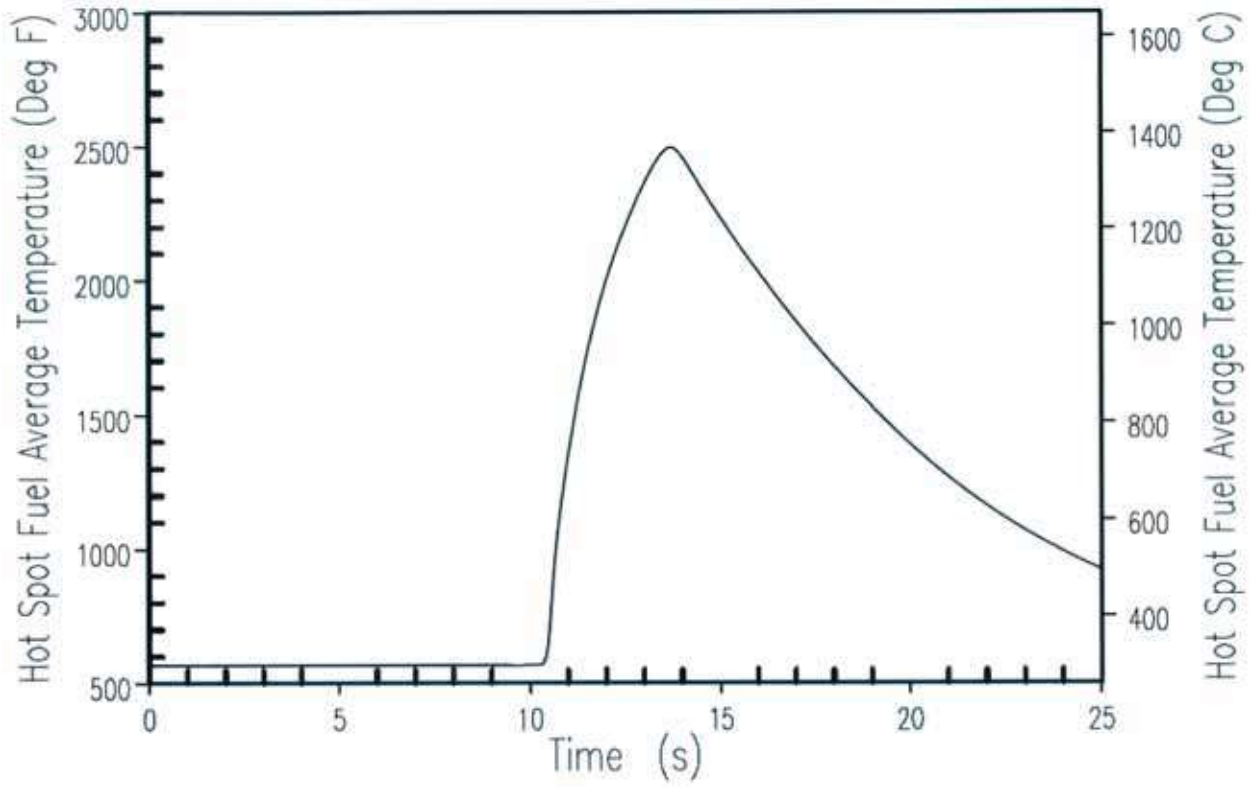


Figure 9.4.1-3. DBA RCCA Withdrawal from Subcritical Hot Spot Fuel Average Temperature

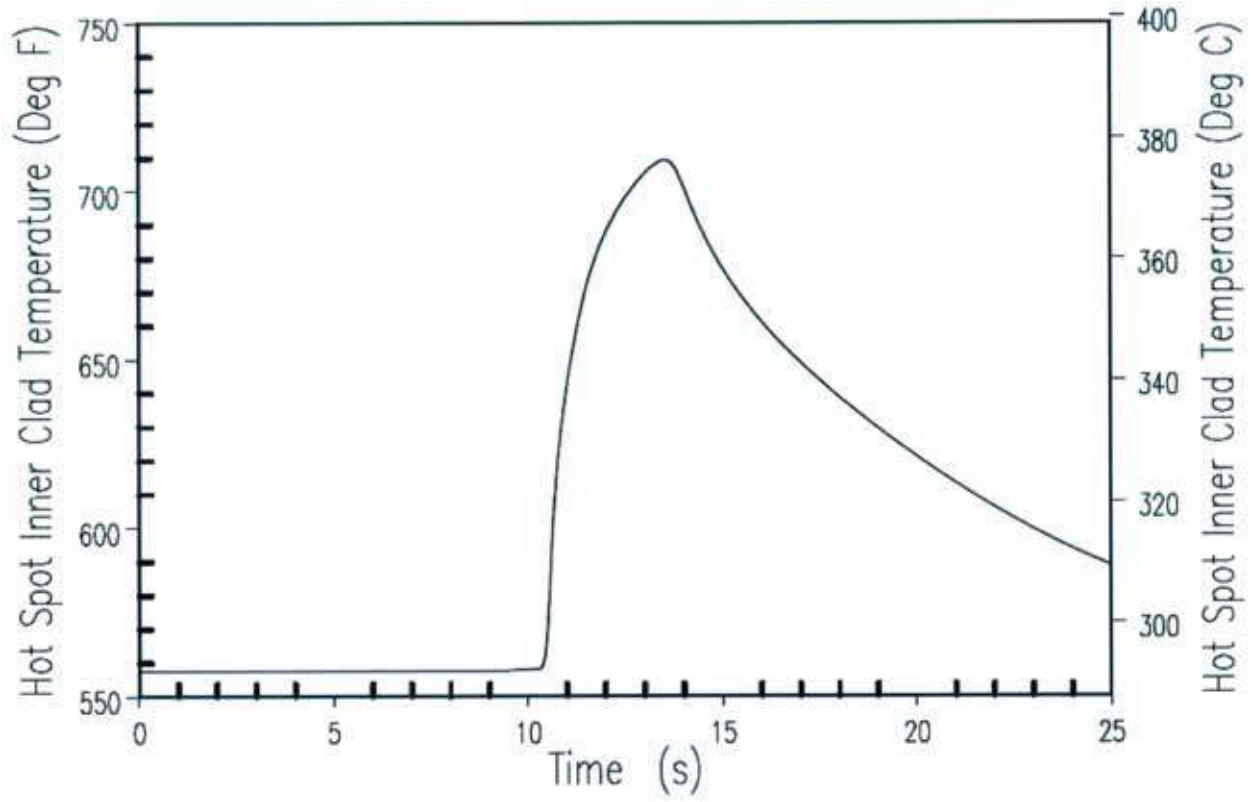


Figure 9.4.1-4. DBA RCCA Withdrawal from Subcritical Hot Spot Cladding Inner Temperature

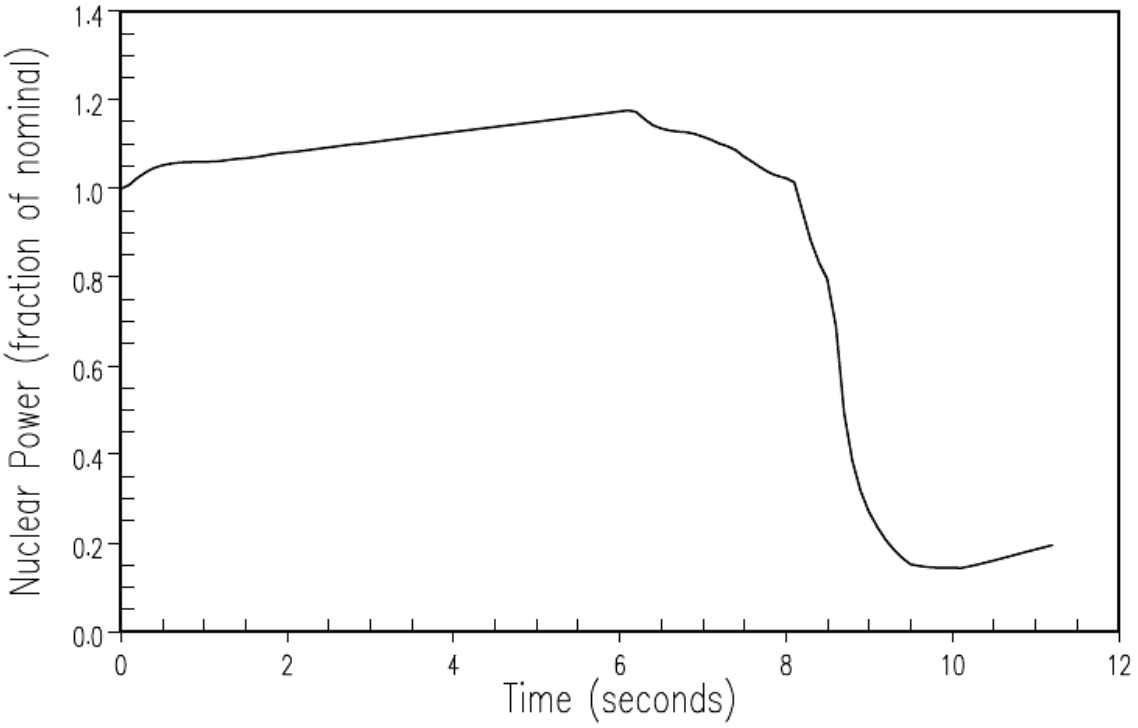


Figure 9.4.2-1. DBA Nuclear Power Transient for an Uncontrolled RCCA Bank Withdrawal from Full Power with Maximum Reactivity Feedback (80 pcm/s)

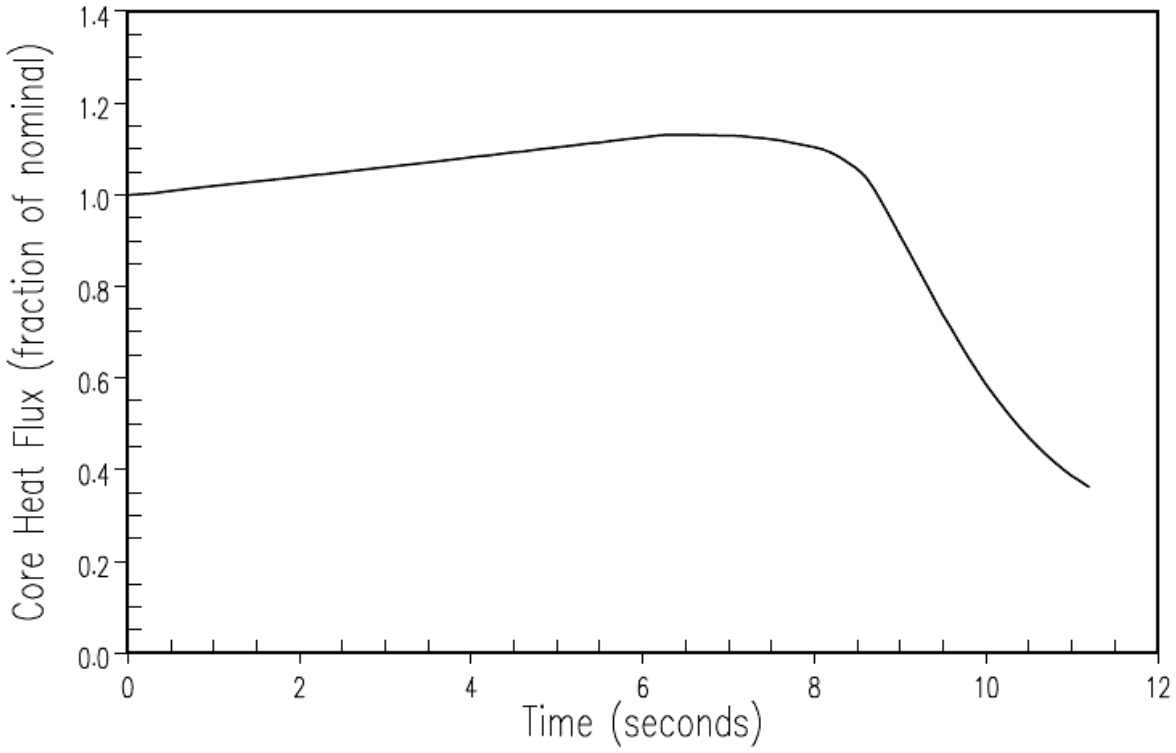


Figure 9.4.2-2. DBA Core Heat Flux Transient for an Uncontrolled RCCA Bank Withdrawal from Full Power with Maximum Reactivity Feedback (80 pcm/s)

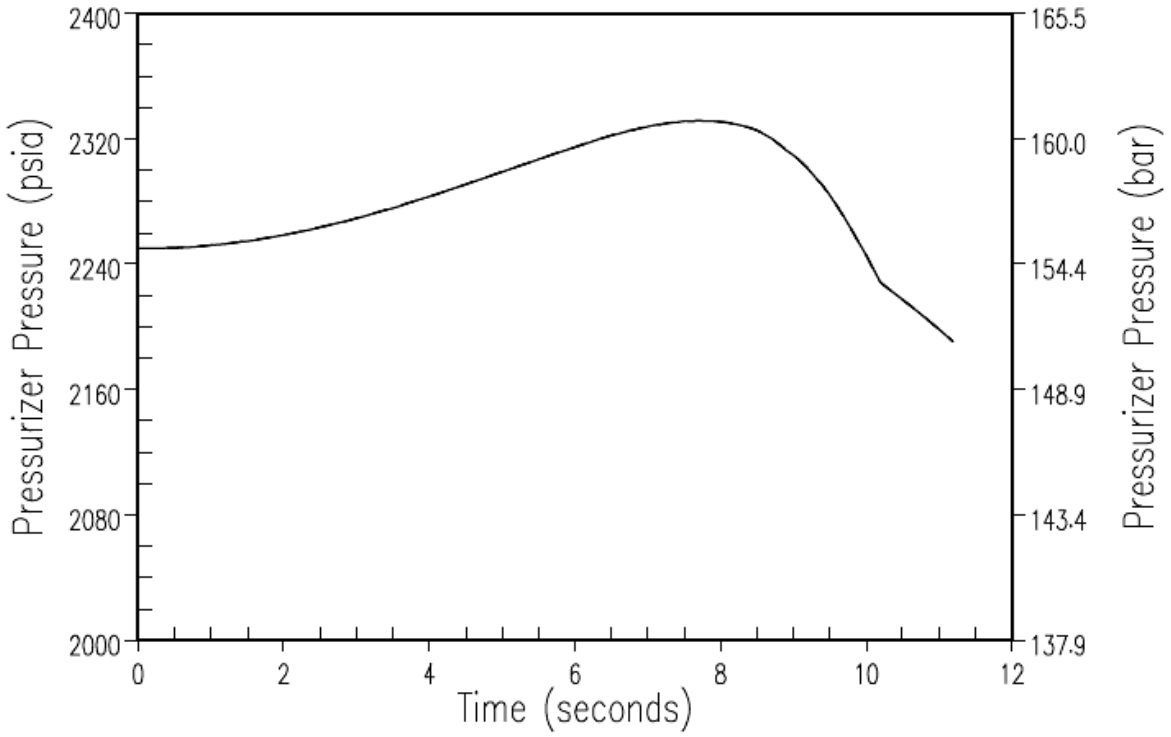


Figure 9.4.2-3. DBA Pressuriser Pressure Transient for an Uncontrolled RCCA Bank Withdrawal from Full Power with Maximum Reactivity Feedback (80 pcm/s)

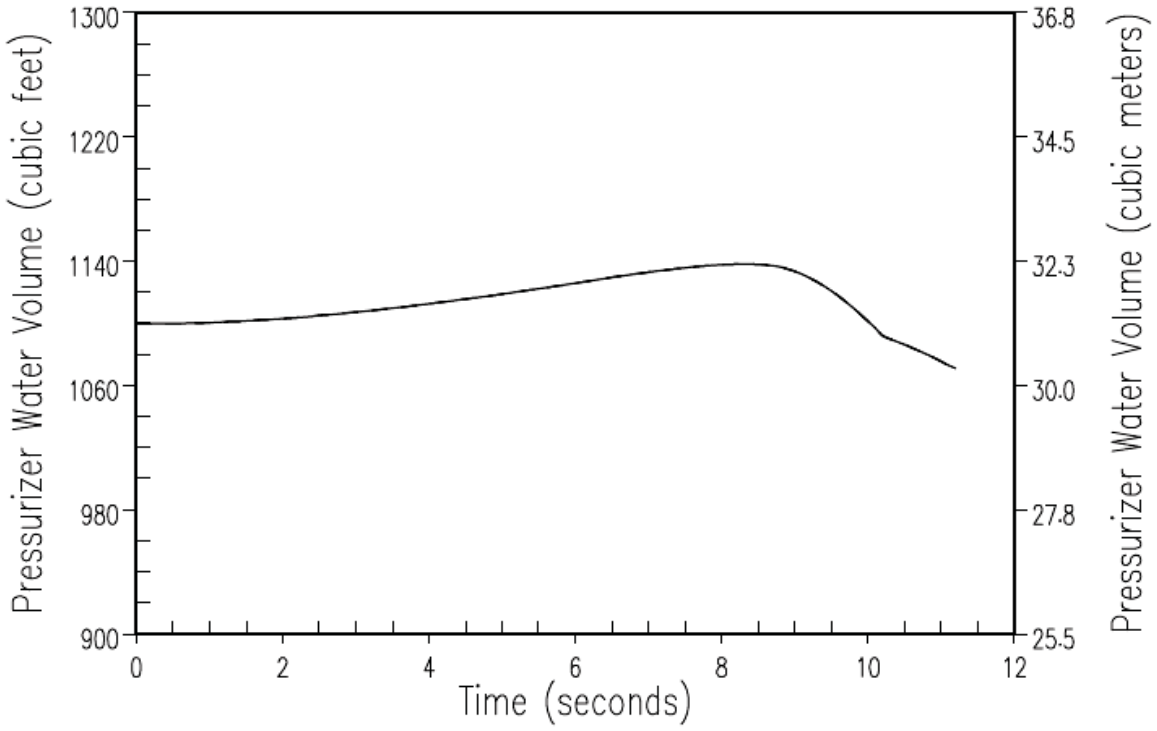


Figure 9.4.2-4. DBA Pressuriser Water Volume Transient for an Uncontrolled RCCA Bank Withdrawal from Full Power with Maximum Reactivity Feedback (80 pcm/s)

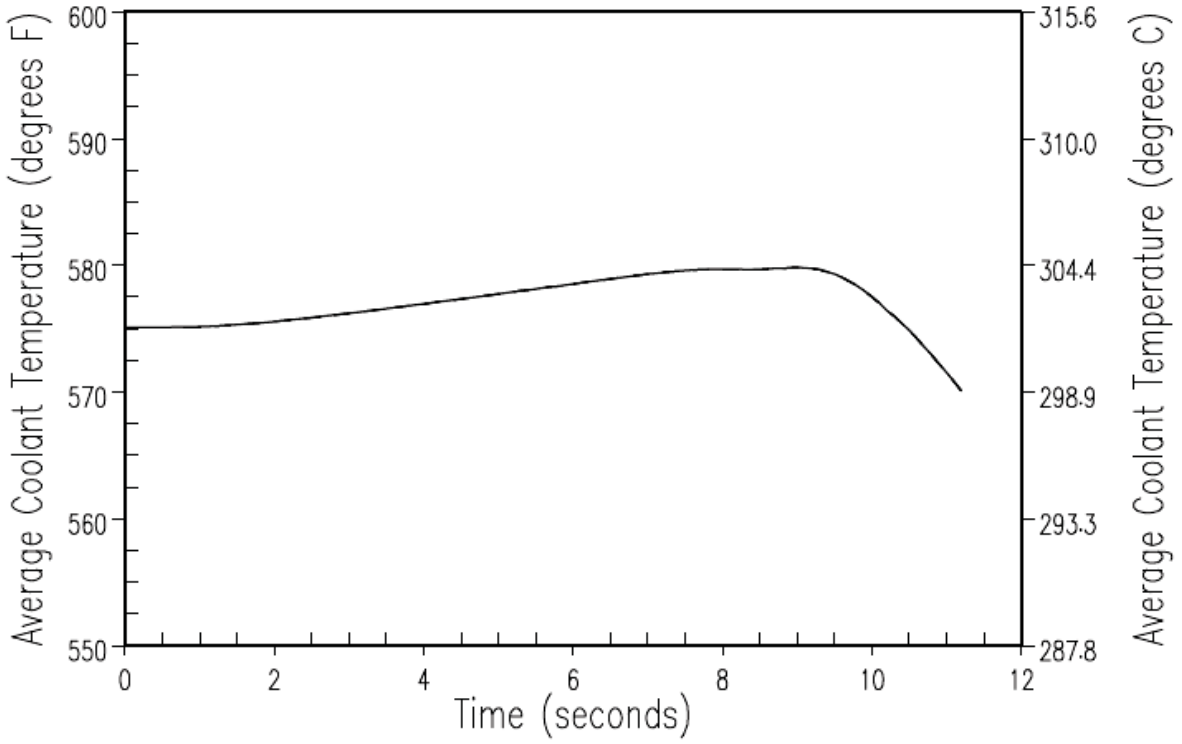


Figure 9.4.2-5. DBA Core Coolant Average Temperature Transient for an Uncontrolled RCCA Bank Withdrawal from Full Power with Maximum Reactivity Feedback (80 pcm/s)

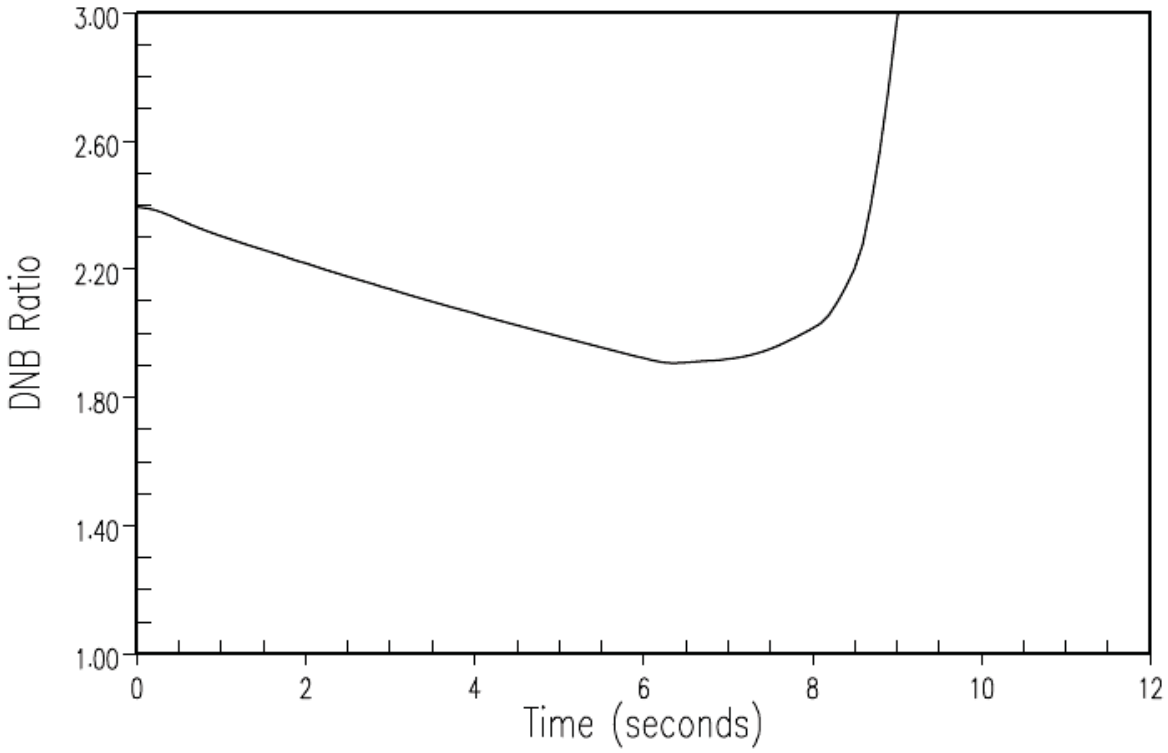


Figure 9.4.2-6. DBA DNBR Transient for an Uncontrolled RCCA Bank Withdrawal from Full Power with Maximum Reactivity Feedback (80 pcm/s)

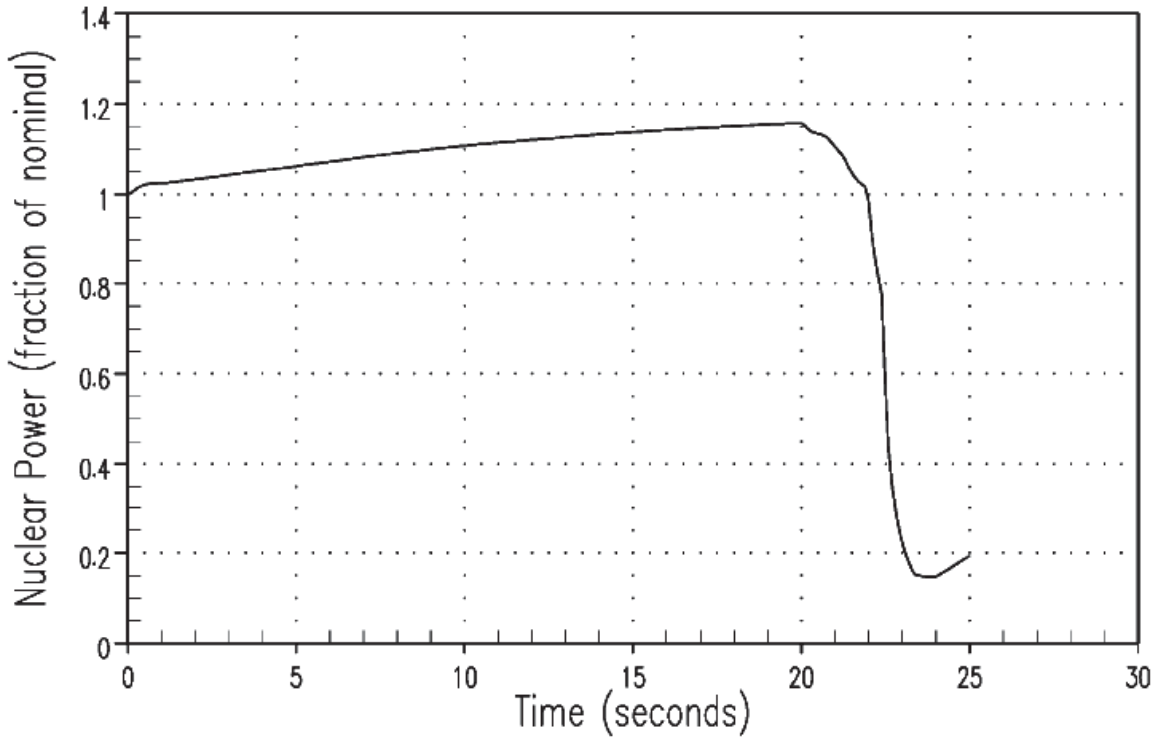


Figure 9.4.2-7. DBA Nuclear Power Transient for an Uncontrolled RCCA Bank Withdrawal from Full Power with Maximum Reactivity Feedback (34 pcm/s)

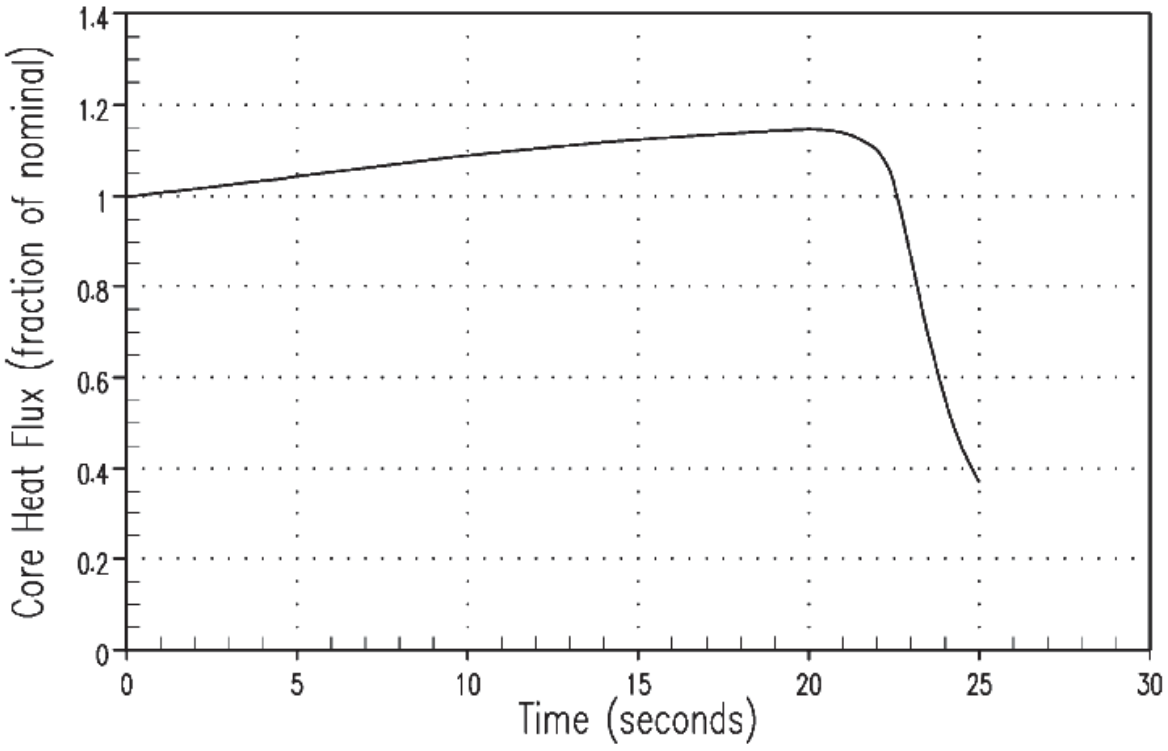


Figure 9.4.2-8. DBA Core Heat Transient for an Uncontrolled RCCA Bank Withdrawal from Full Power with Maximum Reactivity Feedback (34 pcm/s)

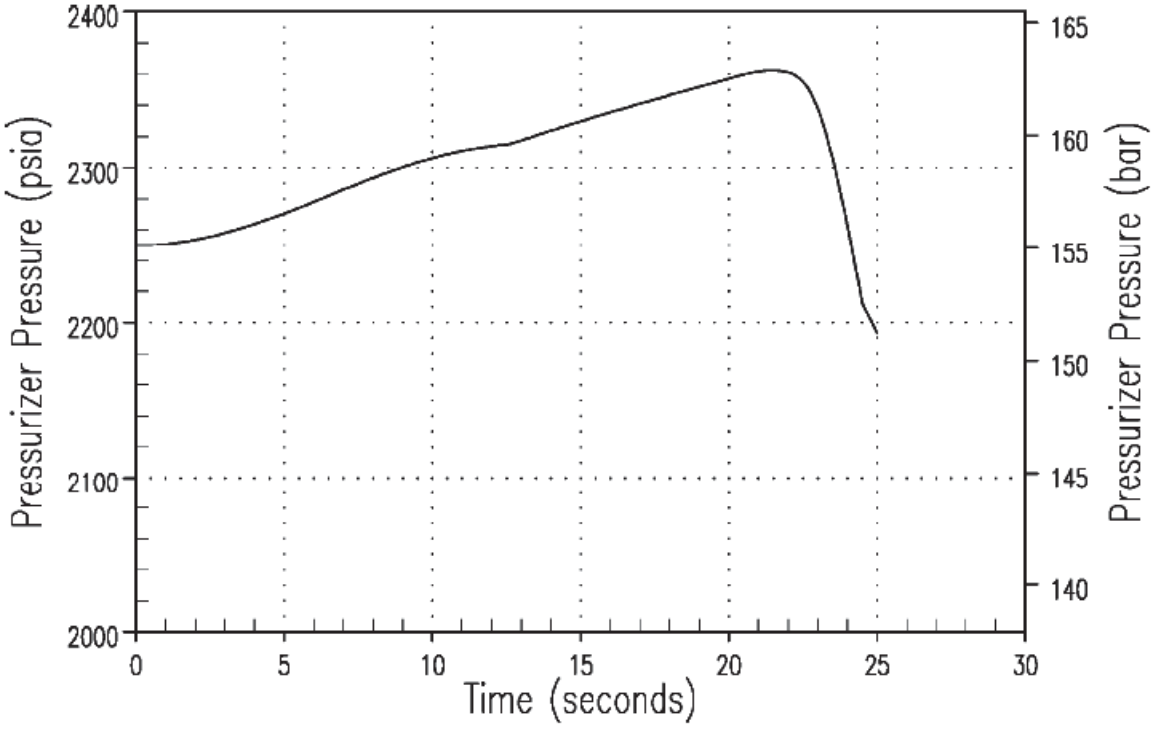


Figure 9.4.2-9. DBA Pressuriser Pressure Transient for an Uncontrolled RCCA Bank Withdrawal from Full Power with Maximum Reactivity Feedback (34 pcm/s)

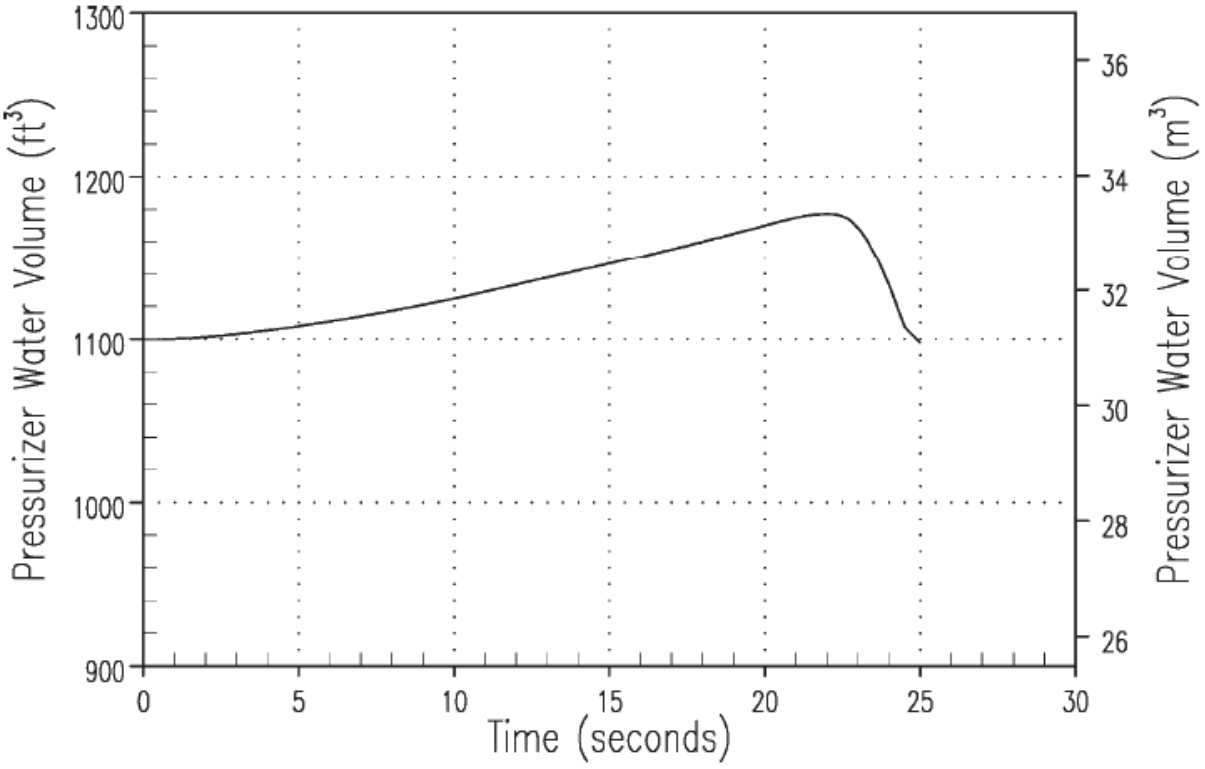


Figure 9.4.2-10. DBA Pressuriser Water Volume Transient for an Uncontrolled RCCA Bank Withdrawal from Full Power with Maximum Reactivity Feedback (34 pcm/s)

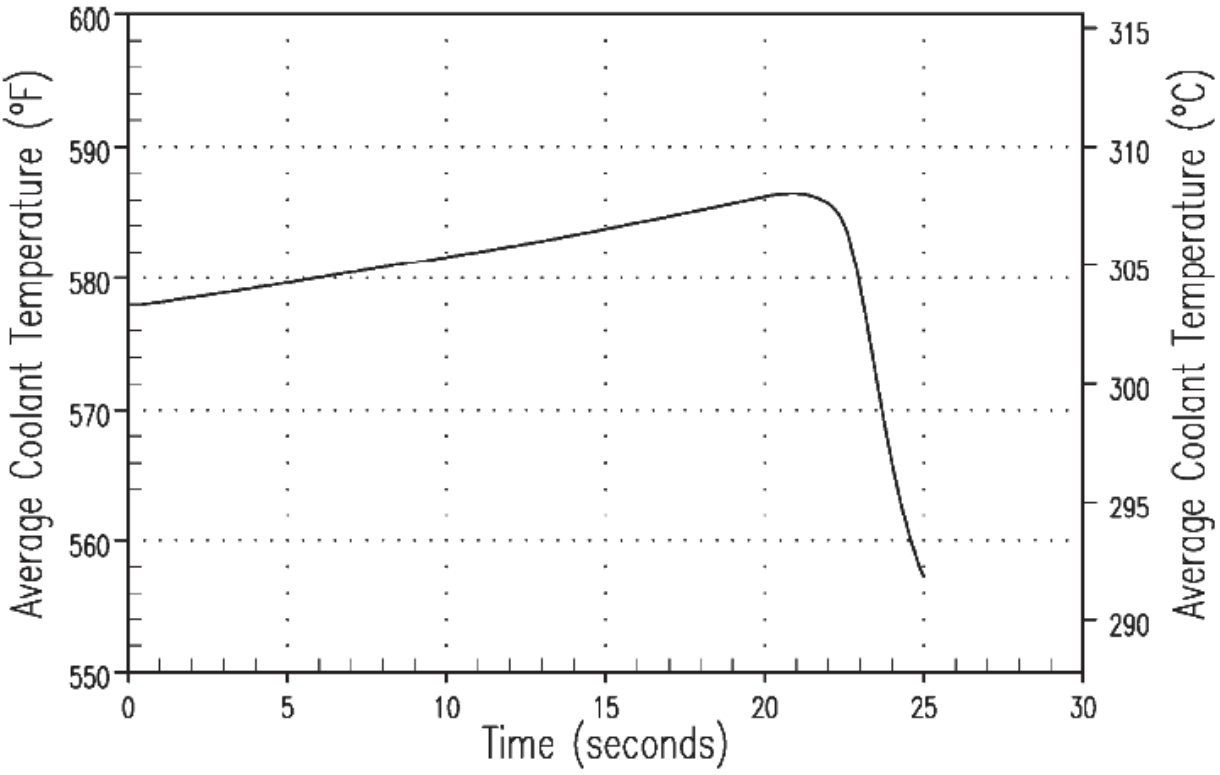


Figure 9.4.2-11. DBA Core Coolant Average Temperature Transient for an Uncontrolled RCCA Bank Withdrawal from Full Power with Maximum Reactivity Feedback (34 pcm/s)

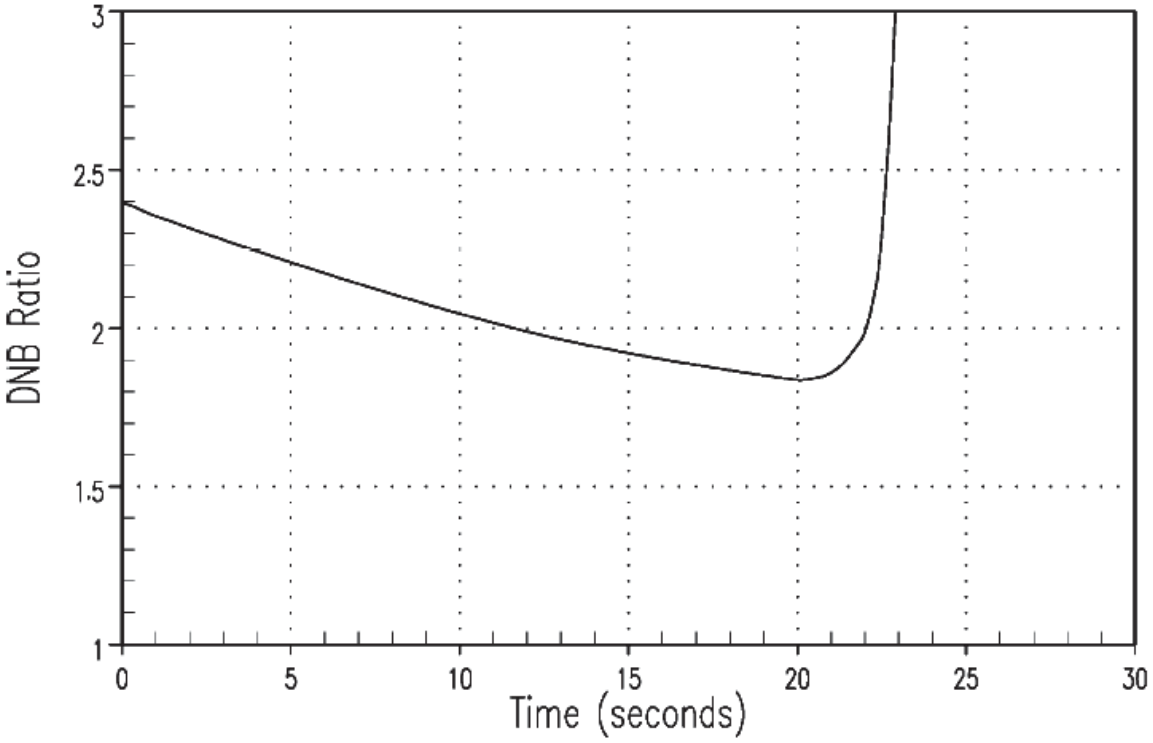


Figure 9.4.2-12. DBA DNBR Transient for an Uncontrolled RCCA Bank Withdrawal from Full Power with Maximum Reactivity Feedback (34 pcm/s)

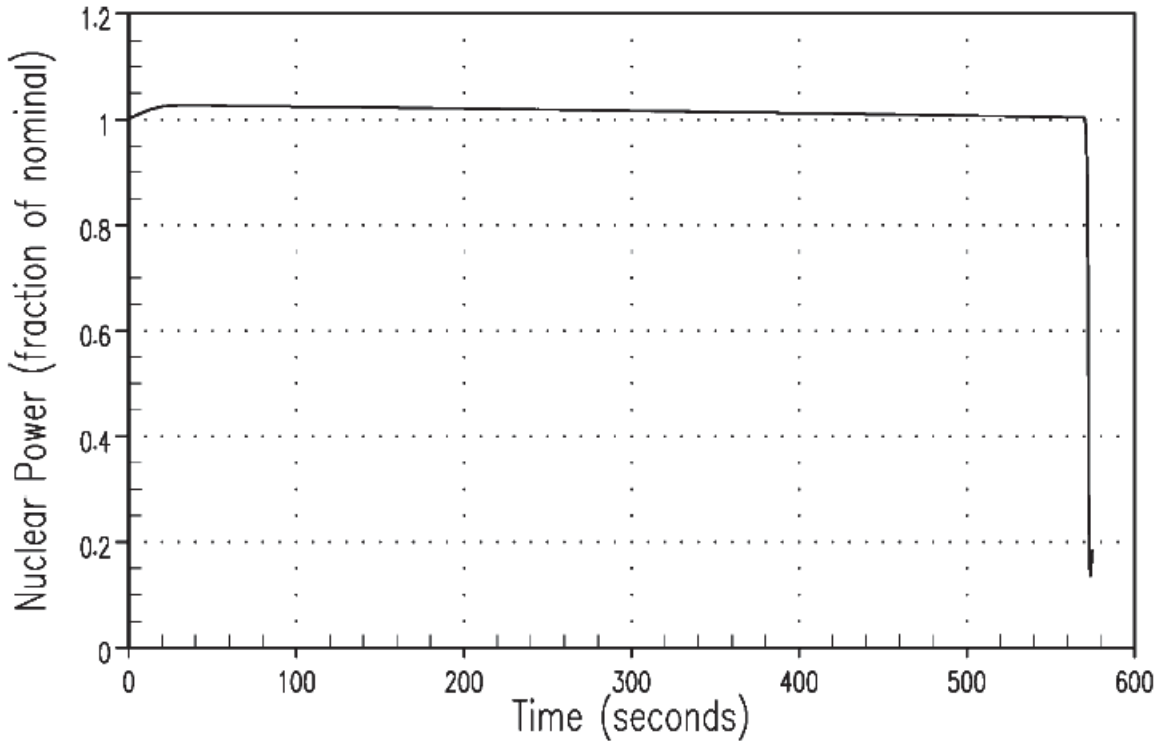


Figure 9.4.2-13. DBA Nuclear Power Transient for an Uncontrolled RCCA Bank Withdrawal from Full Power with Maximum Reactivity Feedback (5 pcm/s)

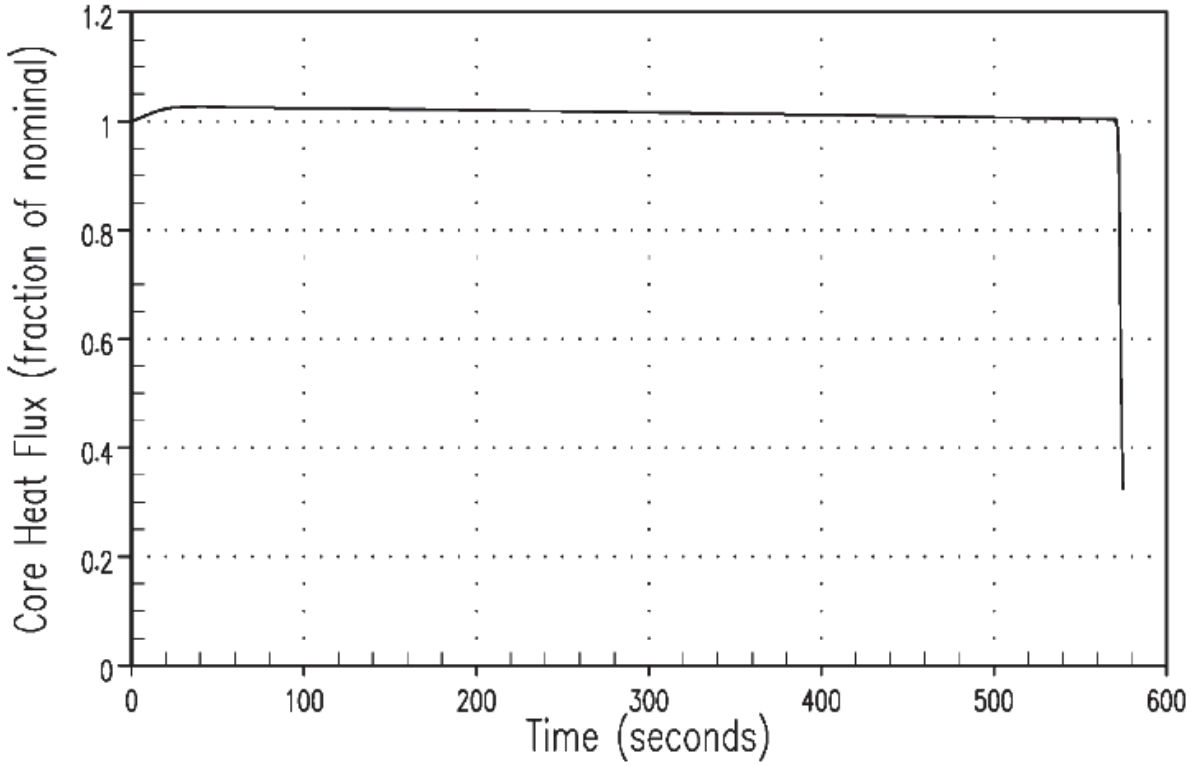


Figure 9.4.2-14. DBA Core Heat Transient for an Uncontrolled RCCA Bank Withdrawal from Full Power with Maximum Reactivity Feedback (5 pcm/s)

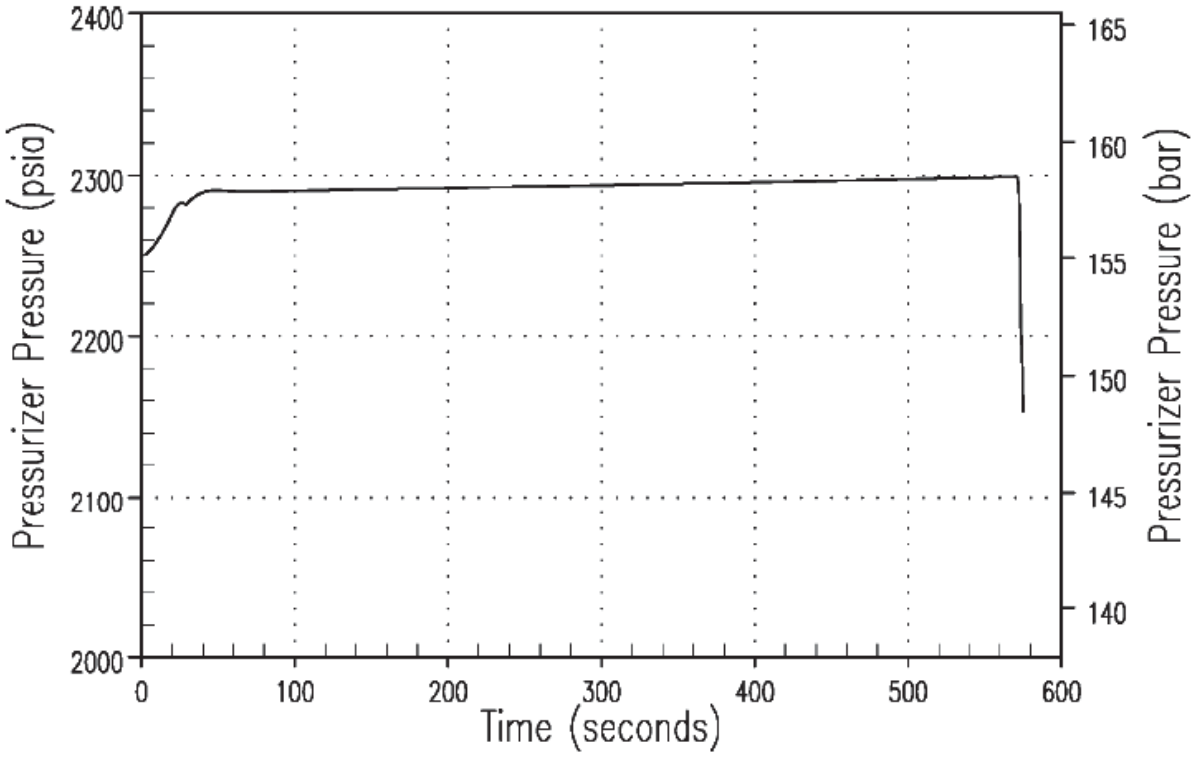


Figure 9.4.2-15. DBA Pressuriser Pressure Transient for an Uncontrolled RCCA Bank Withdrawal from Full Power with Maximum Reactivity Feedback (5 pcm/s)

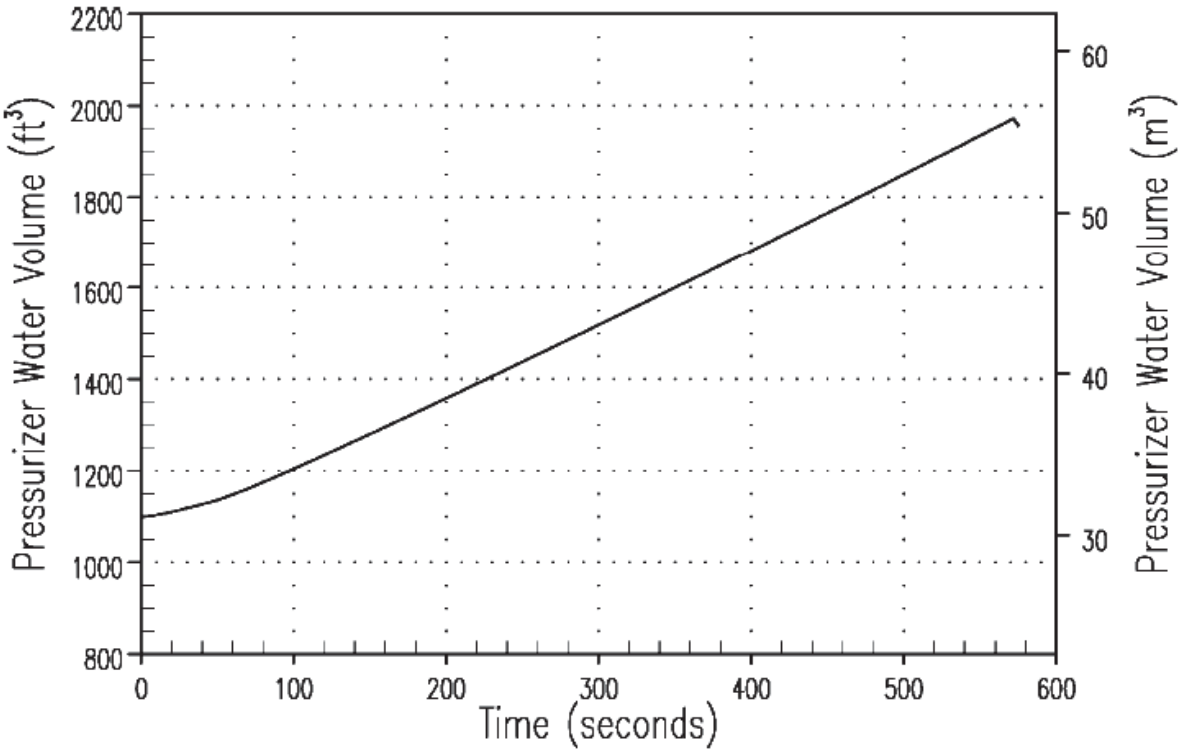


Figure 9.4.2-16. DBA Pressuriser Water Volume Transient for an Uncontrolled RCCA Bank Withdrawal from Full Power with Maximum Reactivity Feedback (5 pcm/s)

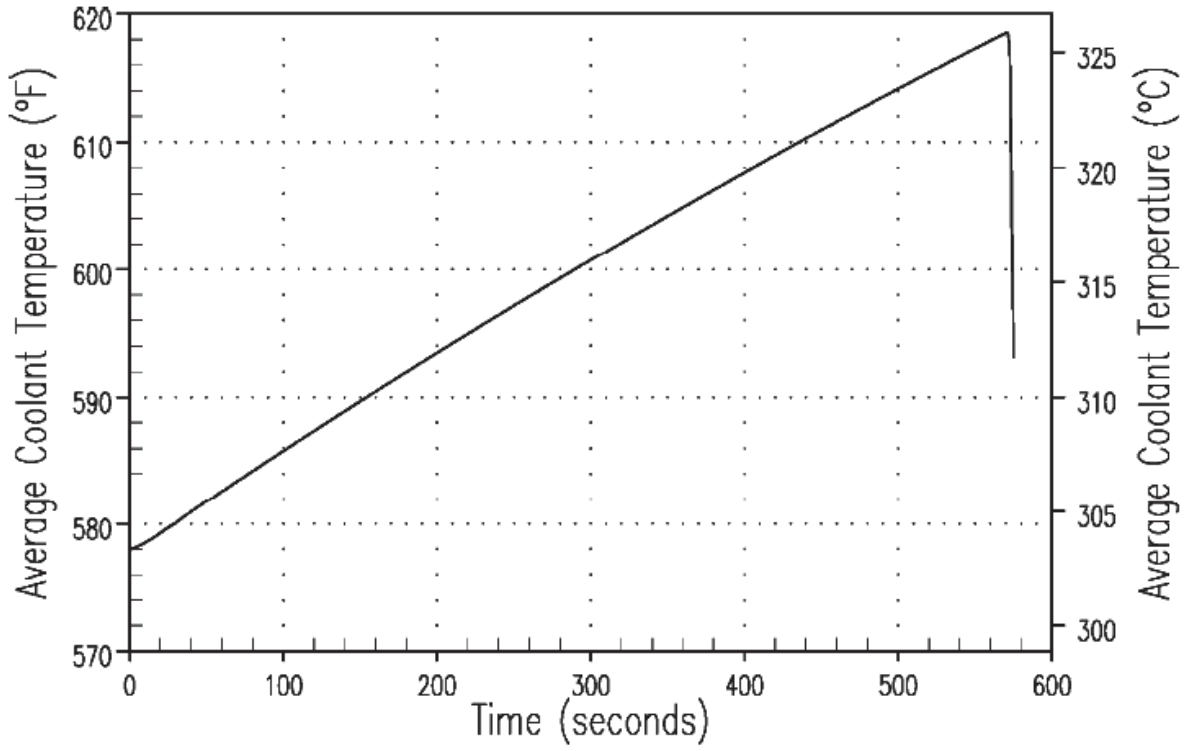


Figure 9.4.2-17. DBA Core Coolant Average Temperature Transient for an Uncontrolled RCCA Bank Withdrawal from Full Power with Maximum Reactivity Feedback (5 pcm/s)

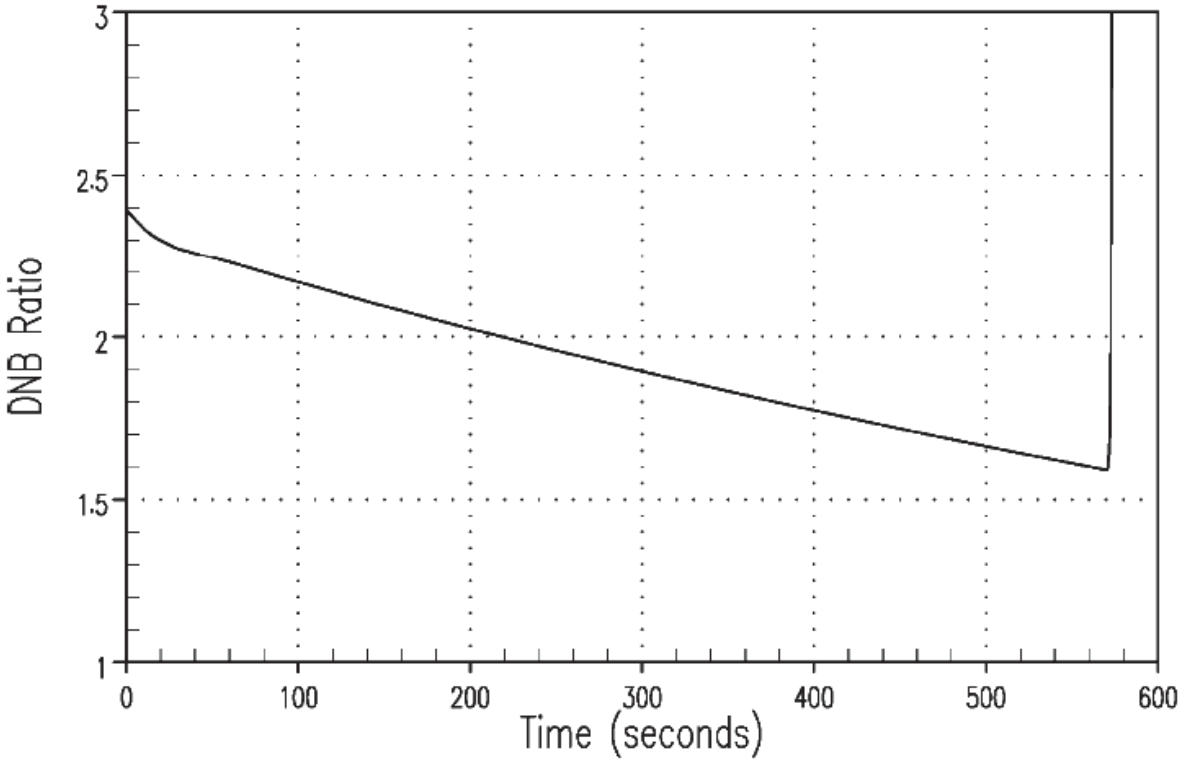


Figure 9.4.2-18. DBA DNBR Transient for an Uncontrolled RCCA Bank Withdrawal from Full Power with Maximum Reactivity Feedback (5 pcm/s)

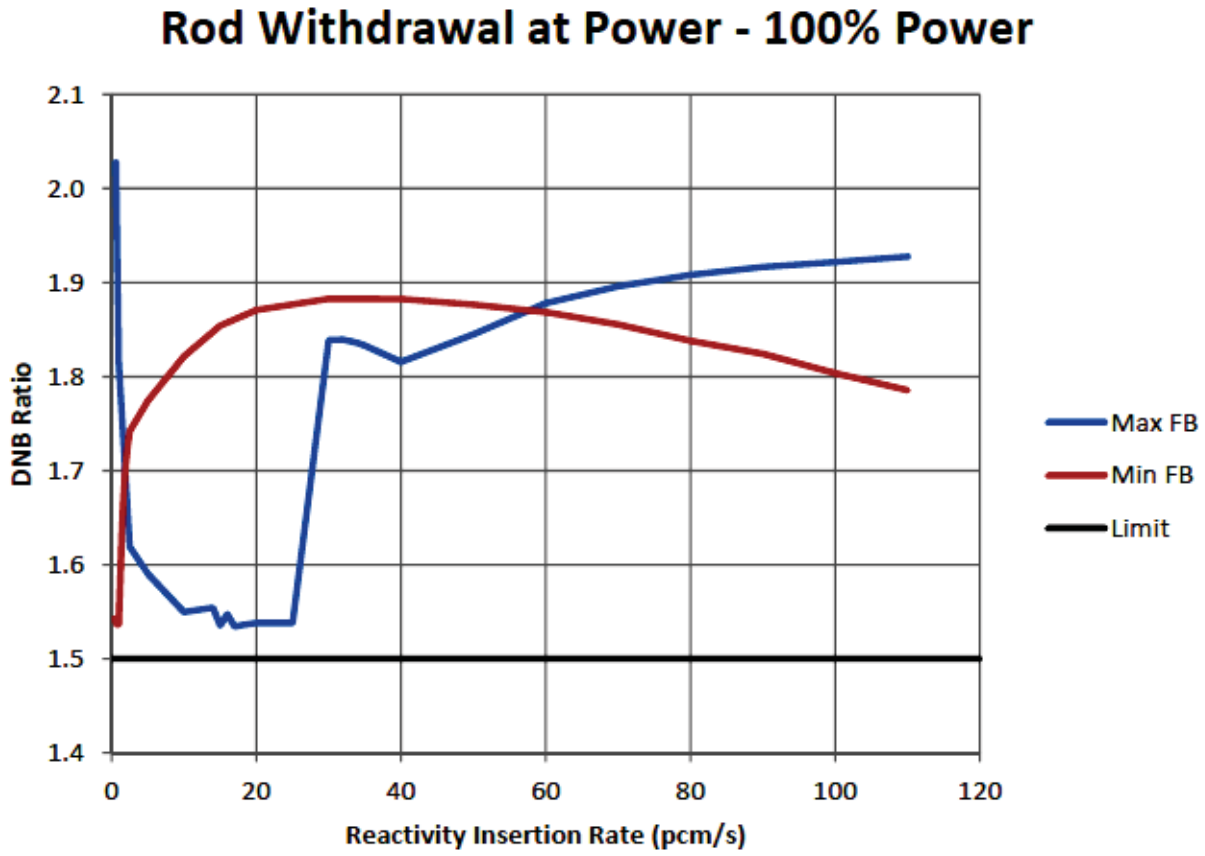


Figure 9.4.2-19. DBA Minimum DNBR Versus Reactivity Insertion Rate for Rod Withdrawal at 100-percent Power

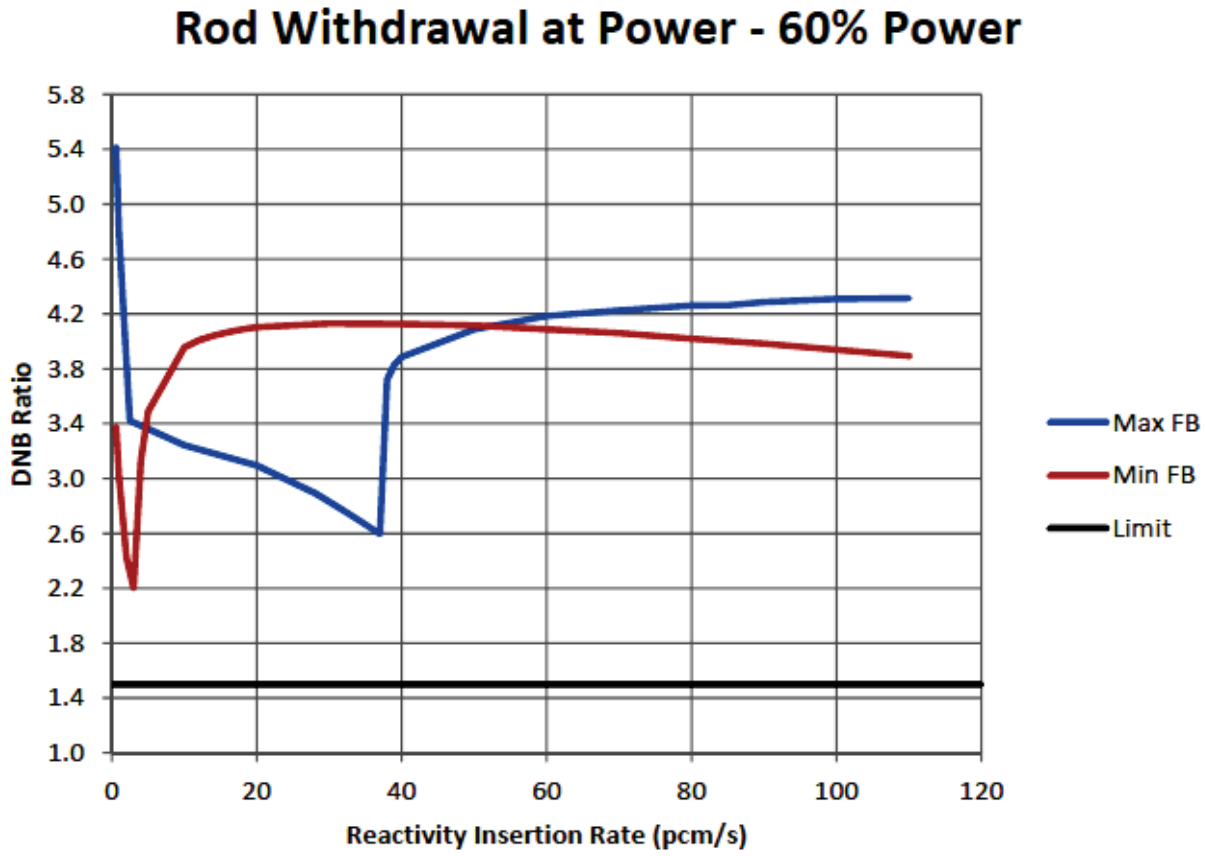


Figure 9.4.2-20. DBA Minimum DNBR Versus Reactivity Insertion Rate for Rod Withdrawal at 60-percent Power

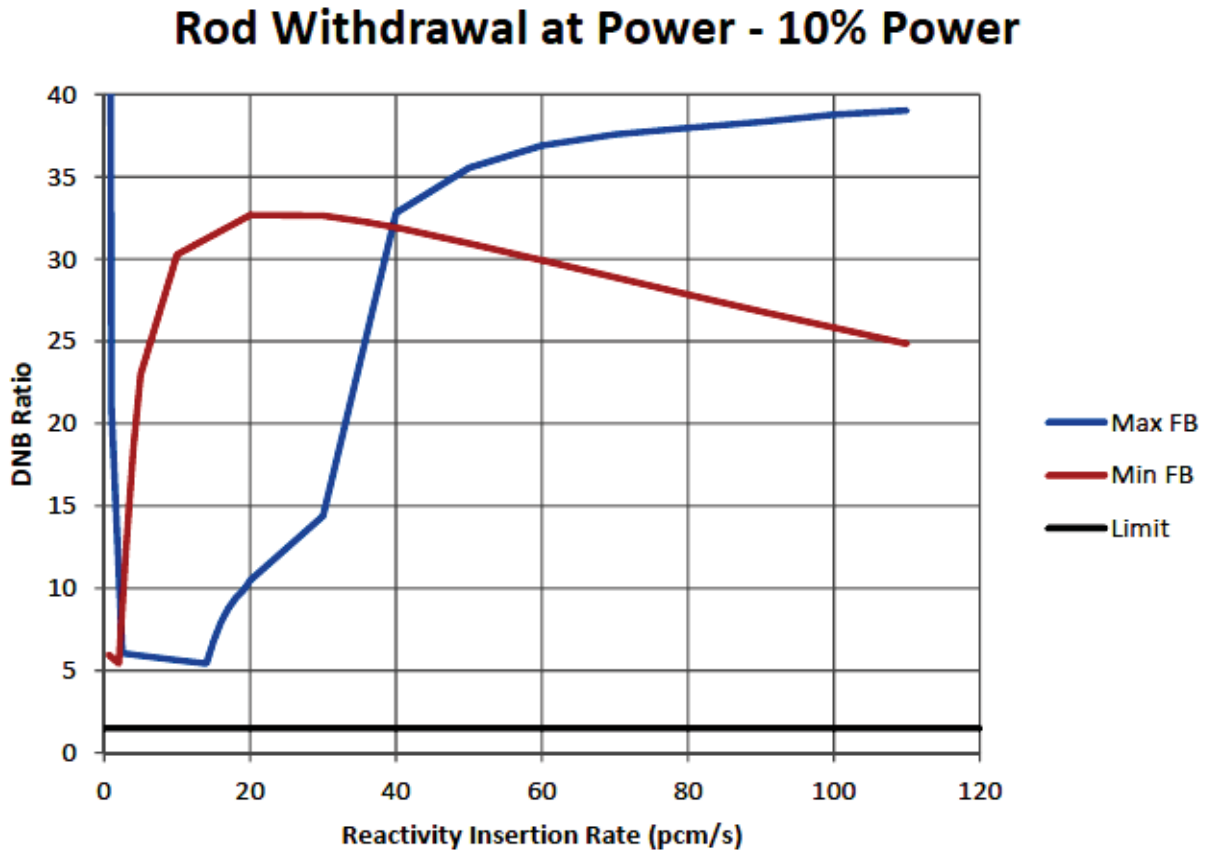


Figure 9.4.2-21. DBA Minimum DNBR Versus Reactivity Insertion Rate for Rod Withdrawal at 10-percent Power

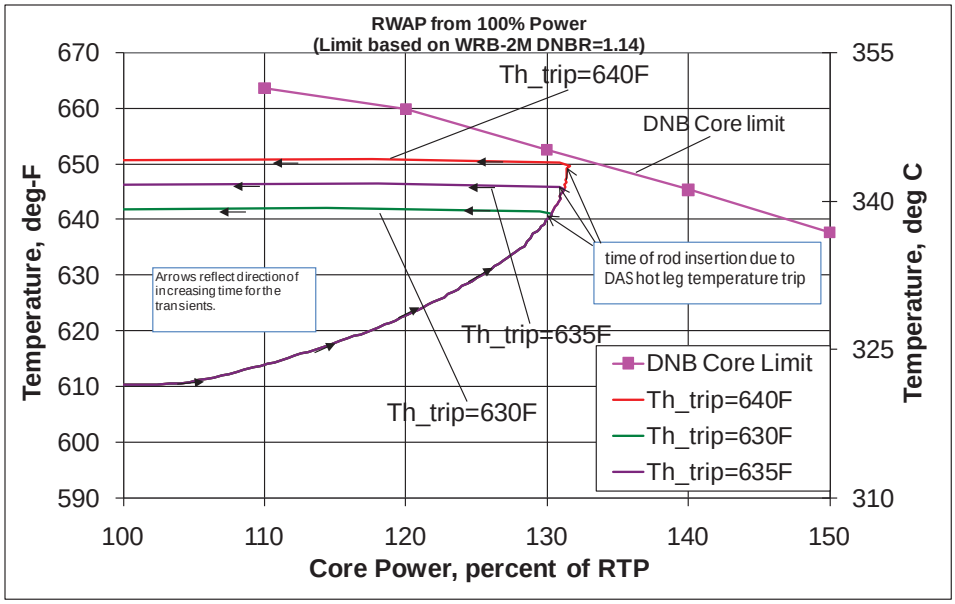


Figure 9.4.2-22. ATWT DNBR Limit for RWAP Diverse Mitigation Analysis from 100 Percent Power with Maximum Hypothetical Reactivity Insertion

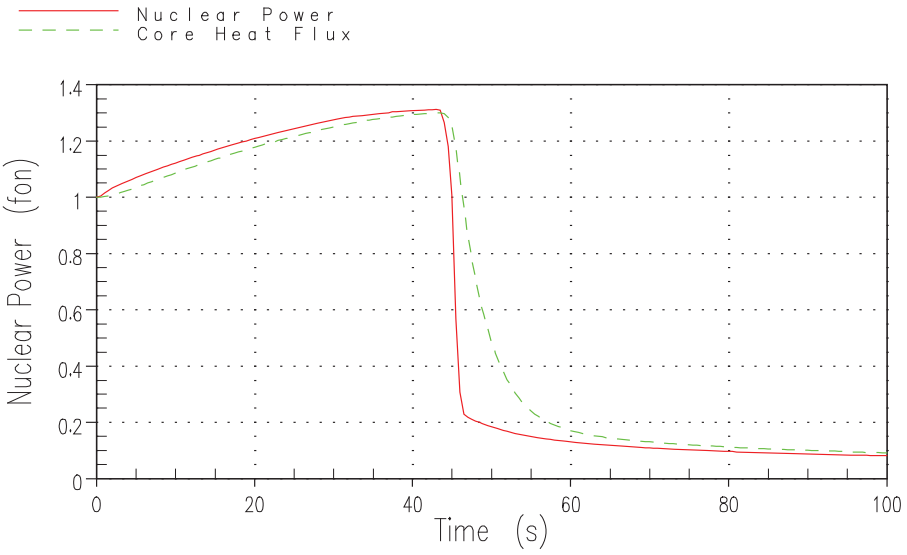


Figure 9.4.2-23. ATWT Nuclear Power for RWAP Diverse Mitigation Analysis from 100 Percent Power with Maximum Hypothetical Reactivity Insertion

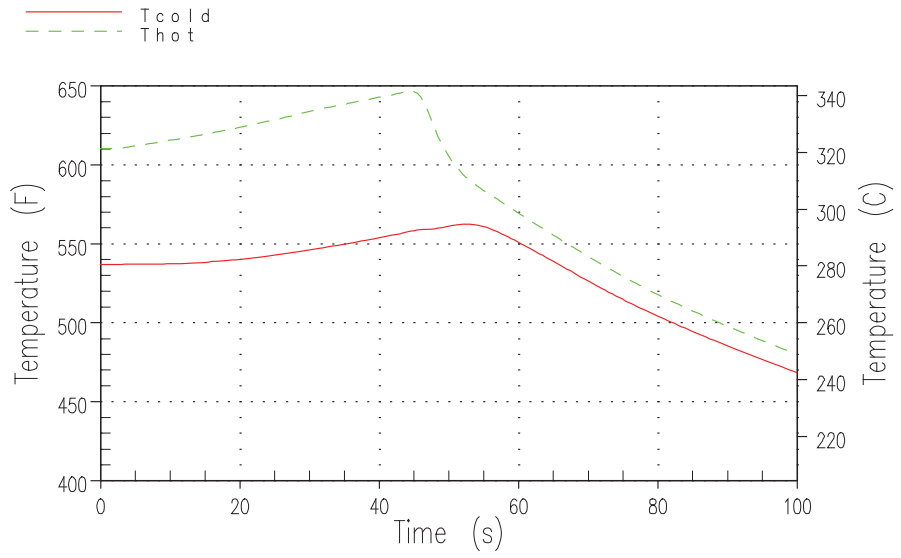


Figure 9.4.2-24. ATWT RCS Loop Temperatures for RWAP Diverse Mitigation Analysis from 100 Percent Power with Maximum Hypothetical Reactivity Insertion

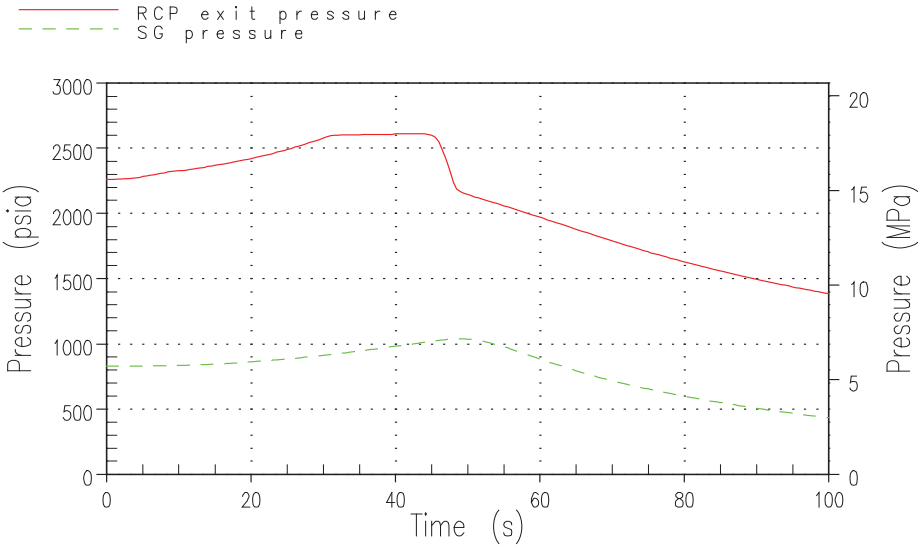


Figure 9.4.2-25. ATWT RCS and Secondary Pressure for RWAP Diverse Mitigation Analysis from 100 Percent Power with Maximum Hypothetical Reactivity Insertion

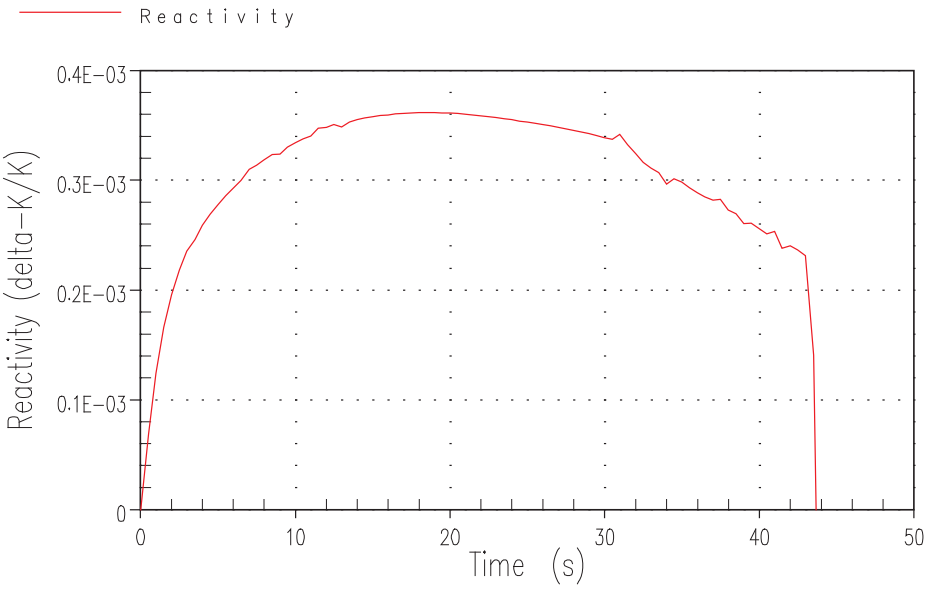


Figure 9.4.2-26. ATWT Core Reactivity for RWAP Diverse Mitigation Analysis from 100 Percent Power with Maximum Hypothetical Reactivity Insertion

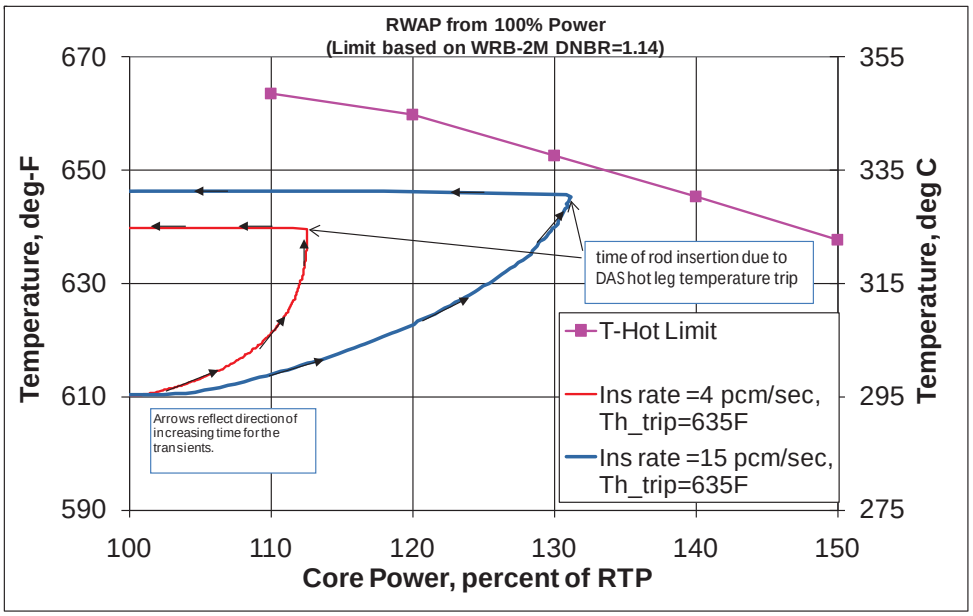


Figure 9.4.2-27. ATWT DNBR Limit for RWAP Diverse Mitigation Analysis 100 Percent Power with Realistic Reactivity Insertion

Figure 9.4.2-28. Not Used

Figure 9.4.2-29. Not Used

Figure 9.4.2-30. Not Used

Figure 9.4.2-31. Not Used

Figure 9.4.2-32. Not Used

Figure 9.4.2-33. Not Used

Figure 9.4.2-34. Not Used

Figure 9.4.2-35. Not Used

Figure 9.4.2-36. Not Used

Figure 9.4.2-37. Not Used

Figure 9.4.2-38. Not Used

Figure 9.4.2-39. Not Used

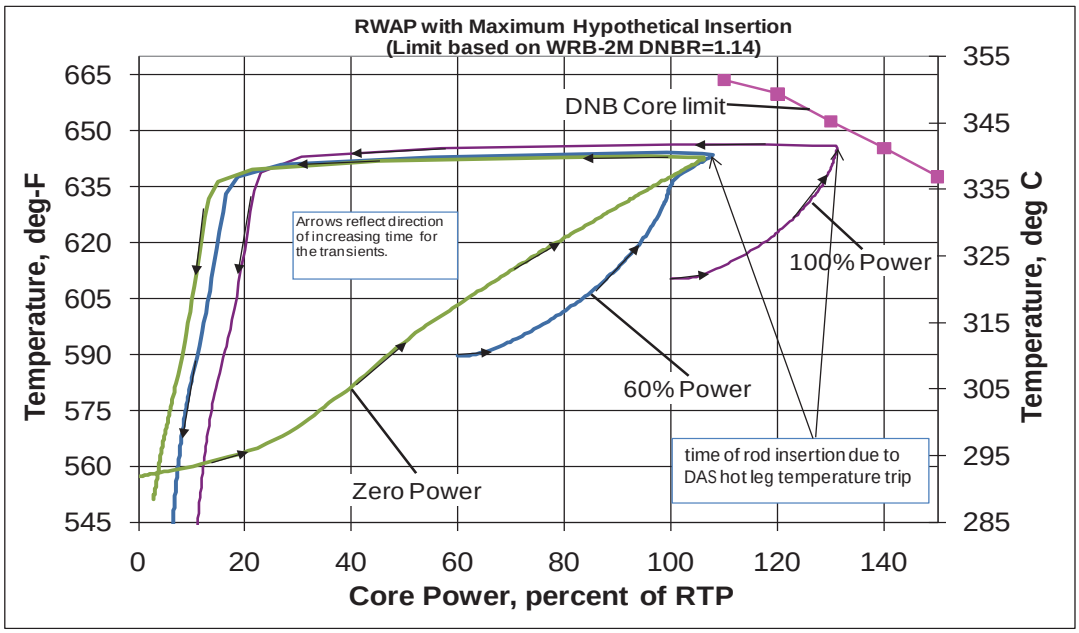


Figure 9.4.2-40. ATWT DNB Margin Impact for RWAP Diverse Mitigation Analysis versus Initial Power with maximum Hypothetical Reactivity Insertion

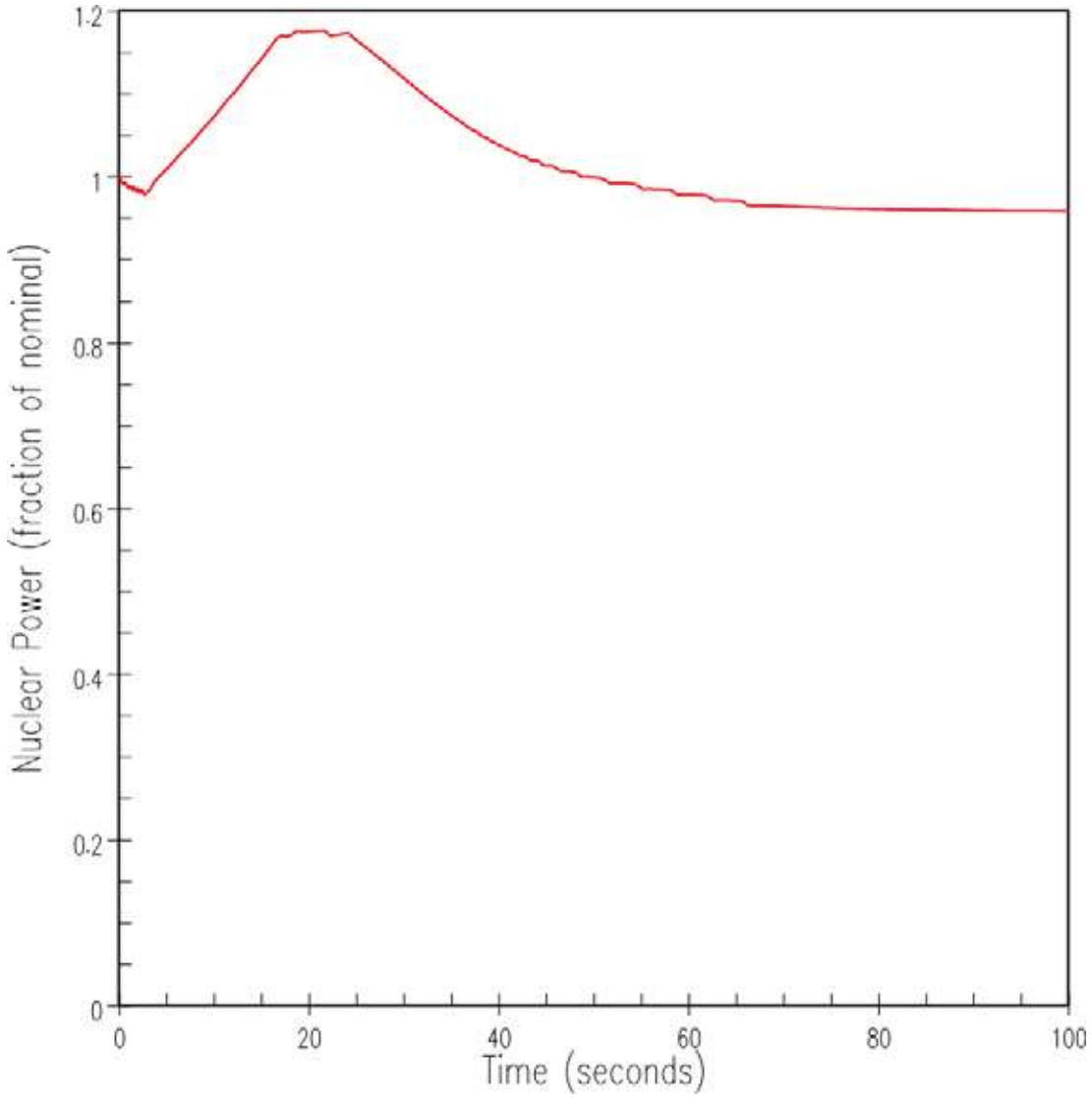


Figure 9.4.3-1. DBA Nuclear Power Transient for Dropped RCCA

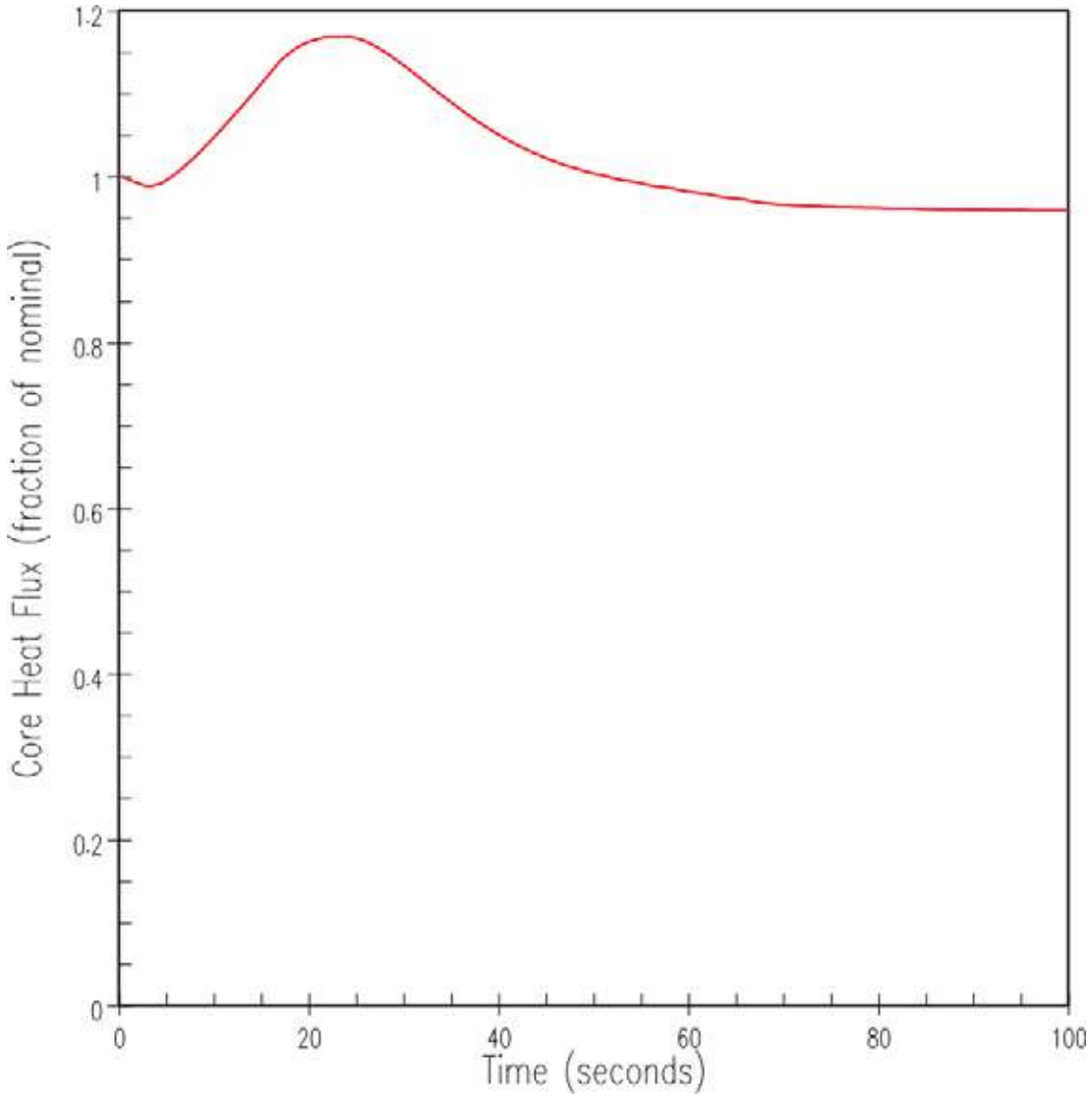


Figure 9.4.3-2. DBA Core Heat Flux Transient for Dropped RCCA

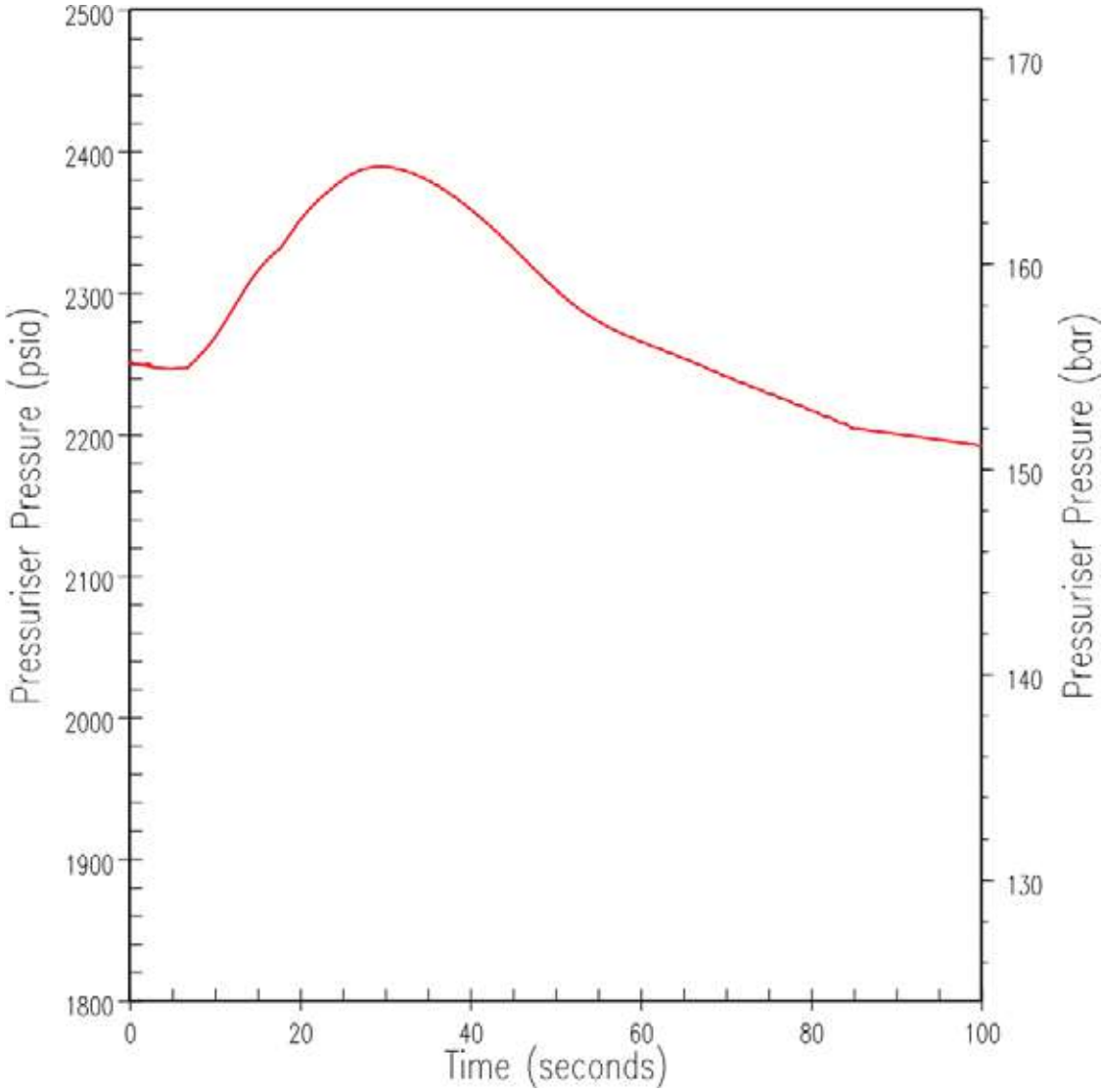


Figure 9.4.3-3. DBA Pressuriser Pressure Transient for Dropped RCCA

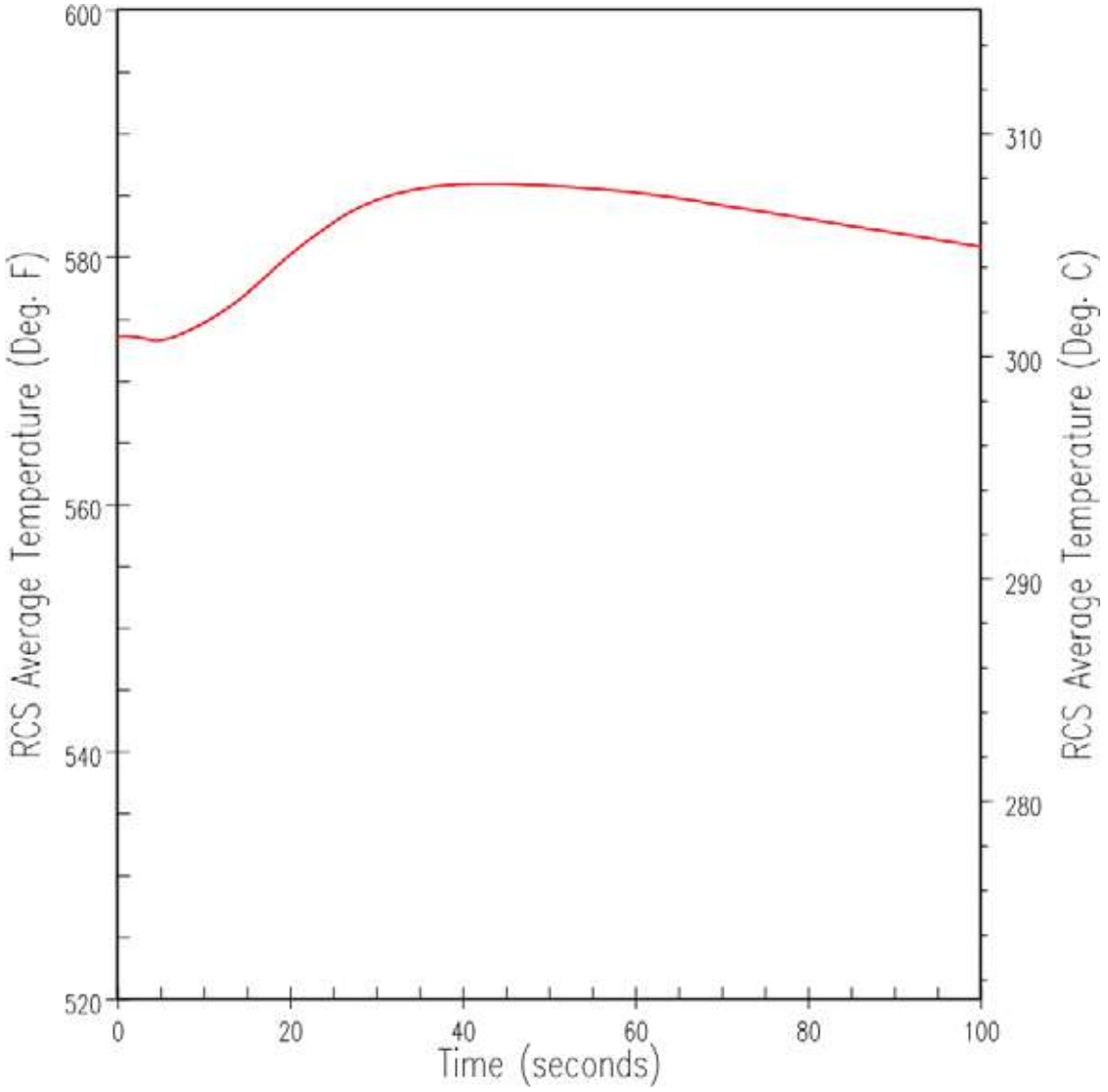


Figure 9.4.3-4. DBA RCS Average Temperature Transient for Dropped RCCA

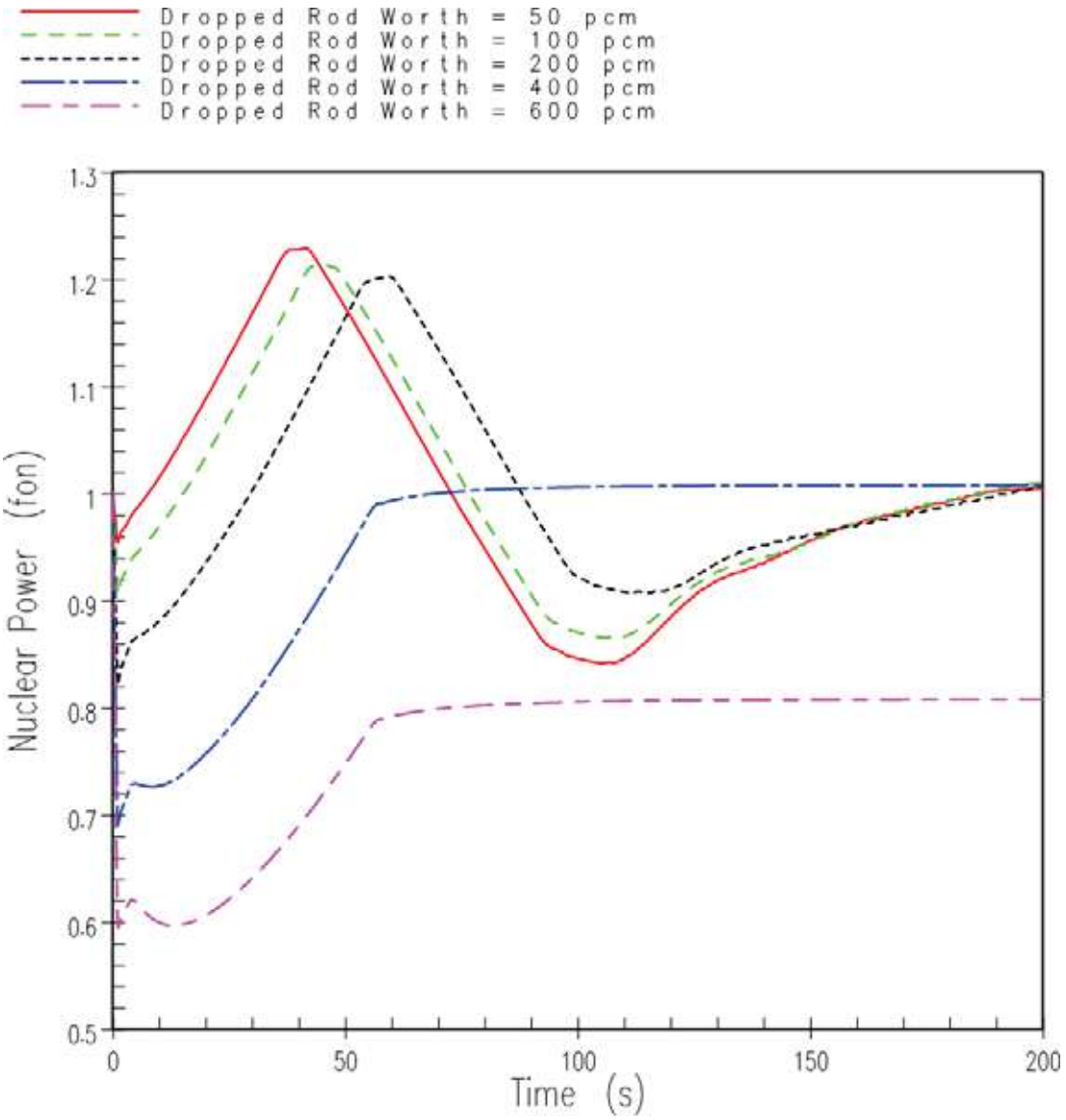


Figure 9.4.3-5. ATWT Nuclear Power Transient for Dropped RCCA

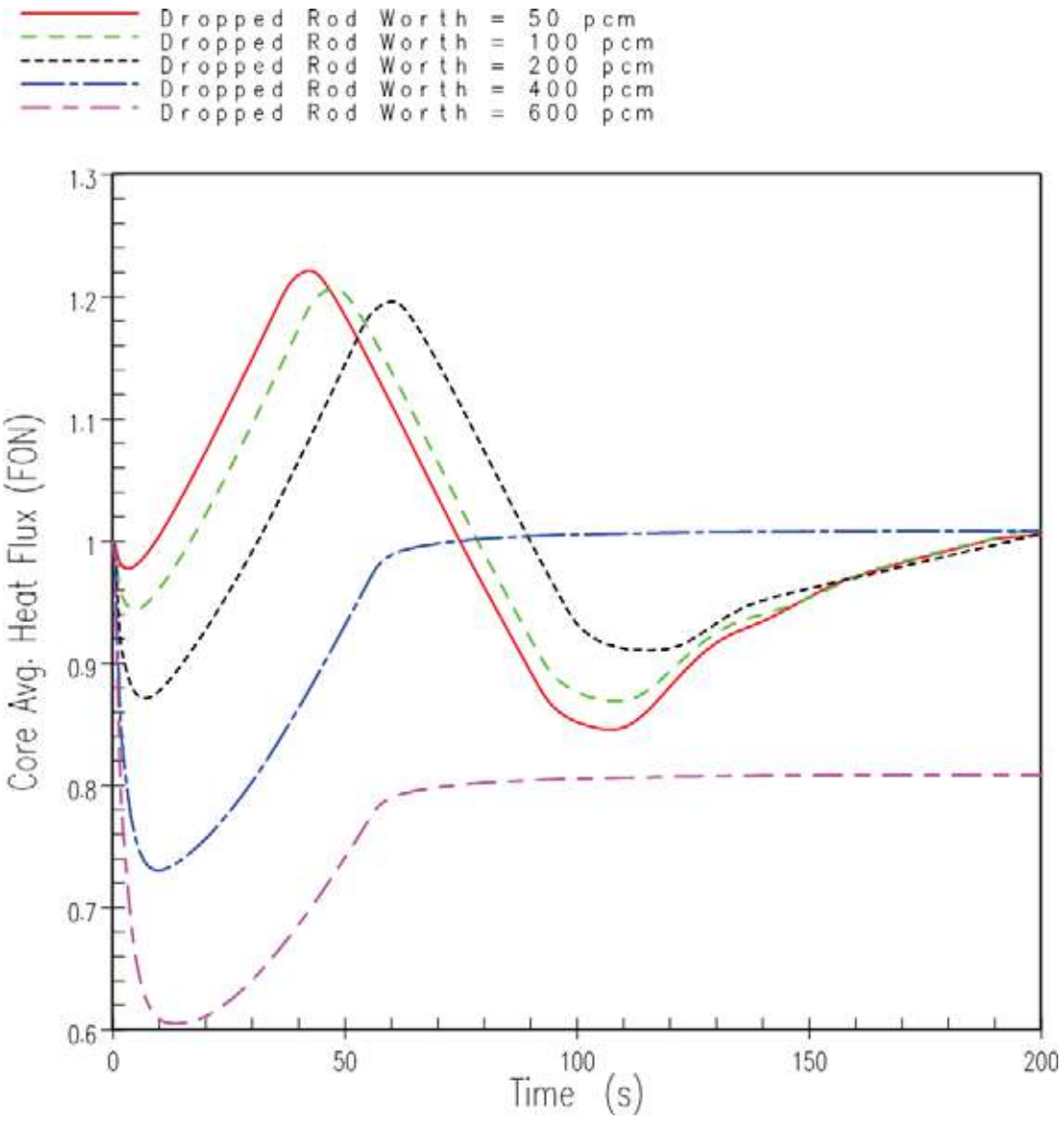


Figure 9.4.3-6. ATWT Core Heat Flux Transient for Dropped RCCA

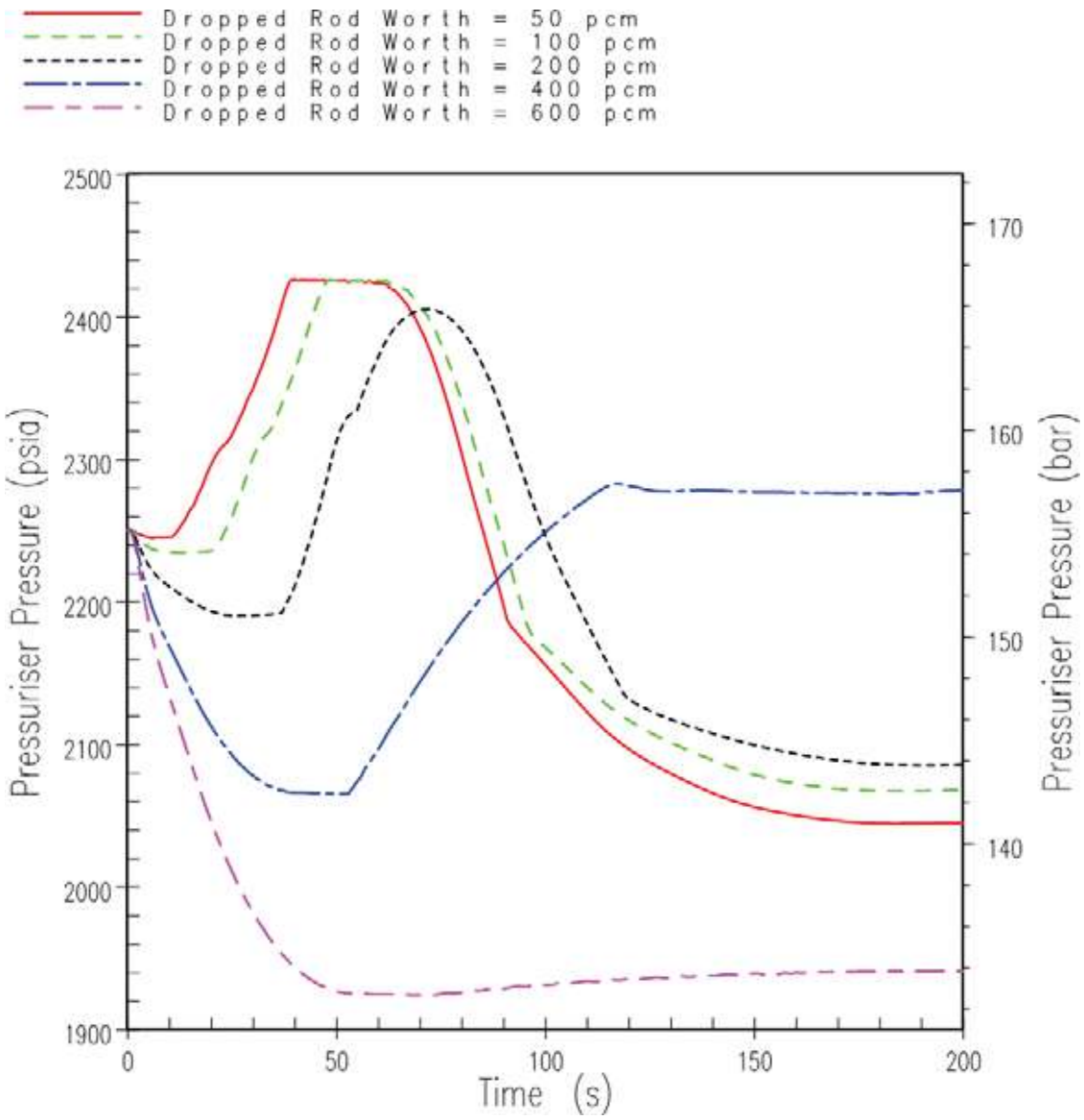


Figure 9.4.3-7. ATWT Pressuriser Pressure Transient for Dropped RCCA

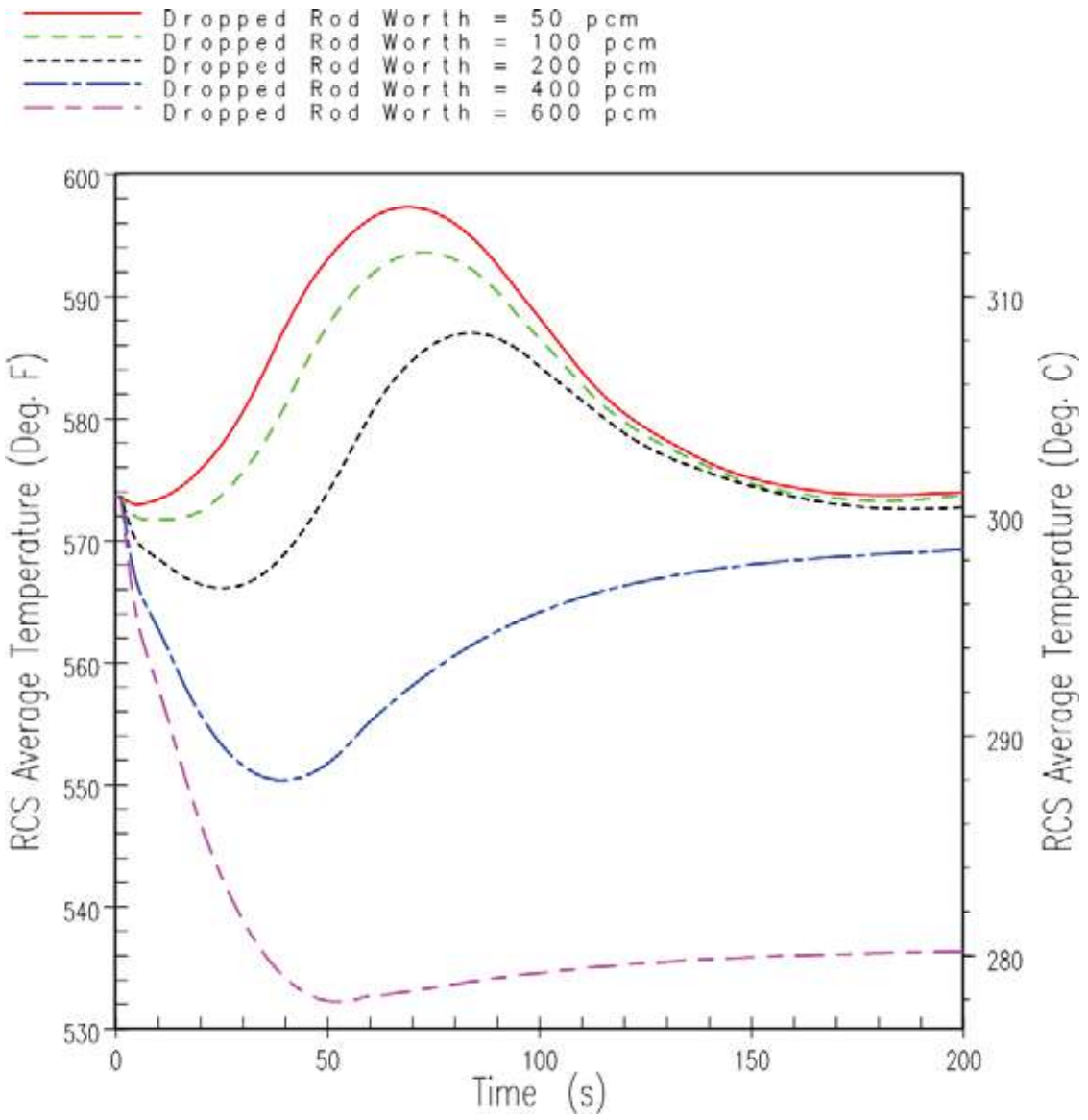


Figure 9.4.3-8. ATWT RCS Average Temperature Transient for Dropped RCCA

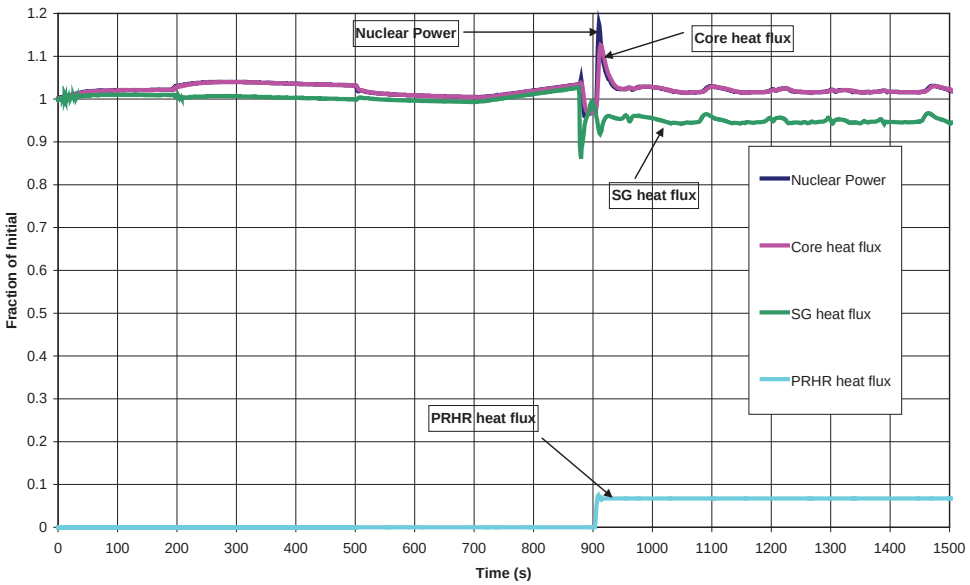


Figure 9.4.6-1. ATWT Power and Heat Transfer for a Boron Dilution with a RCCA Mechanical CCF in Manual Rod Control

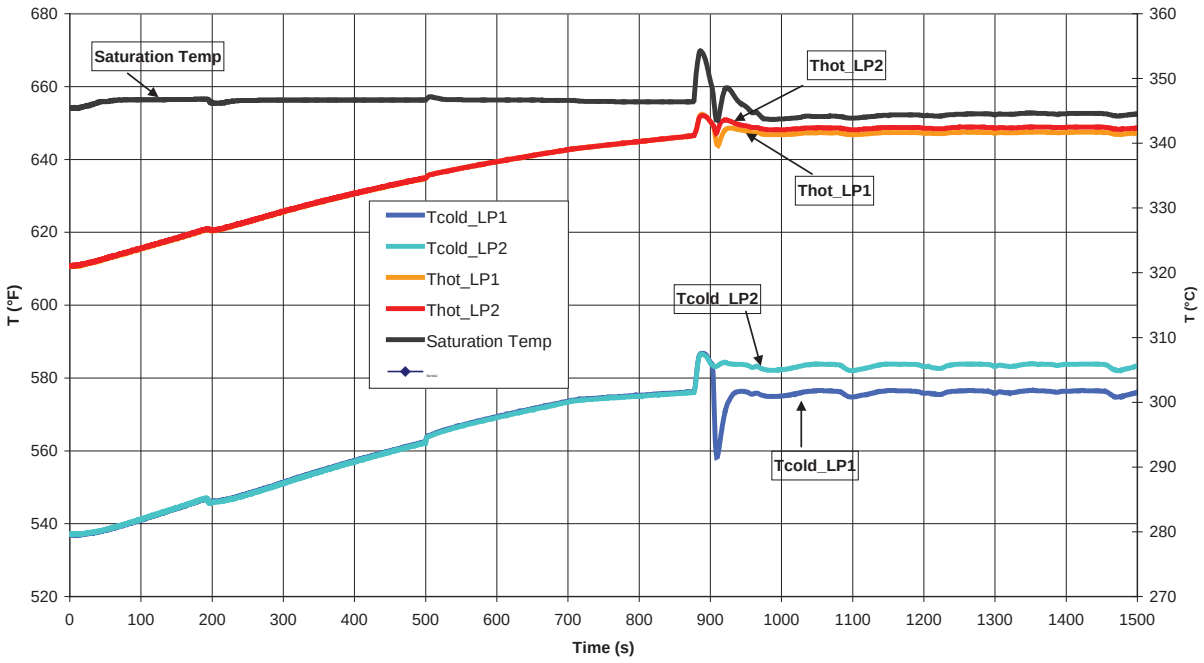


Figure 9.4.6-2. ATWT Primary Loop Temperatures for a Boron Dilution with a RCCA Mechanical CCF in Manual Rod Control

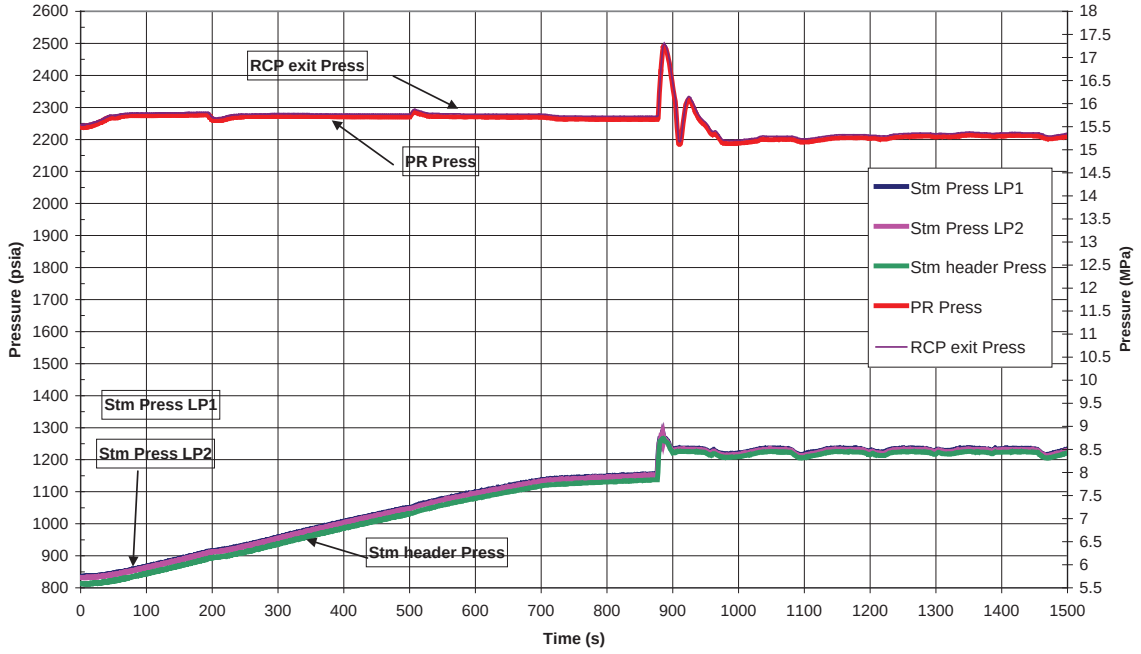


Figure 9.4.6-3. ATWT Primary and Secondary System Pressures for a Boron Dilution with a RCCA Mechanical CCF in Manual Rod Control

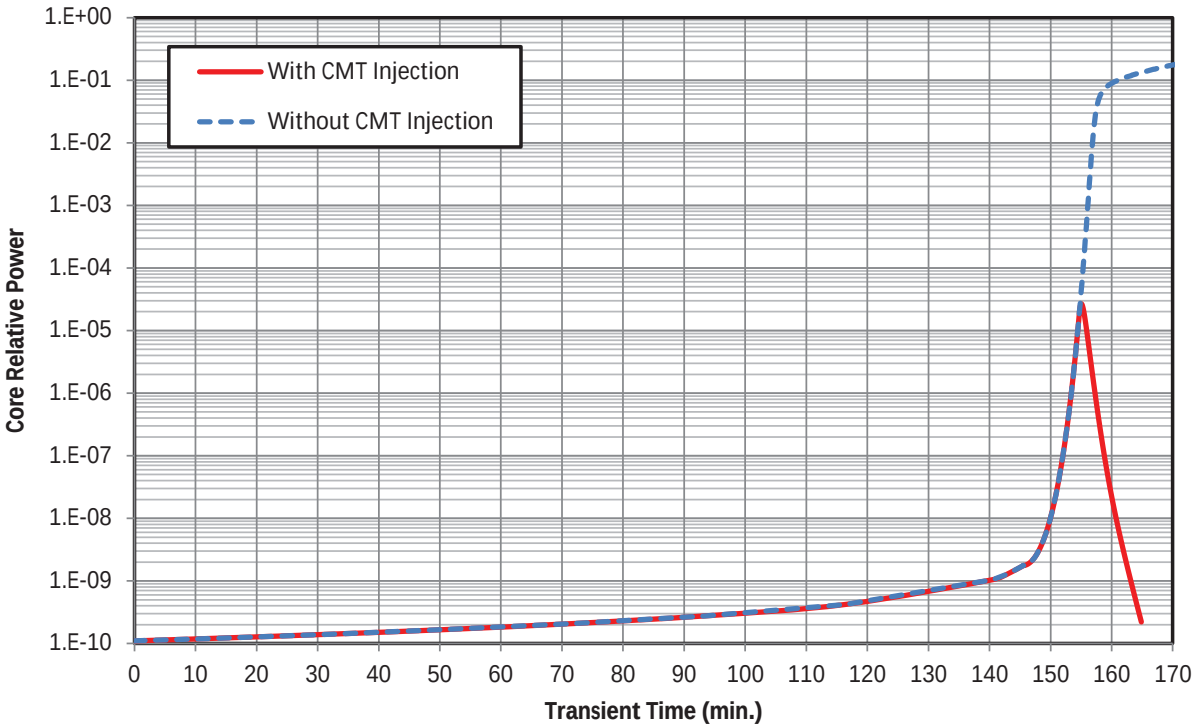


Figure 9.4.6-4. Diverse Boron Dilution at Shutdown Simulation for the Beginning of Cycle 1

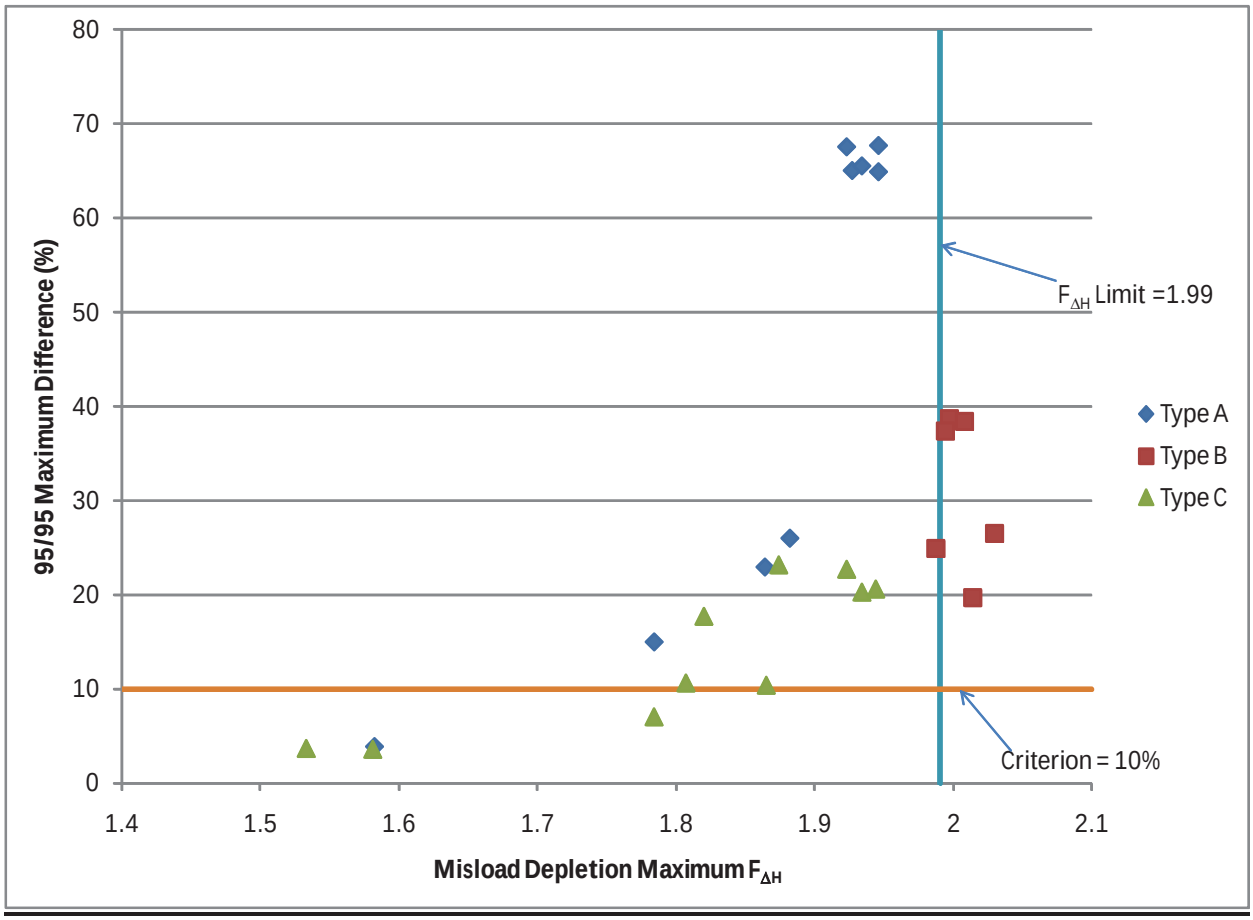


Figure 9.4.7-1. Detectability Assessments at the 30% Power Startup Condition as a Function of Misload Type and Misload Maximum $F_{\Delta H}$

	R	P	N	M	L	K	J	H	G	F	E	D	C	B	A
1							-0.7	-0.6	-0.7						
2					-0.5	-0.2	0.0	0.1	0.3	0.4	0.4				
3				-0.6	-0.4	0.1	0.4	0.8	1.1	1.2	1.0	0.9			
4			-0.8	-0.6	-0.2	0.2	0.7	1.1	1.4	1.4	1.4	1.1	1.0		
5		-1.0	-0.8	-0.4	0.0	0.6	1.4	1.8	1.9	2.1	1.9	1.5	1.2	0.8	
6		-0.9	-0.7	-0.2	0.3	1.2	3.5	6.5	7.5	6.7	3.9	1.9	1.4	1.0	
7	-1.3	-1.1	-0.8	-0.1	0.4	1.3	6.1	15.3	20.8	15.5	6.6	2.0	1.3	0.9	0.3
8	-1.3	-1.3	-1.0	-0.2	0.3	0.9	6.6	20.3	28.7	20.2	7.1	1.7	1.3	0.9	0.4
9	-1.6	-1.5	-1.3	-0.6	-0.3	0.4	4.9	13.9	19.2	14.1	5.4	1.2	0.7	0.5	0.1
10		-1.6	-1.6	-1.3	-1.1	-0.8	1.1	3.7	4.7	4.0	1.6	0.0	-0.1	-0.1	
11		-2.0	-2.1	-2.2	-2.4	-2.5	-2.6	-2.6	-2.6	-2.3	-2.0	-1.8	-1.4	-1.0	
12			-2.7	-3.2	-3.5	-4.0	-5.4	-7.0	-7.5	-6.8	-4.9	-3.3	-2.3		
13				-4.1	-4.4	-4.9	-8.0	-13.5	-16.7	-13.8	-8.1	-4.2			
14					-5.8	-6.7	-11.3	-20.6	-26.3	-21.3	-12.1				
15							-16.5	-25.2	-30.3						

FID Location.....%

High Reactivity Misload Location (Type A)

Low Reactivity Misload Location (Type A)

(Note: Misload locations are also FID locations.)

Difference = [(M-P)/P]*100%

Maximum 95/95 Measured vs. Predicted Difference (%)	25.2
Maximum 95/95 Symmetry Difference (%)	26.0
Misload Maximum Depletion $F_{\Delta H}$	1.882

Figure 9.4.7-2. Percent Difference between the Mean Measured and Predicted Power Distributions for an Assembly Swap Misload of Region E and Region D Fuel Assemblies at the 30% Power Startup Condition

	R	P	N	M	L	K	J	H	G	F	E	D	C	B	A
1							-3.2	-3.0	-3.2						
2					-3.3	-3.1	-3.1	-3.1	-3.2	-3.3	-3.7				
3				-3.1	-3.2	-3.1	-3.1	-3.1	-3.3	-3.5	-3.7	-3.9			
4			-3.0	-3.0	-3.0	-3.0	-3.0	-3.0	-3.2	-3.4	-3.6	-3.8	-5.1		
5		-3.0	-3.0	-2.9	-2.9	-2.8	-2.7	-2.7	-2.7	-2.9	-3.3	-3.8	-5.9	-10.5	
6		-2.9	-2.9	-2.9	-2.7	-2.6	-2.4	-2.1	-1.9	-2.0	-2.8	-4.5	-8.0	-13.6	
7	-2.9	-2.8	-2.8	-2.8	-2.6	-2.3	-1.8	-1.3	-0.6	-0.2	-1.2	-4.7	-10.6	-17.2	-23.7
8	-2.7	-2.7	-2.6	-2.6	-2.5	-1.9	-1.2	-0.4	1.5	3.9	4.5	0.6	-7.7	-16.2	-23.1
9	-2.8	-2.6	-2.6	-2.5	-2.1	-1.4	-0.6	0.5	3.8	9.7	14.5	13.3	5.2	-6.4	-16.6
10		-2.5	-2.5	-2.3	-1.8	-1.0	-0.2	1.1	5.0	13.5	21.9	24.9	19.8	7.7	
11		-2.6	-2.4	-2.1	-1.6	-0.8	0.1	1.5	5.2	12.0	19.6	24.7	23.5	15.0	
12			-2.3	-2.0	-1.4	-0.7	0.2	1.6	4.1	7.9	12.7	17.9	19.4		
13				-1.9	-1.4	-0.7	0.1	1.3	2.8	5.2	8.4	12.3			
14					-1.4	-0.7	0.1	1.0	2.3	4.3	6.7				
15							-0.1	0.9	1.9						

FID Location

High Reactivity Misload Location (Type B)

Low Reactivity Misload Location (Type B)

%Difference = [(M-P)/P]*100%

Maximum 95/95 Measured vs. Predicted Difference (%)	22.7
Maximum 95/95 Symmetry Difference (%)	25.0
Misload Maximum Depletion $F_{\Delta H}$	1.987

Figure 9.4.7-3. Percent Difference between the Mean Measured and Predicted Power Distributions for an Assembly Swap Misload of Region E and Region B Fuel Assemblies at the 30% Power Startup Condition

	R	P	N	M	L	K	J	H	G	F	E	D	C	B	A
1							-3.4	-3.2	-3.3						
2					-3.3	-3.1	-3.0	-2.9	-2.9	-2.9	-3.2				
3				-3.0	-2.9	-2.8	-2.7	-2.6	-2.7	-2.7	-2.9	-3.0			
4			-2.8	-2.8	-2.6	-2.5	-2.4	-2.3	-2.3	-2.4	-2.5	-2.7	-2.8		
5		-2.7	-2.6	-2.4	-2.1	-1.8	-1.6	-1.5	-1.5	-1.7	-2.0	-2.3	-2.5	-2.7	
6		-2.5	-2.3	-2.0	-1.3	-0.3	0.6	1.1	0.7	-0.2	-1.2	-1.9	-2.2	-2.3	
7	-2.5	-2.3	-2.1	-1.7	-0.2	2.2	4.6	5.6	4.7	2.3	-0.2	-1.6	-2.0	-2.1	-2.4
8	-2.2	-2.0	-1.8	-1.2	0.7	4.6	8.6	10.1	8.6	4.7	0.7	-1.2	-1.8	-2.0	-2.2
9	-2.1	-1.8	-1.6	-1.0	1.4	5.8	10.2	11.9	10.2	5.7	1.3	-1.0	-1.7	-1.9	-2.3
10		-1.6	-1.5	-0.9	1.2	5.1	9.0	10.4	8.9	5.0	1.1	-0.9	-1.4	-1.7	
11		-1.6	-1.5	-0.9	0.5	2.9	5.3	6.2	5.3	2.9	0.4	-0.9	-1.4	-1.7	
12			-1.4	-1.1	-0.3	0.7	1.5	1.9	1.5	0.6	-0.3	-1.1	-1.4		
13				-1.1	-0.8	-0.5	-0.4	-0.2	-0.3	-0.5	-0.9	-1.2			
14					-1.0	-0.7	-0.6	-0.6	-0.6	-0.7	-1.0				
15							-0.6	-0.4	-0.6						

FID Location
High Reactivity Misload Location (Type C)

%Difference = [(M-P)/P]*100%

Maximum 95/95 Measured vs. Predicted Difference (%)	10.3
Maximum 95/95 Symmetry Difference (%)	6.5
Misload Maximum Depletion FΔH	1.865

Figure 9.4.7-4. Percent Difference between the Mean Measured and Predicted Power Distributions for a Single Assembly Misload of a Region E Assembly for a Region D Assembly at the 30% Power Startup Condition

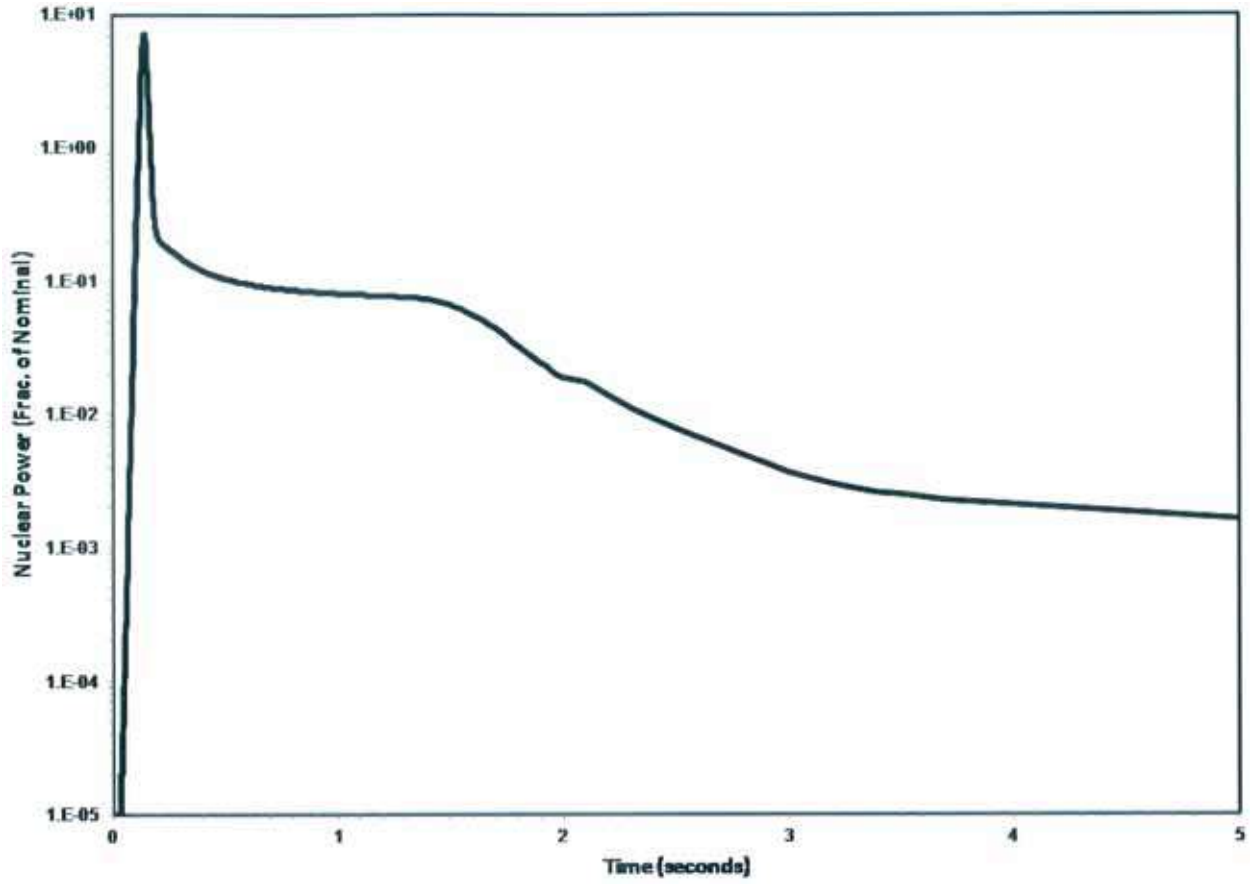


Figure 9.4.8-1. DBA Nuclear Power Transient Versus Time for the PCMI Rod Ejection Accident

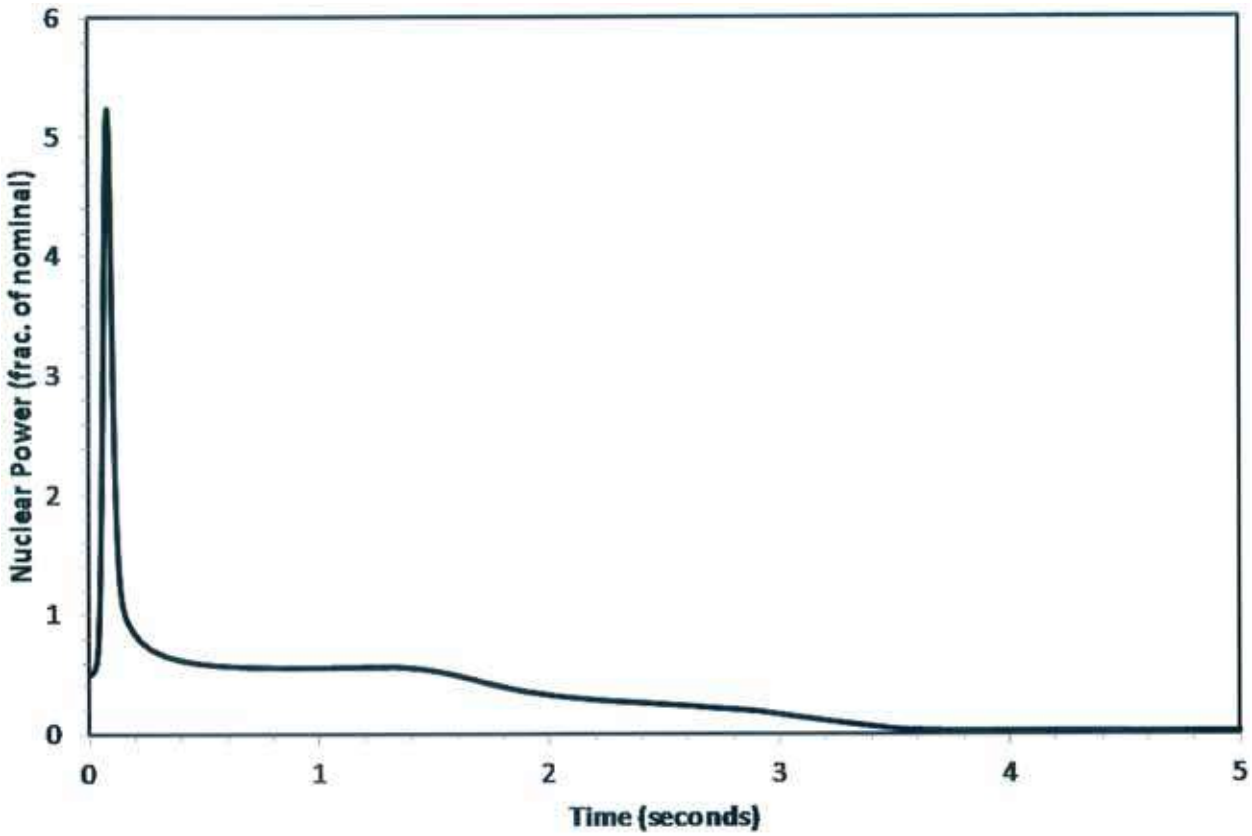


Figure 9.4.8-2. DBA Nuclear Power Transient Versus Time for the High Cladding Temperature Rod Ejection Accident

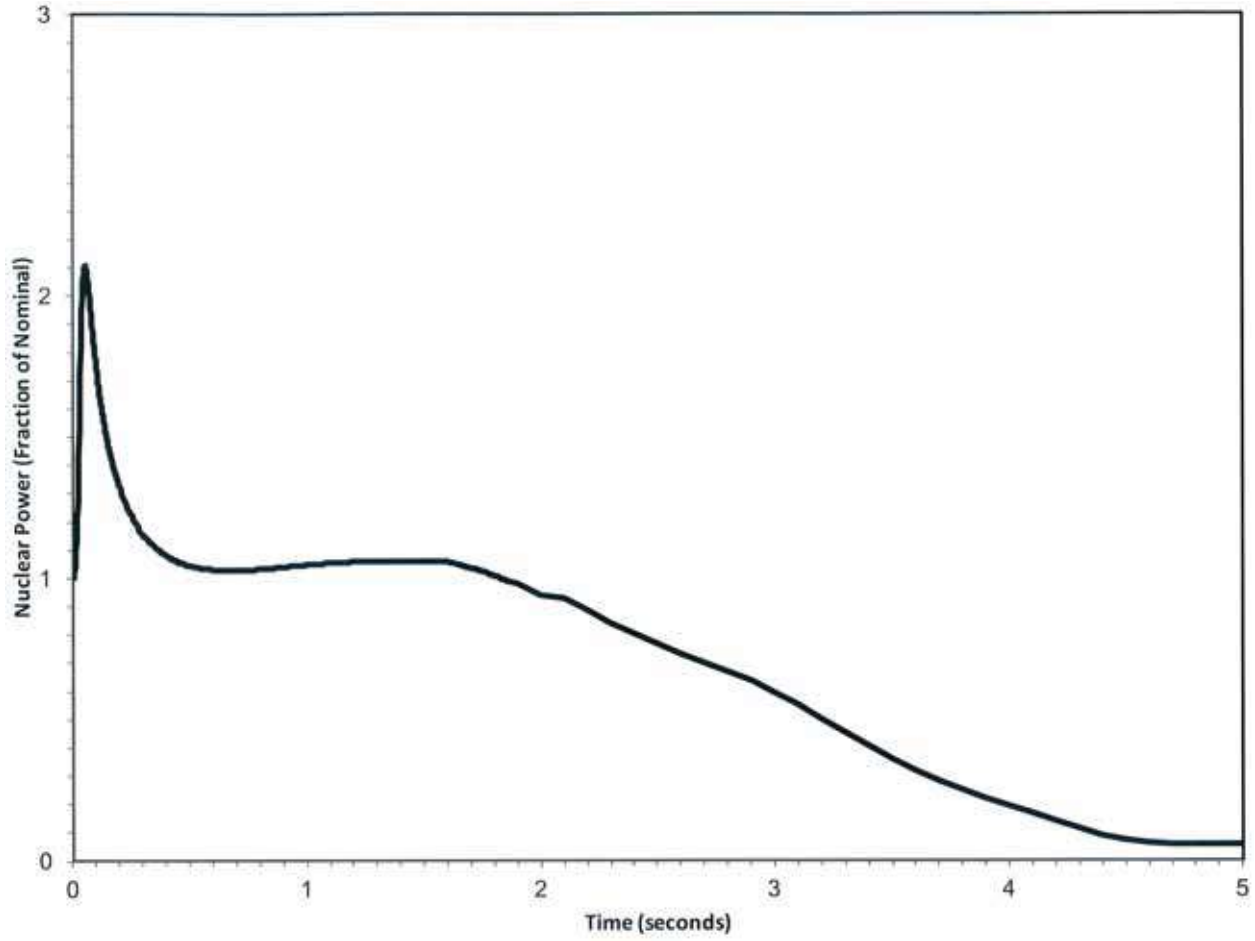


Figure 9.4.8-3. DBA Nuclear Power Transient Versus Time for the Peak Enthalpy and Fuel Centreline Temperature Rod Ejection Accident

9.5 Increase in Reactor Coolant System Water Inventory Faults

A number of faults that could result in an increase in reactor coolant inventory are postulated. The events are discussed in this section. Detailed analyses are presented for the most limiting of the primary system coolant increase events.

9.5.0 Introduction and Overview of Fault

This section addresses two faults:

- Inadvertent operation of a CMT
- CVS malfunction that increases reactor coolant inventory

The inadvertent operation of a CMT and the chemical and volume control system malfunction faults both lead to increases in the reactor coolant inventory and have similar plant responses. However, they are treated separately because the inadvertent operation of one of the CMTs means that, for this fault, only one CMT is available after the reactor has tripped.

Section 9.5 considers both faults in turn. Each fault is first described; the initiating event frequency and the design basis class are provided. The analysed faults are presented individually in Table 8A-2.

The analysed fault(s) are then described in additional detail in the subsequent sections to complete the safety case for each fault, including:

- Identification of Causes and Accident Description
- Design Basis Analysis of Effects and Consequences
- Assessment of the Radiological Consequences for the DBA
- Diverse Mitigation and ATWT for Frequent Faults
- ALARP Assessment
- Conclusions

ATWT analyses presented herein are based on Reference 9.5-3.

9.5.0.1 Inadvertent Operation of a Core Makeup Tank during Power Operation

Description

In this fault one CMT is inadvertently actuated while the reactor is operating at power.

Initiating Event Frequency[1]

The fault schedule in Appendix 8A indicates that this event is expected to have a frequency in the range of 0.1 to 0.01/yr, which makes the fault a frequent fault.

1. As discussed in Chapter 8, the frequency for initiating events from the PSA is used in both Chapters 8 and 9 with the sole purpose of supporting the categorisation of the fault to a specific DB category. As noted in Chapter 8, these probabilities should not be considered to be representative of actual frequency of the events, and for several events they can be significantly conservative. Detailed PSA results and their basis are discussed in Chapter 10 of this PCSR.

Design Basis Class

The unmitigated consequences of an inadvertent CMT actuation are assumed to be greater than the Target 4 BSL for frequent faults (1 mSv offsite and 20 mSv onsite). Given the IEF above, the event is in the DB2 class.

9.5.0.2 Chemical and Volume Control System Malfunction That Increases Reactor Coolant Inventory

Description

In this fault a CVS malfunction causes an increase of reactor coolant inventory at power.

Initiating Event Frequency[1]

The fault schedule in Appendix 8A indicates that this event is expected to have a frequency in the range of 0.1 to 0.01/yr, which makes the fault a frequent fault.

Design Basis Class

The unmitigated consequences of inadvertent actuation of the CVS are assumed to be greater than the Target 4 BSL for frequent faults (1 mSv offsite and 20 mSv onsite). Given the IEF above, the event is in the DB2 class.

9.5.1 Inadvertent Operation of a Core Makeup Tank During Power Operation (Fault 1.12.1)

9.5.1.1 Identification of the Causes and Accident Description

Spurious core makeup tank operation at power could be caused by an operator error, a false electrical actuation signal, or a valve malfunction. A spurious signal may originate from any of the safeguards ("S") actuation channels identified in Table 6-4. The AP1000 protection logic is such that a single failure cannot actuate both core makeup tanks without also actuating the PRHR heat exchanger. A scenario such as this is the spurious "S" signal event. However, if one core makeup tank is inadvertently actuated by a single failure, the event may progress with the plant at power until a reactor trip is reached. For the plant under automatic rod control, a reactor trip on High-3 pressuriser water level is expected to occur followed by the PRHR actuation and eventually by an "S" signal, which would then actuate the second core makeup tank. When a consequential loss of offsite power is assumed, this event is more conservative than the spurious "S" signal event.

The inadvertent opening of the core makeup tank discharge valves, due to operator error or valve failure, results in significant core makeup tank injection flow leading to a boration transient similar to that resulting from a chemical and volume control system malfunction event. If the automatic rod control system is operable, it will begin to withdraw rods from the core to counteract the reactivity effects of the boration. As a result, the core makeup tank will continue injection and slowly increase the pressuriser level until the High-2 pressuriser level setpoint is reached and continues until the High-3 pressuriser level reactor trip setpoint is reached. A loss of offsite power is assumed to occur as a consequence of the reactor trip. The primary effect of this assumption is the coastdown of the reactor coolant pumps. The core makeup tank injection will increase as the steam generator outlet temperature increases resulting in a lower density in the CMT balance line. This event will then proceed similarly to a spurious "S" signal or chemical and volume control system malfunction event. However, this event is more limiting primarily due to the higher pressuriser level at the time of reactor trip and to the significant heat up of the injected

fluid during the pre-trip phase of the accident. Thus, the inadvertent core makeup tank actuation event with a consequential loss of offsite power is analysed here.

Upon receipt of the High-3 pressuriser level reactor trip signal, the reactor is tripped; then the turbine is tripped after a 5-second delay and 3 seconds after turbine trip a consequential loss of offsite power is assumed. The basis for the 3-second delay is described in Section 9.0.12. The High-3 pressuriser level signal also actuates the PRHR heat exchanger and blocks the pressuriser heaters, but a 15-second delay is built in to prevent unnecessary actuation of the PRHR heat exchanger if offsite power is maintained.

Following reactor trip, the reactor power drops and the average reactor coolant system temperature decreases with subsequent coolant shrinkage, which avoids PRHR actuation immediately following the first High-3 pressuriser level trip signal. However, due to the assumed loss of offsite power, the reactor coolant cold leg temperature, in the loop without the PRHR, increases and the core makeup tank starts injecting cold water into the reactor coolant system at a much higher rate. The initial primary coolant system shrinkage is counteracted by the core makeup tank injection, and the pressuriser water volume starts to increase because of the heatup of the cold injected fluid by the decay heat. The High-3 pressuriser level setpoint is once again reached, and after a 15-second delay, the signal is sent to actuate the PRHR heat exchanger and block the pressuriser heaters.

The PRHR heat exchanger extracts heat from the reactor coolant system leading to an "S" signal on a Low-2 T_{cold} signal. The PRHR heat exchanger may inject asymmetrically into the steam generator outlet plenum such that a higher percentage of the PRHR flow is in one of two cold legs coming from the steam generator on the PRHR loop. To account for this, the analysis assumes that the Low T_{cold} setpoint is reached coincident with PRHR heat exchanger actuation. This actuates the second core makeup tank sooner in the transient, which is more limiting with respect to filling the pressuriser.

Both core makeup tanks inject mass into the reactor coolant system, and the pressuriser level continues to increase until the operators take action to end the pressuriser level increase transient. The operators are assumed to be alerted to a potential filling event on the High-2 pressuriser level signal, which occurs well before the reactor trip on the first of two High-3 pressuriser level signals. The operator action assumed in the analysis is to open the reactor vessel head vent following receipt of the second High-3 pressuriser level signal; this action is at least 30 minutes (45 minutes as analysed) after the operator has been alerted by the High-2 pressuriser level signal. When the head vent is opened, the pressuriser level increase slows and ultimately the level begins to decrease.

9.5.1.2 Design Basis Mitigation

Analysis is performed to demonstrate the adequacy of the PMS to detect and mitigate the fault and show that the safety analysis criteria are satisfied including:

- No fuel failures (confirmed using minimum DNBR and fuel melt criteria),
- The RCS pressure criterion is met,
- The MSS pressure criterion is met, and
- The pressuriser does not fill (which could result in a LOCA).

With respect to RCS and MSS overpressurisation and fuel failure criteria, this event is not limiting because cold, borated water is added to the RCS until the time of reactor trip, which produces a modest thermal transient without significant power excursion. Therefore, although these parameters are tracked, the primary acceptance criterion is precluding pressuriser overfill or, if

overfill would occur, to ensure that the operators have enough time to take corrective action to prevent it.

9.5.1.2.1 DBA Method of Analysis

The plant response to an inadvertent core makeup tank actuation is analysed by using a modified version of the computer program LOFTRAN (References 9.5-1 and 9.5-2) described in Section 9.0.9.2. The code simulates the neutron kinetics, reactor coolant system, pressuriser, pressuriser safety valves, pressuriser spray, steam generator, steam generator safety valves, PRHR heat exchanger, and core makeup tanks. The program computes pertinent plant variables, including temperatures, pressures, and power level.

As noted previously, with respect to RCS and main steam system overpressurisation and minimum DNBR, this event is not limiting. Therefore, the DB analysis is structured to maximize the risk of pressuriser filling. Core makeup tank and PRHR system performance is conservatively simulated. Core makeup tank enthalpies have been maximised. This is conservative because it minimizes the cooling provided by the core makeup tanks as flow recirculates and thereby increases the peak pressuriser water volume during the transient. Core makeup tank injection and balance lines pressure drop is minimized. This maximises the core makeup tank flow injected in the primary system. During this event, the core makeup tanks remain filled with water. The volume of injection flow leaving the core makeup tanks is offset by an equal volume of recirculation flow that enters the core makeup tanks via the balance lines. PRHR heat transfer capability has been minimized.

Plant characteristics and initial conditions are further discussed in Section 9.0.2.

- Initial operating conditions

  The initial reactor power is assumed to be 101 percent of nominal. The initial pressuriser pressure is assumed to be 0.345 MPa (50 psi) below nominal. The initial reactor coolant system average temperature is assumed to be 4.4°C (8°F) below nominal.

- Control systems

  The pressuriser spray system and automatic rod control system are conservatively assumed to operate. The pressuriser heaters are automatically blocked on a High-3 pressuriser level signal, so they cannot add heat to the system during the period of thermal expansion that produces the peak pressuriser water volume. Thus, the pressuriser heaters are assumed to be inoperable during this event. Other control systems are conservatively not assumed to function during the transient.

- Moderator and Doppler coefficients of reactivity

  A least-negative moderator temperature coefficient, a low (absolute value) Doppler power coefficient, and a minimum boron worth are assumed. With these minimum feedback parameters and the operability of the pressuriser spray system and automatic rod control system assumed, the reactivity effects of the boron injection from the core makeup tanks is counteracted. As a result, the High-3 pressuriser level signal is the first reactor trip signal generated during the transient.

- Boron injection

  The transient is initiated by an inadvertent opening of the discharge valves of one of the two core makeup tanks. The core makeup tank injects 3400 ppm borated water.

- Protection and safety monitoring system actuations

  The operators are assumed to be alerted to the pressuriser level increase transient by the High-2 pressuriser level signal. Reactor trip is initiated by the first of two High-3 pressuriser level signals. The second High-3 pressuriser level signal triggers the operators to open the reactor vessel head vent; this action is verified to be at least 30 minutes after the operator has been alerted by the High-2 pressuriser level signal.

  The PRHR heat exchanger is automatically actuated on second instance of the High-3 pressuriser level signal, which occurs after the reactor trip. The core decay heat is removed by the PRHR heat exchanger. The worst single failure is assumed to occur in the outlet line of the PRHR heat exchanger. One of the two parallel isolation valves is assumed to fail to open.

9.5.1.2.2 DBA Credited SSCs

For the DB, all claimed SSCs are Class 1. The claimed Class 1 SSCs are listed in Table 9.0-10. The primary core cooling is provided by the PRHR and passive containment cooling. Other SSCs include the CMTs, containment isolation, pressuriser SVs and reactor vessel head vent valves. The PMS provides the following

- RT on High-3 pressuriser water level
- PRHR actuation on High-3 pressuriser water level
- 2nd CMT and containment isolation on Low-2 CL temperature
- Manual head vent valve operation on High-2 pressuriser level
- PCS on High-2 containment pressure

9.5.1.2.3 DBA Results

The calculated sequence of events is shown in Table 9.5-1.

Figures 9.5.1-1 through 9.5.1-8 show the transient response to the inadvertent operation of one of the two core makeup tanks during power operation. The inadvertent opening of the core makeup tank discharge valves occurs at 10 seconds. As the core makeup tank continues to add inventory to the primary system, the pressuriser level begins to increase until the High-2 pressuriser level setpoint is reached (at 556.1 seconds) and continues until the High-3 pressuriser level reactor trip setpoint is reached at 2,589.3 seconds. After a 2-second delay, the neutron flux starts decreasing due to the reactor trip, which is followed by turbine trip after a 5-second turbine trip delay. Following reactor trip, the reactor power drops and the average reactor coolant system temperature decreases with subsequent coolant shrinkage. Due to the assumed loss of offsite power, the reactor coolant pumps trip at 2,599.3 seconds. The cold leg temperature increases and the core makeup tank starts injecting cold water into the reactor coolant system at a higher rate due to the increased driving head resulting from the density decrease in the balance line and due to the reduced pressure drop between the cold leg and the injection line connection on the reactor vessel

following the trip of the reactor coolant pumps. The post-trip primary coolant system shrinkage is counteracted by the core makeup tank injection, and the pressuriser water volume starts to increase because of the heatup of the cold injected fluid by the decay heat. The High-3 pressuriser level setpoint is once again reached at 2,736.6 seconds, and after a 15-second delay, the signal is sent to actuate the PRHR heat exchanger and block the pressuriser heaters. Following a conservative 17-second delay, the valves are assumed to open to actuate the PRHR heat exchanger at 2,768.6 seconds.

If the PRHR heat exchanger coolant asymmetrically injects into the steam generator outlet plenum, then one cold leg could reach the Low-2 T_{cold} "S" setpoint more quickly than if the flow were split evenly. To conservatively account for this effect, the Low-2 T_{cold} "S" signal is modelled to actuate simultaneously with the actuation of the PRHR heat exchanger (at 2,768.6 seconds). The Low-2 T_{cold} "S" signal activates the second core makeup tank, which then begins injecting additional mass into the reactor coolant system. Previous analyses have demonstrated that a more limiting pressuriser fill transient is calculated the earlier the second core makeup tank is actuated.

As the second core makeup tank begins injecting, the pressuriser level continues to increase. The operators are assumed to be alerted by the High-2 pressuriser level signal (at 556.1 seconds) that a pressuriser level increase transient is underway, and it is assumed that the operators are ready to take corrective action at least 30 minutes later. In this analysis, since pressuriser level continues to increase, the High-3 pressuriser level reactor trip setpoint is reached within this time. The operator action assumed in this case is to open the reactor vessel head vent to preclude pressuriser overfill following receipt of the second High-3 pressuriser level signal (at 3,256.1 seconds); this action is at least 30 minutes (45 minutes as analysed) after the operator has been alerted by the High-2 pressuriser level signal.

The safety-related reactor vessel head vent is opened by the operators, and the pressuriser water level increase slows and eventually the level begins to decrease. This demonstrates that the capacity of the reactor vessel head vent is sufficient to preclude pressuriser overfill as a result of an inadvertent actuation of a core makeup tank.

During the event, the DNBR never drops significantly below the initial value due to the addition of highly borated water from the core makeup tanks to the reactor coolant system. At the time of reactor trip, core power and heat flux drop rapidly and the DNBR is well above the design limit value defined in Section 22.7.1.1. The analysis demonstrates that no reactor coolant system overpressurisation occurs.

As noted above, the limiting case presented here models explicit operator action 45 minutes after receipt of the High-2 pressuriser level signal and demonstrates that pressuriser filling is precluded. For pressuriser level increase events, the operator would take action to reduce the increase in coolant inventory. As the pressuriser water level would increase above the high pressuriser water level that normally isolates chemical and volume control system makeup (High-2), the normal letdown line could be placed into service to reduce the increase in coolant inventory. If letdown could not be placed into service, the operator could use the safety related reactor vessel head vent valves to reduce the increase in coolant inventory (this is explicitly modelled in the case presented here). For these events, following the procedures outlined in the Emergency Response Guidelines AFR-I.1, there is sufficient time for the operator to mitigate the consequences of this event and anticipate operator action upon receipt of the second High-3 pressuriser level signal.

Appendix 9C provides discussion and analysis of long term safe shutdown for non-LOCA events.

9.5.1.3 Diverse Mitigation

In addition to the Class 1 passive systems credited in the DBA, the plant also provides diverse mitigation capability that is able to supply the Category A safety functions for frequent faults. The diverse features are also Class 1 except for the C&I, which is Class 2.

The diverse core cooling is provided by passive feed and bleed using PXS injection and ADS venting (Class 1). The DAS provides diverse reactor trip and safety system actuation (Class 2).

Table 9.5-2 summarizes the SSCs from this fault assessment. As this is a frequent fault, a diverse means of providing the Category A safety functions is provided. The information provided in Table 9.5-2 is from Reference 9.5-4, which documents the diversity for the frequent faults and provides additional information on the diverse mitigation functions. Table 9.5-3 provides the operator actions utilized in the diverse safety case.

9.5.1.3.1 Diverse Mitigation for ATWT

Inadvertent operation of a CMT involves trip of the RCPs and opening of the CMT discharge valves.

If the CMT discharge valves are opened without RCP trip, then the pressure gradients will prevent flow through the CMT. A check valve in the CMT discharge line prevents reverse flow. There will be no impact on the NSSS operating conditions. In the long term, possible valve leakage in the check valves may flush out the CMT very slowly, leading to increased boron concentration in the RCS, and the need to dilute to limit control rod motion. Since this would occur over many hours or days, there is ample time for operators to respond to the incorrect CMT discharge valve position.

If the RCPs are tripped (but the control rods are not tripped), the resulting transient is addressed as a loss of RCS flow in Section 9.3.2.3.1.

Therefore, no separate analysis or evaluation is provided in this section.

9.5.1.3.2 Diverse Mitigation for Core Cooling

The loss of normal feedwater diverse core cooling, as analysed in Section 9.2.7.3.2, was determined to be bounding of all non-LOCA events.

9.5.1.4 Radiological Consequences

Design Basis

In the case where offsite power remains available, there is no release of activity to the environment and the Target 4 BSOs (0.01 mSv offsite and 0.1 mSv onsite) are met.

In the case where offsite power is lost, a small release of activity may occur as a result of steam dump to the atmosphere due to unavailability of the condensers. With no fuel damage and primary and secondary circuits intact, the initiating event has no impact on the doses. The doses are a consequence of the assumed loss of offsite power. Therefore, the loss of offsite power doses from Section 9.2.6.4 are presented. The calculated maximum doses for all relevant pathways (inhalation, cloudshine, and groundshine) are as follows:

- Offsite dose: 0.05 mSv Worker dose: 1.5 mSv

These doses are within the Target 4 BSL for frequent faults (1 mSv offsite and 20 mSv onsite).

Diverse Mitigation

Both the diverse ATWT and diverse core cooling scenarios demonstrate that the RCS does not overpressurise and there is no significant fuel damage. For a diverse mitigation radiological consequences analysis better estimate assumptions would be credited. This would include reactor coolant system activity levels significantly lower than those modelled for the DBA and better activity retention in containment and in the steam generators. In addition better estimate atmospheric dispersion factors would be used. Therefore, a diverse mitigation radiological consequences analysis would show that the doses for the diverse ATWT scenario would be less than those reported for the non-LOCA DBAs and doses for the diverse core cooling scenario would be much less than for the design basis LOCA. The diverse mitigation analyses would not have to meet the Target 4 BSL for frequent faults and would meet the Target 4 BSL for infrequent faults.

9.5.1.5 As Low As Reasonably Practicable Assessment

For this event, the identification of the primary safety functions as Class 1 SSCs has been shown to be adequate to meet DB requirements.

The diverse mitigation functions, including other Class 1 safety functions and the DAS function, which is Class 2, is also shown by analysis to meet applicable requirements for the inadvertent operation of a CMT during power operation event. See Reference 9.5-4 for additional discussions on these diverse mitigation features.

Additionally, the AP1000 plant design has a third level of redundancy provided by the DiD systems. The applicable DiD functions include:

- CVS boration for long-term reactivity control
- CVS make-up for RCS inventory control
- SFW with steam dump for short-term decay heat removal
- RNS cooling of the RCS for long-term decay heat removal. The RNS requires support from the CCS and SWS cooling water systems.
- Control by the PLS C&I

The characteristics of the above features were compared to improvements that were evaluated for the RNS for its mitigation of cliff edge small LOCAs. First it should be recognized that in this situation the RNS provides the second level of defence for this event and is therefore more important than the above DiD features which provide a 3rd level of defence. The RNS improvements included making the RNS alignment and actuation automatic, increasing the RNS pump head, and adding a RNS suction supply tank that is separate from the Class 1 system. None of these potential improvements were found to be ALARP (See Section 9.1.4.5). However, the SFW and CVS already include characteristics similar to these proposed improvements. Another improvement that could be made to these DiD systems is to upgrade them to Class 1. This would be very expensive especially and would have wide reaching impacts to the design of SSCs; notable would be the impact on component and building design to address hazards including seismic and storm winds/missiles. Such a change would not be ALARP because the cost would be grossly disproportional to its benefit.

As discussed in Chapter 9.0.15, the AP1000 has incorporated ALARP thinking throughout its development. In addition, the current risk of a large radioactivity release is significantly less than the SAP Target 9 BSO (1E-7 pa). Considering the ALARP thinking that went into the AP1000

development, its low risk profile and the additional level of defence discussed above (including their performance characteristics), improving the Class 2 DiD to better remove decay heat or shutdown the reactor would be grossly disproportional to the risk reduction that might be achieved. As a result, the current design is considered ALARP.

9.5.1.6 Conclusions

The DB analysis demonstrates that inadvertent operation of a core makeup tank during power operation does not adversely affect the core, the reactor coolant system, or the steam system. The pressuriser does not fill; therefore, water is not relieved from the pressuriser safety valves. DNBR always remains above the design limit values, and reactor coolant system and steam generator pressures remain below 110 percent of their design values.

This event has also been adequately assessed with respect to ATWT considerations.

Diverse core cooling capabilities have been demonstrated.

DBA radiological consequences are within the Target 4 BSL for frequent faults (1 mSv offsite and 20 mSv onsite). Thus, the identification of necessary Class 1 SSCs is adequate to meet DB requirements.

It has been shown that the AP1000 plant design includes adequate systems for the protection of this fault, which limit the radiological consequences such that they are compliant with the SAP targets and the risks have been reduced to be ALARP.

9.5.2 Chemical and Volume Control System Malfunction That Increases Reactor Coolant Inventory (Fault 1.12.4)

9.5.2.1 Identification of Causes and Accident Description

An increase of reactor coolant inventory, which results from addition of cold unborated water to the reactor coolant system, is analysed in Section 9.4.6.

In this Section, the increase of reactor coolant system inventory due to the addition of borated water is analysed.

The increase of reactor coolant system coolant inventory may be due to the spurious operation of one or both of the chemical and volume control system pumps or by the closure of the letdown path. If the chemical and volume control system is injecting highly borated water into the reactor coolant system, the reactor experiences a negative reactivity excursion due to the injected boron, causing a decrease in reactor power and subsequent coolant shrinkage. The load decreases due to the effect of reduced steam pressure after the turbine control valve fully opens.

At high chemical and volume control system boron concentration, low reactivity feedback conditions, and reactor in manual rod control, an “S” signal will be generated by either the Low-2 T_{cold} or Low-2 steam line pressure setpoints before the chemical and volume control system can inject a significant amount of water into the reactor coolant system. In this case, the chemical and volume control system malfunction event proceeds similarly to, and is only slightly more limiting than, a spurious “S” signal event. If the automatic rod control is modelled and the pressuriser spray functions properly to prevent a high pressure reactor trip signal, no “S” signals are generated and this specific event is terminated by automatic isolation of the chemical and volume control system on the safety-related High-2 pressuriser level setpoint.

Under typical operating conditions for the AP1000, the boron concentration of the injected chemical and volume control system water is equal to that of the reactor coolant system. If the chemical and volume control system is functioning in this manner and the pressuriser spray system functions properly to prevent a high pressure reactor trip signal, no "S" signals are generated and this specific event is also terminated by automatic isolation of the chemical and volume control system on the safety-related High-2 pressuriser level setpoint.

While these scenarios are the most probable outcomes of a chemical and volume control system malfunction, several combinations of boron concentration, feedback conditions, and plant system interactions have been identified which can result in more limiting scenarios with respect to pressuriser overfill. The key factors that make this event more limiting than a spurious "S" signal event are that the reactor coolant system is at a lower average temperature, higher pressure, and a higher pressuriser level at the time an "S" signal is generated. These factors produce a greater volume of higher density water and, thus, a larger reactor coolant system mass at the time of the "S" signal. In addition, at lower reactor coolant system average temperature, the PRHR is less effective in removing decay heat, which results in greater expansion of the cold water injected by the core makeup tanks.

The limiting analysis scenario minimizes reactor coolant system average temperature, maximises reactor coolant system mass, and maximises pressuriser water volume at the time of an "S" signal. This scenario is as follows:

- Both of the chemical and volume control system pumps spuriously begin delivering flow at a boron concentration slightly higher than that of the reactor coolant system. (Assuming that a chemical and volume control system malfunction results in both chemical and volume control system pumps delivering flow is a conservative assumption. One chemical and volume control system pump is automatically controlled and one is manually controlled.)

- The non-safety-related pressuriser spray is assumed to be available, so that a High-2 pressuriser pressure reactor trip is prevented.

Due to the boron addition in the core, the plant cools down until an "S" signal is generated on Low-2 cold leg temperature. On the "S" signal, the reactor is tripped, the core makeup tank discharge valves are opened, the reactor coolant pumps are tripped, the pressuriser heaters are blocked, and the main feedwater lines, steam lines, and chemical and volume control system are isolated. After a conservative 17-second delay, the PRHR heat exchanger is actuated.

Normally, the reactor coolant pumps would be tripped 15 seconds after the receipt of the "S" signal. A loss of offsite power is assumed to occur as a consequence of reactor trip. The primary effect of this assumption is the coastdown of the reactor coolant pumps. Following reactor trip and a 5-second timer delay, the turbine is tripped. 3 seconds after a turbine trip a consequential loss of offsite power is assumed. The basis for the 3-second delay is described in Section 9.0.12. As a result, the reactor coolant pumps are conservatively assumed to trip about 10 seconds before they would otherwise trip due to the "S" signal.

9.5.2.2 Design Basis Mitigation

Analysis is performed to demonstrate the adequacy of the PMS to detect and mitigate the fault and show that the safety analysis criteria are satisfied including:

- No fuel failures (confirmed using minimum DNBR and fuel melt criteria),
- The RCS pressure criterion is met,
- The MSS pressure criterion is met, and
- The pressuriser does not fill (which could result in a LOCA).

With respect to RCS and MSS overpressurisation and fuel failure criteria, this event is not limiting because cold, borated water is added to the RCS until the time of reactor trip, which produces a modest thermal transient without significant power excursion. Therefore, although these parameters are tracked, the primary acceptance criterion is precluding pressuriser overfill or, if overfill would occur, to ensure that the operators have enough time to take corrective action.)

9.5.2.2.1 DBA Method of Analysis

The malfunction of the chemical and volume control system is analysed by using a modified version of the computer program LOFTRAN (Reference 9.5-1 and 9.5-2) described in Section 9.0.9.2. The code simulates the neutron kinetics, reactor coolant system, pressuriser, pressuriser safety valves, pressuriser spray, steam generator, steam generator safety valves, PRHR heat exchanger, and core makeup tanks. The program computes pertinent plant variables including temperatures, pressures, and power level.

Because of the power and temperature reduction during the transient, operating conditions do not approach the core limits. The analysis demonstrates that no reactor coolant system overpressurisation occurs.

The assumptions are as follows:

- Initial operating conditions

  The initial reactor power is assumed to be 101 percent of nominal. The initial pressuriser pressure is assumed to be 0.345 MPa (50 psi) above nominal. The initial reactor coolant system average temperature is assumed to be 4.4°C (40°F) above nominal.

- Moderator and Doppler coefficients of reactivity

  A least-negative moderator temperature coefficient, a low (absolute value) Doppler power coefficient, and a minimum boron worth are assumed. For a different set of reactivity feedback parameters, a different chemical and volume control system boron concentration can result in an identical transient.

- Reactor control

  Rod control is not modelled.

- Pressuriser heaters

  The pressuriser heaters are automatically blocked on an “S” signal, and do not add heat to the system during the period of fluid thermal expansion that produces the peak pressuriser water volume. Thus, the pressuriser heaters are assumed to be inoperable during this event.

- Pressuriser spray

  The spray system controls the pressuriser pressure so that a High-2 pressuriser pressure reactor trip is prevented.

- Boron injection

  After 10 seconds at steady state, the chemical and volume control system pumps start injecting borated water, which is slightly above the reactor coolant system boron

concentration. Upon receipt of an "S" signal, the core makeup tanks begin injecting 3400 ppm borated water. The chemical and volume control system pumps are isolated on a High-2 pressuriser level signal. In this analysis, the boron concentration of the chemical and volume control system is iterated upon until the High-2 pressuriser level and the Low T_{cold} "S" setpoint are reached at the same time. This begins core makeup tank injection when the chemical and volume control system pumps are isolated, which is conservative with respect to filling the pressuriser.

- Turbine load

  The turbine load is assumed constant until the turbine digital electrohydraulic control (D-EHC) drives the control valve wide open. Then the turbine load drops as steam pressure drops.

- Protection and safety monitoring system actuations

  If the automatic rod control system is modelled and the pressuriser spray system functions properly, no reactor trip signal is expected to occur. Instead, the event is terminated by automatic isolation of the chemical and volume control system on the safety grade high-2 pressuriser level setpoint. If the automatic rod control system is not active and the pressuriser spray system is assumed to be available, reactor trip may be initiated on either Low-2 T_{cold} "S" or a Low-2 steam line pressure "S" signal.

  The core decay heat is removed by the PRHR heat exchanger. The worst single failure is assumed to occur in the outlet line of the PRHR heat exchanger. One of the two parallel isolation valves is assumed to fail to open.

9.5.2.2.2 DBA Credited SSCs

For the DB, all claimed SSCs are Class 1. The claimed Class 1 SSCs are listed in Table 9.0-10. The primary core cooling is provided by the PRHR and passive containment cooling. Other SSCs include the CMTs, containment isolation, pressuriser SVs and reactor vessel head vent valves. The PMS provides the following:

- RT on Low-2 cold leg temperature (T_{cold}) "S" signal

- PRHR actuation on High-3 pressuriser water level

- CMTs and containment isolation on Low-2 CL temperature

- Manual head vent valve operation on High-2 pressuriser level

- PCS on High-2 containment pressure

9.5.2.2.3 DBA Results

The calculated sequence of events is shown in Table 9.5-1.

Figures 9.5.2-1 through 9.5.2-9 show the transient response to a chemical and volume control system malfunction that results in an increase of reactor coolant system inventory.

As the chemical and volume control system injection flow increases reactor coolant system inventory, pressuriser water volume begins increasing while the primary system is cooling down. A reactor trip is modelled to occur on the Low-2 T_{cold} "S" signal (conservatively modelled to occur simultaneously with High-2 pressuriser water level) at 2,270.8 seconds. Once the Low-2 T_{cold} setpoint is reached, the reactor trips on the resulting "S" signal, and the control rods start moving into the core. At the same time, the High-2 pressuriser level setpoint is reached and after a conservative delay, the chemical and volume control system injection is isolated.

The turbine is tripped as a result of the reactor trip following a 5-second turbine trip timer delay. After a 3-second delay following turbine trip, a consequential loss of offsite power is assumed and the reactor coolant pumps trip. The basis for the 3-second delay is described in Section 9.0.12. Soon after reactor trip, the pressuriser heaters are blocked and the main feedwater lines, steam lines, and chemical and volume control system are isolated. After a conservative 17-second delay, the PRHR heat exchanger is actuated and the core makeup tank discharge valves are opened. The core makeup tanks work in recirculation mode, meaning they are always filled with water because cold borated water injected through the injection lines is replaced by hot water coming from the cold leg balance lines.

The operation of the PRHR heat exchanger and the core makeup tanks cools down the plant. Due to the swelling of the core makeup tank water, the pressuriser level continues to increase. The operators are assumed to be alerted by the High-2 pressuriser level signal (at 2,270.8 seconds) that a pressuriser level increase transient is underway, and it is assumed that the operators are ready to take corrective action at least 30 minutes later. The specific operator action assumed in this case is to open the reactor vessel head vent to preclude pressuriser overfill following the High-3 pressuriser level signal (at 4,070.8 seconds); this action is at least 30 minutes after the operator has been alerted by the High-2 pressuriser level signal.

The safety-related reactor vessel head vent is opened by the operators, and the pressuriser water level increase slows and eventually the level begins to decrease. This demonstrates that the capacity of the reactor vessel head vent is sufficient to preclude pressuriser overfill as a result of a chemical and volume control system malfunction that causes an increase in reactor coolant inventory.

During the event, the DNBR never drops significantly below the initial value since both the chemical and volume control system and the core makeup tanks add borated water to the reactor coolant system. At the time of the reactor trip, core power and heat flux drop rapidly and the DNBR is well above the design limit value defined in Section 22.7.1.1.

The limiting case presented here models operator action to open the reactor vessel head vent following receipt of the High-3 pressuriser level signal; this action is at least 30 minutes after the operator has been alerted by the High-2 pressuriser level signal. For pressuriser level increase events, the operator could take other actions to reduce the increase in coolant inventory. As the pressuriser water level would increase above the high pressuriser water level that normally isolates chemical and volume control system makeup, the normal letdown line could be placed into service to reduce the increase in coolant inventory. If letdown could not be placed into service, the operator would use the safety-related reactor vessel head vent valves to reduce the increase in coolant inventory. For these events, following operations procedures, there is sufficient time for the operator to mitigate the consequences of this event.

Appendix 9C provides discussion and analysis of long term safe shutdown for all non-LOCA events.

9.5.2.3 Diverse Mitigation

As this is classified a frequent fault, alternative means of providing the required Category A safety functions are required. For this frequent fault event the diverse features are also Class 1 except for the C&I, which is Class 2.

The diverse core cooling is provided by passive feed and bleed using PXS injection and ADS venting (Class 1). The DAS provides diverse reactor trip and safety system actuation (Class 2).

Table 9.5-2 summarizes the SSCs from this fault assessment. As this is a frequent fault, a diverse means of providing the Category A safety functions is provided. The information provided in Table 9.5-2 is from Reference 9.5-4, which documents the diversity for the frequent faults and provides additional information on the diverse mitigation functions. Table 9.5-3 provides the operator actions utilized in the diverse safety case.

9.5.2.3.1 Diverse Mitigation for ATWT

An increase in reactor coolant inventory, which results from addition of cold unborated water to the reactor coolant system, is presented in the boron dilution discussion in Section 9.4.6.3. For purposes of this discussion, the increase of reactor coolant system inventory is due to the addition of borated water.

The increase of RCS coolant inventory may be due to the spurious operation of one or both of the CVS pumps or the closure of the letdown path. If the CVS is injecting highly borated water into the RCS, the reactor experiences a negative reactivity excursion due to the injected boron, causing a decrease in reactor power and subsequent coolant shrinkage. The load decreases due to the effect of reduced steam pressure after the turbine control valve fully opens.

At high CVS boron concentration, low reactivity feedback conditions, and reactor in manual rod control, an "S" signal will be generated by either the low T_{cold} or low steam line pressure setpoints before the CVS can inject a significant amount of water into the RCS. In this case, the CVS malfunction event proceeds similarly to, and is only slightly more limiting than, a spurious "S" signal event. If the automatic rod control is modelled and the pressuriser spray functions properly to prevent a high pressure reactor trip signal, no "S" signals are generated, and this specific event is terminated by automatic isolation of the CVS on the Class 1 High-2 pressuriser level setpoint.

Under typical operating conditions for the AP1000 reactor, the boron concentration of the injected CVS water is equal to that of the RCS. If the CVS is functioning in this manner and the pressuriser spray system functions properly to prevent a high pressure reactor trip signal, no "S" signals are generated and this specific event is also terminated by automatic isolation of the CVS on the High-2 pressuriser level setpoint.

For the above two cases, no trip signal is generated, as a trip is not necessary to protect the plant. Thus, ATWT is not applicable to this transient.

While these scenarios are the most probable outcomes of a CVS malfunction, several combinations of boron concentration, feedback conditions, and plant system interactions have been identified that can result generating an "S" signal and a reactor trip. This scenario is evaluated for ATWT and assumes the following:

- One or both of the chemical and volume control system pumps spuriously begin delivering flow at a boron concentration slightly higher than that of the reactor coolant system.

- The pressuriser spray is assumed to be available, so that a high pressuriser pressure reactor trip is prevented.

- Due to the boron addition in the core, the plant cools down until an "S" signal is generated on low cold-leg temperature. On the "S" signal, the reactor is tripped (rods do not drop, either because the rods are mechanically stuck or the trip breakers fail to open), the RCPs are tripped, the pressuriser heaters are blocked, and the main feedwater lines, steam lines, and CVS are isolated.

Because these actions occur at lower than normal reactor coolant temperatures, the loss of ac power ATWT (Section 9.2.6.3.1) is more limiting than this scenario.

If the rods fail to drop due to a failure of the PMS, the "S" signal will not be generated, RCS temperatures will continue to fall, the CVS will be isolated on a High-2 pressuriser level setpoint, and the reactor will stabilise at a lower RCS temperature. For a PMS CCF, CVS would not be isolated; however, the main result of this failure would be pressuriser filling (with pressuriser safety valve (PSV) water relief), which is not an ATWT acceptance criteria (see Reference 9.5-3). Eventually, the operators would diagnose the problem and isolate the CVS. Alternatively, manual reactor trip or CMT actuation via the DAS is available.

9.5.2.3.2 Diverse Mitigation for Core Cooling

The loss of normal feedwater diverse core cooling, as analysed in Section 9.2.7.3.2, was determined to be bounding of all non-LOCA events.

9.5.2.4 Radiological Consequences

In the case where offsite power remains available, there is no release of activity to the environment and the Target 4 BSOs (0.01 mSv offsite and 0.1 mSv onsite) are met.

In the case where offsite power is lost, a small release of activity may occur as a result of steam dump to the atmosphere due to unavailability of the condensers. With no fuel damage and primary and secondary circuits intact, the initiating event has no impact on the doses. The doses are a consequence of the assumed loss of offsite power. Therefore, the loss of offsite power event doses from Section 9.2.6.4 are presented. The calculated maximum doses for all relevant pathways (inhalation, cloudshine, and groundshine) are as follows:

- Offsite dose: 0.05 mSv Worker dose: 1.5 mSv

These doses are within the Target 4 BSL for frequent faults (1 mSv offsite and 20 mSv onsite).

Diverse Mitigation

Both the diverse ATWT and diverse core cooling scenarios demonstrate that the RCS does not overpressurise and there is no significant fuel damage. For a diverse mitigation radiological consequences analysis better estimate assumptions would be credited. This would include reactor coolant system activity levels significantly lower than those modelled for the DBA and better activity retention in containment and in the steam generators. In addition better estimate atmospheric dispersion factors would be used. Therefore, a diverse mitigation radiological consequences analysis would show that the doses for the diverse ATWT scenario would be less than those reported for the non-LOCA DBAs and doses for the diverse core cooling scenario would be much less than for the design basis LOCA. The diverse mitigation analyses would not

have to meet the Target 4 BSL for frequent faults and would meet the Target 4 BSL for infrequent faults.

9.5.2.5 As Low as Reasonably Practicable Assessment

The ALARP discussion for this event is the same as for the inadvertent operation of a core makeup tank, as described in Section 9.5.1.5.

9.5.2.6 Conclusions

The DB analysis demonstrates that a chemical and volume control system malfunction does not adversely affect the core, the reactor coolant system, or the steam system. The pressuriser does not fill; therefore, water is not relieved from the pressuriser safety valves. DNBR remains above the design limit values, and reactor coolant system and steam generator pressures remain below 110 percent of their design values.

This event has also been adequately assessed with respect to ATWT considerations.
Diverse core cooling capabilities have been demonstrated.

DBA Radiological consequences are within the Target 4 BSL for frequent faults (1 mSv offsite and 20 mSv onsite). Thus, the identification of necessary Class 1 SSCs is adequate to meet DB requirements.

It has been shown that the AP1000 plant design includes adequate systems for the protection of this fault, which limit the radiological consequences such that they are compliant with the SAP targets and the risks has have been reduced to be ALARP.

9.5.3 References

9.5-1 Westinghouse Documents WCAP-7907-P-A, Rev. 0 (Proprietary) and WCAP-7907-A, Rev. 0 (Non-Proprietary), “LOFTRAN Code Description,” April 1984.

9.5-2 Westinghouse Documents WCAP-15644-P, Rev. 2 (Proprietary) and WCAP-15644-NP, Rev. 2 (Non-Proprietary), “AP1000 Code Applicability Report,” March 2004.

9.5-3 Westinghouse Report UKP-GW-GLR-016, Rev. B, “Evaluation of ATWS Events for UK AP1000™ Pressurized Water Reactor,” October 2010.

9.5-4 Westinghouse Report UKP-GW-GL-067, Rev. 1, “AP1000 Assessment of Diverse Mitigation of Frequent Faults for the UK,” December 2011.

Table 9.5-1 (Sheet 1 of 2). DBA Time Sequence Of Events For Incidents Which Result In An Increase In Reactor Coolant Inventory

Accident	Event	Time (seconds)
Inadvertent operation of a core makeup tank during power operation	Core makeup tank discharge valves open	10
	High-2 pressuriser level setpoint reached	556.1
	High-3 pressuriser level setpoint reached	2,589.3
	Rod motion begins	2,591.3
	Loss of offsite power	2,599.3
	Reactor coolant pumps trip	2,599.3
	High-3 pressuriser level setpoint reached	2,736.6
	PRHR heat exchanger actuated	2,768.6
	Low-2 T_{cold} "S" setpoint is reached	2,768.6
	Second CMT starts recirculating	2,768.6
	Main steam and feed lines are isolated	2,780.6
	Operators open the reactor vessel head vent after the High-3 pressuriser level signal is reached (at least 30 minutes after High-2 pressuriser level setpoint is reached)	3,256.1
	Peak pressuriser water volume occurs	5,460.0

Table 9.5-1 (Sheet 2 of 2). DBA Time Sequence Of Events For Incidents Which Result In An Increase In Reactor Coolant Inventory

Accident	Event	Time (seconds)
Chemical and volume control system malfunction that increases reactor coolant inventory	Chemical and volume control system charging pumps start	10.0
	Low-2 T_{cold} "S" signal and High-2 pressuriser level signals are reached	2,270.8
	Core makeup tank discharge valves open	2,271.4
	Rod motion begins	2,272.8
	Loss of offsite power	2,280.8
	Reactor coolant pumps trip	2,280.8
	Main steam and feed lines are isolated	2,283.4
	PRHR heat exchanger actuated	2,288.4
	Chemical and volume control system charging pumps are isolated	2,308.9
	Operators open the reactor vessel head vent after the High-3 pressuriser level signal is reached (at least 30 minutes after High-2 pressuriser level setpoint is reached)	4,070.8
	Peak pressuriser water volume occurs	5,078.0
	Pressuriser water volume begins to decrease	5,484.0

Table 9.5-2. Incidents Which Result In An Increase In Reactor Coolant Inventory Mitigation Features

Category A Safety Function	Provision	SSCs	Classification
Short-term reactivity control	Primary means	Reactor trip Breakers (PMS)	1
	Diverse means	Motor-generator set field breakers (DAS)	2
Long-term reactivity control	Primary means	CMT Recirculation	1
	Diverse means	Passive feed and bleed	1
Decay heat removal	Primary means	PRHR HX	1
	Diverse means	Passive feed and bleed	1
RCS pressure control	Primary means	Pressuriser safety valve	1
	Diverse means	PRHR HX	1
RCS inventory control	Primary means	CMTs, RV head vent	1
	Diverse means	Passive feed and bleed	1
Containment cooling	Primary means	PCS AOVs	1
	Diverse means	PCS MOVs	1

Table 9.5-3. Incidents Which Result In An Increase In Reactor Coolant Inventory Potential Operator Actions

Operator Action	Class
On failure of automatic shutdown, initiate shutdown manually using DAS.	2
On failure of shutdown rods to insert, initiate RCP trip and actuation of CMTs to achieve shutdown by boration of the primary circuit.	1
If PRHR fails, activate ADS to allow automatic actuation of recirculation RHR via the IRWST.	1
Manually align the normal letdown line to help reduce the increase in coolant inventory.	2
If manual alignment of the normal letdown line is not possible, use the reactor head vent valves to help reduce the increase in coolant inventory.	1

Table 9.5-4. Not Used

Table 9.5-5. Not Used

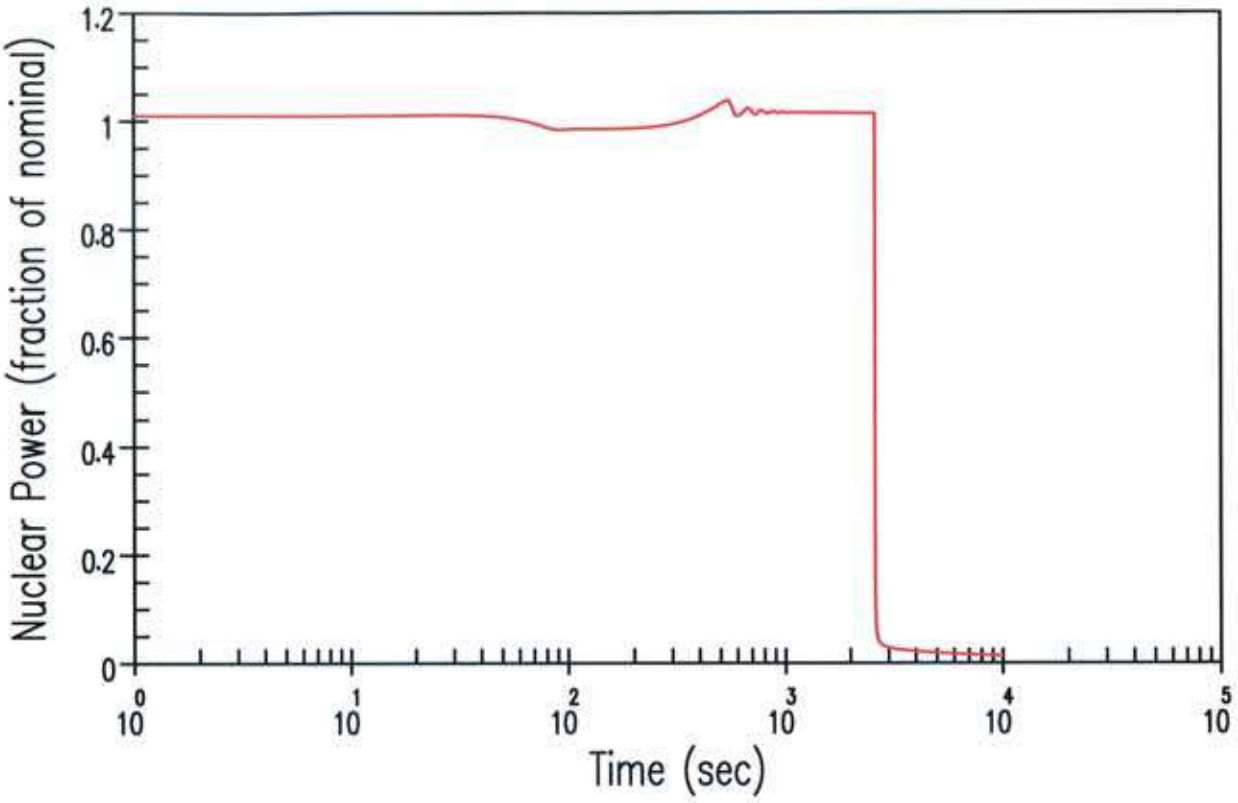


Figure 9.5.1-1. DBA Core Nuclear Power Transient for Inadvertent Operation of a Core Makeup Tank

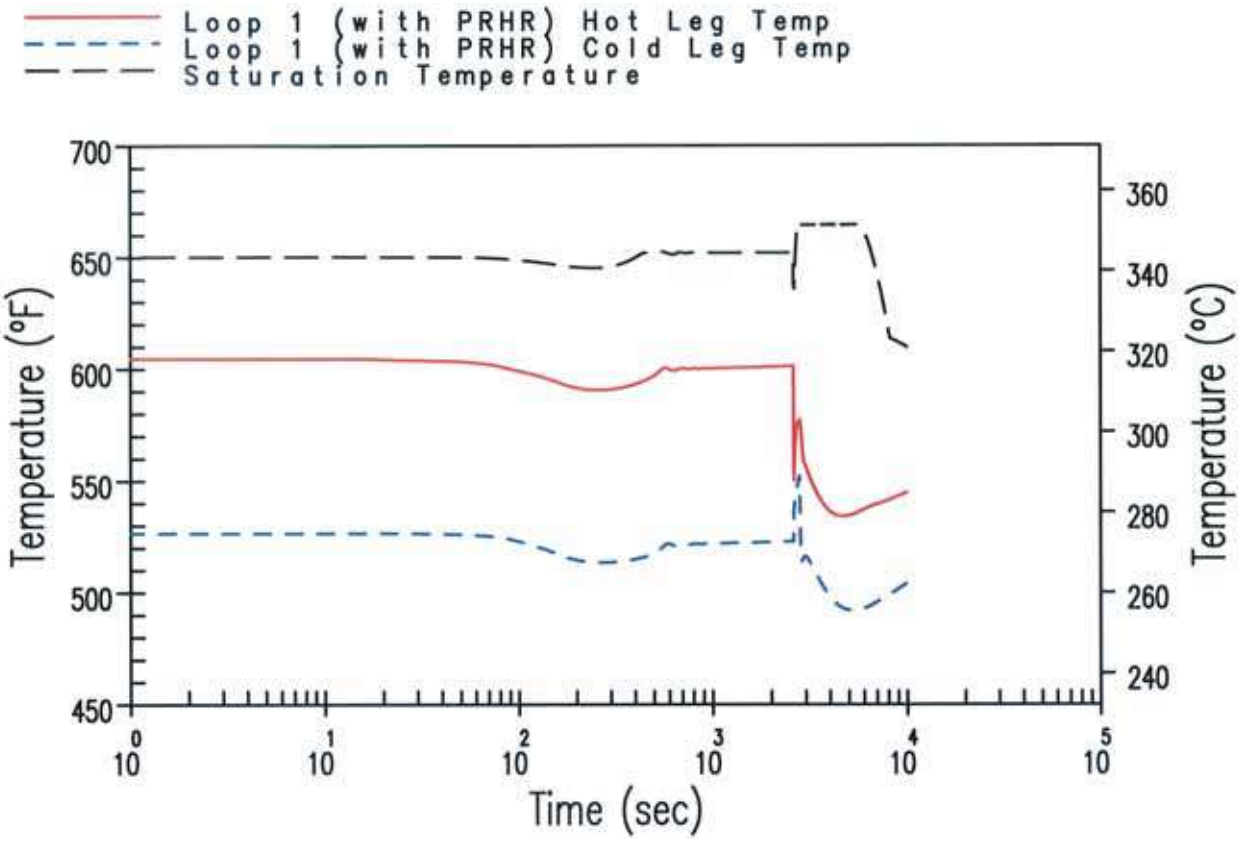


Figure 9.5.1-2. DBA RCS Temperature Transient in Loop Containing the PRHR for Inadvertent Operation of a Core Makeup Tank

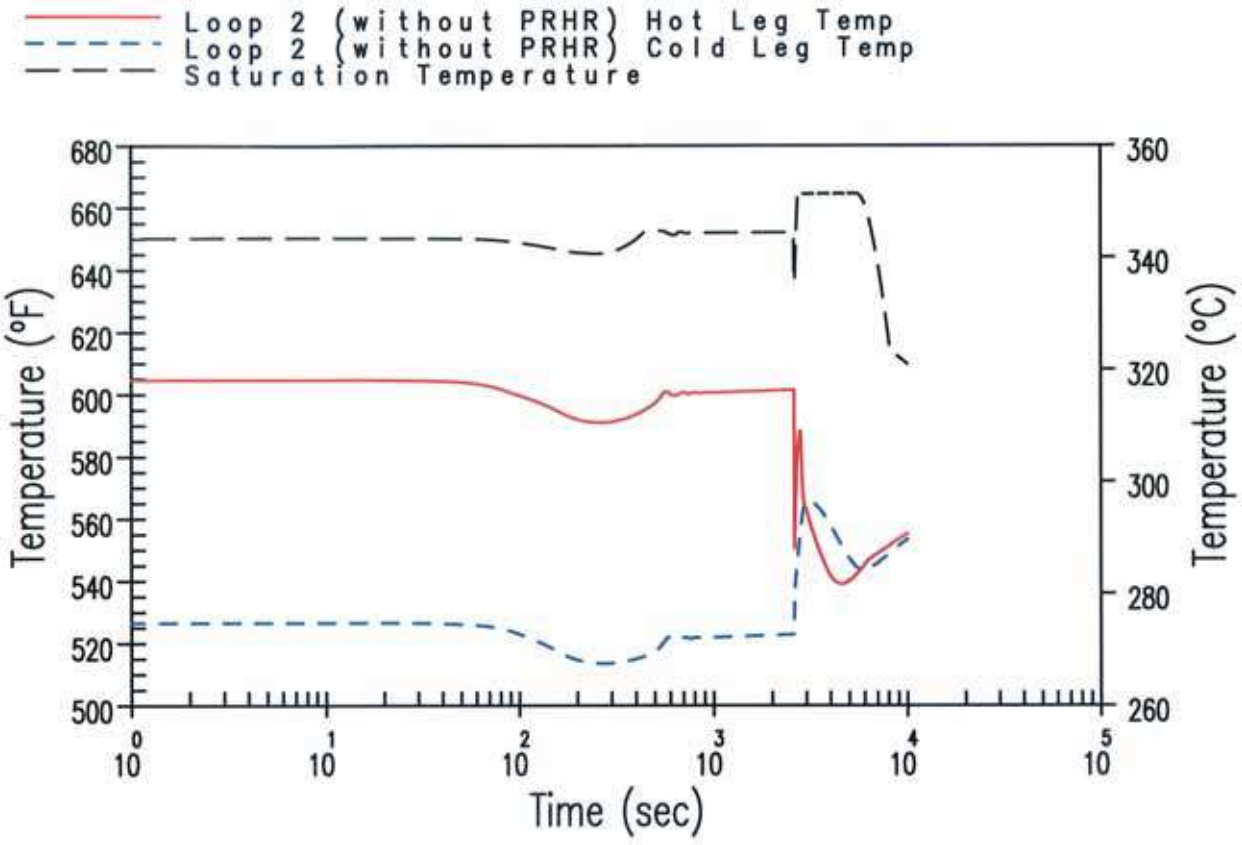


Figure 9.5.1-3. DBA RCS Temperature Transient in Loop Not Containing the PRHR for Inadvertent Operation of a Core Makeup Tank

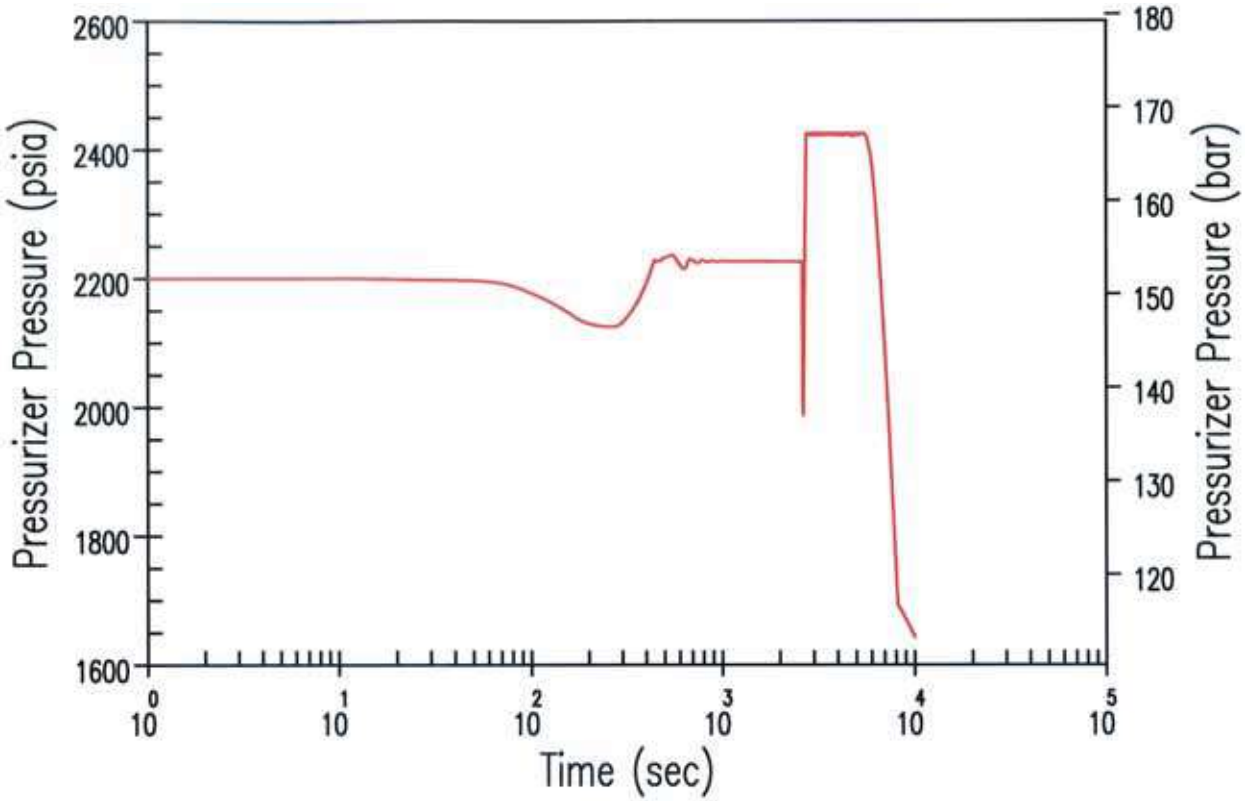


Figure 9.5.1-4. DBA Pressuriser Pressure Transient for Inadvertent Operation of a Core Makeup Tank

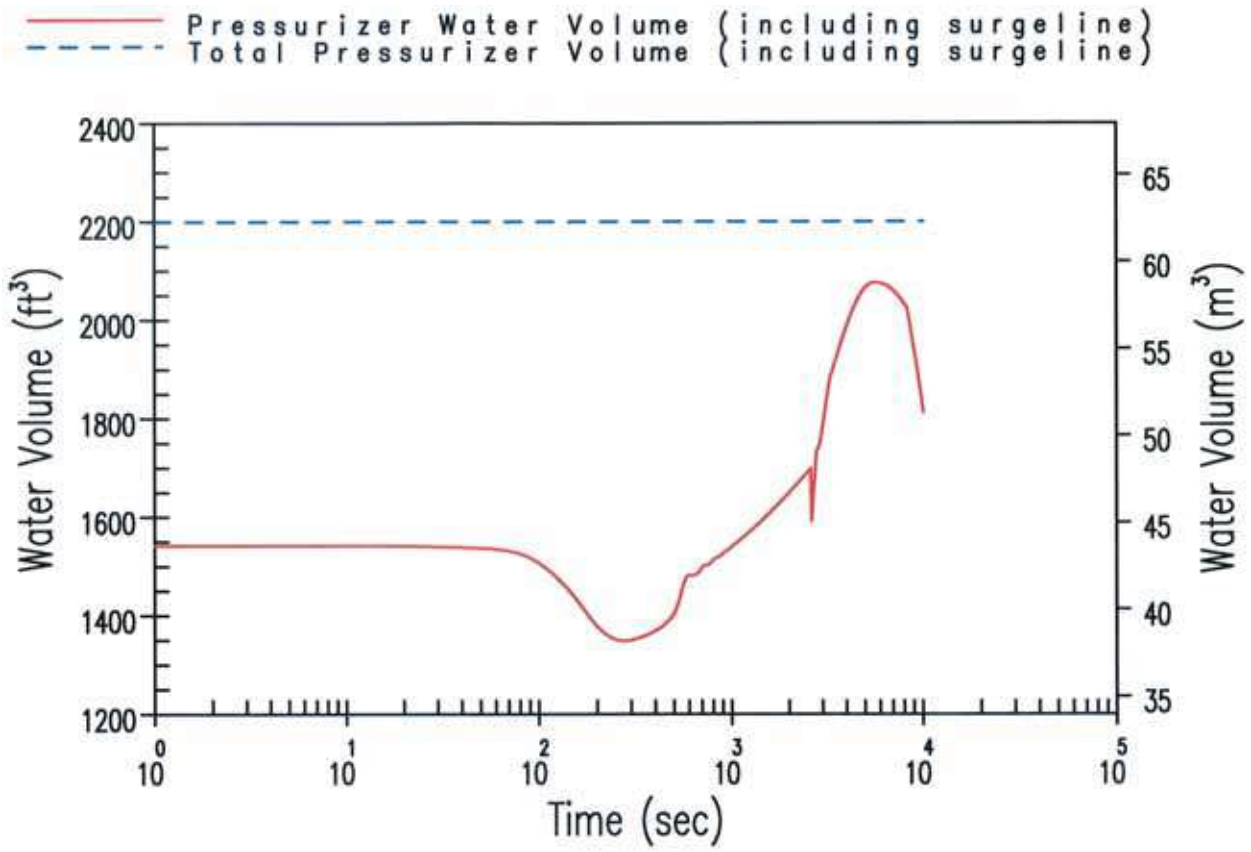


Figure 9.5.1-5. DBA Pressuriser Water Volume Transient for Inadvertent Operation of a Core Makeup Tank

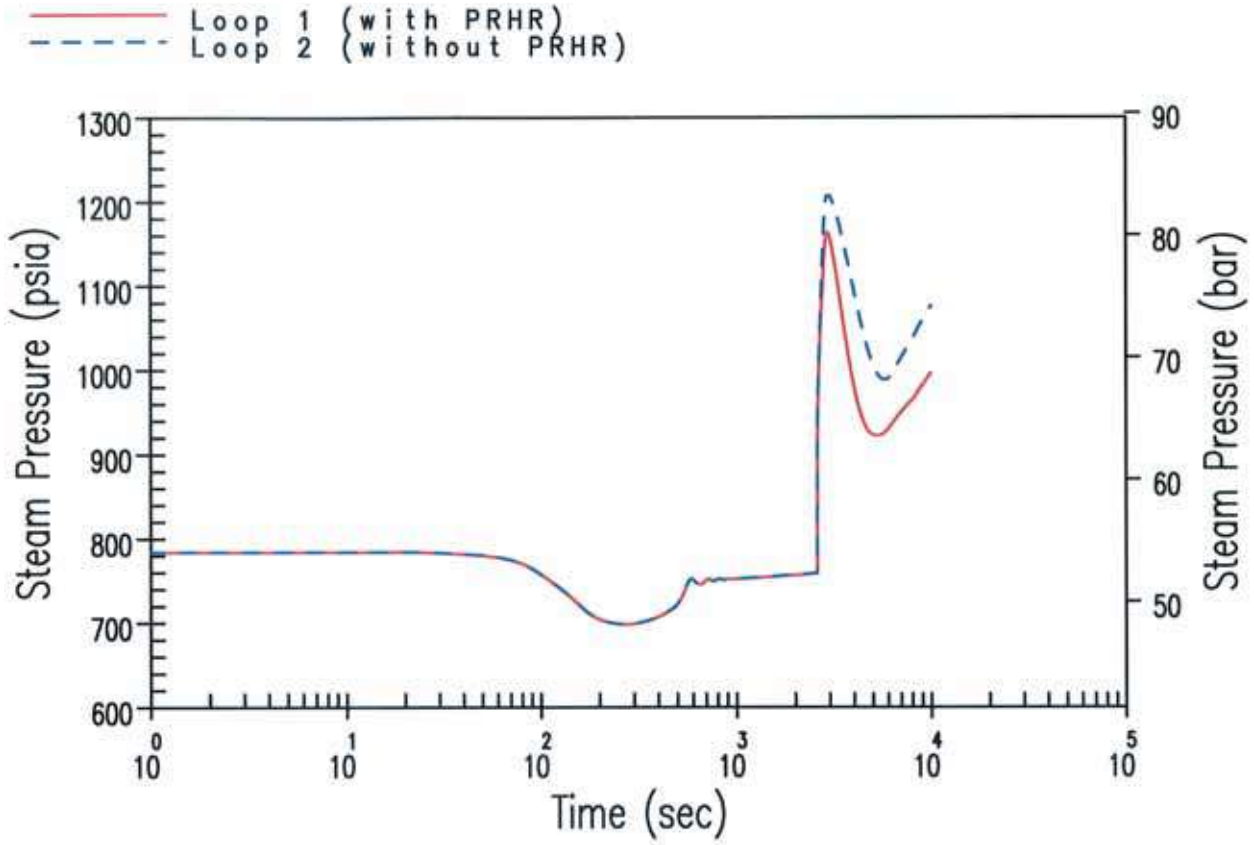


Figure 9.5.1-6. DBA Steam Generator Pressure Transient for Inadvertent Operation of a Core Makeup Tank

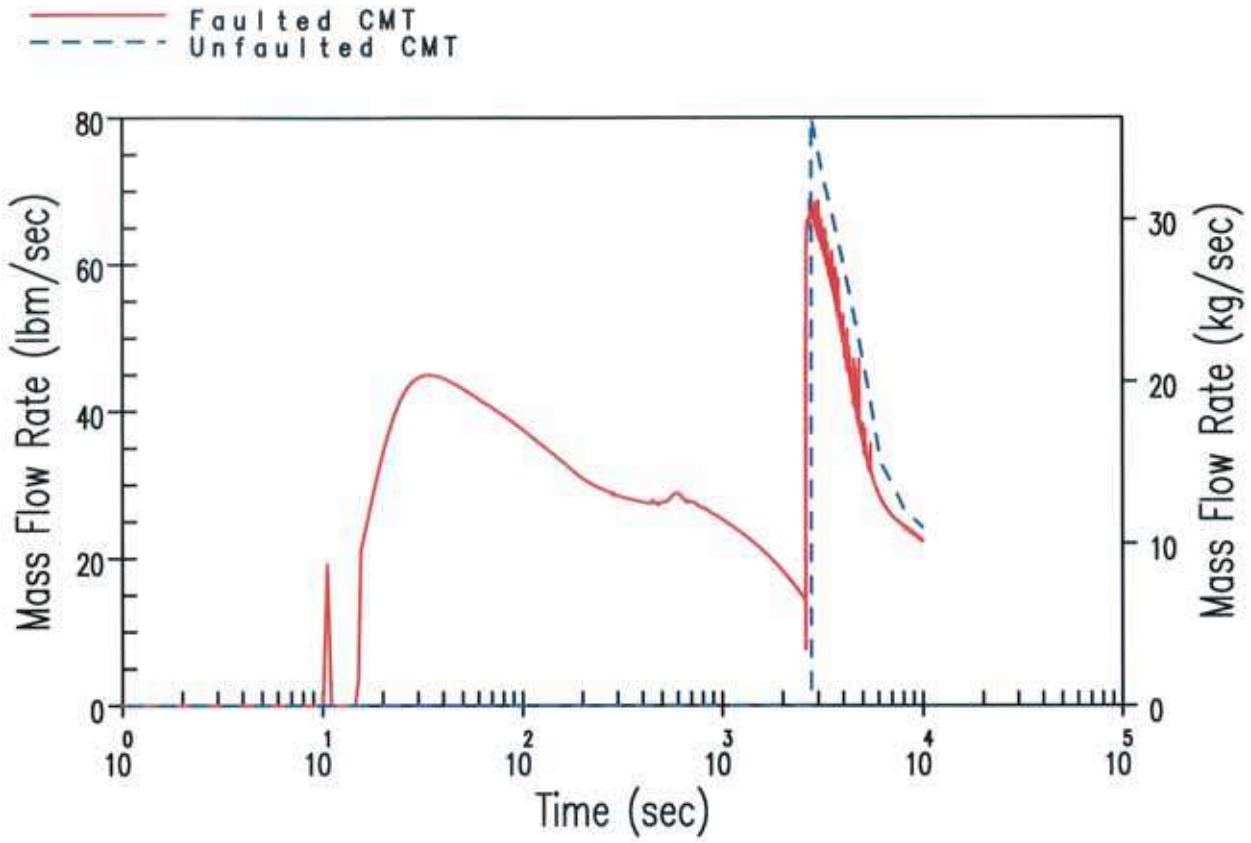


Figure 9.5.1-7. DBA CMT Flow Rate Transient for Inadvertent Operation of a Core Makeup Tank

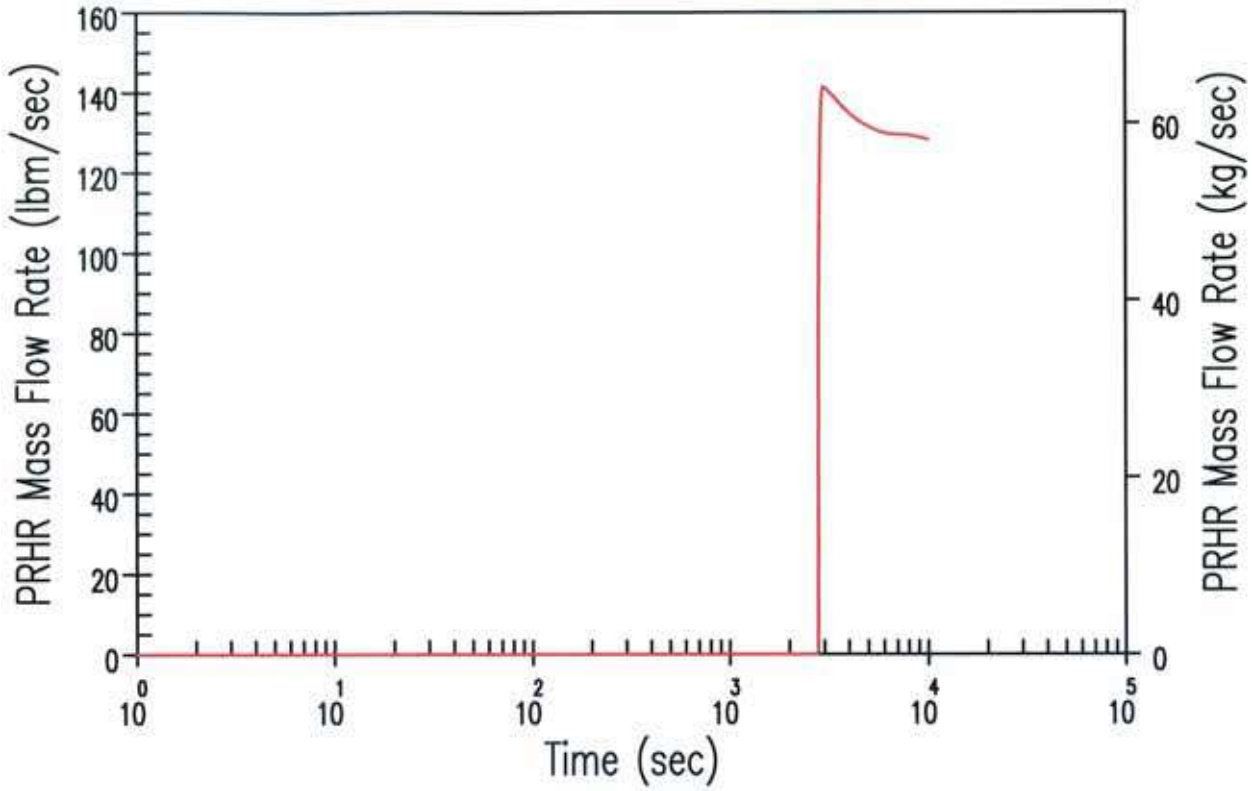


Figure 9.5.1-8. DBA PRHR Flow Rate Transient for Inadvertent Operation of a Core Makeup Tank

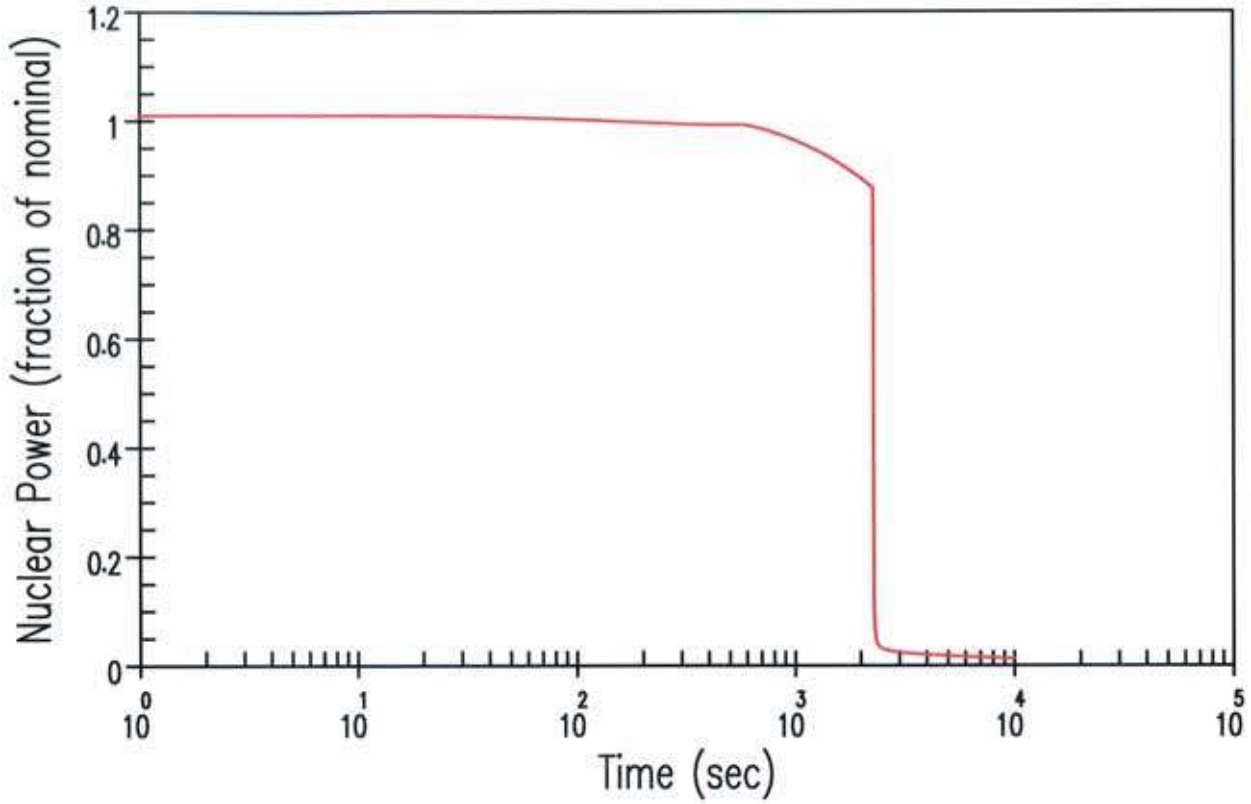


Figure 9.5.2-1. DBA Core Nuclear Power Transient for Chemical and Volume Control System Malfunction

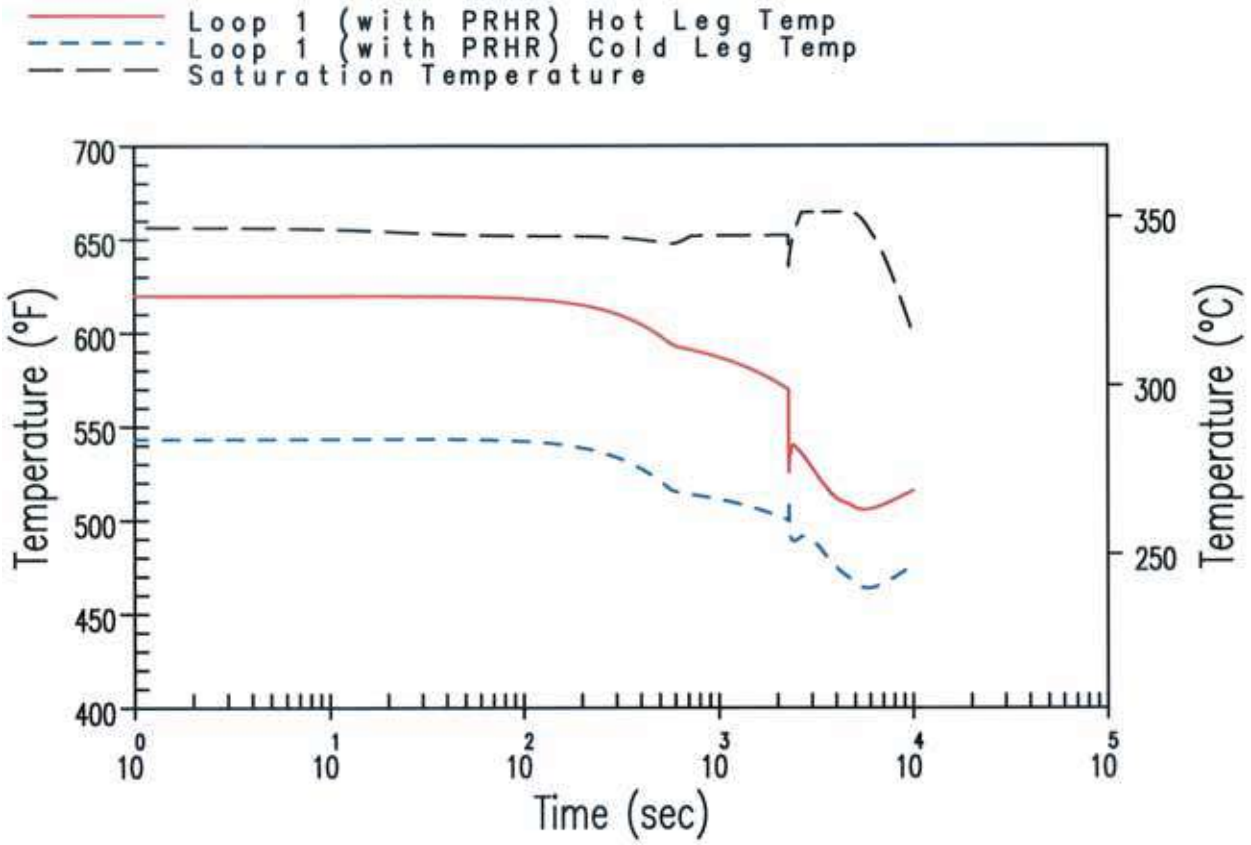


Figure 9.5.2-2. DBA RCS Temperature Transient in Loop Containing the PRHR for Chemical and Volume Control System Malfunction

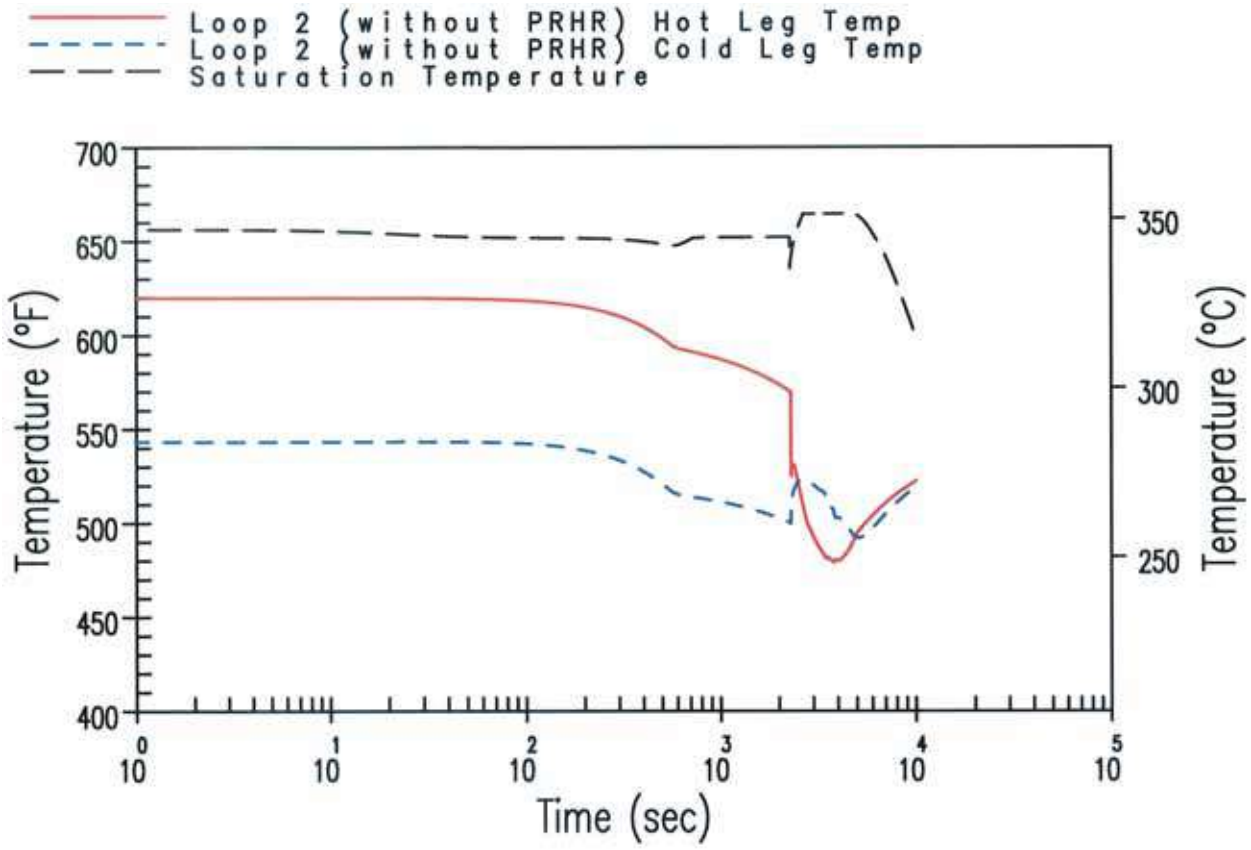


Figure 9.5.2-3. DBA RCS Temperature Transient in Loop Not Containing the PRHR for Chemical and Volume Control System Malfunction

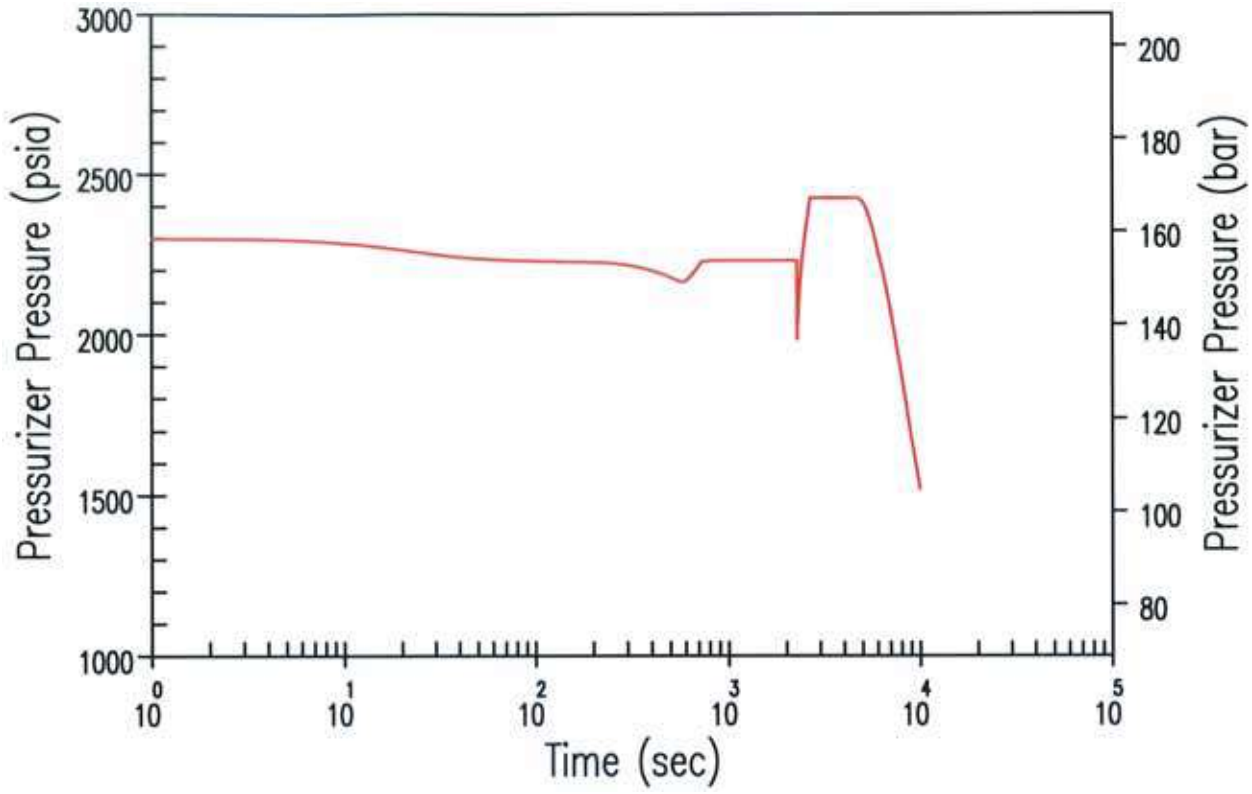


Figure 9.5.2-4. DBA Pressuriser Pressure Transient for Chemical and Volume Control System Malfunction

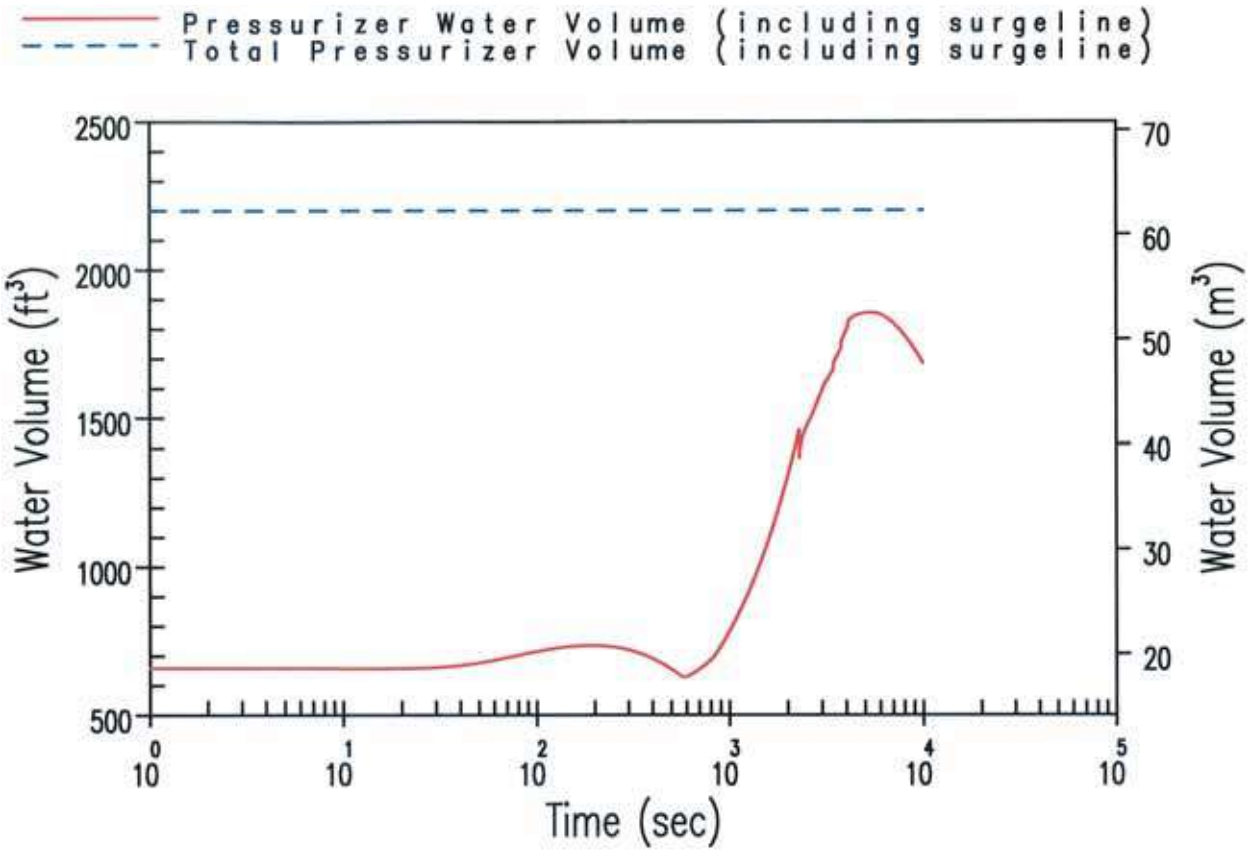


Figure 9.5.2-5. DBA Pressuriser Water Volume Transient for Chemical and Volume Control System Malfunction

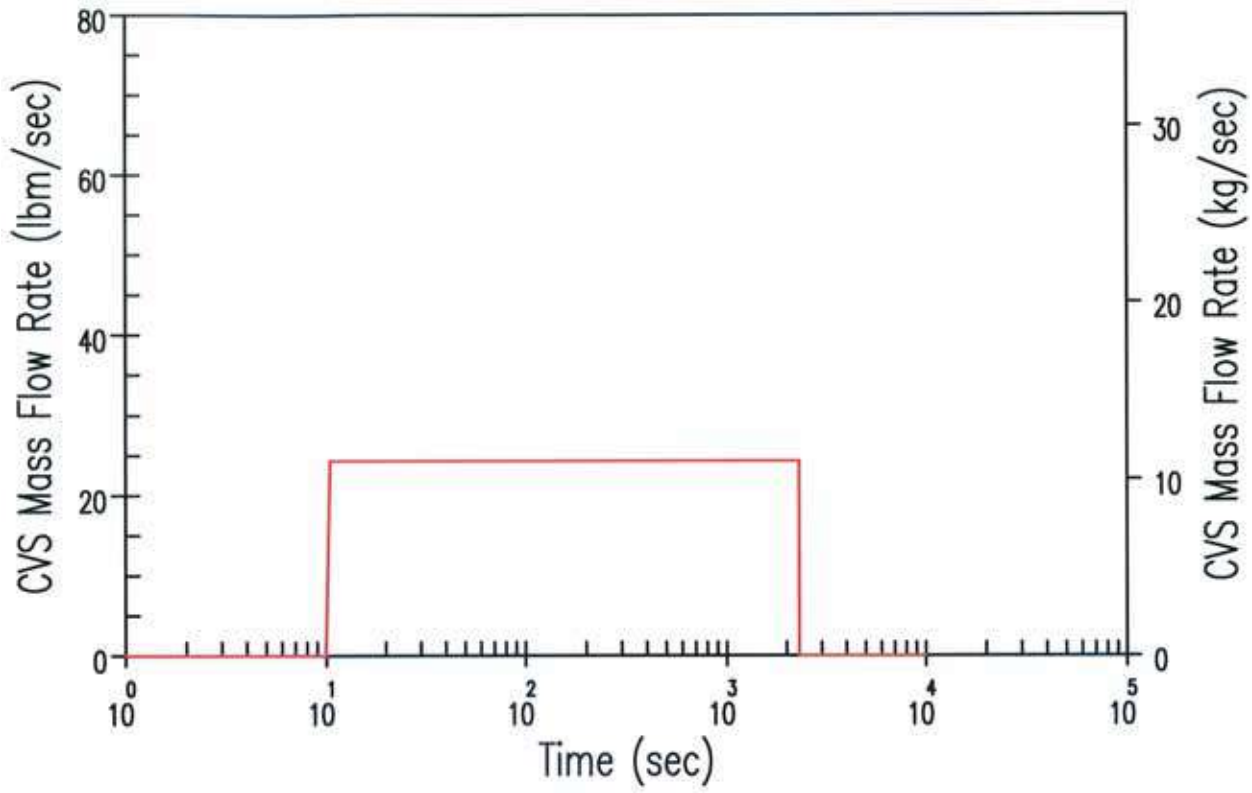


Figure 9.5.2-6. DBA CVS Flow Rate Transient for Chemical and Volume Control System Malfunction

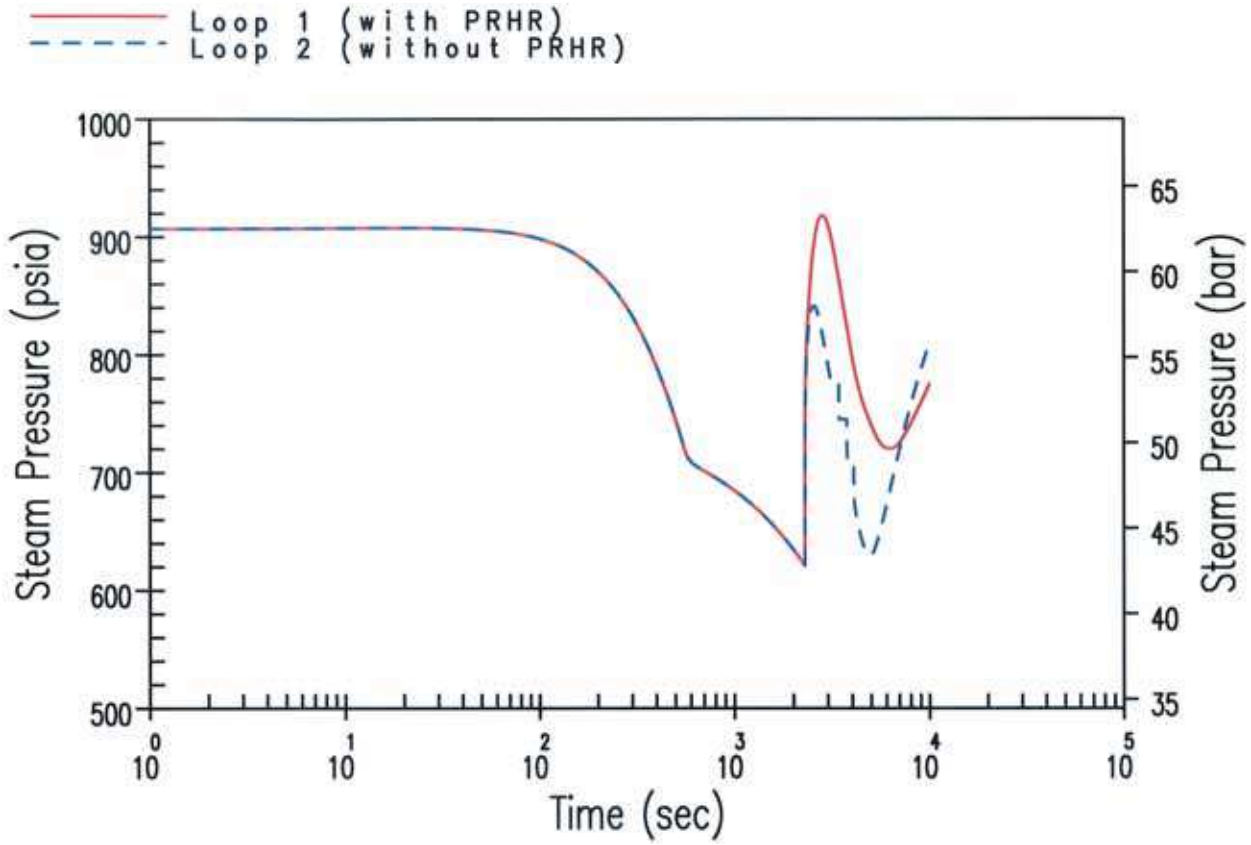


Figure 9.5.2-7. DBA Steam Generator Pressure Transient for Chemical and Volume Control System Malfunction

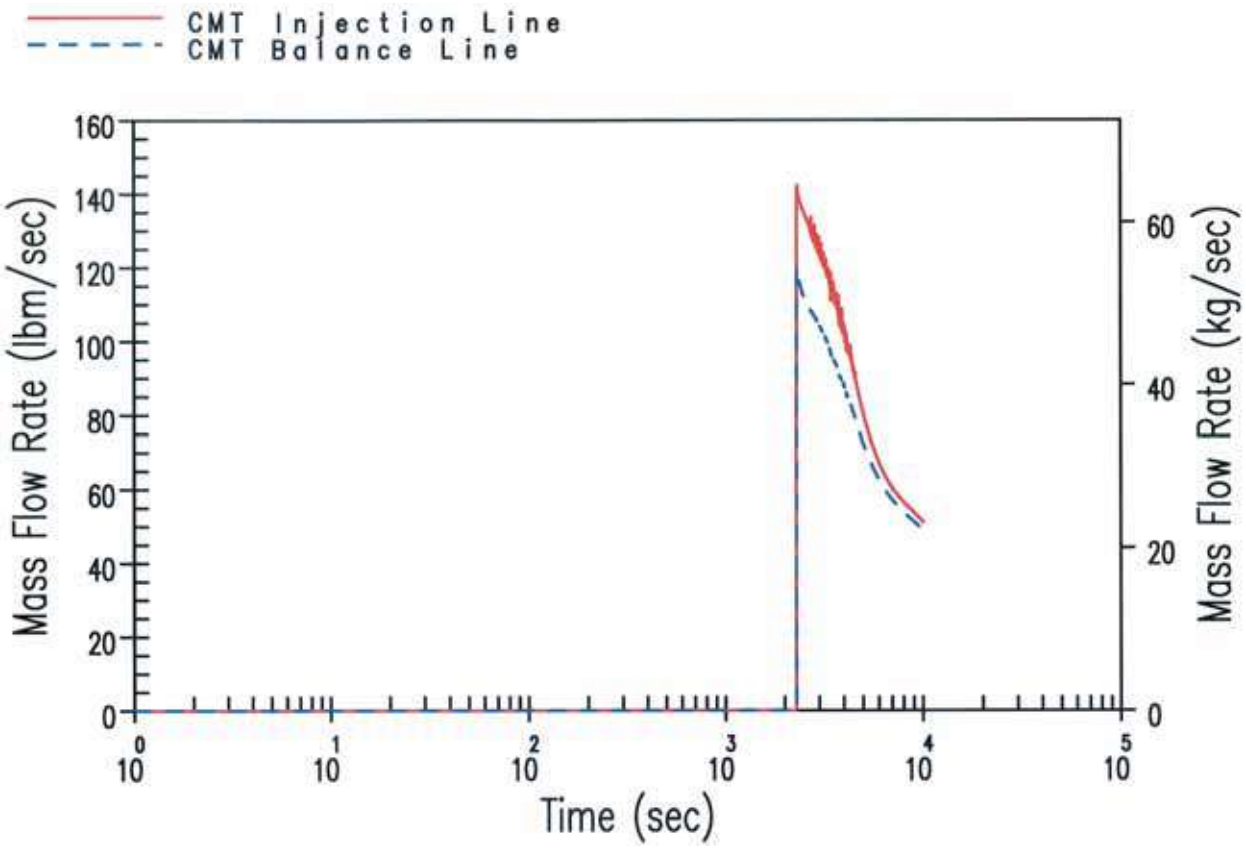


Figure 9.5.2-8. DBA CMT Injection Line and Balance Line Flow Transient for Chemical and Volume Control System Malfunction

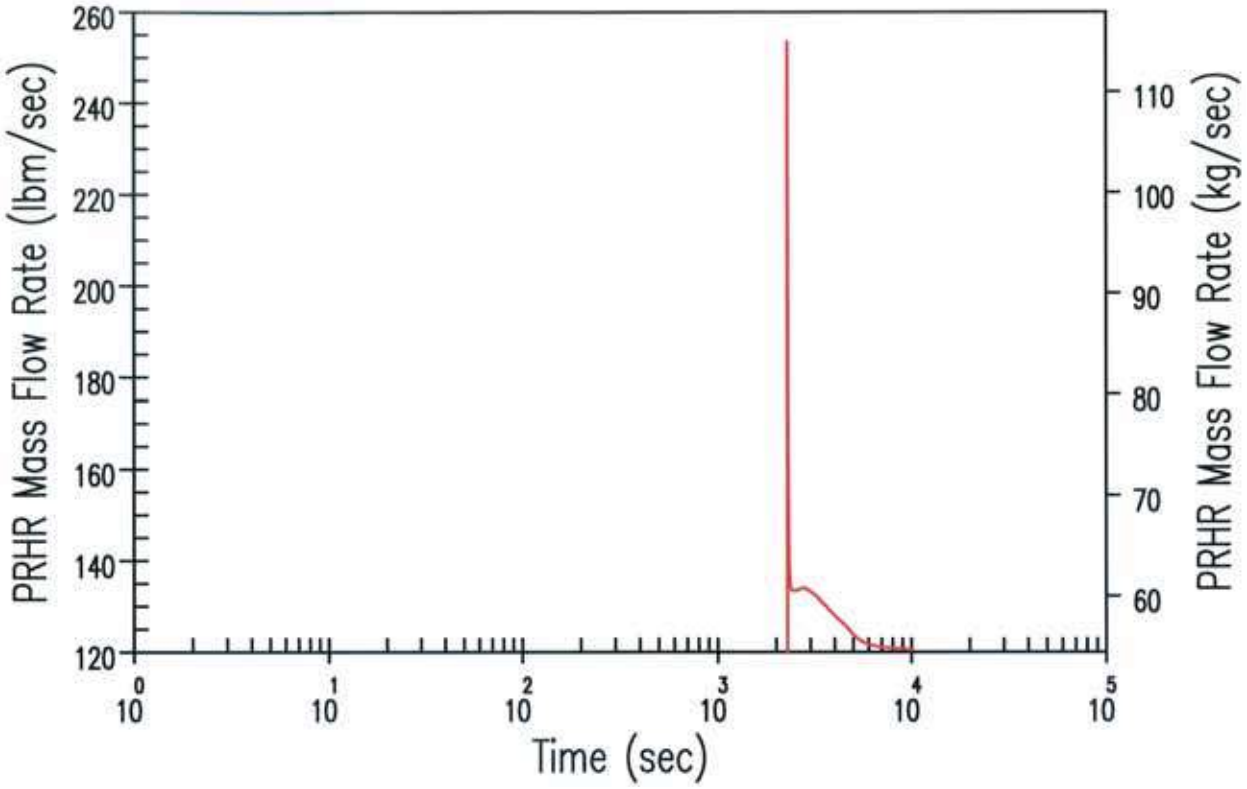


Figure 9.5.2-9. DBA PRHR Flow Rate Transient for Chemical and Volume Control System Malfunction

9.6 Decrease in Reactor Coolant Inventory

The following sections evaluate faults dealing with decreases in reactor coolant system water inventory.

9.6.1 Inadvertent Opening of a Pressuriser Safety Valve or Inadvertent Operation of the ADS

9.6.1.0 Introduction and Overview of Faults

Section 9.6.1 evaluates the short term effects on the plant as a result of two inadvertent depressurisation faults (Fault 1.5.2):

- Inadvertent operation of ADS valves leading to a medium-break loss-of-coolant accident (MBLOCA)
- Inadvertent opening of a pressuriser safety valve

The long term effects for these faults are examined in Section 9.6.5.

Spurious actuation of the ADS is defined as an inadvertent valve-opening event. Depending on the number of the ADS lines spuriously opening, the frequency of ADS spurious actuation can be classified as MBLOCA or large-break loss-of-coolant accident (LBLOCA). Spurious ADS actuation leading to an LBLOCA is addressed in Section 9.6.4.

Spurious actuation of ADS consisting of Stages 1-3 opening in sequence (equivalent to a spurious C&I actuation signal) is categorised and analysed as a medium LOCA. Spurious ADS Stage 4 is categorised as a large LOCA.

The valve stroke times assumed reflect the DB of the AP1000 plant. The accidents addressed in this section were evaluated for the effect of these assumed DB valve stroke times. The results of this evaluation have shown that there is a small impact on the analysis and the conclusions remain valid. The output provided in this section for the analyses is representative of the transient phenomenon.

The analysed fault(s) are described in additional detail in the subsequent sections to complete the safety case for each fault, including:

- Identification of Causes and Accident Description
- Design Basis Analysis of Effects and Consequences
- Assessment of the Radiological Consequences for the DBA
- Diverse Mitigation and ATWT for Frequent Faults
- ALARP Assessment
- Conclusions

Initiating Event Frequency[1]

The fault schedule (Appendix 8A) gives a frequency of <1E-07/yr for spurious ADS operation leading to an MBLOCA and a frequency of 3.9E-04/yr for a stuck-open pressuriser valve event. These two types of inadvertent depressurisations are considered to be infrequent faults.

Design Basis Class

As noted in the MBLOCA assessment, given that the unmitigated consequences of an MBLOCA are assumed to be greater than the Target 4 BSL for frequent faults (1 mSv offsite and 20 mSv onsite) and given the IEF above, the event is in the DB1 class.

9.6.1.1 Identification of Causes and Accident Description

Two types of inadvertent depressurisations are discussed in this section. One covers the inadvertent operation of ADS valves. The other covers inadvertent opening of a pressuriser safety valve.

An inadvertent depressurisation of the reactor coolant system can occur as a result of an inadvertent opening of a pressuriser safety valve or ADS valves. Initially, the event results in a rapidly decreasing reactor coolant system pressure. The pressure decrease causes a decrease in power via the moderator density feedback. The average coolant temperature decreases slowly, but the pressuriser level increases until reactor trip.

The reactor may be tripped by the following reactor protection system signals:

- Overtemperature ΔT
- Pressuriser low pressure

The ADS system consists of four stages of depressurisation valves. The ADS stages are interlocked. For example, Stage 1 is initiated first and subsequent stages are not actuated until previous stages have completed actuation. Each stage includes two redundant parallel valve paths with two valves in series in each path such that no single failure prevents operation of the ADS stage when it is called upon to actuate and the spurious opening of a single ADS valve does not initiate ADS flow. Since each ADS path includes two valves in series, no mechanical failure could result in an inadvertent operation of an ADS stage. The ADS Stage 4 squib valves cannot be opened while the reactor coolant system is at nominal operating pressure. To actuate the ADS manually from the main control room, the operators actuate two separate controls positioned at some distance apart on the main control board. Therefore, one unintended operator action does not cause ADS actuation.

ADS Stage 1 has a minimum opening time of 20 seconds and a maximum effective flow area of 0.0045 m^2 (7 in^2). ADS Stages 2 and 3 have a minimum opening time of 60 seconds and a maximum effective flow area of 0.018 m^2 (28 in^2).

---

1. As discussed in Chapter 8, the frequency for initiating events from the PSA is used in both Chapters 8 and 9 with the sole purpose of supporting the categorisation of the fault to a specific DB category. As noted in Chapter 8, these probabilities should not be considered to be representative of actual frequency of the events, and for several events they can be significantly conservative. Detailed PSA results and their basis are discussed in Chapter 10 of this PCSR.

For this analysis, multiple failures and or errors are assumed which actuate both Stage 1 ADS paths. Although ADS Stages 2 and 3 have larger depressurisation valves, the opening time of the Stage 1 depressurisation valves is faster. This results in a more severe reactor coolant system depressurisation due to ADS operation with the reactor at power.

Inadvertent opening of a pressuriser safety valve can only be postulated due to a mechanical failure. Although a pressuriser safety valve is smaller than the combined two Stage 1 ADS valves, the pressuriser safety valve is postulated to open in a shorter time.

Analyses are presented in this section for the inadvertent opening of a pressuriser safety valve and the inadvertent opening of a path of Stage 2 or 3 of the ADS. These analyses are performed to demonstrate that the DNBR does not decrease below the design limit values (see Section 22.7.1.1) while the reactor is at power. Performance following reactor trip for these faults is examined in Section 9.6.5.

The effects of a possible consequential loss of ac power during an RCS depressurisation event have been evaluated to not adversely impact the analysis results. This conclusion is based on a review of the time sequence associated with a consequential loss of ac power in comparison to the reactor shutdown time for an RCS depressurisation event. The primary effect of the loss of ac power is to cause the RCPs to coast down. The protection and safety monitoring system includes a five second minimum delay between the reactor trip and the turbine trip. In addition, a three second delay between the turbine trip and the loss of offsite ac power is assumed, consistent with the discussion in Section 9.0.12. Considering these delays between the time of the reactor trip and RCP coastdown due to the loss of ac power, it is clear that the plant shutdown sequence will have passed the critical point and the control rods will have been completely inserted before the RCPs begin to coast down. Therefore, the consequential loss of ac power does not adversely impact this analysis because the plant will be shut down well before the RCPs begin to coast down.

9.6.1.2 Design Basis Mitigation

Analysis is performed to demonstrate the adequacy of the PMS to detect and mitigate the fault and show that the safety analysis criteria are satisfied including:

- No fuel failures (confirmed using minimum DNBR and fuel melt criteria),
- The RCS pressure criterion is met,
- The MSS pressure criterion is met, and
- The pressuriser does not fill (which could result in a LOCA).

RCS and MSS overpressure criteria are bounded by DB analysis of Section 9.2.3 analysis and, therefore, it is not explicitly calculated for this event. Pressuriser filling is not challenged in this event.

9.6.1.2.1 Method of Analysis

The accidental depressurisation transient is analysed by using the computer code LOFTRAN (References 9.6.1-1 and 9.6.1-2). The code simulates the neutron kinetics, reactor coolant system, pressuriser, pressuriser safety valves, main steam isolation valves, pressuriser spray, steam generator, and steam generator safety valves. The code computes pertinent plant variables including temperatures, pressures, and power level.

Plant characteristics and initial conditions are discussed in Section 9.0.2. The following assumptions are made to give conservative results in calculating the DNBR during the transient:

- Initial conditions are discussed in Section 9.0.2. Uncertainties in initial conditions are included in the DNBR limit as discussed in WCAP-11397-P-A (Reference 9.6.1-3).

- A least negative moderator temperature coefficient is assumed. The spatial effect of voids resulting from local or subcooled boiling is not considered in the analysis with respect to reactivity feedback or core power shape.

- A large (absolute value) Doppler coefficient of reactivity is used such that the resulting amount of positive feedback is conservatively high to retard any power decrease.

Plant systems and equipment necessary to mitigate the effects of reactor coolant system depressurisation are discussed in Section 9.0.4 and are listed in Table 9.0-10.

Normal reactor control systems are not required to function. The rod control system is assumed to be in the automatic mode to maintain the core at full power until the reactor trip protection function is reached. This is a worst case assumption. The reactor protection system functions to trip the reactor on the appropriate signal. No single active failure prevents the reactor protection system from functioning properly.

9.6.1.2.2 DBA Credited SSCs

For the short-term DB (until shortly after reactor trip,) all claimed SSCs are Class 1. The available Class 1 systems are listed in Table 9.0-10. The presented DBA ends shortly after reactor trip; however, essential safety functions for the long term safe shutdown analysis (Appendix 9C) bound safe shutdown response for this event. The primary core cooling is provided by the PRHR and passive containment cooling. Other SSCs include the CMTs and containment isolation. The PMS provides the following:

- RT on:
  - Low-2 pressuriser pressure
  - Overtemperature ΔT

- PRHR actuation on Low-2 SG NR level coincident with Low-2 SFW flow

- CMTs and containment isolation on Low-2 CL temperature

- PCS on High-2 containment pressure

For the long-term post-trip DBA of the spurious ADS activation scenarios, the Class 1 systems listed under the MBLOCA event are available, and the same performance requirements also apply.

9.6.1.2.3 Results

The system response to an inadvertent opening of a pressuriser safety valve is shown in Figures 9.6.1-1 through 9.6.1-4. The calculated sequence of events for the inadvertent opening of a pressuriser safety valve scenario is shown in Table 9.6.1-1.

A pressuriser safety valve is assumed to step open at the start of the event. The reactor coolant system then depressurises until the low pressuriser pressure reactor trip setpoint is reached. Figure 9.6.1-3 shows the pressuriser pressure transient.

Prior to tripping of the reactor, the core power remains relatively constant (Figure 9.6.1-1). The minimum DNBR during the event occurs shortly after the rods begin to be inserted into the core (Figure 9.6.1-2). The DNBR remains above the design limit values as discussed in Section 22.7.1.1 throughout the transient.

The system response for inadvertent operation of the ADS is shown in Figures 9.6.1-5 through 9.6.1-8. The sequence of events is provided in Table 9.6.1-1. The system response for inadvertent operation of the ADS is very similar to that obtained for inadvertent opening of a pressuriser safety valve.

9.6.1.3 Diverse Mitigation

Diverse mitigation for this event is not required as it is an infrequent fault classified as DB1.

9.6.1.4 Radiological Consequences

Design Basis

For the purposes of comparison of radiological dose with SAPs Target 4, the spurious activation of the ADS and opening of the pressuriser relief valve are included in the assessment for the MBLOCA scenario. This is a conservative assumption, as the analysis described above shows that there is no core heatup during these events.

The analysis results presented in Section 9.6.1.2.4 show that there is no fuel damage for this event. The radiological consequences of the MBLOCA presented in Section 9.6.5.3.6.3 assumed 10 percent of the fuel rods are damaged. Therefore, the MBLOCA doses bound those of this event. The MBLOCA doses from Section 9.6.5.3.6.3.5 are presented. The calculated maximum doses for all relevant pathways (inhalation, cloudshine, and groundshine) are as follows:

- Offsite dose: 2.6 mSv worker dose: 6.0 mSv

These doses are within the Target 4 BSL for infrequent faults (10 mSv offsite and 200 mSv onsite).

9.6.1.5 As Low As Reasonably Practicable Assessment

The spurious activation of the ADS and opening of the pressuriser relief valve are included in the ALARP assessment for the MBLOCA scenario (Section 9.6.5.3.6.5).

9.6.1.6 Conclusion

The DB results of the analysis show that the low pressuriser pressure reactor protection system signal provides adequate protection against the reactor coolant system depressurisation events. The calculated DNBR remains above the design limit defined in Section 22.7.1.1. The long-term plant responses due to a stuck-open ADS valve or pressuriser safety valve, which cannot be isolated, are bounded by the small-break LOCA analysis.

DBA radiological consequences are within the Target 4 BSL for infrequent faults (i.e., 10 mSv offsite and 200 mSv onsite).

It has been shown that the AP1000 plant design includes adequate systems for the protection of this fault, which limit the radiological consequences such that they are compliant with the SAPs targets and the risks have been reduced to be ALARP.

9.6.1.7 References

9.6.1-1 Westinghouse Documents WCAP-15644-P, Rev. 2 (Proprietary) and WCAP-15644-NP, Rev. 2 (Non-Proprietary), "AP1000 Code Applicability Report," March 2004.

9.6.1-2 Westinghouse Documents WCAP-7907-P-A, Rev. 0 (Proprietary) and WCAP-7907-A, Rev. 0 (Non-Proprietary), "LOFTRAN Code Description," April 1984.

9.6.1-3 Westinghouse Documents WCAP-11397-P-A (Proprietary) and WCAP-11397-A (Non-Proprietary), "Revised Thermal Design Procedure," April 1989.

Table 9.6.1-1. DBA Time Sequence Of Events For Incidents That Cause A Decrease In Reactor Coolant Inventory

Accident	Event	Time (seconds)
Inadvertent opening of a pressuriser safety valve	Pressuriser safety valve opens fully	0.00
	Low pressuriser pressure reactor trip setpoint reached	20.30
	Rods begin to drop	22.30
	Minimum DNBR occurs	23.00
Inadvertent opening of an ADS Stage 2 or 3 train	ADS valves begin to open	0.0
	Low pressuriser pressure reactor trip setpoint reached	26.30
	Rods begin to drop	28.30
	Minimum DNBR occurs	29.10
	ADS valves fully open	60.00

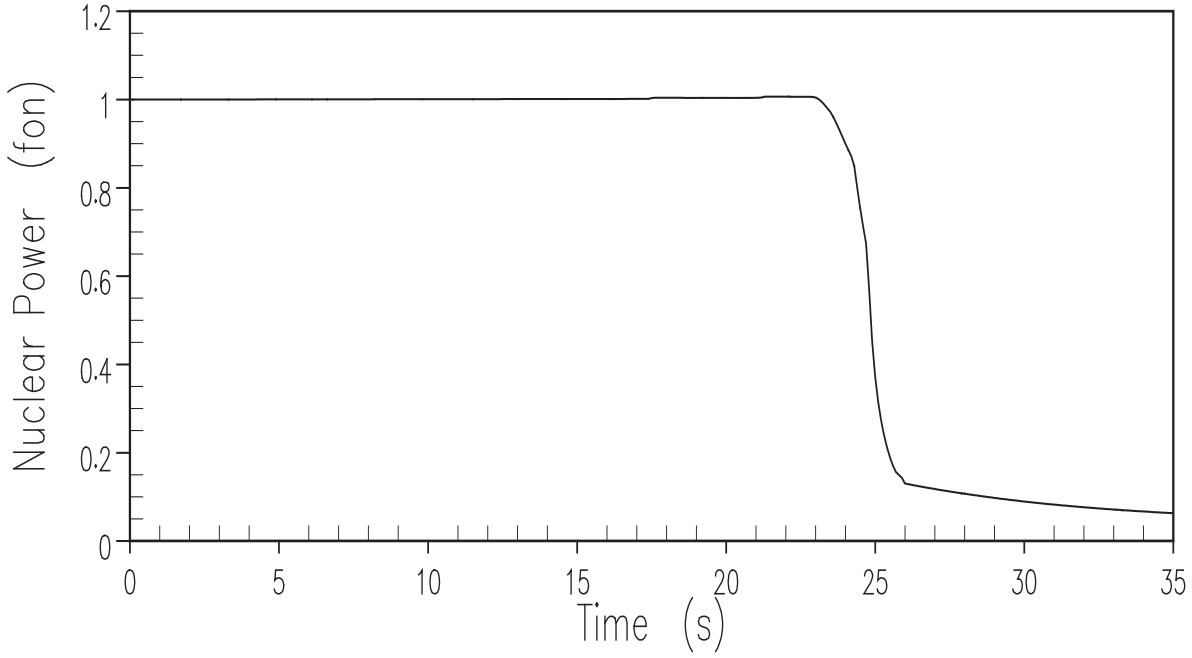


Figure 9.6.1-1. DBA Nuclear Power Transient Inadvertent Opening of a Pressuriser Safety Valve

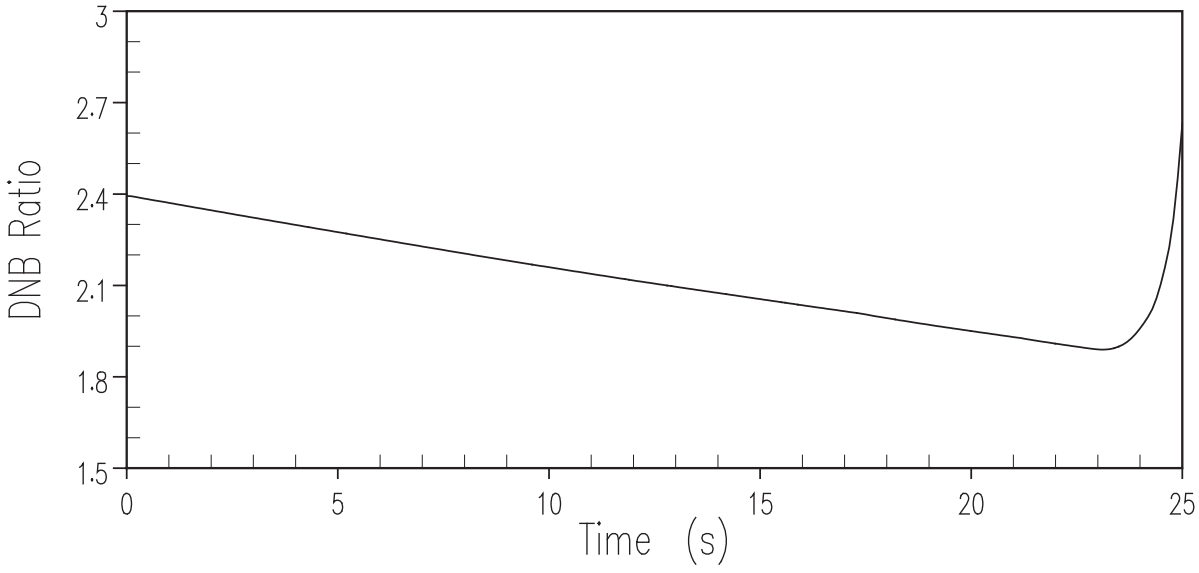


Figure 9.6.1-2. DBA DNBR Transient Inadvertent Opening of a Pressuriser Safety Valve

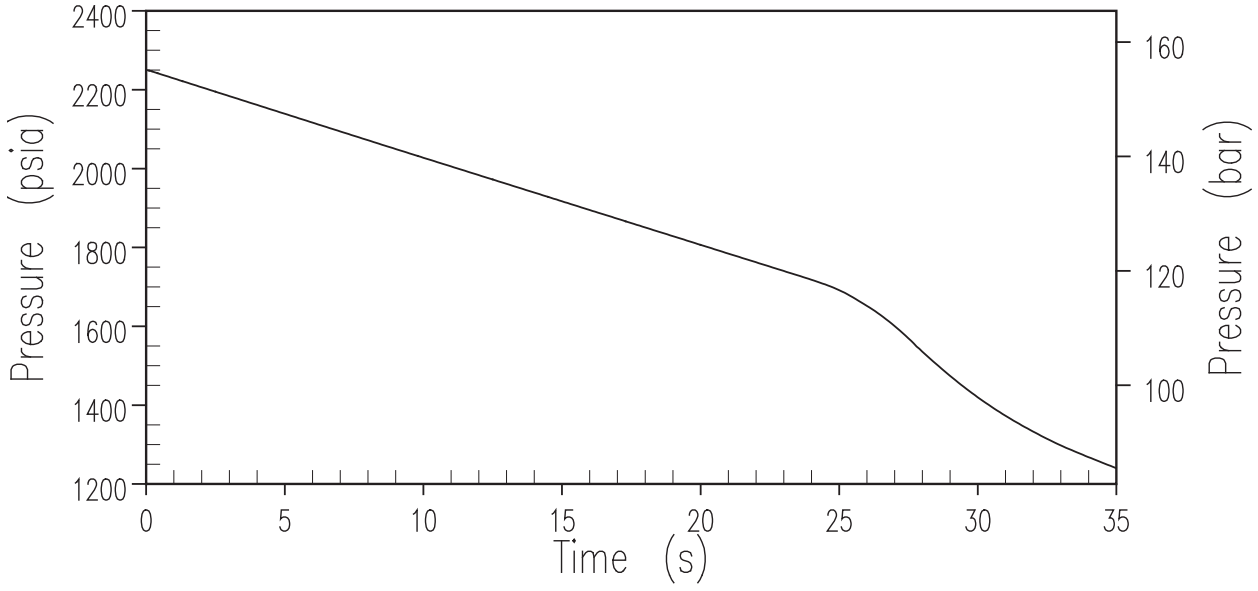


Figure 9.6.1-3. DBA Pressuriser Pressure Transient Inadvertent Opening of a Pressuriser Safety Valve

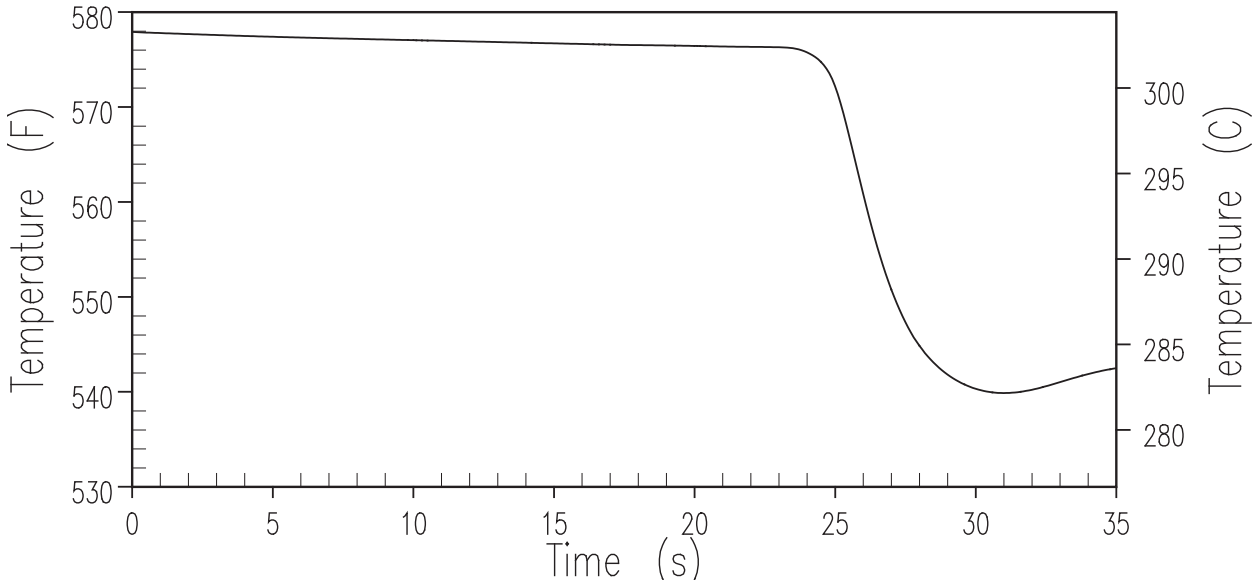


Figure 9.6.1-4. DBA Core Average Temperature Transient Inadvertent Opening of a Pressuriser Safety Valve

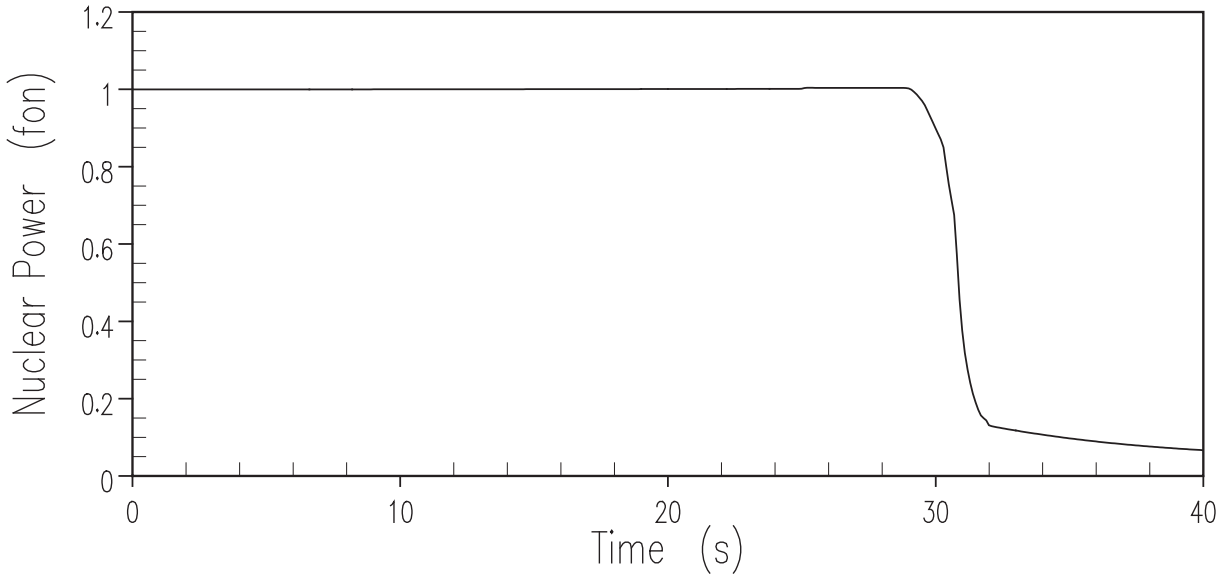


Figure 9.6.1-5. DBA Nuclear Power Transient Inadvertent Opening of an ADS Stage 2 or 3 Train

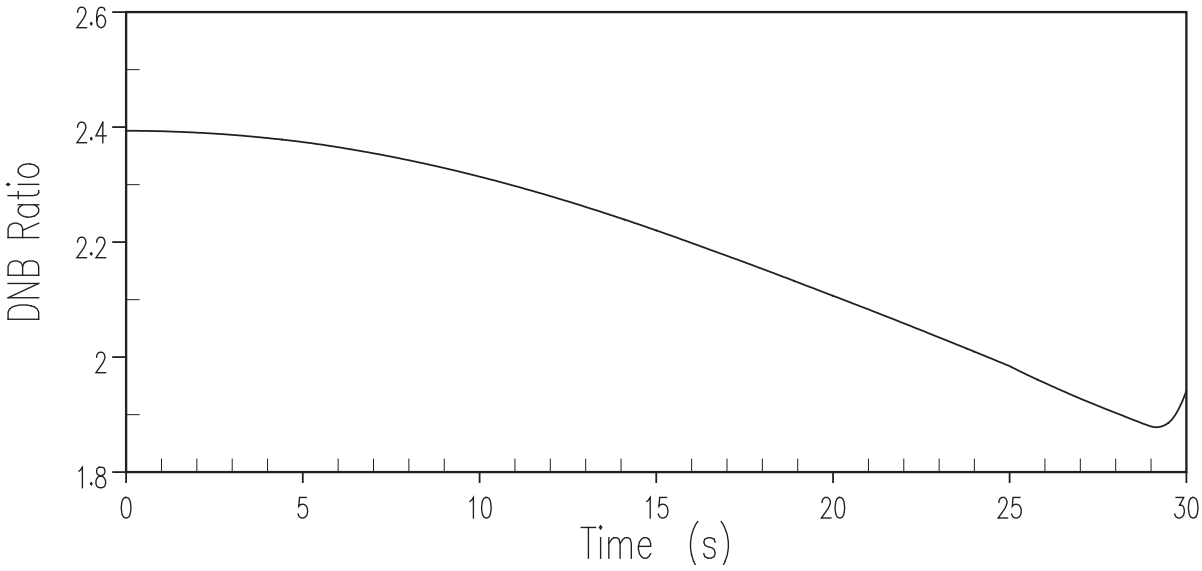


Figure 9.6.1-6. DBA DNBR Transient Inadvertent Opening of an ADS Stage 2 or 3 Train

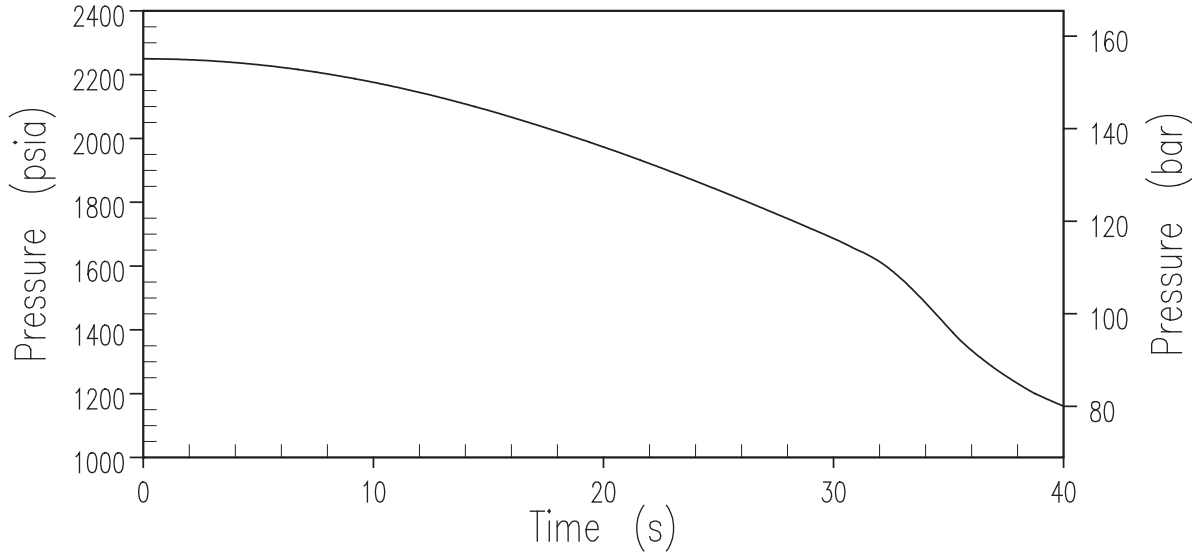


Figure 9.6.1-7. DBA Pressuriser Pressure Transient Inadvertent Opening of an ADS Stage 2 or 3 Train

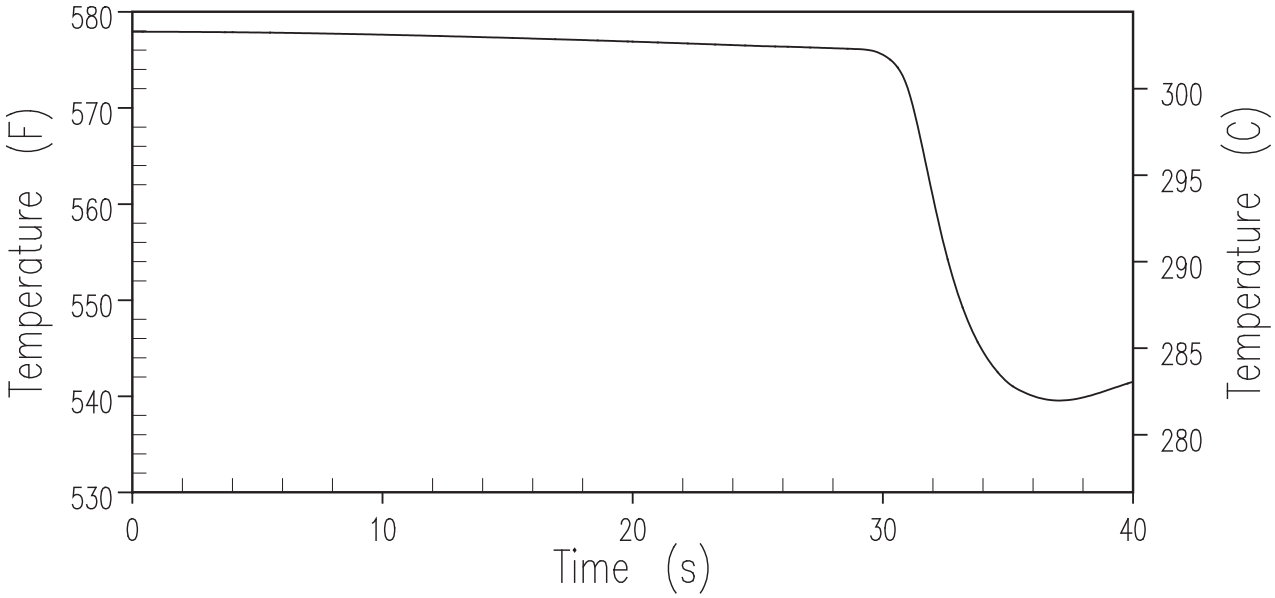


Figure 9.6.1-8. DBA Core Average Temperature Transient Inadvertent Opening of an ADS Stage 2 or 3 Train

9.6.2 Failure of Small Lines Carrying Primary Coolant outside the Containment

9.6.2.0 Introduction and Overview of Faults

A number of small lines are associated with the primary reactor circuit, two of which carry primary coolant outside containment. These are the RCS sample line and the discharge line from the CVS to the liquid radwaste system (WLS). No instrument lines carry primary coolant outside the containment.

Although technically a break in a small line is classed as a LOCA-type event, the maximum volumetric rate of loss of coolant is well within the capacity of normal operational coolant makeup by the CVS. In the absence of another concurrent compounding fault, the loss of coolant aspects of the event would be managed without any call on the emergency coolant makeup systems. For the CVS and sample lines; however, breaks can occur outside the containment, with the potential for local discharge of primary coolant and a release of radioactivity into the environment.

The fault is first described; the initial event frequency and the design basis class is provided and the bounding fault or faults are identified (if needed). The analysed faults are presented individually in Table 8A-2.

The analysed fault(s) are described in additional detail in the subsequent sections to complete the safety case for each fault, including:

- Identification of Causes and Accident Description
- Design Basis Analysis of Effects and Consequences
- Assessment of the Radiological Consequences for the DBA
- Diverse Mitigation and ATWT for Frequent Faults
- ALARP assessment
- Conclusions

Description

Two faults are considered (see Appendix 8A):

- Rupture in the discharge line from the CVS to the WLS (Fault 3.4.1)
- Rupture in the RCS sample line outside containment (Fault 1.9.2)

Initiating Event Frequency[1]

Faults involving a break in a small line, or instrumentation line, are considered to be a fault of moderate frequency (i.e., in the range of 0.1 to 0.01/yr). Instrument line breaks are included with RCS leakage faults in the PSA with an IEF for the all of these faults of 1.4E-03/yr (Fault 1.9.1, Table 8A-2). The bottom end of the range (i.e., 1E-02/yr) was selected as the frequency of the fault. Therefore, the sample line break event is considered to be a frequent fault (i.e., >1E-3/yr) for the purposes of DB classification.

1. As discussed in Chapter 8, the frequency for initiating events from the PSA is used in both Chapters 8 and 9 with the sole purpose of supporting the categorisation of the fault to a specific DB category. As noted in Chapter 8, these probabilities should not be considered to be representative of actual frequency of the events, and for several events they can be significantly conservative. Detailed PSA results and their basis are discussed in Chapter 10 of this PCSR.

Design Basis Class

On the basis of the assessed frequency (>1E-3/y) and an unmitigated offsite radiological consequence for a member of the public of <1 mSv and unmitigated onsite radiological consequence for a worker of < 20 mSv, the bounding sample line break fault is classified as an HFLC fault, as discussed in Chapter 8.

9.6.2.0.1 Rupture in the Chemical and Volume Control System Discharge Line

When excess primary coolant is generated because of boron dilution operations, the CVS purification flow is diverted out of containment to the WLS. Before passing outside containment, the flow stream passes through the CVS heat exchangers (HXs) and mixed-bed demineraliser. The flow leaving the containment is at a temperature of less than 60.0°C (140°F) and has been cleaned by the demineraliser. The flow out of a postulated break in this line is limited to the CVS purification flow rate of 22.71 m^3/hr (100 gpm), which supports small (<3/8-inch (0.95 cm) diameter break) LOCA.

9.6.2.0.2 Rupture in the Reactor Coolant System Sample Line

The liquid sample lines that penetrate the containment convey liquid samples from their RCS sources to either the grab sample panel (GSP) or the laboratory. The GSP is situated in the sampling room in the auxiliary building, and the radiological chemistry facility is located immediately above this room. The liquid lines contain one containment isolation valve inside the containment and one containment isolation valve outside the containment. One liquid sample line set of valves are normally open only when RCS hot leg sampling is being performed. The failure of the sample line is postulated to occur between the isolation valve outside the containment and the grab sample panel. The maximum loss of coolant from the primary circuit for the RCS sample line break is calculated to be 22.71 m^3/hr (100 gpm) The nozzles where the sample lines connect to the reactor coolant piping include an orifice with a 3/8-inch (0.95 cm) hole. This hole restricts the flow so that the loss through a break in one of the sample lines can be made up by normal charging flow provided by CVS.

9.6.2.1 Failure of Small Lines Carrying Primary Coolant Outside Containment (Fault 1.9.2)

When excess primary coolant is generated because of boron dilution operations, the chemical and volume control system purification flow is diverted out of containment to the liquid radwaste system. Before passing outside containment, the flow stream passes through the chemical and volume control system heat exchangers and mixed bed demineralizer. The flow leaving the containment is at a temperature of less than 60°C (140°F) and has been cleaned by the demineralizer. The flow out a postulated break in this line is limited to the chemical and volume control system purification flow rate of 22.71 m^3/hr (100 gpm). Considering the low temperature of the flow and the reduced iodine activity because of demineralization, this event is not analysed. The postulated sample line break is more limiting.

A continuous sample of the RCS hot legs flows through normally open isolation valves inside and outside containment when sampling. The failure of the sample line is postulated to occur between the isolation valve outside the containment and the sample panel. Because the isolation valves are open only when sampling, the loss of sample flow provides indication of the break to plant personnel. In addition, a break in a sample line results in activity release and a resulting actuation of area and air radiation monitors. The loss of coolant reduces the pressuriser level and creates a demand for makeup to the reactor coolant system. Upon indication of a sample line break, the operator would take action to isolate the break.

The sample line includes a flow restrictor at the point of sample to limit the break flow to less than 22.71 m^3/hr (100 gpm). The nozzles where the sample lines connect to the reactor coolant piping include an orifice with a 3/8-inch (0.95 cm) hole. This hole restricts the flow so that the loss through a break in one of the sample lines can be made up by normal charging flow provided by CVS.

The liquid sampling lines passing through the containment are 0.635 cm (1/4 inch) tubing which further restricts the break flow of a sampling line outside containment to much less than the flow that could pass through the 3/8-inch (0.95 cm) restrictor inside containment. Doses are based on a conservative break flow of 29.53 m^3/hr (130 gpm) with isolation after 30 minutes.

Given the fact that the leak being considered is large enough to solicit immediate operator attention and the plant abnormal operating procedures will provide direct guidance to isolate RCS sampling as part of RCS leak rate determination, the 30 minute period assumed for manual operator action to isolate a sample line leak is a valid assumption.

In common with other radiologically controlled areas in the auxiliary and annex buildings, the sampling area is serviced by the radiologically controlled area ventilation system (VAS). The VAS consists of two separate subsystems, the fuel handling area ventilation subsystem, and the auxiliary or annex building ventilation subsystem. These are combined into a single extract. Both of these subsystems are once-through-type ventilation systems.

The sample line break fault was assigned an HFLC DB classification (see Section 9.6.2.0 above), and while there is no formal requirement regarding safety measures for this class, it is considered best practice to identify one Class 2 system for each Category B safety function (see Chapter 8). With the present arrangements, the Category B functional requirement is for environmental release control that is met by manual operator action following local radiation or contamination alarm as a Class 2 system. The ALARP aspects of introducing possible additional safety measures are discussed below in Section 9.6.2.1.4.

9.6.2.1.2 Radiological Consequences

There is no fuel damage as a result of the accident. Therefore, the most significant radionuclide releases are the noble gases, alkali metals, and iodines that are present in the primary coolant, become airborne, and are released to the environment as a result of the accident.

9.6.2.1.2.1 Release Pathway

The consequence assessment conservatively considers the release of 29.53 m^3/hr (130 gpm) of primary coolant into the sample room in the auxiliary building for 30 minutes. The reactor coolant that is spilled from the break is assumed to be at high temperature and pressure. A portion of the radionuclides released are assumed to become airborne. The radionuclides are assumed to be released directly to the environment, although a large fraction of the airborne iodine and alkali metals are expected to deposit on building surfaces.

9.6.2.1.2.2 Dose Calculation Models

The models used to calculate doses are provided in Appendix 9A.

9.6.2.1.2.3 Analytical Assumptions and Parameters

The assumptions and parameters used in the analysis are listed in Table 9.6.2-1.

9.6.2.1.2.4 Doses

The calculated maximum doses for all relevant pathways (inhalation, cloudshine, and groundshine) are as follows:

- Offsite dose: 0.52 mSv Worker dose: 1.6 mSv

These doses are within the Target 4 BSL for frequent faults (1 mSv offsite and 20 mSv onsite).

The limiting conditions for operation of the Technical Specifications used in the dose assessment are provided in Table 9.6.2-2. The Table 9.6.2-2 values ensure the Target 4 BSL is met.

9.6.2.1.3 Diverse Mitigation

The primary protection for this fault category is the RMS radiation alarm, which is a Class 1 SSC (see Table 9.6.2-3). Table 9.6.2-4 provides the operator actions utilized in the design basis analysis. Diverse protection via Class 1 or Class 2 SSCs is not available for this event; however, the consequences of the unmitigated event are low and the operator has the capability of detecting the event via main control room indications. Reactor protection, both primary and diverse, is bounded by the SBLOCA fault (1.8.1 – 1.8.3).

9.6.2.1.4 As Low As Reasonably Practicable Assessment

Although the DB requirements for the sample line break fault have been met, consideration has been given to including high-efficiency particulate air (HEPA) filtration into the ventilation train as an additional safety measure. The VFS HEPA filtration could provide a dose reduction if the VAS flow was isolated and diverted to this system on a high-radiation signal. Nevertheless, the cost of implementing such a measure is considered to be grossly disproportionate to benefit, since it would take a spillage of over 28000 kg (28 m^3) of primary coolant to cause an offsite consequence >1 mSv, and so faults involving spillage of a few tens of litres of primary coolant would not represent a significant radiological hazard.

In addition to the visual flow behaviour and local radiological alarms, the CVS makeup system would also provide a general indication of RCS leakage. The CVS makeup balance inventory is performed on a regular basis and can identify a minimum detectable leak of 2.95E-2 m^3/hr (0.13 gpm). This detection limit is much lower than the flow rate considered for the bounding fault.

9.6.2.1.5 Conclusions

Radiological consequences are within the Target 4 BSL for frequent faults (i.e., 1 mSv offsite and 20 mSv onsite). Thus, the identification of necessary Class 1 SSC is adequate to meet DB requirements.

It has been shown that the AP1000 plant design includes adequate systems for the protection of this fault, which limit the radiological consequences such that they are compliant with the SAP targets and the risks have been reduced to be ALARP.

9.6.2.2 References

9.6.2-1 Not Used.

Table 9.6.2-1. Parameters Used In Evaluating The Radiological Consequences Of A Small Line Break Outside Containment

Reactor coolant iodine activity	Initial activity equal to the operating limit for reactor coolant activity of 9.25E6 Bq/kg (0.25 µCi/g) dose equivalent I-131 (see Table 9A-1)
Reactor coolant noble gas activity	Equal to the operating limit for reactor coolant activity of 2.6E9 Bq/kg (70 µCi/g) dose equivalent Xe-133 (see Table 9A-1)
Reactor coolant alkali metal activity	Design basis activity (see Table 9A-1)
Break flow rate	29.53 (1) m^3/hr (130 gpm)
Activity in break flow becoming airborne (fraction) Iodine Noble Gases Alkali Metals	 0.1 1.0 0.1
Duration of accident	0.5 hr
Offsite atmospheric dispersion factors	See Table 9A-5
Control room modelling	See Appendix 9A

Note:

1. At density of 1000 kg/m^3 (62.4 lbm/ft^3).

Table 9.6.2-2. Small Line Break Outside Containment Technical Specifications Used In Dose Analysis

Limit or Condition	Tech Spec Identification and Notes
Primary coolant specific activity	3.4.10 dose equivalent specific activity to be < 9.25E6 Bq/kg (0.25 μCi/g) for I-131 and < 2.6E9 Bq/kg (70 μCi/g) for Xe-133

Table 9.6.2-3. Small Line Break Outside Containment Mitigation Features

Category B Safety Function	Provision	SSCs	Classification
Environmental release control	Primary means	Local radiation alarm	2

Note:
The operator response is to isolate the sample line at a safe point (maybe inside containment), as well as implement evacuation procedure.

Table 9.6.2-4. Small Line Break Outside Containment Potential Operator Actions

Operator Action	Class
Isolate sample line at a safe point (may be inside containment) as well as implement evacuation procedure	2

9.6.3 Steam Generator Tube Rupture (Fault 1.11.1)

9.6.3.0 Introduction and Overview of Fault

A steam generator tube rupture (SGTR) is defined as the sudden failure of one or more SG tubes, giving rise to a leakage with a rate that is beyond the makeup capability of the CVS. Depending upon the size of the leakage and the plant operating conditions at the initiation of the fault, SGTR can lead to significant contamination of the secondary system because of ingress of coolant from the RCS. The range of breach sizes covered by SGTR falls within the SBLOCA category.

This section analyses SGTRs at power conditions, Fault 1.11.1 (see Appendix 8A).

The AP1000 design provides automatic protective actions to mitigate the consequences of an SGTR. The automatic actions include reactor trip, actuation of the PRHR HX, initiation of CMT flow, termination of pressuriser heater operation, and isolation of CVS flow and SFW flow on High-3 SG level coincident with reactor trip (P-4). These protective actions result in automatic cooldown and depressurisation of the RCS, termination of the break flow and release of steam to the atmosphere, and long-term maintenance of stable conditions in the RCS. These protection systems serve to prevent SG overfill and to maintain radiological consequences within the allowable guideline values for a DB SGTR. The operator may take actions that would provide a more rapid mitigation of the consequences of an SGTR.

Because of the series of alarms, the operator can readily determine when an SGTR occurs, identify and isolate the ruptured SG, and complete the required recovery actions to stabilise the plant and terminate the primary-to-secondary break flow. The recovery procedures are completed on a time scale that terminates break flow to the secondary system before SG overfill occurs and limits the doses to acceptable levels without actuation of the ADS. Indications and controls are provided to enable the operator to carry out these functions, but if operator intervention were to fail, automatic protective action would be initiated.

For the purposes of the DB analysis, no credit is taken for operator actions and it is assumed that offsite power is not available (e.g., because of a turbine trip). Under these pessimistic circumstances, an SGTR fault is likely to result in some release of contaminated steam from the secondary circuit through the steam release valves to the atmosphere. This release will be terminated as a result of automatic recovery actions. Therefore, the release is limited in duration, but has the potential to give a radiological dose to members of the public near the site boundary and to onsite workers, including control room staff.

The significant radionuclide releases from the SGTR are noble gases, alkali metals (caesium and rubidium), and iodines that become airborne and are released to the environment as a result of the accident. These originate from the reactor fuel, a small fraction of which is tolerated by the Tech Specs to have defective cladding. A small amount of activity leaks out through these defects into the primary coolant (RCS).

During normal, steady operation, the concentration of activity in the RCS reaches an equilibrium value when the release rate from the fuel equals the rate of removal by decay and cleanup. During a transient such as an SGTR, the release rate of iodine and other radionuclides increases. This phenomenon is known as spiking and can result in much higher concentrations of activity in the RCS than the equilibrium value for a short time (some hours). The spiking phenomenon is taken into account in the assessment of radiological release from the fault.

In the sections below, the fault is first described in more detail; the initial event frequency and the design basis class are provided and the bounding fault or faults are identified (if needed). The analysed faults are presented individually in Table 8A-2.

The analysed fault(s) are described in additional detail in the subsequent sections to complete the safety case for each fault, including:

- Identification of Causes and Accident Description
- Design Basis Analysis of Effects and Consequences
- Assessment of the Radiological Consequences for the DBA
- Diverse Mitigation and ATWT for Frequent Faults
- ALARP assessment
- Conclusions

9.6.3.0.1 Steam Generator Tube Rupture Fault Description

Description

This fault has the potential to release radioactivity to the environment through the secondary circuit steam release valves. Therefore, it represents a loss of containment by the primary circuit through leakage to the secondary circuit.

The more severe fault is considered to be a single tube rupture, since the plant response to a multiple SGTR is substantially the same as, or more favourable than, the response to a single SGTR. A larger break introduces mass into the ruptured SG at a faster rate. However, the larger flow rate also results in earlier actuation of the passive safety systems CMT and PRHR, which terminates the event earlier. Using transient analysis, runs were performed to investigate the impact of multiple SGTRs on the AP1000 reactor (Reference 9.6.3-1). The impact of these competing effects was investigated for 0.5 tube, one tube, two tubes, and five tubes and it was found that the limiting case is one ruptured tube.

The fault is further subdivided into two cases. In one case, referred to as the accident-initiated iodine spike case, an iodine spike is assumed to be initiated by the accident, with the spike causing an increasing level of iodine in the reactor coolant. In the second case, referred to as the pre-accident spike case, the iodine spike is assumed to have occurred before the tube ruptures, with the reactor coolant iodine concentration reaching a maximum at the time the accident occurs. The probability of this second case occurring is small.

Initiating Event Frequency[1]

The fault schedule (Appendix 8A) gives the IEF for SGTR as 3.3E-03/yr (Table 8A-2), which makes the fault a frequent fault in the UK definition. The fault is assessed as a frequent fault (DB2).

1. As discussed in Chapter 8, the frequency for initiating events from the PSA is used in both Chapters 8 and 9 with the sole purpose of supporting the categorization of the fault to a specific DB category. As noted in Chapter 8, these probabilities should not be considered to be representative of actual frequency of the events, and for several events they can be significantly conservative. Detailed PSA results and their basis are discussed in Chapter 10 of this PCSR.

9.6.3.1 Identification of Cause and Accident Description

9.6.3.1.1 Introduction

The accident examined is the complete severance of a single steam generator tube. The accident is assumed to take place at power with the reactor coolant contaminated with fission products corresponding to continuous operation with a limited number of defective fuel rods within the allowance of the Technical Specifications. The accident leads to an increase in contamination of the secondary system due to leakage of radioactive coolant from the reactor coolant system. In the event of a coincident loss of offsite power, or a failure of the condenser steam dump, discharge of radioactivity to the atmosphere takes place via the steam generator power-operated relief valves or the safety valves.

The assumption of a complete tube severance is conservative because the steam generator tube material is a corrosion-resistant and ductile material. The more probable mode of tube failure is one or more smaller leaks of undetermined origin. Activity in the secondary side is subject to continual surveillance, and an accumulation of such leaks, which exceeds the limits established in the Technical Specifications, is not permitted during operation.

The AP1000 design provides automatic protective actions to mitigate the consequences of an SGTR. The automatic actions include reactor trip, actuation of the PRHR heat exchanger, initiation of core makeup tank flow, termination of pressuriser heater operation, and isolation of chemical and volume control system flow and startup feedwater flow on High-3 steam generator level coincident with reactor trip (P-4). These protective actions result in automatic cooldown and depressurisation of the reactor coolant system, termination of the break flow and release of steam to the atmosphere, and long-term maintenance of stable conditions in the reactor coolant system. These protection systems serve to prevent steam generator overfill (see discussion in Sections 9.6.3.1.2 and 9.6.3.1.3) and to maintain offsite radiological consequences within the allowable guideline values for a design basis SGTR.

Although not required, the operator may take actions that would provide a more rapid mitigation of the consequences of an SGTR. Because of the series of alarms described next, the operator can readily determine when an SGTR occurs, identify and isolate the ruptured steam generator, and complete the required recovery actions to stabilize the plant and terminate the primary-to-secondary break flow. The recovery procedures are completed on a time scale that terminates break flow to the secondary system before steam generator overfill occurs and limits the offsite doses to acceptable levels without actuation of the ADS. Indications and controls are provided to enable the operator to carry out these functions.

9.6.3.1.2 Sequence of Events for a Steam Generator Tube Rupture, Primary

The following sequence of events occurs following an SGTR:

- Pressuriser low pressure and low level alarms are actuated and chemical and volume control system makeup flow and pressuriser heater heat addition starts or increases in an attempt to maintain pressuriser level and pressure. On the secondary side, main feedwater flow to the affected steam generator is reduced because the primary-to-secondary break flow increases steam generator level.

- The condenser air removal discharge radiation monitor, steam generator blowdown radiation monitor, and/or main steam line radiation monitor alarm indicate an increase in radioactivity in the secondary system.

- Continued loss of reactor coolant inventory leads to a reactor trip generated by a Low-2 pressuriser pressure or over-temperature ΔT signal. Following reactor trip, the SGTR leads to a decrease in reactor coolant pressure and pressuriser level, counteracted by chemical and volume control system flow and pressuriser heater operation. A safeguards ("S") signal from low pressuriser pressure actuates the core makeup tanks. The "S" signal automatically terminates the normal feedwater supply and trips the reactor coolant pumps. The core makeup tank actuation signal will actuate the PRHR heat exchanger and trip pressuriser heaters. Startup feedwater flow is initiated on a Low-2 steam generator narrow range level signal and controls the steam generator levels to the programmed level.

- The reactor trip automatically trips the turbine, and if offsite power is available, the steam dump valves open permitting steam dump to the condenser. In the event of a loss of offsite power or loss of the condenser, the steam dump valves automatically close to protect the condenser. The steam generator pressure rapidly increases resulting in steam discharge to the atmosphere through the steam generator power-operated relief valves and/or the safety valves.

- Following reactor trip and core makeup tank and PRHR actuation, the PRHR heat exchanger operation – combined with startup feedwater flow, borated core makeup tank flow, and chemical and volume control system flow – provides a heat sink that absorbs the decay heat. This reduces the amount of steam generated in the steam generators and steam bypass to the condenser. In the case of loss of offsite power, this reduces steam relief to the atmosphere.

- Injection of the chemical and volume control system and core makeup tank flow stabilizes reactor coolant system pressure and pressuriser water level, and the reactor coolant system pressure trends toward an equilibrium value, where the total injected flow rate equals the break flow rate.

9.6.3.1.3 Steam Generator Tube Rupture Automatic Recovery Actions

The AP1000 incorporates several protection system and passive design features that automatically terminate a steam generator tube leak and stabilize the reactor coolant system. Following an SGTR, the injecting chemical and volume control system flow (and pressuriser heater heat addition if the pressure control system is operating) maintains the primary-to-secondary break flow and the ruptured steam generator secondary level increases as break flow accumulates in the steam generator. Eventually, the ruptured steam generator secondary level reaches the high and High-3 steam generator narrow range level setpoint, which is near the top of the narrow range level span.

The AP1000 protection system automatically provides several Class 1 actions to cool down and depressurise the reactor coolant system, terminate the break flow and steam release to the atmosphere, and stabilize the reactor coolant system in a safe condition. The Class 1 actions include initiation of the PRHR system heat exchanger, isolation of the chemical and volume control system pumps and pressuriser heaters, and isolation of the startup feedwater pumps. In addition, the protection and safety monitoring system provides a Class 1 signal to trip the redundant, Class 2 related pressuriser heater breakers.

Actuating the PRHR heat exchanger transfers core decay heat to the IRWST and initiates a cooldown (and a consequential depressurisation) of the reactor coolant system.

Isolation of the chemical and volume control system pumps and pressuriser heaters

minimizes the repressurisation of the primary system. This allows primary pressure to equilibrate with the secondary pressure, which effectively terminates the primary-to-secondary break flow. Because the core makeup tank continues to inject when needed to provide boration following isolation of the chemical and volume control system pumps, isolating the chemical and volume control system pumps does not present a safety concern.

Isolation of the startup feedwater provides protection against a failure of the startup feedwater control system, which could potentially result in the ruptured steam generator being overfilled.

With decay heat removal by the PRHR heat exchanger, steam generator steaming through the power-operated relief valves ceases and steam generator secondary level is maintained.

9.6.3.1.4 Steam Generator Tube Rupture Assuming Operator Recovery Actions

Operator actions are not required for the primary safety case of the SGTR event; however, likely operator actions are explained below.

In the event of an SGTR, the operators can diagnose the accident and perform recovery actions to stabilize the plant, terminate the primary-to-secondary leakage, and proceed with orderly shutdown of the reactor before actuation of the automatic protection systems. The operator actions for SGTR recovery are provided in the plant emergency operating procedures. The major operator actions include the following:

- Identify the ruptured steam generator – The ruptured steam generator can be identified by an unexpected increase in steam generator narrow range level or a high radiation indication from any main steam line monitor, steam generator blowdown line monitor, or steam generator sample.

- Isolate the ruptured steam generator – Once the steam generator with the ruptured tube is identified, recovery actions begin by isolating steam flow from and stopping feedwater flow to the ruptured steam generator.

- Cooldown of the reactor coolant system using the intact steam generator or the PRHR system – After isolation of the ruptured steam generator, the reactor coolant system is cooled as rapidly as possible to less than the saturation temperature corresponding to the ruptured steam generator pressure. This provides adequate subcooling in the reactor coolant system after depressurisation of the reactor coolant system to the ruptured steam generator pressure in subsequent actions.

- Depressurise the reactor coolant system to restore reactor coolant inventory – When the cooldown is completed, the chemical and volume control system and core makeup tank injection flow increases the reactor coolant system pressure until break flow matches the total injection flow. Consequently, these flows must be terminated or controlled to stop primary-to-secondary leakage. However, adequate reactor coolant inventory must first be provided. This includes both sufficient reactor coolant subcooling and pressuriser inventory to maintain a reliable pressuriser level indication after the injection flow is stopped.

Because leakage from the primary side continues after the injection flow is stopped, until reactor coolant system and ruptured steam generator pressures equalise, the reactor coolant system is depressurised to provide sufficient inventory to verify that the pressuriser level remains on span after the pressures equalise.

- Termination of the injection flow to stop primary to secondary leakage – The previous actions establish adequate reactor coolant system subcooling, a secondary side heat sink, and sufficient reactor coolant inventory to verify that injection flow is no longer needed. When these actions are completed, core makeup tank and chemical and volume control system flow is stopped to terminate primary-to-secondary leakage. Primary-to-secondary leakage continues after the injection flow is stopped until the reactor coolant system and ruptured steam generator pressures equalise. Chemical and volume control system makeup flow, letdown, pressuriser heaters, and decay heat removal via the intact steam generator or the PRHR heat exchanger are then controlled to prevent repressurisation of the reactor coolant system and reinitiation of leakage into the ruptured steam generator.

Following the injection flow termination, the plant conditions stabilize and the primary-to-secondary break flow terminates. At this time, a series of operator actions is performed to prepare the plant for cooldown to cold shutdown conditions. The actions taken depend on the available plant systems and the plan for further plant repair and operation.

9.6.3.2 Design Basis Mitigation

An SGTR results in the leakage of contaminated reactor coolant into the secondary system and subsequent release of a portion of the activity to the atmosphere. An analysis is performed to demonstrate that the offsite radiological consequences resulting from an SGTR are within the allowable guidelines.

One of the concerns for an SGTR is the possibility of steam generator overfill because this can potentially result in a significant increase in the offsite radiological consequences. Automatic protection and passive design features are incorporated into the AP1000 design to automatically terminate the break flow to prevent overfill during an SGTR. These features include actuation of the PRHR system, isolation of chemical and volume control system flow, and isolation of startup feedwater.

An analysis is performed, without modelling expected operator actions to isolate the ruptured steam generator and cool down and depressurise the reactor coolant system, to demonstrate the role that the AP1000 design features have in preventing steam generator overfill. The limiting single failure for the overfill analysis is assumed to be the failure of the startup feedwater control valve to throttle flow when nominal steam generator level is reached. Other conservative assumptions that maximize steam generator secondary volume (such as high initial steam generator level, minimum initial reactor coolant system pressure, loss of offsite power, maximum chemical and volume control system injection flow, maximum pressuriser heater addition, maximum startup feedwater flow, and minimum startup feedwater delay time) are also assumed.

The results of this analysis demonstrate the effectiveness of the AP1000 protection system and passive system design features and support the conclusion that an SGTR event would not result in steam generator overfill.

For determining the offsite radiological consequences, an SGTR analysis is performed assuming the limiting single failure and limiting initial conditions relative to offsite doses. Because steam generator overfill is prevented for the AP1000, the results of this analysis

represent the limiting radiological consequences for an SGTR.

A thermal-hydraulic analysis is performed to determine the plant response for a design basis SGTR, the integrated primary-to-secondary break flow, and the mass releases from the ruptured and intact steam generators to the condenser and to the atmosphere. This information is then used to calculate the radioactivity release to the environment and the resulting radiological consequences.

9.6.3.2.1 DBA Method of Analysis

9.6.3.2.1.1 Computer Program

The plant response following an SGTR until the primary-to-secondary break flow is terminated is analysed with the LOFTTR2 program (Reference 9.6.3-2). The LOFTTR2 program is modified to model the PRHR system, core makeup tanks, and protection system actions appropriate for the AP1000. These modifications to LOFTTR2 are described in WCAP-14234, Revision 1 (Reference 9.6.3-3).

9.6.3.2.1.2 Analysis Assumptions

The accident modelled is a double-ended break of one steam generator tube located at the top of the tube sheet on the outlet (cold leg) side of the steam generator. The location of the break on the cold leg side of the steam generator results in higher initial primary-to-secondary leakage than a break on the hot side of the steam generator.

The reactor is assumed to be operating at full power at the time of the accident, and the initial secondary mass is assumed to correspond to operation at nominal steam generator mass minus an allowance for uncertainties. Offsite power is assumed to be lost and the rods are assumed to be inserted at the start of the event because continued operation of the reactor coolant pumps has been determined to reduce flashing of primary-to-secondary break flow and, consequently, lower offsite radiological doses. Maximum chemical and volume control system flows and pressuriser heater heat addition are assumed immediately (even though offsite power is not available) to conservatively maximize primary-to-secondary leakage. The steam dump system is assumed to be inoperable, consistent with the loss of offsite power assumption, because this results in steam release from the steam generator power-operated relief valves to the atmosphere following reactor trip. The chemical and volume control system and pressuriser heater modelling is conservatively chosen to delay the Low-3 pressuriser pressure “S” and the low-2 pressuriser level signal and associated protection system actions.

The limiting single failure is assumed to be the failure of the ruptured steam generator power-operated relief valve. Failure of this valve in the open position causes an uncontrolled depressurisation of the ruptured steam generator, which increases primary-to-secondary leakage and the mass release to the atmosphere.

It is assumed that the ruptured steam generator power-operated relief valve fails open when the low-2 pressuriser level signal is generated. This results in the maximum integrated flashed primary-to-secondary break flow.

The valve is subsequently isolated when the associated block valve is automatically closed on a low steam line pressure protection system signal.

No operator actions are modelled in this limiting analysis, and the plant protection system provides the protection for the plant. Not modelling operator actions is conservative because

the operators are expected to have sufficient time to recover from the accident and supplement the automatic protection system. In particular, the operator would take action to reduce the primary pressure before the High-3 steam generator level coincident with reactor trip (P-4) chemical and volume control and startup feedwater system shutoff signals are generated. It is also expected that the operator can close the block valve to the ruptured steam generator power-operated relief valve in much shorter time than the automatic protection signal. The operators can quickly diagnose a power-operated relief valve failure based on the rapid depressurisation of the steam generator and increase in steam flow. They can then close the block valve from the control panel.

Consistent with the assumed loss of offsite power, the main feedwater pumps coast down and no startup feedwater is assumed to conservatively minimize steam generator secondary inventory and thus maximize secondary activity concentration and steam release.

9.6.3.2.2 DBA Credited SSCs

For the DB, all of the claimed SSCs are Class 1, and are listed in Table 9.0-10. The presented DBA ends when break flow is terminated; however, essential safety functions for the long term safe shutdown analysis (Appendix 9C) bound safe shutdown response for this event. The primary core cooling is provided by the PRHR and passive containment cooling. Other SSCs include the steam generator safety and/or relief valves. The PMS provides the following:

- RT on Low-2 pressuriser level (analysed at event initiation)
- CMTs on Low-2 pressuriser level
- PRHR on Low-2 pressuriser level (via CMT actuation signal)
- Containment isolation on Low-2 steamline pressure
- PCS on High-2 containment pressure

9.6.3.2.3 DBA Results

The sequence of events for this transient is presented in Table 9.6.3-1. The system responses to the SGTR accident are shown in Figures 9.6.3-1 to 9.6.3-9.

Offsite power is lost concurrent with the rupture of the tube. The reactor trips due to the loss of offsite power. The main feedwater pumps are assumed to coast down following reactor trip. The startup feedwater pumps are conservatively assumed not to start. Following the tube rupture, reactor coolant flows from the primary into the secondary side of the ruptured steam generator. In response to this loss of reactor coolant, pressuriser level and reactor coolant system pressure decreases as shown in Figures 9.6.3-1 and 9.6.3-2. As a result of the decreasing pressuriser level and pressure, two chemical and volume control system pumps are automatically initiated to provide makeup flow and the pressuriser heaters turn on.

After reactor trip, core power rapidly decreases to decay heat levels and the core inlet to outlet temperature differential decreases. The turbine stop valves close, and steam flow to the turbine is terminated. The steam dump system is conservatively assumed to be inoperable. The secondary side pressure increases rapidly after reactor trip until the steam generator power-operated relief valves (and safety valves, if their setpoints are reached) lift to dissipate the energy, as shown in Figure 9.6.3-3.

Maximum heat addition to the pressuriser from the pressuriser heaters increases the primary pressure.

As the leak flow continues to deplete primary inventory, low pressuriser level "S" and core makeup tank and PRHR actuation signals are reached. Power to the pressuriser heaters is shut off so that they will not provide additional heat to the primary should the pressuriser level return. The ruptured steam generator power-operated relief valve is assumed to fail open at this time.

The failure causes the intact and ruptured steam generators to rapidly depressurise (Figure 9.6.3-3). This results in an initial increase in primary-to-secondary leakage and a decrease in the reactor coolant system temperatures. Both the intact and ruptured steam generators depressurise because the steam generators communicate through the open steam line isolation valves.

The decrease in the reactor coolant system temperature results in a decrease in the pressuriser level and reactor coolant system pressure (Figures 9.6.3-1 and 9.6.3-2). Depressurisation of the primary and secondary systems continues until the Low-2 steam line pressure setpoint is reached. As a result, the steam line isolation valves and intact and ruptured steam generator power-operated relief block valves are closed.

Following closure of the block valves, the primary and secondary pressures and the ruptured steam generator secondary water volume and mass increase as break flow accumulates. This increase continues until the steam generator secondary level reaches the High-3 narrow range level when the chemical and volume control and startup feedwater systems are isolated.

With continued reactor coolant system cooldown, depressurisation provided by the PRHR heat exchanger, and with the chemical and volume control system isolated, primary system pressure eventually falls to match the secondary pressure. The break flow terminates as shown in Figure 9.6.3-5, and the system is stabilized in a safe condition. As shown in Figure 9.6.3-8, steam release through the intact loop, unfaulted power-operated relief valve does not occur following PRHR initiation because the PRHR is capable of removing the core decay heat.

As shown in Figure 9.6.3-9, the core makeup tank flow trends toward zero because the gravity head diminishes as the core makeup tank temperature approaches the reactor coolant system temperature due to the continued balance line flow. The core makeup tank remains full, and ADS actuation does not occur.

The ruptured steam generator water volume is shown in Figure 9.6.3-6. The water volume in the ruptured steam generator when the break flow is terminated is significantly less than the total steam generator volume of greater than 255 m^3 (9000 ft^3).

Appendix 9C provides the means for safe shutdown.

9.6.3.2.3.1 Fuel Damage

The design basis SGTR event does not result in fuel failures. In the event of an SGTR, the reactor coolant system depressurises due to the primary-to-secondary leakage through the ruptured steam generator tube. This depressurisation reduces the calculated DNBR. The depressurisation prior to reactor trip for the SGTR has been compared to the depressurisation for the reactor coolant system pressurisation accidents analysed in Section 9.6.1. The rate of depressurisation is much slower for the SGTR than for the reactor coolant system

depressurisation accidents. Following reactor trip, the DNBR increases rapidly. Thus, the conclusion of Section 9.6.1, that the calculated DNBR remains above the limit, is extended to the SGTR analysis, justifying the assumption of no failed fuel.

9.6.3.2.3.2 Steam Generator Overfill

One of the concerns for an SGTR is the possibility of SG overfill because it can potentially result in a significant increase in the offsite radiological consequences. Automatic protection and passive design features are incorporated into the AP1000 design to automatically terminate the break flow to prevent overfill during an SGTR. These features include actuation of the PRHR system, isolation of CVS flow, and isolation of SFW.

An essential step in the SGTR DB justification is to demonstrate that margin to SG overfill is maintained for an appropriate, fully conservative, bounding case. A thermal-hydraulic analysis has been performed for such a case (referred to as the margin to overfill (MTO) case). As for the associated thermal-hydraulic modelling to support the radiological consequences assessment for SGTR, this has been done without modelling expected operator actions to isolate the ruptured SG, and to cool down and depressurise the RCS. For this case, SFW is modelled with a maximum flow rate and minimum start delay time. The limiting single failure for the overfill analysis is assumed to be the failure of the SFW control valve to throttle flow when nominal SG level is reached. The remaining assumptions identified previously for the analysis of the DB fault apply in this case.

The sequence of events is listed in Table 9.6.3-2. The calculated ruptured SG water volume is shown as a function of time in Figure 9.6.3-10. The peak water volume, prior to primary to secondary break flow termination at 19,767 sec, is determined to be 252 m^3 (8898 ft^3), corresponding to a margin to overfill of 3.7 m^3 (129 ft^3).

The results of this analysis therefore support the conclusion that an SGTR event would not result in SG overfill.

9.6.3.3 Diverse Mitigation

9.6.3.3.1 Diverse Mitigation for ATWT

As this is a DB2 frequent fault, a diverse means of providing the Category A safety functions is provided. For this event the diverse features are also Class 1 except for the C&I, which is Class 2. Table 9.6.3-5 summarizes the SSCs from this fault assessment, and this information is supported by Reference 9.6.3-4. Table 9.6.3-6 provides the operator actions utilized in the diverse safety case. DAS provides the following:

- Rods are assumed to not insert due to a mechanical CCF
- PRHR and CMTs on Low pressuriser level
- PCS and containment isolation on High containment temperature

An analysis evaluating diverse mitigation has not been explicitly performed; however, this will be addressed during site licensing. This is considered acceptable for GDA as the consequences of this fault are bounded by other those of a SBLOCA (See Section 9.6.5).

9.6.3.3.2 Diverse Mitigation for Core Cooling

The diverse core cooling is provided by passive feed and bleed using PXS injection and ADS

venting (all Class 1) via DAS (Class 2). The DAS provides the following:

- RT on Low SG WR level
- Manual ADS, IRWST injection, and containment recirculation
- PCS and containment isolation on High containment temperature

The loss of normal feedwater diverse core cooling, as analysed in Section 9.2.7.3.2, is bounding of this event.

9.6.3.4 Radiological Consequences

9.6.3.4.1 DBA Source Term

There is no fuel damage as a result of the accident. Therefore, the most significant radionuclide releases from the SGTR are the noble gases, alkali metals, and iodines that are present in the primary and secondary coolants, become airborne, and are released to the environment as a result of the accident.

The evaluation assumes that the reactor has been operating with a limited number of fuel rods containing cladding defects and that leaking steam generator tubes have resulted in a build-up of activity in the secondary coolant.

The methodology assesses two different reactor coolant iodine source terms, both of which consider the iodine-spiking phenomenon. In one case, the initial iodine concentrations are assumed to be those associated with the equilibrium operating limit for primary coolant iodine activity. The iodine spike is assumed to be initiated by the accident, with the spike causing an increasing level of iodine in the reactor coolant.

The second case assumes that the iodine spike occurs prior to the accident and that the maximum resulting reactor coolant iodine concentration exists at the time the accident occurs.

The secondary coolant iodine and alkali metal concentrations are assumed to be 10 percent of the primary concentrations. Noble gases are not assumed to accumulate in the secondary coolant

9.6.3.4.2 DBA Release Pathways

Activity release for an SGTR occurs through two pathways.

- Activity is transferred to the secondary system via primary-to-secondary leakage and break flow, and is then released to the environment through steaming from the intact and ruptured steam generators. Iodine, alkali metal, and noble gas activity is released via this transfer.
- Activity that is present in the secondary coolant prior to the accident is released to the environment via steaming from the intact and ruptured steam generators. Iodine and alkali metal activity is released via this transfer.

9.6.3.4.3 DBA Dose Calculation Models

The models used to calculate doses are provided in Appendix 9A.

9.6.3.4.4 DBA Analytical Assumptions and Parameters

The sequence of events in listed in Table 9.6.3-1. The assumptions and parameters used in the analysis are listed in Table 9.6.3-3.

9.6.3.4.5 DBA Doses

In the case where offsite power remains available, there is no release of activity to the environment and the Target 4 BSOs (0.01 mSv offsite and 0.1 mSv onsite) are met.

In the case where offsite power is lost, the highest doses are found to be for the accident-initiated iodine spike. The calculated maximum doses for all relevant pathways (inhalation, cloudshine, and groundshine) are as follows:

Offsite dose: 0.91 mSv Worker dose: 4.8 mSv

These doses are within the Target 4 BSL for frequent faults (1 mSv offsite and 20 mSv onsite).

The limiting conditions for operation of the Technical Specifications used in the dose assessment are provided in Table 9.6.3-4. The Table 9.6.3-4 values ensure the Target 4 BSLs are met.

9.6.3.4.6 Diverse Mitigation

Both diverse ATWT and diverse core cooling scenarios discussed in Section 9.6.3.3 demonstrate that there is no significant fuel damage expected. For a diverse mitigation radiological consequences analysis better estimate assumptions would be credited. This would include reactor coolant system activity levels significantly lower than those modelled for the DBA and better activity retention in containment and in the steam generators. In addition better estimate atmospheric dispersion factors would be used. Therefore, a diverse mitigation radiological consequences analysis would show that the doses for the diverse ATWT scenario would be less than those reported for the non-LOCA DBAs and doses for the diverse core cooling scenario would be much less than for the design basis LOCA. The diverse mitigation analyses would not have to meet the Target 4 BSL for frequent faults and would meet the Target 4 BSL for infrequent faults.

9.6.3.5 As Low As Reasonably Practicable Assessment

For the SGTR event, the identification of the primary safety functions as Class 1 SSCs has been shown to be adequate to meet DB requirements. Diverse mitigation functions are also available for mitigation of the event for this cliff edge frequent fault. See Reference 9.6.3-4 for additional discussions on these diverse mitigation features.

Additionally, the AP1000 plant design has a third level of redundancy provided by the DiD systems. The DiD functions applicable to the SGTR include:

- CVS boration for long-term reactivity control
- CVS make-up for RCS inventory control
- CVS auxiliary spray to reduce the RCS pressure, equalize it with the SG pressure and terminate the RCS inventory loss into the SG

- Isolation of the faulted SG by closing its MSIV
- SFW with steam dump for short–term decay heat removal
- RNS cooling of the RCS for long-term decay heat removal. The RNS requires support from the CCS and SWS cooling water systems.
- Control by the PLS C&I

Some of the above functions require operators to take actions and they have sufficient time to take these actions to mitigate this event independent of the protections discussed above.

Providing further means of removing decay heat or tripping the reactor in addition to these functions would not significantly reduce the PSA risk for this event.

9.6.3.6 SGTR Conclusions

The results of the SGTR analysis show that the overfill protection logic and the passive system design features provide protection to prevent steam generator overfill. The AP1000 protection system and passive design features initiate automatic actions that can terminate a steam generator tube leak and stabilize the reactor coolant system in a safe condition while preventing steam generator overfill and ADS actuation.

No operator actions are required to bring the AP1000 to a safe, stable state following an SGTR. However, the operators can identify and isolate the ruptured steam generator and complete the actions to terminate the primary-to-secondary break flow before steam generator overfill or ADS actuation occurs.

Radiological consequences are within the Target 4 BSL for frequent faults (1 mSv offsite and 20 mSv onsite). Thus, the identification of necessary Class 1 SSCs is adequate to meet DB requirements for this fault.

It has been shown that the AP1000 design includes adequate systems for the protection of the fault, which limit the radiological consequences such that they are compliant with the SAPs targets and the risks have been reduced to be ALARP.

9.6.3.7 References

9.6.3-1 Westinghouse Calculation Note UKP-SSAR-GSC-005, Rev. 0, “AP1000 – Examination of the Impact of Multiple Steam Generator Tube Ruptures,” February 2011.

9.6.3-2 Westinghouse Documents WCAP-10698-P-A (Proprietary) and WCAP-10750-A (Non-Proprietary), “SGTR Analysis Methodology to Determine the Margin to Steam Generator Overfill,” August 1987.

9.6.3-3 Westinghouse Documents WCAP-14234, Rev. 1 (Proprietary) and WCAP-14235, Rev. 1 (Non-Proprietary), “LOFTRAN & LOFTTR2 AP600 Code Applicability Document,” August 1997.

9.6.3-4 Westinghouse Report UKP-GW-GL-067, Rev. 1, “AP1000 Assessment of Diverse Mitigation of Frequent Faults for the UK,” December 2011.

Table 9.6.3-1. DBA Steam Generator Tube Rupture Mass Release For Dose Sequence Of Events

Events	Time (sec)
Double-ended SGTR	0
Loss of offsite power (LOOP)	0
Reactor trip	0
RCPs and MFW pumps assumed to trip and begin to coast down	0
Two chemical and volume control pumps actuated and pressuriser heaters turned on	0
Low-2 pressuriser level signal generated	2,577
Ruptured SG PORV fails open	2,577
CMT injection and PRHR begin (following maximum delay)	2,594
Ruptured SG PORV block valve closes on low-2 steam line pressure signal	3,157
Flashing of break flow stops	3,429
Ruptured SG water level reaches SG dryer inlet	13,789
CVS isolated on high-3 SG narrow-range level setpoint	14,909
Break flow terminated	33,989
Steam releases from the intact SG terminated	57,389

Table 9.6.3-2. DBA Steam Generator Tube Rupture Margin To Overfill Sequence Of Events

Events	Time (sec)
Double-ended SGTR	0
LOOP	0
Reactor trip	0
Two chemical and volume control pumps actuated and pressuriser heaters turned on	0
Low-2 pressuriser level signal generated	797
CMT injection and PRHR begin	797
CVS isolated on high-3 SG narrow-range level setpoint	839
SFW isolated on high-3 SG narrow-range level setpoint	869
Break flow terminated	19,767

Table 9.6.3-3. DBA Parameters Used in Evaluating the Radiological Consequences of a Steam Generator Tube Rupture

Reactor coolant iodine activity	
– Accident-initiated spike	Initial activity equal to the operating limit for reactor coolant activity of 9.25E6 Bq/kg (0.25 μCi/g) dose equivalent I-131 (see Table 9A-1) with an assumed iodine spike that increases the rate of iodine release from fuel into the coolant (see Table 9A-2) by a factor of 335. Duration of spike is 8 hours.
– Pre-accident spike	Equal to the abnormal operating limit for reactor coolant activity of 5.55E8 Bq/kg (15 μCi/g) dose equivalent I-131 (a factor of 60 times the iodine values in Table 9A-1)
Reactor coolant noble gas activity	Equal to the operating limit for reactor coolant activity of 2.6E9 Bq/kg (70 μCi/g) dose equivalent Xe-133 (see Table 9A-1)
Reactor coolant alkali metal activity	Design basis activity (see Table 9A-1)
Secondary coolant initial iodine and alkali metal activity	10% of design basis reactor coolant concentrations at maximum equilibrium conditions
Reactor coolant mass	1.684E5 kg (3.713E5 lbm)
Sequence of Events	See Table 9.6.3-1
Steam generator in ruptured loop	
– Initial secondary coolant mass	6.8E4 kg (1.5E5 lbm)
– Primary-to-secondary break flow	See Figure 9.6.3-5
– Steam release rate	See Figure 9.6.3-7
Steam generator in intact loop	
– Initial secondary coolant mass	6.8E4 kg (1.5E5 lbm)
– Primary to secondary leak rate	3.95E-01 (1) kg/min (0.871 lbm/min)
– Steam released Prior to break flow termination After break flow termination	 See Figure 9.6.3-8 4.14E5 kg (9.13E5 lbm)
Partition coefficient in steam generators Volatile (iodine) Particulates (iodine, alkali metals) Water below SG dryer inlet Water above SG dryer inlet	See Appendix 9A.4 1.0 0.0005 0.004
Volatile iodine fraction With primary-to-secondary flashing Without primary-to-secondary flashing	See Appendix 9A.5.3 0.002 0.001
Offsite atmospheric dispersion factors	See Table 9A-5
Control room modelling	See Appendix 9A

Notes:

1. Equivalent to 0.57 m^3 (150 gal) per day per SG cooled liquid at 1000 kg/m^3 (62.4 lbm/ft^3).

Table 9.6.3-4. DBA Steam Generator Tube Rupture Technical Specifications Used In Dose Analysis

Limit or Condition	Tech Spec Identification and Notes
Primary-to-secondary leakage rate	3.4.7 leak rate to be < 0.57 m^3 (150 gal) per day through any one SG
Primary coolant specific activity	3.4.10 dose equivalent specific activity to be < 9.25E6 Bq/kg (0.25 μCi/g) for I-131 and < 2.6E9 Bq/kg (70 μCi/g) for Xe-133 3.4.10 dose equivalent specific activity to be < 5.55E8 Bq/kg (15 μCi/g) for I-131 short term abnormal operation only
Secondary coolant specific activity	3.7.4 dose equivalent I-131 specific activity to be < 9.25E5 Bq/kg (0.025 μCi/g)

Table 9.6.3-5. Steam Generator Tube Rupture Mitigation Features

Category A Safety Function	Provision	SSCs	Classification
Short-term reactivity control	Primary means	Reactor trip Breakers (PMS)	1
	Diverse means	Motor-generator set field breakers (DAS)	2
Long-term reactivity control	Primary means	CMTs	1
	Diverse means	Passive feed and bleed	1
Decay heat removal	Primary means	PRHR HX	1
	Diverse means	Passive feed and bleed	1
RCS pressure control	Primary means	Not required – SGTR results in RCS depressurisation	
	Diverse means		
RCS inventory control	Primary means	CMT	1
	Diverse means	Passive feed and bleed	1
Containment cooling	Primary means	PCS AOVs	1
	Diverse means	PCS MOVs	1

Table 9.6.3-6. Steam Generator Tube Rupture Potential Operator Actions

Operator Action	Class
On failure of automatic shutdown, initiate shutdown manually using DAS.	2
On failure of shutdown rods to insert, initiate RCP trip and actuation of CMTs to achieve shutdown by boration of the primary circuit.	1
If PRHR fails, activate ADS to allow automatic actuation of recirculation RHR via the IRWST.	1

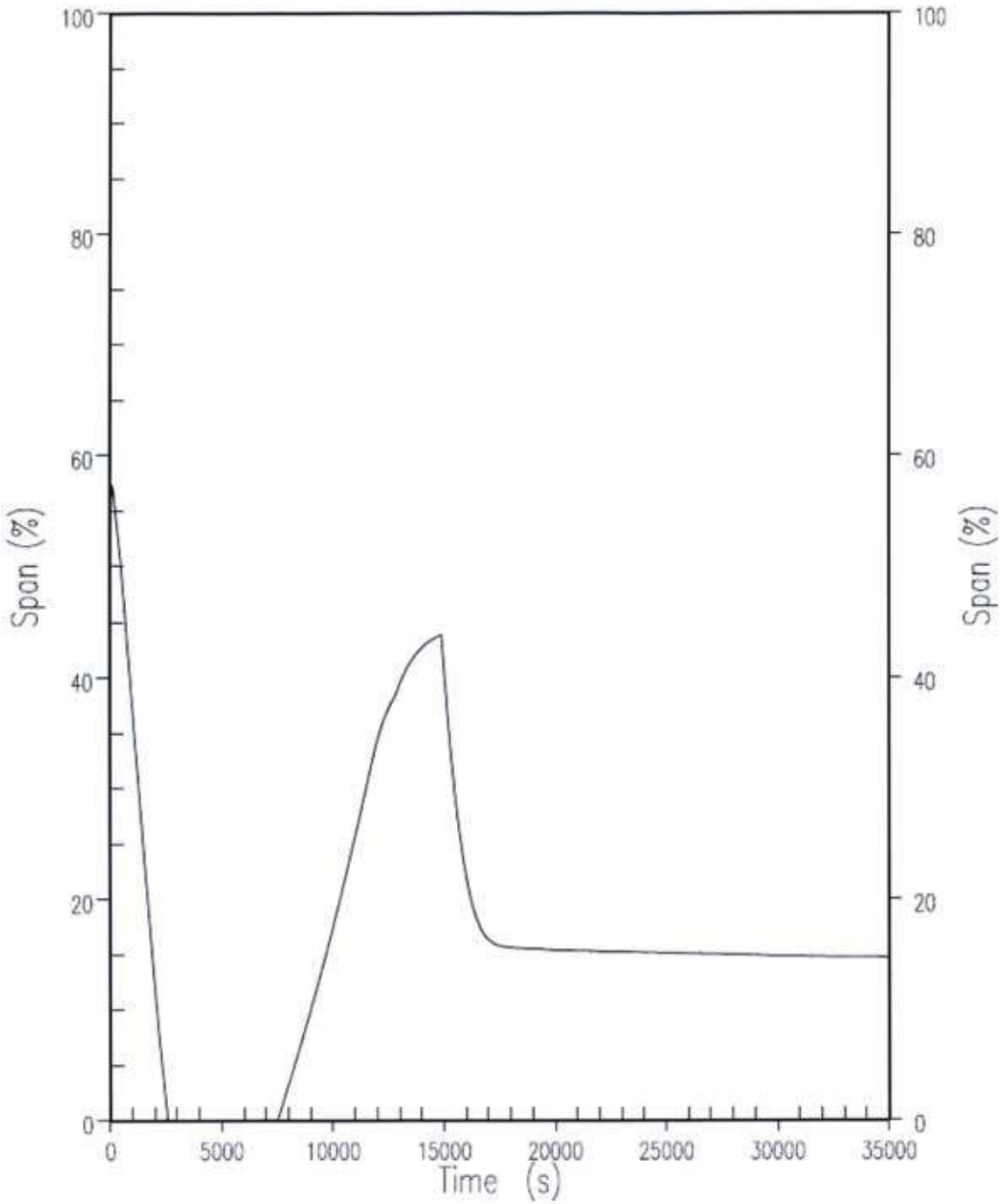


Figure 9.6.3-1. DBA Pressuriser Level for SGTR

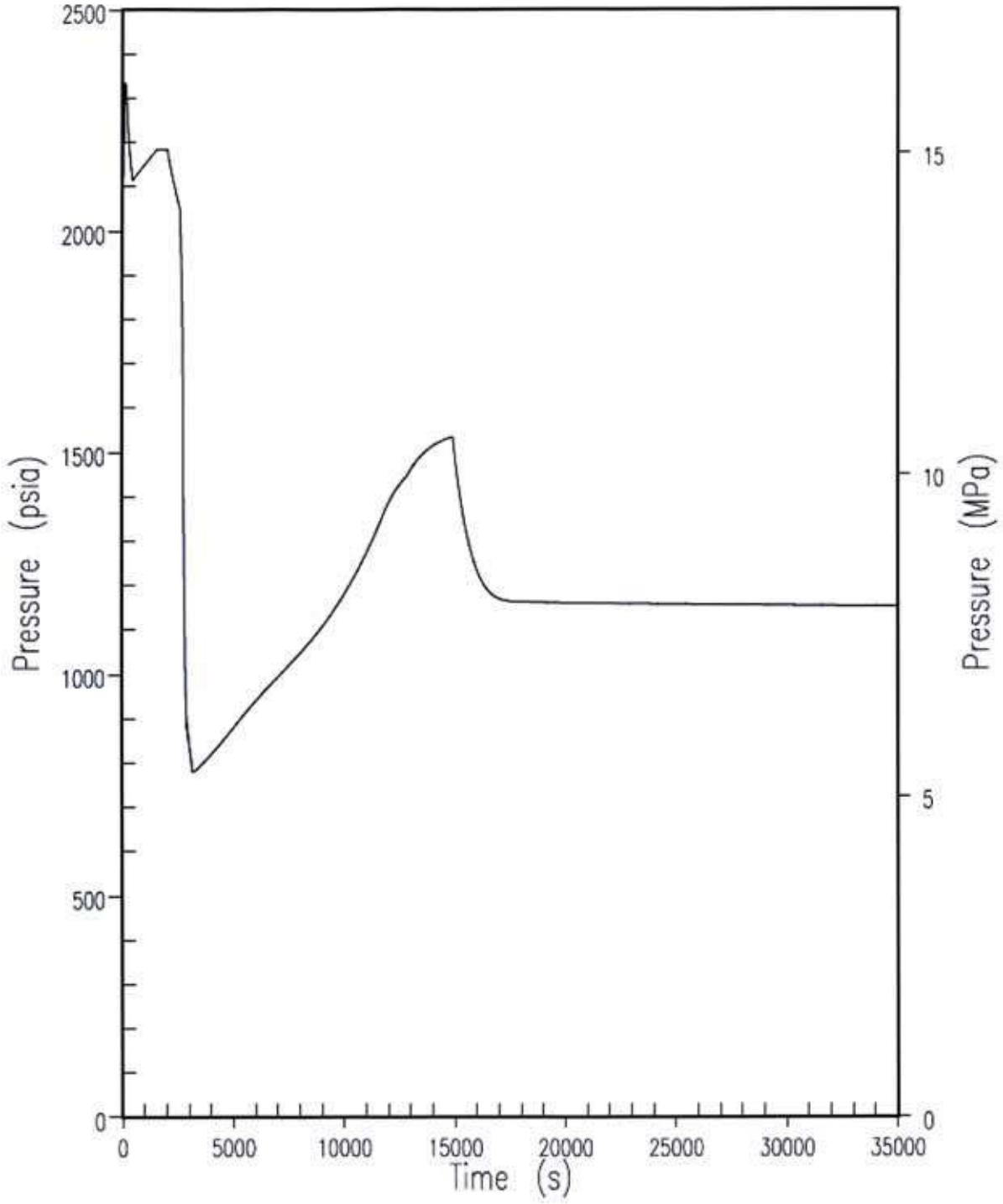


Figure 9.6.3-2. DBA Reactor Coolant System Pressure for SGTR

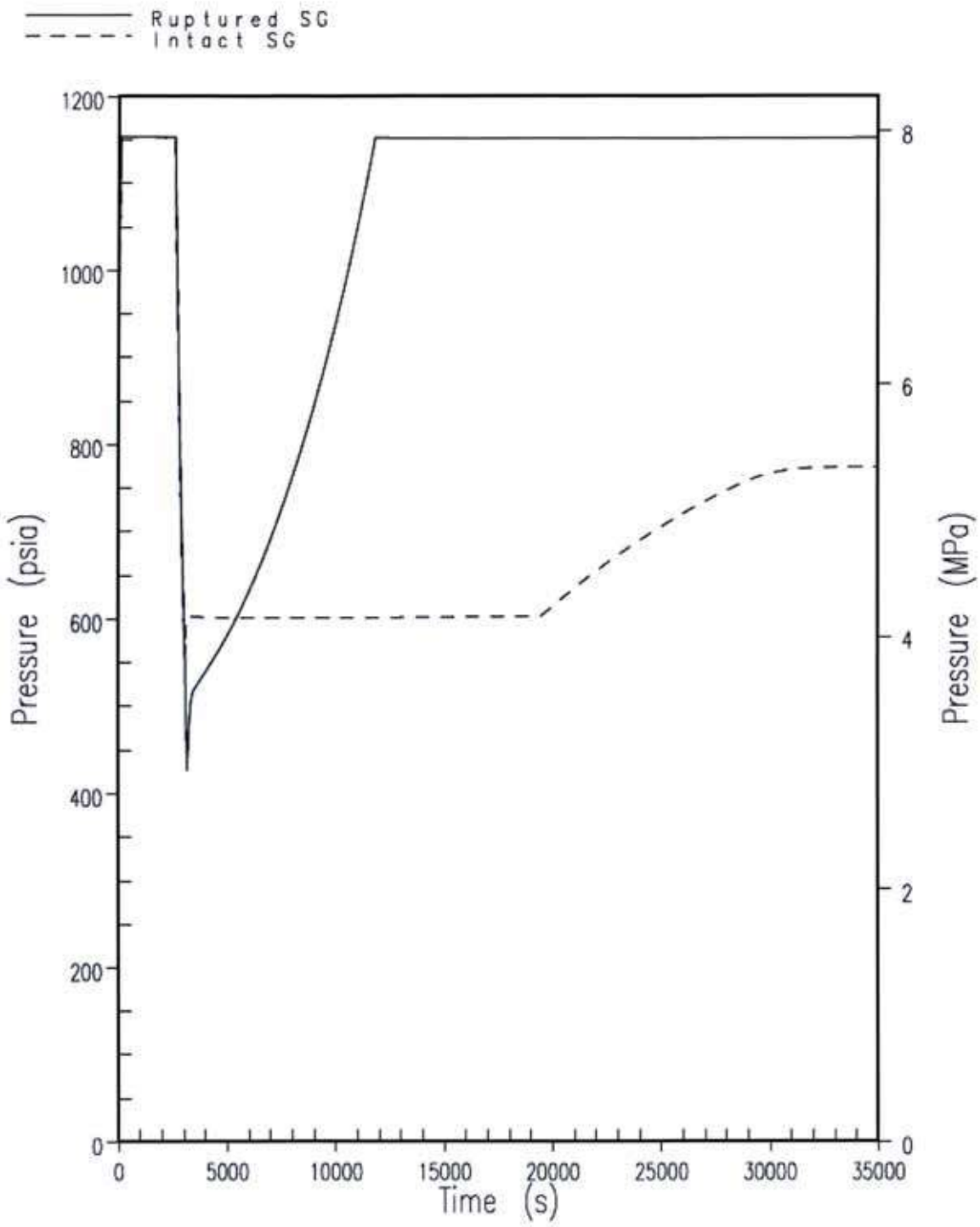


Figure 9.6.3-3. DBA Secondary Pressure for SGTR

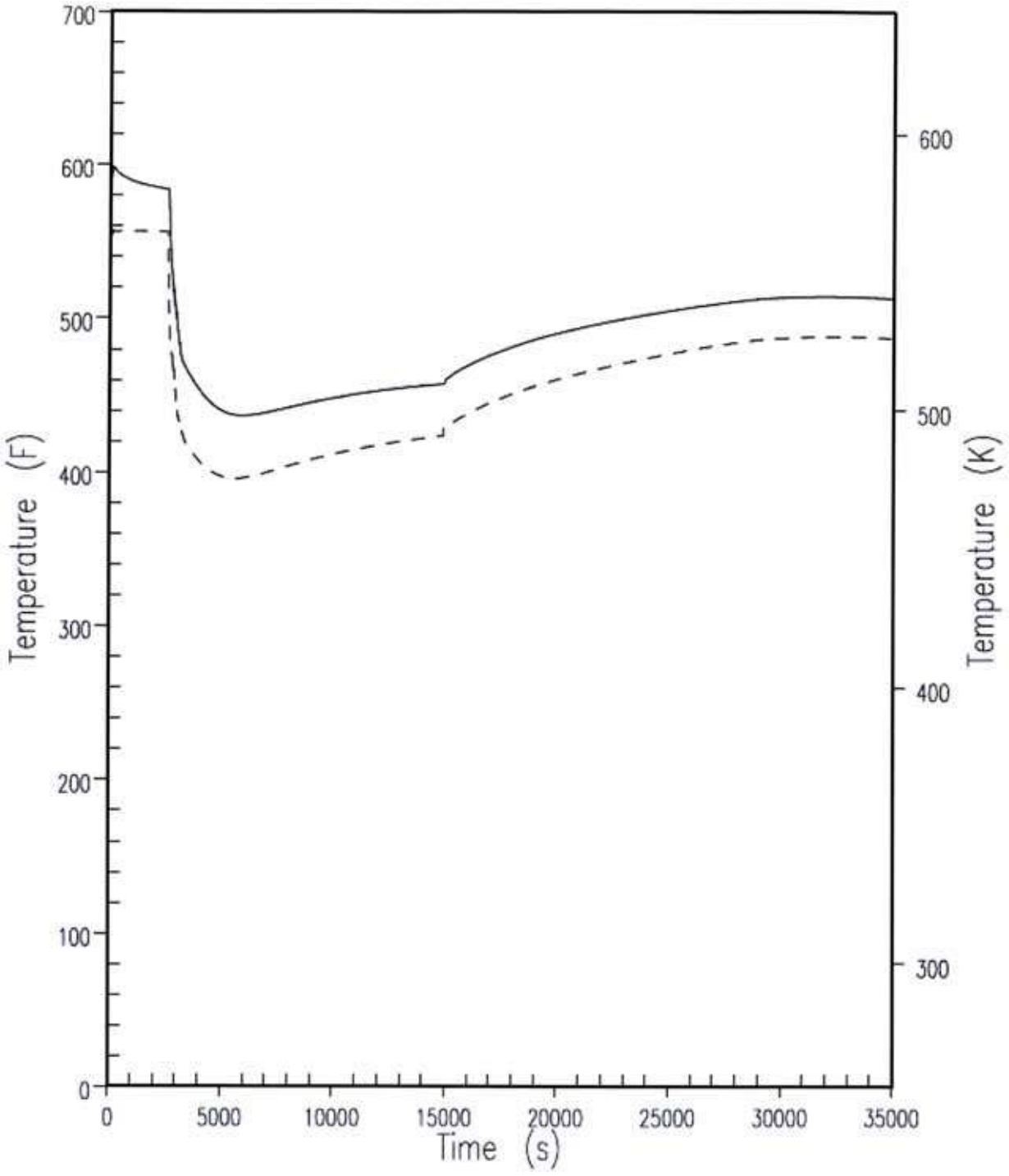


Figure 9.6.3-4. DBA Intact Loop Hot and Cold Leg Reactor Coolant System Temperature for SGTR

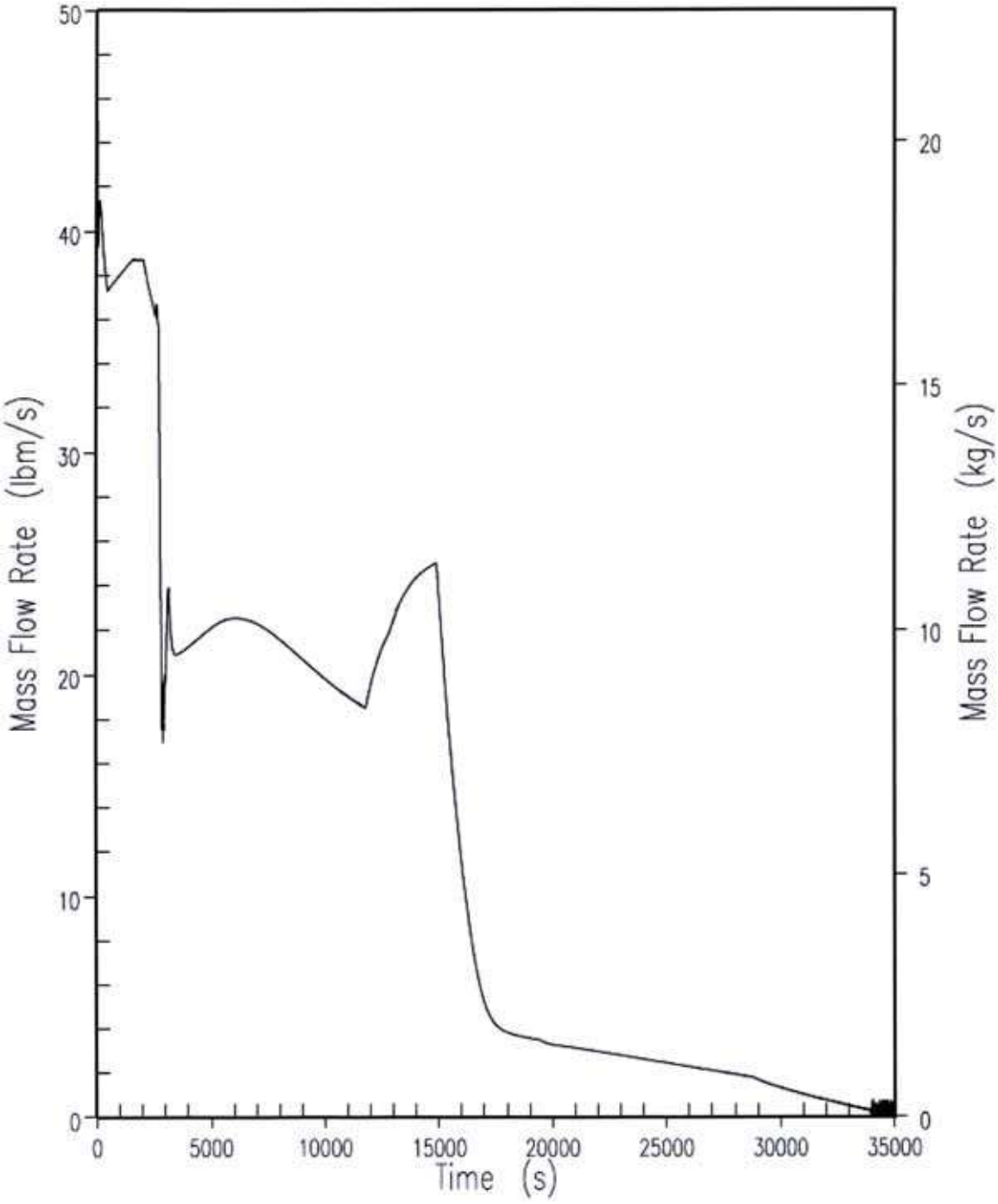


Figure 9.6.3-5. DBA Primary-to-Secondary Break Flow Rate for SGTR

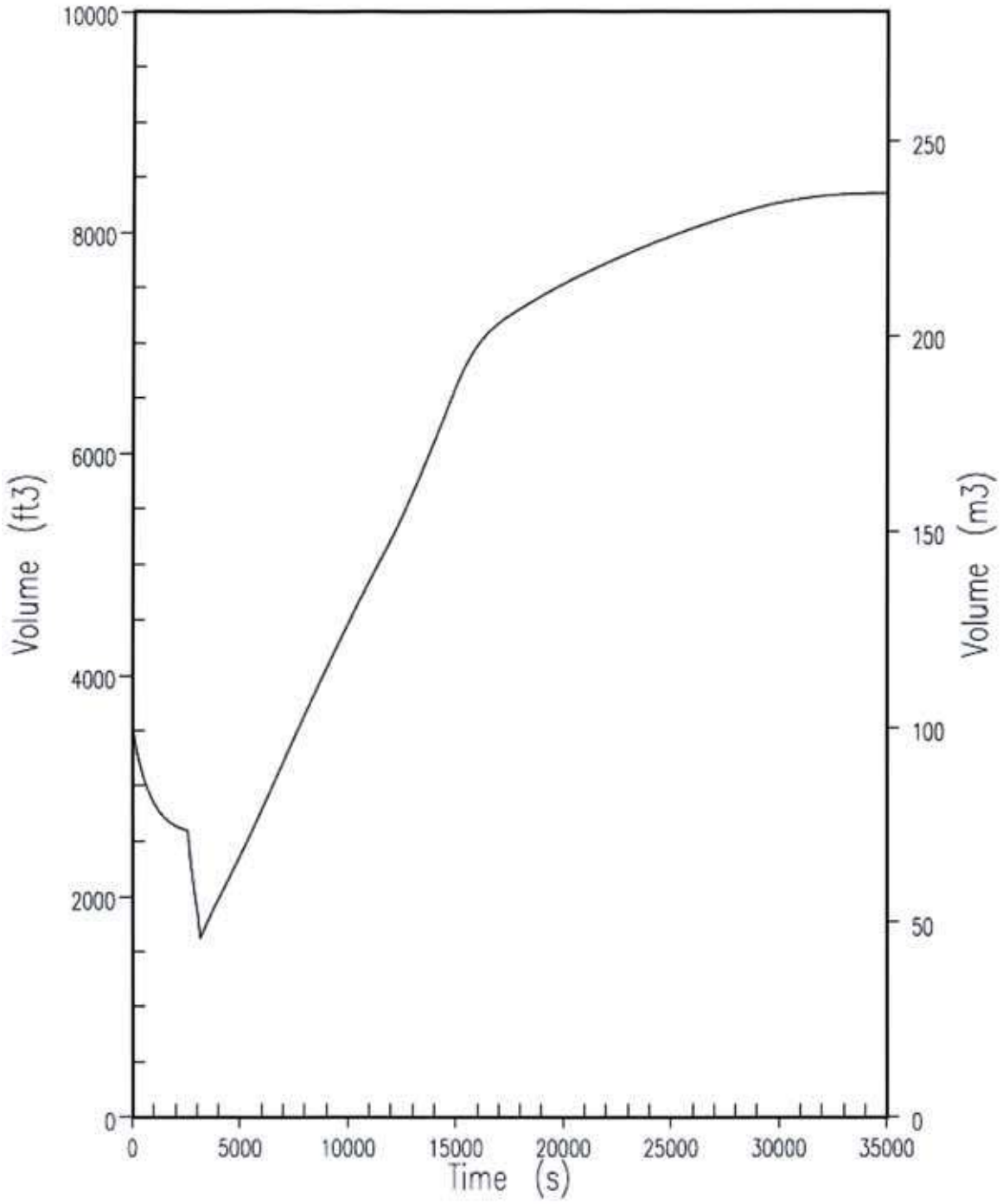


Figure 9.6.3-6. DBA Ruptured Steam Generator Water Volume for SGTR

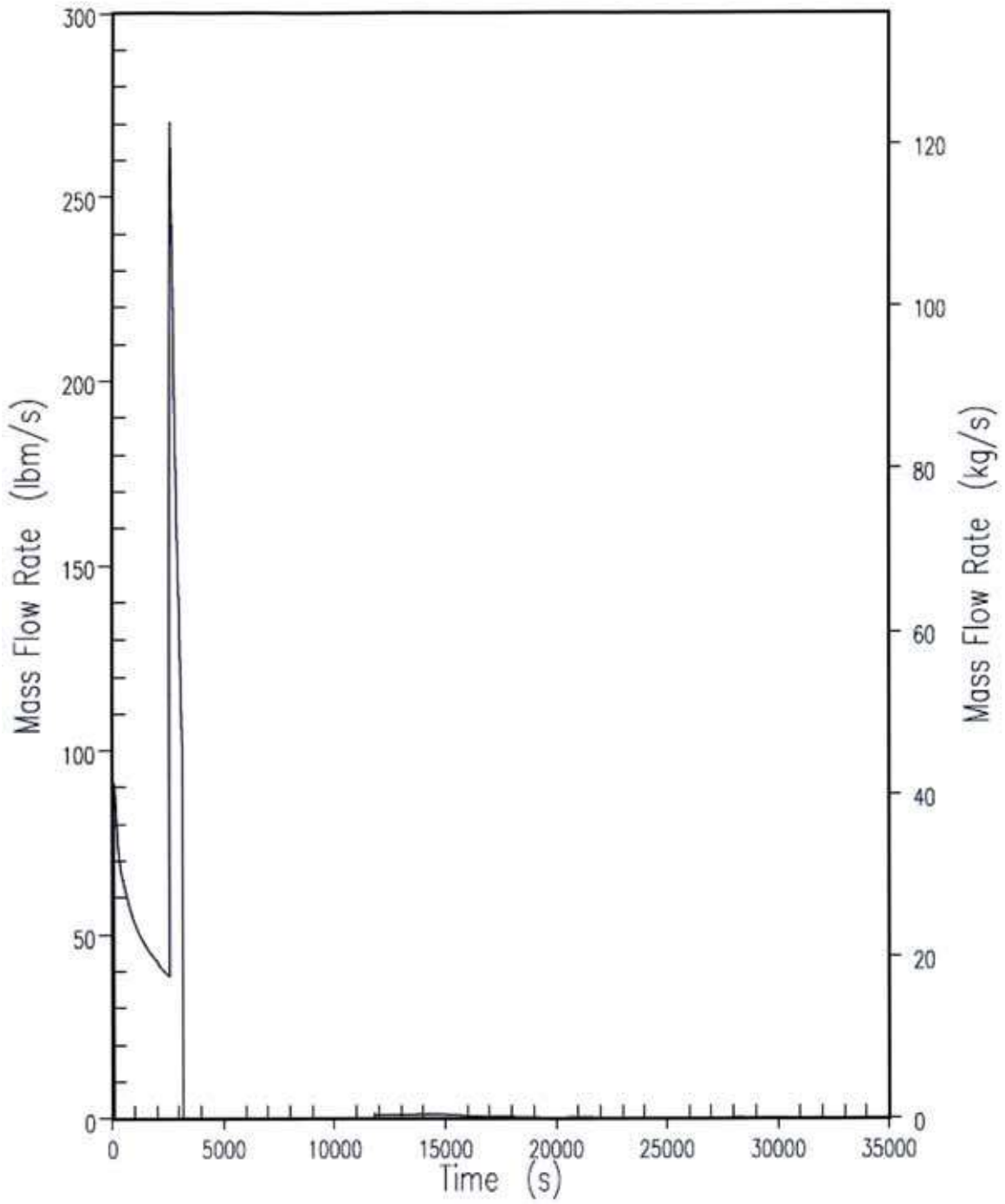


Figure 9.6.3-7. DBA Ruptured Steam Generator Mass Release Rate to the Atmosphere for SGTR

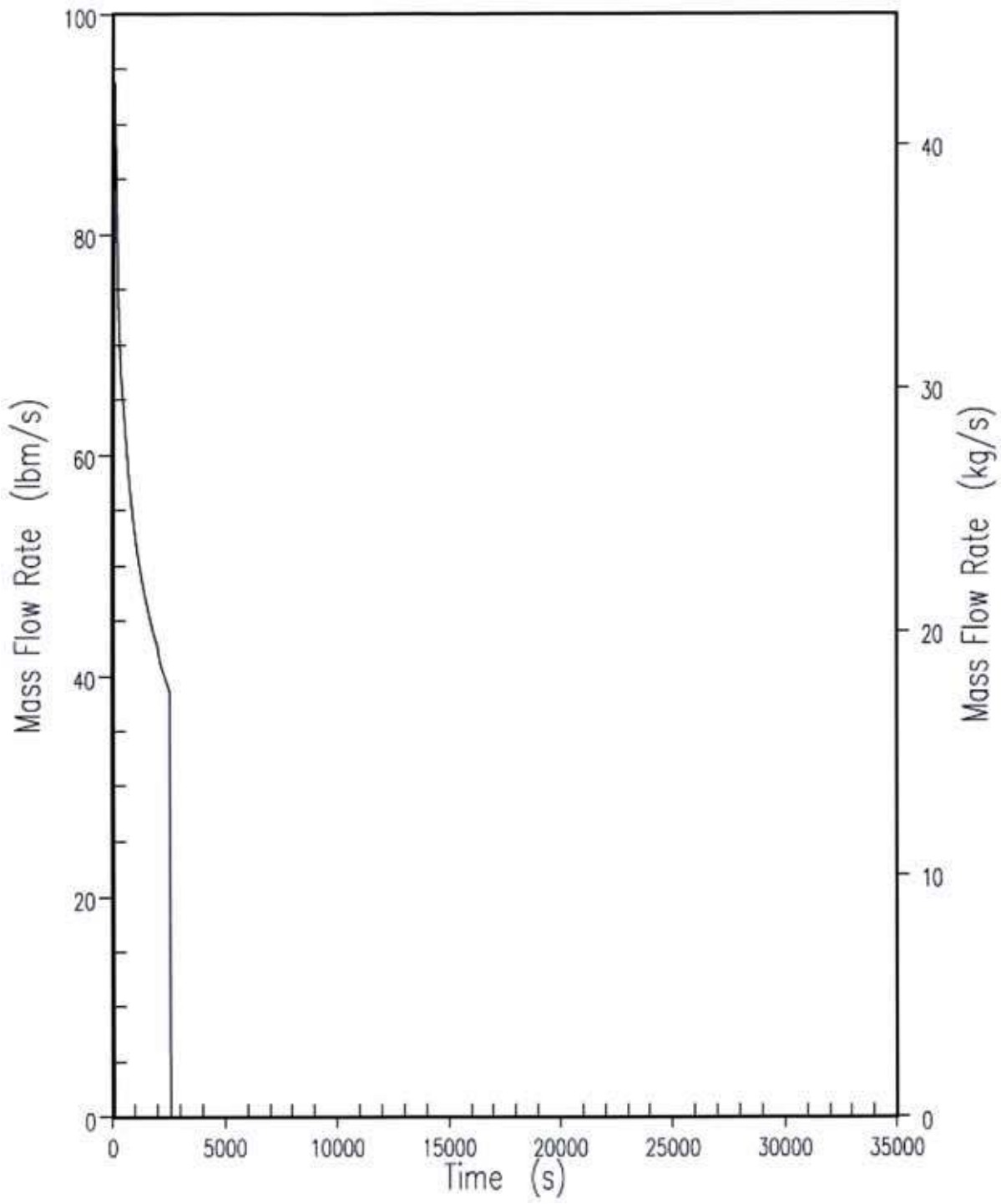


Figure 9.6.3-8. DBA Intact Steam Generator Mass Release Rate to the Atmosphere for SGTR

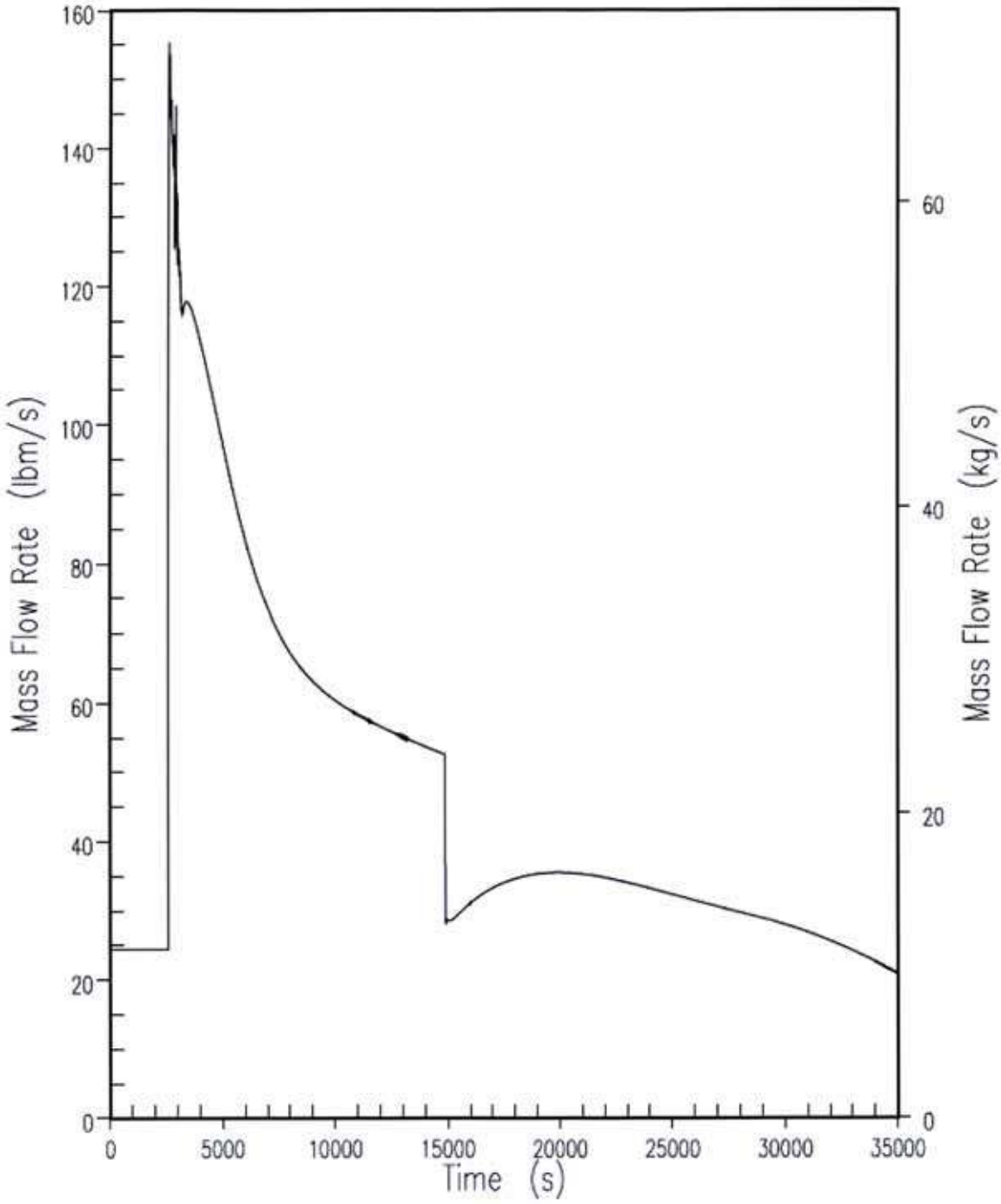


Figure 9.6.3-9. DBA Ruptured Loop Chemical and Volume Control System and Core Makeup Tank Injection Flow for SGTR

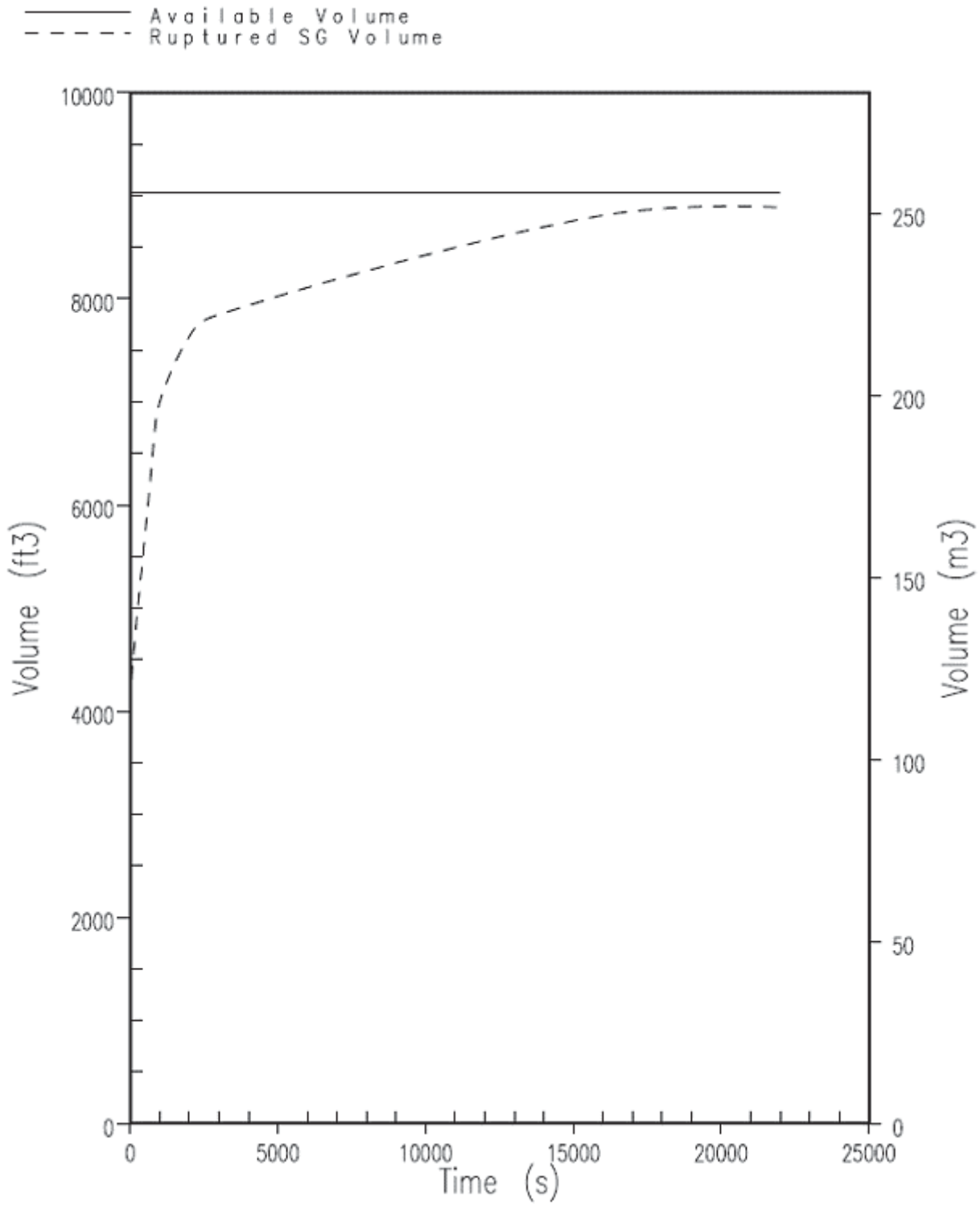


Figure 9.6.3-10. DBA Ruptured SG Water Volume for SGTR MTO Case

9.6.4 Large Break Loss of Coolant Accident (Fault 1.2.1)

A number of faults that could result in a loss of RCS inventory are postulated. This section discusses the largest postulated loss. Detailed analysis is presented for this most limiting of the RCS inventory loss events.

9.6.4.0 Introduction and Overview of Faults

A LOCA is the result of a pipe rupture of the RCS pressure boundary. The LBLOCA event is defined in the AP1000 design as all RCS ruptures with break sizes sufficient to produce a depressurisation of the RCS that allows gravity injection from the IRWST. The break size corresponding to this category is a 229 mm (9 inch) equivalent diameter or larger break, up to the size of a double-ended break of a cold or hot leg.

In the sections below, the fault is first described; the initial event frequency and the design basis class are provided. The analysed faults are presented in Table 8A-2.

The analysed fault(s) are described in additional detail in the subsequent sections to complete the safety case for each fault, including

- Identification of Causes and Accident Description
- Design Basis Analysis of Effects and Consequences
- Assessment of the Radiological Consequences for the DBA
- Diverse Mitigation and ATWT for Frequent Faults
- ALARP Assessment
- Conclusions

9.6.4.0.1 Large Break Loss of Coolant Accident Fault

Description

The fault includes the rupture of any RCS pressure boundary pipe sufficient to produce a depressurisation of the RCS that allows gravity injection from the IRWST, that is, with an equivalent diameter equal to or greater than 229 mm (9 inches). Because these faults involve a leak path to the containment and may lead to core uncovery and heatup, they are considered to have the potential to release radioactivity to the environment.

Initiating Event Frequency[1]

The AP1000 plant PSA gives the IEF for a LBLOCA event as 8.4E-07/yr. This places the fault just outside the DB in the UK definition but in practice the LBLOCA fault is evaluated within the DB as an infrequent fault. Spurious actuation of ADS stage 4 is classified as a LBLOCA but has a low IEF of <1.0E-08/yr.

1 As discussed in Chapter 8, the frequency for initiating events from the PSA is used in both Chapters 8 and 9 with the sole purpose of supporting the categorisation of the fault to a specific DB category. As noted in Chapter 8, these probabilities should not be considered to be representative of actual frequency of the events, and for several events they can be significantly conservative. Detailed PSA results and their basis are discussed in Chapter 10 of this PCSR.

Design Basis Class

The unmitigated consequences of a LBLOCA are assumed to be greater than the Target 4 BSL for frequent faults (1 mSv offsite and 20 mSv onsite). Although the assessed IEF is just less than 1.0E-05/yr, the event is considered to be in the low probability design basis event DBL class, in line with its evaluation as an infrequent fault with significant potential consequences.

This classification is due to historical LOCA experience, the AP1000 design approach of reduced quantity of piping, fewer welds, use of bent pipe rather than fittings, better materials, etc., and the special leak before break piping analysis approach used for the AP1000 design. The core cooling response is conservatively analysed with DB assumptions (best estimate plus full uncertainty evaluation). The dose and reactor internal structures are analysed with assumptions that are conservative, but not necessarily bounding. The structural and dose acceptance criteria are also relaxed consistent with their low probability.

9.6.4.1 Large Break LOCA Analysis Methodology and Results

Westinghouse applies the WCOBRA/TRAC computer code to perform best-estimate large-break LOCA analyses in compliance with the following criteria:

- The calculated maximum fuel element cladding temperature will not exceed 1204.4°C (2200°F).
- Localised cladding oxidation will not exceed 17 percent of the total cladding thickness before oxidation.
- The amount of hydrogen generated from fuel element cladding reacting chemically with water or steam will not exceed 1 percent of the total amount if all metal cladding were to react.
- The core remains amenable to cooling for any calculated change in core geometry.
- The core temperature is maintained at a low value, and decay heat is removed for the extended period of time required by the long-lived radioactivity remaining in the core.

These criteria are established to provide significant margin in emergency core cooling system (ECCS) performance following a LOCA.

Demonstration that the loads resulting from an LBLOCA event do not threaten the integrity of the containment is presented in Appendix 9D.

WCOBRA/TRAC is a thermal- hydraulic computer code that calculates realistic fluid conditions in a PWR during the blowdown and reflood of a postulated large-break LOCA. The methodology used for the AP1000 analysis is documented in WCAP-12945-P-A, WCAP-14171, Revision 2, WCAP-16009-P-A (References 9.6.4-2, 9.6.4-3, and 9.6.4-6), and Reference 9.6.4-5.

The automated statistical treatment of uncertainty method (ASTRUM) best-estimate LOCA methodology (ASTRUM methodology) is utilised for estimating the 95th percentile peak clad temperature (PCT) for two-loop, three-loop and four-loop Westinghouse PWRs and the AP600 plant. An AP1000 design specific application of the ASTRUM methodology was developed (Reference 9.6.4-8) for estimating the 95th percentile PCT for the AP1000 plant. In the ASTRUM methodology, the WCOBRA/TRAC code is used to calculate the effects of initial conditions, power distributions, and global models, and the HOTSPOT code is used to calculate the effects of local models.

In the ASTRUM uncertainty methodology (Reference 9.6.4-6), as used in the AP1000 LBLOCA analysis, global models and initial-condition, power-distribution, and local uncertainties are sampled independently for each of 124 runs over the same ranges of uncertainty and distributions as in References 9.6.4-2, 9.6.4-6, and 9.6.4-7, as described in References 9.6.4-5 and 9.6.4-8. The sampled global models, initial conditions, and power-distribution uncertainties become inputs to each of the WCOBRA/ TRAC calculations. The thermal-hydraulic boundary conditions for the hot rod are input to the local uncertainties calculation performed by the HOTSPOT code.

Results from the calculations are ranked by PCT from highest to lowest. A similar procedure is repeated for maximum local oxidation (MLO) and core-wide oxidation (CWO). In order statistics as applied in the ASTRUM methodology, the limiting case for a parameter, such as PCT, is a conservative estimate of the 95th percentile with 95 percent confidence. The limiting PCT, limiting MLO, and CWO may come from the same case or as many as three different cases because each parameter is assumed to be independent of the other two. The assumption of independence of the calculated licensing parameters is a conservative assumption because there is a dependence of MLO and CWO on cladding temperature.

For the AP1000 large-break LOCA analysis, a plant-specific adaptation of the ASTRUM methodology is applied as described in Reference 9.6.4-5. The plant-specific adaptation explicitly models the effects of thermal conductivity degradation and peaking factor burndown. The post-LOCA long-term core cooling and core boron concentration analyses discussed in Section 9.6.6 are applicable to the large-break LOCA transient.

9.6.4.1.1 General Description of WCOBRA/TRAC Modelling

WCOBRA/TRAC is the best-estimate thermal-hydraulic computer code used to calculate realistic fluid conditions in the PWR during blowdown and reflood of a postulated large-break LOCA.

The WCOBRA/TRAC Code Qualification Document (Reference 9.6.4-2) contains a complete description of the code models and justifies their applicability to PWR large-break LOCA analysis.

Table 9.6.4-1 lists AP1000-specific parameters identified for use in the large-break LOCA analysis. WCOBRA/TRAC studies were performed to establish sensitivities to parameter variations. These studies included effects of ranging steam generator tube plugging, ranging the relative power in the low-power assemblies, loss of offsite power coincident with the break initiation, and break location. The calculated results were used to identify bounding conditions, which are then used in the uncertainty calculations.

The WCOBRA/TRAC vessel nodalization is developed from plant design drawings to divide the vessel into 10 vertical sections. The bottom of section 1 is the inside vessel bottom, and the top of section 10 is the inside top of the vessel upper head. In addition to the major downcomer and core flow paths, the modelled bypass flow paths are the upper head cooling spray, guide thimbles, and core bypass. After defining the elevations for each section, a noding scheme is defined for the WCOBRA/TRAC model as shown in Reference 9.6.4-8. WCOBRA/TRAC assumes a vertical flow path for vertically stacked channels, unless specified otherwise in the input. Positive flow for the vertically connected channels (and cells) is upward. Several of the 10 sections are divided vertically into 2 or more levels; these levels are referred to as cells within a channel.

The WCOBRA/TRAC loop model represents the major primary, secondary, and passive safety systems components. Both loops are explicitly modelled, including the hot leg, the steam generator, and the two cold legs and associated pumps. The loop designated “1” has the pressuriser and the PRHR system connections, and loop “2” cold legs have the core makeup tank

pressure balance line connections. The reactor coolant pump models contain the homologous curves together with appropriate two-phase head and torque multipliers and degradation data. AP1000 design values for pump coastdown characteristics are also applied. The passive safety features are modelled using design data for elevations, liquid volumes, and line losses. Because the ADS is not actuated until long after the time of PCT in large-break LOCA events, it is not modelled in detail.

9.6.4.1.2 Steady-State Calculation

A WCOBRA/TRAC LOCA calculation is initiated from a point at which the flows, temperatures, powers, and pressures are at their approximate steady-state values before the postulated break occurs. Steady-state WCOBRA/TRAC calculations are run for a brief time period to verify that the calculated conditions are steady and that the desired reactor conditions are achieved.

The values used to set the steady-state plant conditions reflect the AP1000 plant parameters for reactor coolant pump flows, core power, and steam generator tube plugging levels. The fuel parameters provide the steady-state fuel temperatures, pressures, and gap conductances as a function of fuel burnup and linear power, accounting for the effects of the thermal conductivity degradation as described in Reference 9.6.4-5. The calculated fuel temperatures from WCOBRA/TRAC are adjusted to match the specified fuel data by adjusting the gap heat transfer coefficient between the pellet and the cladding. Once the vessel fluid temperatures, flows, pressures, loop pressure drop, and core parameters are in agreement with the desired values and are steady, a suitable initial condition is achieved.

9.6.4.1.3 Signal Logic for Large Break LOCA

The reactor trip signal occurs due to compensated pressuriser pressure within the first seconds of the large-break transient; however, control rod insertion is not modelled in WCOBRA/TRAC and no effects of control rod insertion on reactivity ensue. A safeguards “S” signal occurs due to containment high pressure of 0.046 MPa (6.7 psig) at 2.2 seconds of large-break LOCA transients.

As a consequence of this signal, after appropriate delays, the PRHR and core makeup tank isolation valves open, containment isolation occurs, and the reactor coolant automatic trip timer begins. The rapid depressurisation of the primary system during a large-break LOCA leads to the initiation of accumulator injection early in the large-break transient. The accumulator flow diminishes core makeup tank delivery to such an extent that the core makeup tank level does not approach the ADS Stage 1 valve actuation point until after the accumulator tank is empty. The accumulator empties long after the blowdown portion of the large-break LOCA transient is complete. Actuation of the ADS on CMT water level does not occur until long after the PCT is calculated to occur.

9.6.4.1.4 Transient Calculation

Once the steady-state calculation is found to be acceptable, the transient calculation is initiated. The semi-implicit pipe break model is added to the desired break location. Cold-leg breaks are analysed because the hot-leg break location is nonlimiting in the large-break LOCA best-estimate methodology. The break size and type are sampled consistent with the WCAP-16009-P-A (Reference 9.6.4-6) methodology. The containment backpressure is specified consistent with WCAP-16009-P-A (Reference 9.6.4-6) methodology. The steady-state calculation is restarted with the above changes to begin the transient.

Table 9.6.4-2 shows a general sequence of events following a large cold-leg break LOCA and the relationship of these events to the blowdown and reflood portion of the transient.

9.6.4.1.5 DBA Credited SSCs

For the LBLOCA fault, all of the claimed SSCs are Class 1. The claimed Class 1 SSCs are listed in Table 9.0-10. The primary core cooling is provided by the CMTs, IRWST and passive containment cooling. Other SSCs include the accumulators, steam generator safety and/or relief valves. The PMS provides the following:

- RT on Low-2 pressuriser pressure
- CMTs and containment isolation on Low pressuriser pressure
- ADS and IRWST injection on Low CMT level
- Containment recirculation on Low IRWST level
- PCS on High-2 containment pressure

9.6.4.2 Analysis Results

For the AP1000 large-break LOCA analysis, a plant-specific adaptation of the ASTRUM best-estimate LOCA analysis methodology is applied as described in Reference 9.6.4-5. The AP1000 large-break LOCA analysis complies with the criteria listed in Section 9.6.4.1. Sensitivity calculations evaluated the sensitivity to the modelling of the CMT and PRHR relative to the reference transient configuration. A case in which the CMT was isolated from the rest of the plant was analysed, and the calculated PCT was lower than the PCT of the reference transient configuration. Also, a case in which the PRHR was isolated from the rest of the plant was analysed, and the calculated PCT was 1.1°C (2°F) higher than the PCT of the reference transient configuration. The ASTRUM methodology samples the parameters ranged in the global model matrix of calculations, and the final 95 percent uncertainty calculations have been performed for the AP1000 design. Further, local and core-wide cladding oxidation values have been determined using the plant-specific adaptation of the approved Reference 9.6.4-6 methodology as described in Reference 9.6.4-5.

In the AP1000 ASTRUM analysis, the limiting PCT and limiting MLO results were from two different uncertainty calculations. Both the limiting PCT case and the limiting MLO case were double-ended guillotine breaks. Figures 9.6.4-1 through 9.6.4-12 present the parameters of principal interest for the limiting PCT case. Values of the following parameters are presented:

- Highest calculated cladding temperature at any elevation for the five fuel rods modelled
- Hot rod cladding temperature transient at the limiting elevation for PCT
- Core fluid mass flows at the top of the core for the fuel assemblies modelled in WCOBRA/TRAC
- Pressuriser pressure
- Break flow rates
- Core and downcomer collapsed liquid levels
- Accumulator water flow rates
- Core makeup tank flow rates

9.6.4.2,1 Description of AP1000 Large Break LOCA Transient

A description of the limiting PCT case from the AP1000 ASTRUM analysis follows. The limiting PCT case is a double-ended guillotine break. The sequence of events is presented in Table 9.6.4-3.

The break was modelled to occur in one of the cold legs in the loop containing the core makeup tanks. After the break opens, the vessel rapidly depressurises and the core flow quickly reverses. The hot assembly fuel rods dry out and begin to heat up (Figures 9.6.4-1 and 9.6.4-2) after the initial flow reversal (Figure 9.6.4-3).

In Figure 9.6.4-1, "Hot Rod" refers to the hot fuel rod at the maximum linear heat rate for the run, "Hot Assembly" refers to the average fuel rod in the hot assembly that contains the hot rod, "Support Column/Open Hole" refers to the fuel rod in average assemblies under support columns or open holes, "Guide Tubes" refers to the fuel rod in average assemblies under guide tubes, and "Low Power" refers to the fuel rod in the low power peripheral fuel assemblies.

The steam generator secondaries are assumed to be isolated immediately at the inception of the break, which maximizes their stored energy. The massive size of the break causes an immediate, rapid pressurisation of the containment. At 2.2 seconds, an "S" signal is generated due to High-2 containment pressure. Applying the pertinent signal processing delay means that the valves isolating the core makeup tanks from the direct vessel injection line and the PRHR begin to open at 4.2 seconds into the transient. The reactor coolant pumps automatically trip after a 5.3-second delay from the actuation of the core makeup tank isolation valves, which is 9.5 seconds into the transient. Core shutdown occurs due to voiding; no credit is taken for the control rod insertion effect.

The system depressurises rapidly (Figure 9.6.4-4) as the initial mass inventory is depleted due to break flow. The pressuriser drains completely approximately 30 seconds into the transient, and accumulator injection commences 13 seconds into the transient (Figure 9.6.4-5). Accumulator actuation shuts off core makeup tank flow (Figure 9.6.4-6), which has been occurring since the isolation valve opened. The CMT liquid level remains well above the ADS Stage 1 actuation setpoint throughout the LBLOCA cladding temperature excursion, even though CMT injection begins again around 200 seconds.

The dynamics of the 95th percentile estimator PCT case are shown in terms of the flow rates of liquid, vapour, and entrained liquid at the top of the core (Figures 9.6.4-7 through 9.6.4-9) for the peripheral, open hole/support column average power interior, and guide tube average power interior assemblies (the corresponding figure for the hot assembly is Figure 9.6.4-3).

Figure 9.6.4-7 demonstrates that liquid downflow exists through the top of the peripheral core assemblies from approximately 1 to 3 seconds and again from 9 to 20 seconds in the 95th percentile estimator PCT case. The power of the fuel in this region is significantly lower than that of the fuel in the open hole/support column and guide tube locations (Table 9.6.4-1), so liquid downflow occurs earlier on the periphery than in the average power assemblies. Once the upper head begins to flash, liquid drains directly down the guide tubes and that fraction able to penetrate into the core does so, at a maximum flow rate exceeding 453.6 kg/sec (1000 lbm/sec) of total liquid flow between 5 to 23 seconds (Figure 9.6.4-8).

Figure 9.6.4-9 presents the open hole/support column assembly top of core flow behaviour. In this case, liquid downflow into the support column/open hole assemblies is delayed relative to downflow into the guide tubes; there is a continuous liquid flow from approximately 10 seconds until 22 seconds; the entrained liquid flow continues to be significant until 28 seconds as fluid drains through the upper core plate holes into the upper plenum.

The timing of the initial downflow into the hot assembly is similar to that of the downflow into the open hole/support column average assemblies. Around 10 seconds into the transient, liquid that has built up in the global region above the hot assembly begins to flow into the hot assembly (Figure 9.6.4-3). Significant flow of continuous liquid into the hot assembly exists between

10 to 20 seconds. The liquid flow is not enough to quench the hot rod and hot assembly rod or the average rods at all elevations (Figure 9.6.4-1) although some cooling is achieved.

After 13 seconds into the transient, the accumulator begins to inject water into the upper downcomer region, most of which is initially bypassed to the break. The break flow rate diminishes as the transient progresses (Figure 9.6.4-10). At 27.5 seconds, the accumulator injection begins to refill the lower plenum. At approximately 40.0 seconds, the lower plenum fills to the point that water begins to reflood the core from below (Figure 9.6.4-11). The void fraction at the core bottom begins to decrease, and as time passes, core cooling increases substantially. Figure 9.6.4-11 presents the collapsed liquid levels in the core; Figure 9.6.4-12 presents the collapsed liquid levels in the downcomer. The cladding temperature begins to decrease once the core water level has risen high enough in the core.

9.6.4.2.2 Global Model Sensitivity Studies and Uncertainty Evaluation

Section 9.6.4.1 discusses the treatment of the global model parameters and the uncertainty evaluation in the ASTRUM methodology.

9.6.4.3 Diverse Mitigation

Diverse mitigation for this event is not required as it is a low probability design basis fault classified as DBL.

9.6.4.4 Radiological Consequences

The evaluation of the radiological consequences of a postulated large break LOCA assumes that as a result of the accident, 33 percent of the fuel rods are damaged such that the activity contained in the fuel-cladding gap is released to the reactor coolant. This is consistent with the recommendation in Chapter X of Reference 9.6.4-1. Activity is released to the containment via the break. The dose calculations take into account the release of activity by way of the containment purge line prior to its isolation near the beginning of the accident and the release of activity resulting from containment leakage. Purge of the containment for hydrogen control is not an intended mode of operation and is not considered in the dose analysis. While the normal residual heat removal system is capable of post-LOCA cooling, it is not a safety-related system and may not be available following the accident. If it is operable, it would be used only if the source term is not far above the normal shutdown primary coolant source term. It is assumed that core cooling is accomplished by the passive core cooling system, which does not pass coolant outside of containment. Thus, there is no recirculation leakage release path to be modelled.

This section describes the fault study analysis performed for a large break loss of coolant accident. Since this analysis is a design basis accident analysis, and is not an analysis describing the severe accident beyond design basis source term that is generated as a result of the GI-AP1000-RC-01 issue, this section is concluded to not be impacted.

9.6.4.4.1 Source Term

The most significant radionuclide releases are the noble gases, alkali metals, and iodines. The release of activity to the containment consists of two parts. The initial release is the activity contained in the reactor coolant system. This is followed by the release of core activity.

All activity in the fuel rod gap of the damaged fuel is assumed to be released to the coolant. Based on Table 7.3 of Reference 9.6.4-1, the gap fraction is assumed to be 3 percent of the core inventory for iodines, 10 percent for noble gases, and 4 percent for alkali metals. To address the

fact that the failed fuel rods may have been operating at power levels above the core average, the source term is increased by a lead rod radial peaking factor of 1.75 which bounds the COLR limit of 1.72.

From Chapter X of Reference 9.6.4-1, the activity releases from the damaged fuel rods can be modelled as occurring in two phases: the dry phase (when the core is uncovered) and the wet phase (when reflood of the core has been accomplished).

The dry phase is assumed to begin at 30 seconds into the accident. The dry phase is assumed to end at 120 seconds. The fraction of gap activity released during the dry phase is 1.0 for noble gases, 0.1 for iodines, and 0.1 for alkali metals. It is assumed that 0.2% of the iodine released is in the organic form, 2% of the iodine is in the elemental form, and the remainder is in the particulate form.

The wet phase is assumed to begin at the end of the dry phase (120 seconds). The fraction of gap activity released during the wet phase is 0.0 for noble gases, 0.9 for iodines, and 0.9 for alkali metals. The water covering the core is assumed to retain some of the radionuclides released from the core. The iodine activity is all assumed to enter into solution with 60 percent of the iodine assumed to convert to the elemental form and then enter the containment atmosphere, consistent with Section 2.2.1 of Chapter IX of Reference 9.6.4-1. It is assumed that 1% of the iodine released converts to the organic form while the other 99% stays in the elemental form. In practice, the iodine activity released from the fuel would initially enter into solution and is anticipated to be gradually released to the containment atmosphere over an indefinite period of time. However, it is conservatively assumed that all of the iodine releases to the containment atmosphere occur over 60 seconds. This assumption makes the activity quickly available for release to the environment by way of containment leakage. The alkali metals activity is assumed to be retained in the primary coolant and none of it is assumed to enter the containment atmosphere

The AP1000 does not include active systems for the removal of activity from the containment atmosphere. The containment atmosphere is depleted of elemental iodine and of particulates as a result of natural processes within the containment.

Elemental iodine is removed by deposition onto surfaces. Particulates are removed by sedimentation, diffusiophoresis (deposition driven by steam condensation), and thermophoresis (deposition driven by heat transfer). No removal of organic iodine is assumed.

If the post-LOCA cooling solution has a pH of less than 6.0, part of the cesium iodide may be converted to the elemental iodine form. The passive core cooling system provides sufficient trisodium phosphate to the post-LOCA cooling solution to maintain the solution pH at 7.0 or greater following a LOCA.

9.6.4.4.2 Release Pathways

The release pathways are the containment purge line and containment leakage. The activity releases are assumed to be ground level releases.

During the initial part of the accident, before the containment is isolated, it is assumed that containment purge is in operation and that activity is released through this pathway until the purge valves are closed. No credit is taken for the filters in the purge exhaust line.

The majority of the releases due to the LOCA are the result of containment leakage. The containment is assumed to leak at its design leak rate for the first 24 hours and at half that rate for the remainder of the analysis period.

9.6.4.4.3 Dose Calculation Models

The models used to calculate doses are provided in Appendix 9A.

9.6.4.4.4 Analytical Assumptions and Parameters

The assumptions and parameters used in the analysis are listed in Table 9.6.4-8.

9.6.4.4.5 Doses

The calculated maximum doses for all relevant pathways (inhalation, cloudshine, and groundshine) are as follows:

- Offsite dose: 10.2 mSv Worker dose: 14.8 mSv

These doses are within the Target 4 BSL for infrequent faults with IEF<1E-04 (100 mSv offsite and 500 mSv onsite).

The limiting conditions for operation of the Technical Specifications used in the dose assessment are provided in Table 9.6.4-9. The Table 9.6.4-9 values ensure the Target 4 BSLs are met.

9.6.4.5 As Low As Reasonably Practicable Assessment

For the LBLOCA event, the identification of the primary safety functions as Class 1 SSCs (CMTs, the accumulators, full ADS, PCS, and reactor containment) has been shown to be adequate to meet DB requirements.

LBLOCAs are low probability design basis events (DBLs) and have core a low probability of causing a large radioactivity release that is less than the SAP Target 9 BSO (1.0E-7 pa).

In order to provide improved reliability (diversity) the following features would have to be provided:

- Two additional Accumulators with diverse actuation check valves
- Auto start of the RNS pumps; note that ADS 1/2/3 is adequate to support RNS injection and recirculation whereas the diverse ADS 4 is adequate to support PXS IRWST injection / recirculation.

The impact of the addition of two more Accumulators would have a very large impact on the containment design, possibly requiring a larger diameter containment. The additional Accumulators would also increase the radiation exposure to operational personnel for inservice testing and inspection and also to deal with the increased chance of RCS leakage into the new Accumulators. The impact of providing automatic RNS start would not be so costly but would complicate the design and probably make it less reliable for SBLOCAs. As a result, such changes are not considered ALARP because the significant cost increase would be grossly disproportional to the small improvement in safety, especially since the SAP Target 9 BSO is already met.

9.6.4.6 Large Break LOCA Conclusions

The conclusions of the best-estimate large-break LOCA analysis are that there is a high level probability that the following criteria are met.

1. The calculated maximum fuel element cladding temperature (i.e., PCT) will not exceed 1204.4°C (2200°F).

2. The calculated total oxidation of the cladding (i.e., maximum cladding oxidation) will nowhere exceed 0.17 times the total cladding thickness before oxidation.

3. The calculated total amount of hydrogen generated from the chemical reaction of the cladding with water or steam (i.e., maximum hydrogen generation) will not exceed 0.01 times the hypothetical amount that would be generated if all of the metal in the cladding cylinders surrounding the fuel, excluding the cladding surrounding the plenum volume, were to react.

4. The calculated changes in core geometry are such that the core remains amenable to cooling.

   Note that criterion 4 has historically been satisfied by adherence to criteria 1 and 2, and by assuring that fuel deformation due to combined LOCA and seismic loads is specifically addressed. Criteria 1 and 2 are satisfied for best-estimate large-break LOCA applications. The approved methodology specifies that effects of LOCA and seismic loads on core geometry do not need to be considered unless grid crushing extends beyond the assemblies in the low power channel as defined in the WCOBRA/TRAC model. This situation has not been calculated to occur for the AP1000 plant in the standard LOCA analysis. Therefore, acceptance criterion 4 is satisfied.

   An additional assessment was carried out to assess the potential for grid crush to extend beyond the assemblies in the low power channel as a result of a depressurisation of the primary circuit due to a double-ended guillotine (DEG) break of the RCS cold leg. This assessment, documented in Reference 9.6.4-4, analysed the DEG break at the reactor vessel inlet using the standard LOCA methodology and tools. Due to the low IEF of such a break, realistic but conservative operating assumptions were used as described in Reference 9.6.4-4. This assessment concluded that no grid crushing will occur outside of the low power assemblies due to the depressurisation and therefore coolable geometry will be maintained.

5. After successful initial operation of the ECCS, the core temperature will be maintained at an acceptably low value and decay heat will be removed for the extended period of time required by the long-lived radioactivity remaining in the core.

   Criterion 5 is satisfied if a coolable core geometry is maintained and the core is cooled continuously following the LOCA. The AP1000 passive core cooling system provides effective core cooling following a large-break LOCA event, even assuming the limiting single failure of a core makeup tank delivery line isolation valve. The large-break LOCA transient has been extended beyond fuel rod quench to the time at which the CMT liquid level has decreased to the Low-6 setpoint that actuates the fourth-stage ADS valves and IRWST injection. A significant increase in safety injection flow rate occurs when the IRWST becomes active. The analysis performed demonstrates that CMT injection is sufficient to maintain the mass inventory in the core and downcomer, from the period of fuel rod quench until IRWST injection. The PXS provides effective post-LOCA long-term core cooling (Section 9.6.6).

Table 9.6.4-5 presents the calculated 95th percentile PCT, maximum cladding oxidation, maximum hydrogen generation, and core cooling results.

Based on the analysis, the Westinghouse Best-Estimate Large-Break LOCA methodology has shown that the applicable acceptance are satisfied when the burnup-related effects of thermal conductivity degradation and peaking factor burndown are considered.

Radiological consequences are within the Target 4 BSL for infrequent faults with IEF < 1E-04 (100 mSv offsite and 500 mSv onsite). Thus, the identification of necessary Class 1 SSCs is adequate to meet DB requirements for this fault.

An assessment of the large break loss of coolant accident has been completed concluding that the AP1000 plant includes adequate systems for the protection of the fault, which limit the radiological consequences such that they are compliant with the SAP targets and the risks have been reduced to be ALARP.

9.6.4.7 References

9.6.4-1 European Commission Report EUR 19841 EN, "Determination of the in-containment source term for a large-break loss of coolant accident," April 2001.

9.6.4-2 Westinghouse Documents WCAP-12945-P-A (Proprietary) (Volume 1 - Revision 2; Volumes 2 through 5 - Revision 1) and WCAP-14747 (Non-Proprietary), "Code Qualification Document for Best Estimate LOCA Analysis," 1998.

9.6.4-3 Westinghouse Documents WCAP-14171, Rev. 2 (Proprietary) and WCAP-14172, Rev. 2 (Non-Proprietary), "WCOBRA/TRAC Applicability to AP600 Large-Break Loss-of-Coolant Accident," March 1998.

9.6.4-4 Westinghouse Report UKP-GW-GLR-035, Rev. 0, "UK AP1000® Fuel Tolerability of Depressurisation of the Primary Circuit Assessment," August 2016.

9.6.4-5 Westinghouse Letter LTR-NRC-12-86, "Westinghouse Response to NRC RAIs on WCAP-17524, 'AP1000 Core Reference Report' (Proprietary/Non-Proprietary)," January 2, 2013.

9.6.4-6 Westinghouse Documents WCAP-16009-P-A, Rev. 0 (Proprietary) and WCAP-16009-NP-A, Rev. 0 (Non-Proprietary), "Realistic Large-Break LOCA Evaluation Methodology Using the Automated Statistical Treatment Of Uncertainty Method (ASTRUM)," January 2005.

9.6.4-7 Westinghouse Documents WCAP-14449-P-A, Rev. 1 (Proprietary) and WCAP-14450-NP-A, Rev. 1 (Non-Proprietary), "Application of Best Estimate Large Break LOCA Methodology to Westinghouse PWRs with Upper Plenum Injection," October 1999.

9.6.4-8 Westinghouse Document APP-GW-GLE-026, Rev. 1, "Application of ASTRUM Methodology for Best-Estimate Large-Break Loss-of-Coolant Accident Analysis for AP1000," January 2009.

Table 9.6.4-1. Major Plant Parameter Assumptions Used in the Best-Estimate Large-Break LOCA Analysis

Parameter	Value
Plant Physical Configuration	
Steam generator tube plugging level	≤ 10% (10% tube plugging bounds 0%)
Hot assembly location	Under support column (Bounds under open hole or guide tube)
Pressuriser location	In intact loop (Bounds location in broken loop)
Initial Operating Conditions	
Reactor power	Core power < 1.01*3400 MWt
Peak linear heat rate	See Table 9.6.4-4
Hot rod assembly power	See Table 9.6.4-4
Hot assembly power	$P_{HA} \leq 1.654$
Axial power distribution(1)	See Figure 9.6.4-13
Peripheral assembly power	$0.2 \leq P_{LOW} \leq 0.8$
Fluid Conditions	
Reactor coolant system average temperature	$300.9 - 4.4°C \leq T_{AVG} \leq 300.9 + 4.4°C$ $(573.6 - 8.0°F \leq T_{AVG} \leq 573.6 + 8.0°F)$
Pressuriser pressure	15.51 ± 0.34 MPa abs (2250 ± 50 psia)
Pressuriser level (water volume)	28.3 m^3 (1000 ft^3) (nominal)
Accumulator temperature	$10°C \leq T_{ACC} \leq 48.9°C$ ($50°F \leq T_{ACC} \leq 120°F$)
Accumulator pressure	4.5 MPa abs $\leq P_{ACC} \leq$ 5.4 MPa abs (652 psia $\leq P_{ACC} \leq$ 784 psia)
Accumulator water volume	47.2 $m^3 \leq V_{ACC} \leq$ 49.1 m^3 (1666.8 $ft^3 \leq V_{ACC} \leq$ 1732.3 ft^3)
Reactor Coolant System Boundary Conditions	
Single failure assumption	Failure of one CMT isolation valve to open
Offsite power availability	Available (Bounds loss of offsite power at time zero)
RCP automatic trip delay time after receiving S-signal	5.3 s
Containment pressure	Bounded (minimum)

Note:
1. Treatment of axial power distribution consistent with WCAP-16009-P-A (Reference 9.6.4-6) methodology.

Table 9.6.4-2. AP1000 LOCA Chronology

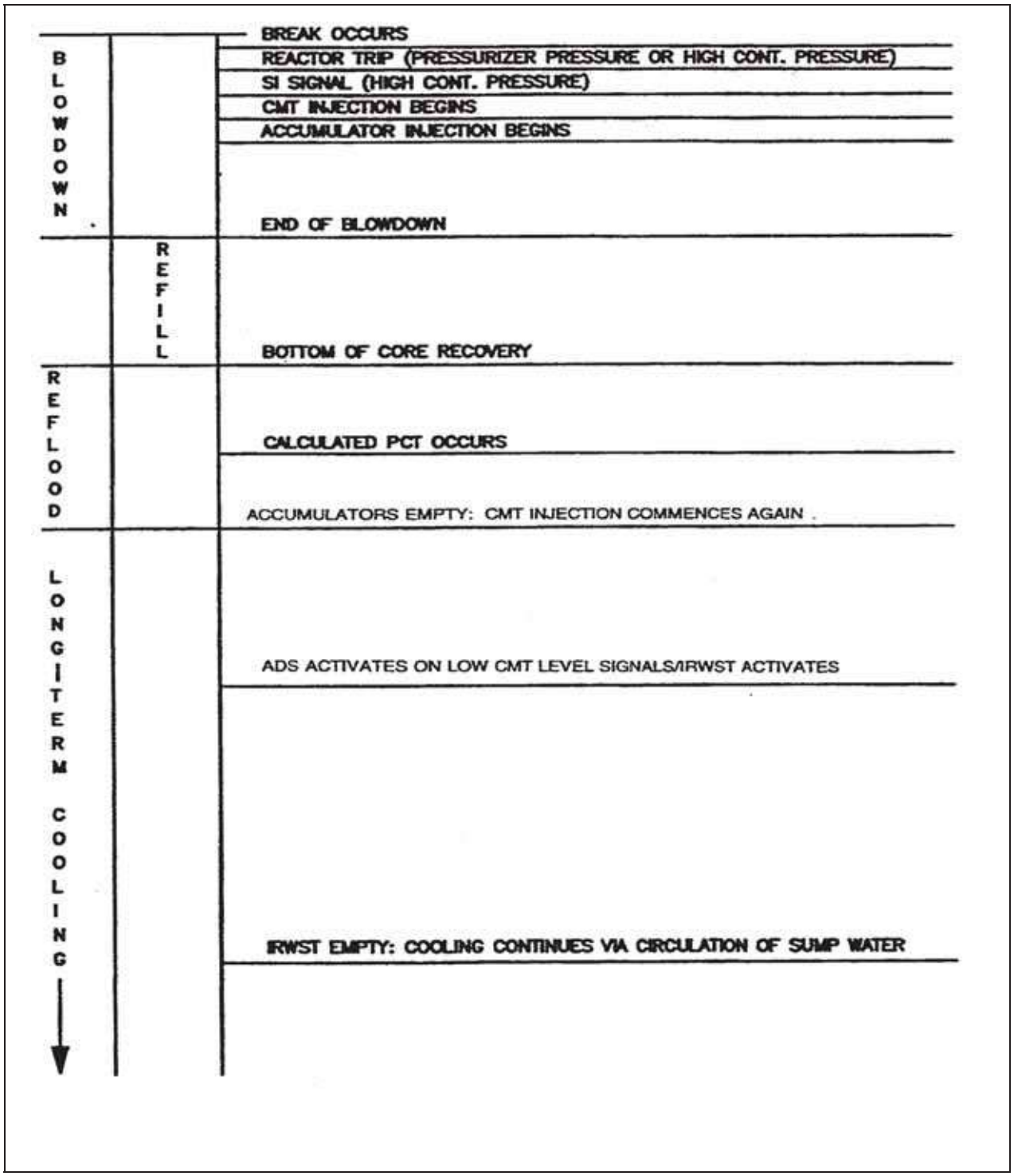


Table 9.6.4-3. Best-Estimate Large-Break Sequence Of Events For The Limiting PCT Case

Event	Time (seconds)
Break initiation	0.0
Safeguards signal	2.2
CMT isolation valves begin to open	4.2
Reactor coolant pumps trip	9.5
Accumulator injection begins	~13
End of blowdown	27.5
Bottom of core recovery	39.5
Calculated PCT occurs	~58
Core quench occurs	~240
CMT injection resumes	~200
End of transient	265

Table 9.6.4-4. Summary Of Peaking Factor Burndown Supported By Best-Estimate Large-Break LOCA

Hot Rod Burnup (GWd/MTU)	FdH (includes uncertainties)[1]	FQ Transient (maximum FQ, includes uncertainties)	FQ SS Baseload (without uncertainties)
0	1.72	2.60	2.10
30	1.72	2.60	2.10
49	1.55	2.30	1.85
55	1.55	2.30	1.85
62	1.40	1.90	1.45

Note:
1. Hot assembly power follows the same burndown since it is a function of FdH.

Table 9.6.4-5. Best-Estimate Large-Break LOCA Results

Requirement	Value	Criteria
Calculated 95th percentile PCT (°C [°F])	1058 [1936][(1)]	≤ 1204.4 [2200]
Maximum local cladding oxidation (%)	4.2	≤ 17
Maximum core-wide cladding oxidation (%)	0.30	≤ 1
Coolable geometry	Core remains coolable	Core remains coolable
Long-term cooling	Core remains cool in long term	Core remains cool in long term

Note:
1. Value contains 1.1°C [2°F] bias for PCT sensitivity to PRHR isolation.

Tables 9.6.4-6 and 9.6.4-7 Not Used.

Table 9.6.4-8. Parameters Used In Evaluating The Radiological Consequences Of A Large-Break LOCA

(Page 1 of 2)

Reactor coolant iodine activity	Equal to the operating limit for reactor coolant activity of 9.25E6 Bq/kg (0.25 μCi/g) dose equivalent I-131 (see Table 9A-1)
Reactor coolant noble gas activity	Equal to the operating limit for reactor coolant activity of 2.6E9 Bq/kg (70 μCi/g) dose equivalent Xe-133 (see Table 9A-1)
Reactor coolant alkali metal activity	Design basis activity (see Table 9A-1)
Reactor coolant mass	1.99E5 kg (4.39E5lbm)
RCS Activity Airborne fractions Iodines Noble gases Alkali metals	 0.5 1.0 0.5
Containment Volume	5.83E4 m^3 (2.06E6 ft^3)
Containment Purge Modelling Flow Rate Isolation Timing	 2.72E4 m^3/hr (1.6E4 cfm) 30 sec
Fraction of fuel rods assumed to fail	0.33
Core activity	See Table 9A-3
Radial peaking factor (for determination of activity in failed fuel rods)	1.75
Fission product gap fractions Iodines Noble gases Alkali metals	 0.03 0.10 0.04
Dry Phase Activity Release (30 seconds to 120 seconds)| Fraction of Gap Activity Released to Containment Atmosphere Iodines Noble gases Alkali metals Airborne Iodine Chemical Fractions Elemental Iodine Organic Iodine Particulate Iodine	 0.1 1.0 0.1 0.02 0.002 0.978

Table 9.6.4-8. Parameters Used In Evaluating The Radiological Consequences Of A Large-Break LOCA

(Page 2 of 2)

Wet Phase Activity Release (120 seconds to 180 seconds)|	
Fraction of Gap Activity Released to RCS	
Iodines	0.9
Noble gases	0.0
Alkali metals	0.9
Fraction of RCS Activity becoming airborne	
Iodines	0.6
Noble gases	0.0
Alkali metals	0.0
Airborne Iodine Chemical Fractions	
Elemental Iodine	0.99
Organic Iodine	0.01
Particulate Iodine	0.0
Removal Coefficients(1)	
Elemental Iodine	1.7 (hr^{-1})
Organic Iodine	0.0 (hr^{-1})
Particulates	0.5 (hr^{-1})
Containment Leakage Rate	
0-24 hours	0.1 (%/day)
24-720 hours	0.05 (%/day)
Offsite atmospheric dispersion factors	See Table 9A-5
Control room modelling	See Appendix 9A

Note:

1. Elemental iodine removal is modelled until a DF of 200 is reached. Particulate removal is modelled until a DF of 1.0E4 is reached.

Table 9.6.4-9. Large-Break LOCA Technical Specifications Used In Dose Analysis

Limit or Condition	Tech Spec Identification and Notes
Primary Containment Leakage Rate	3.6.1 (SR 3.6.1.1) within containment leakage acceptance criteria. 5.5.8 (Containment leakage rate testing program) defines maximum allowable primary containment leak rate to be less than or equal to 0.1 weight-% per day at the calculated peak containment internal pressure for the design basis LOCA.
Primary coolant specific activity	3.4.10 dose equivalent specific activity to be < 9.25E6 Bq/kg (0.25 µCi/g) for I-131 and < 2.6E9 Bq/kg (70 µCi/g) for Xe-133

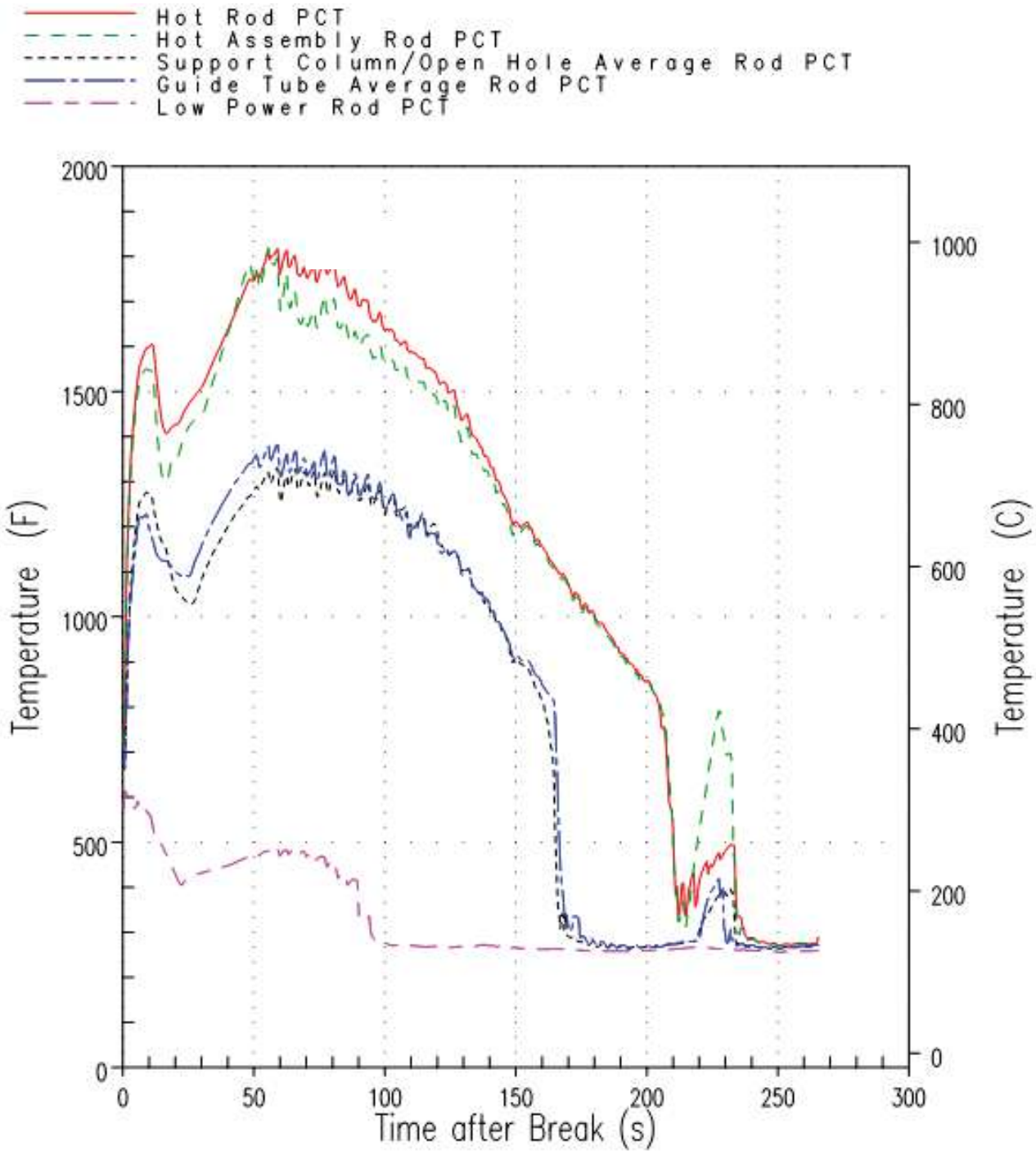


Figure 9.6.4-1. WCOBRA/TRAC Peak Cladding Temperature for All Five Rod Groups for 95th Percentile Estimator PCT/MLO Case

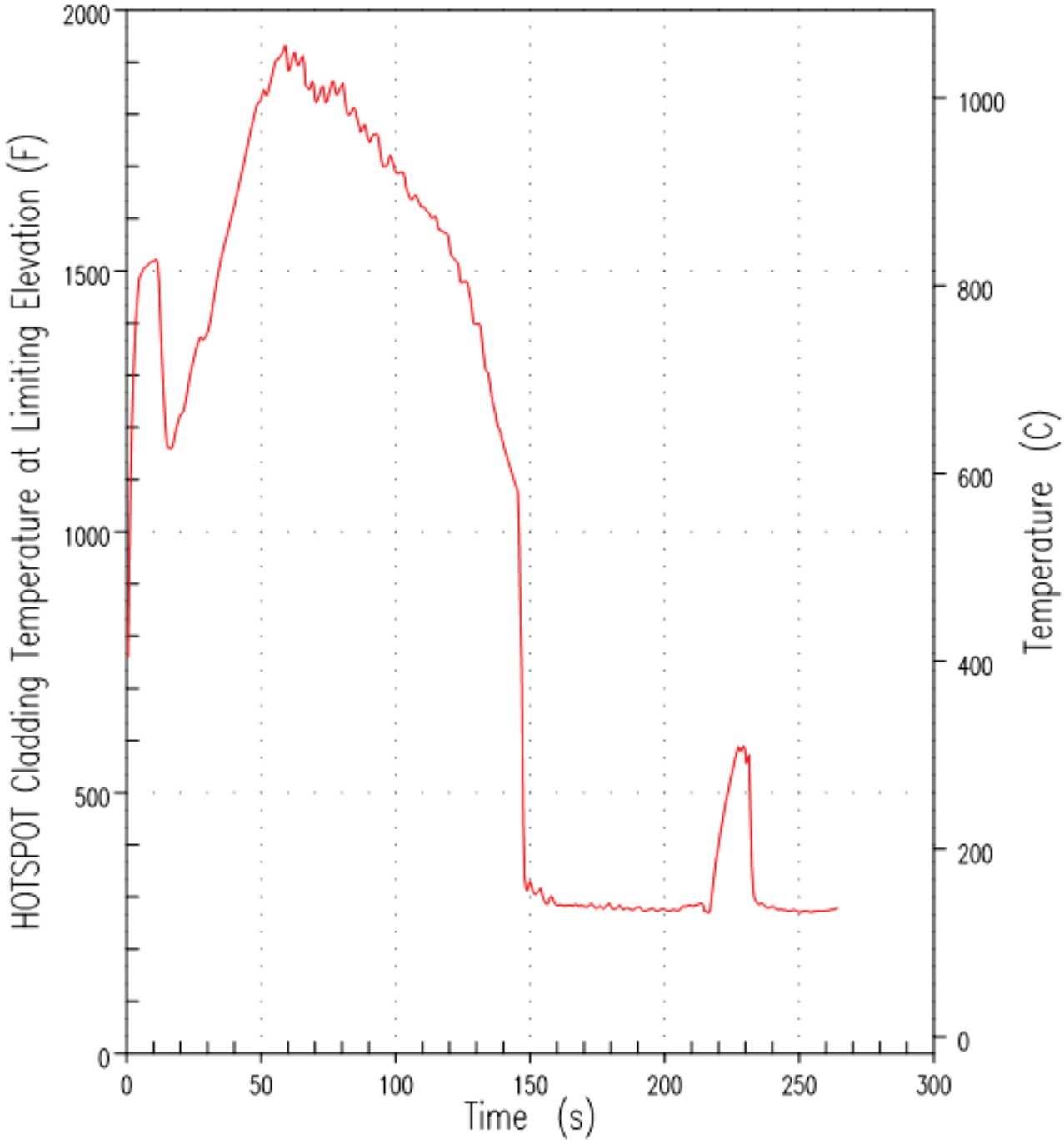


Figure 9.6.4-2. HOTSPOT Cladding Temperature Transient at Limiting Elevation for 95th Percentile Estimator PCT Case

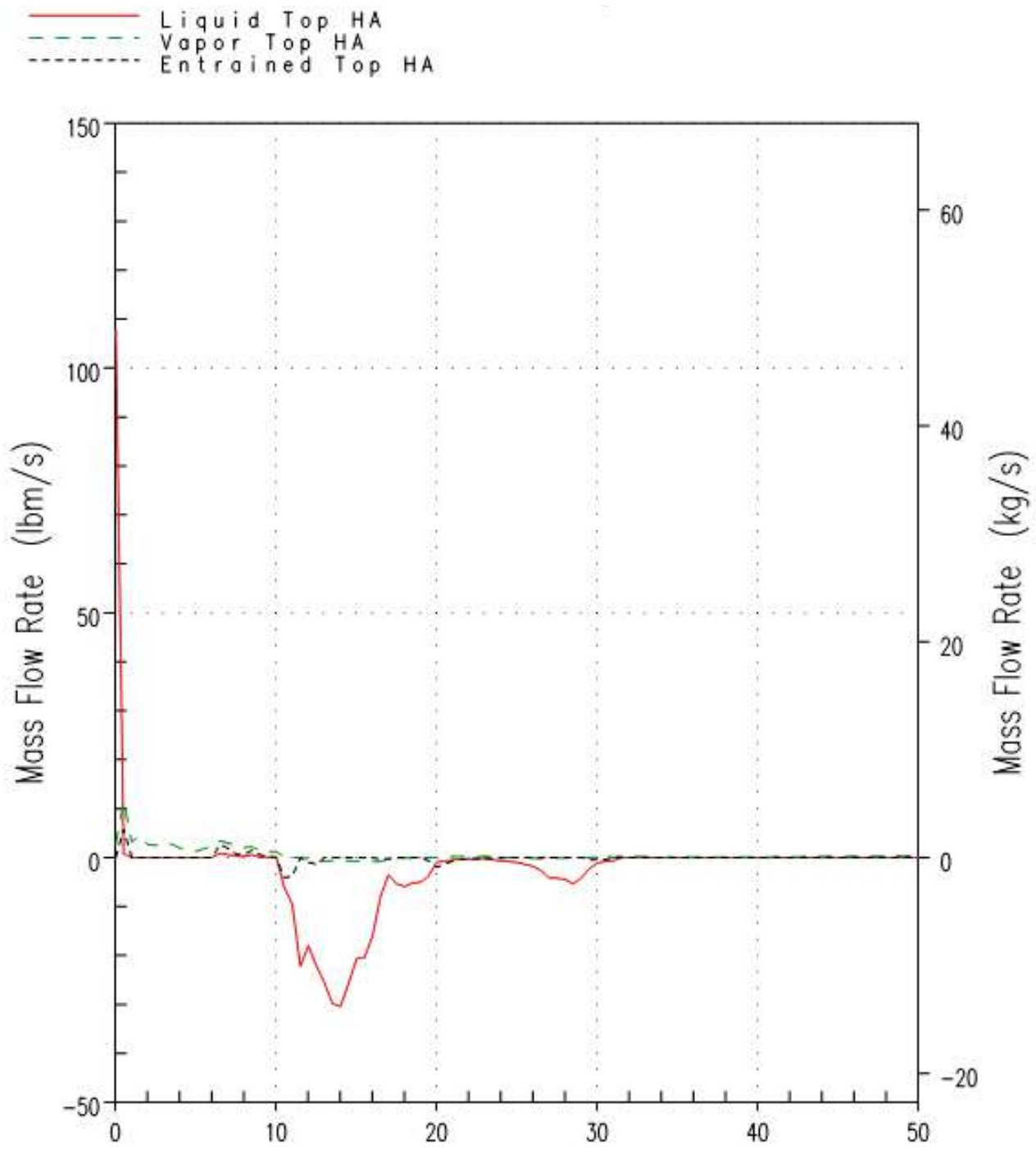


Figure 9.6.4-3. Mass Flow at Top of Hot Assembly Channel for 95th Percentile Estimator PCT Case

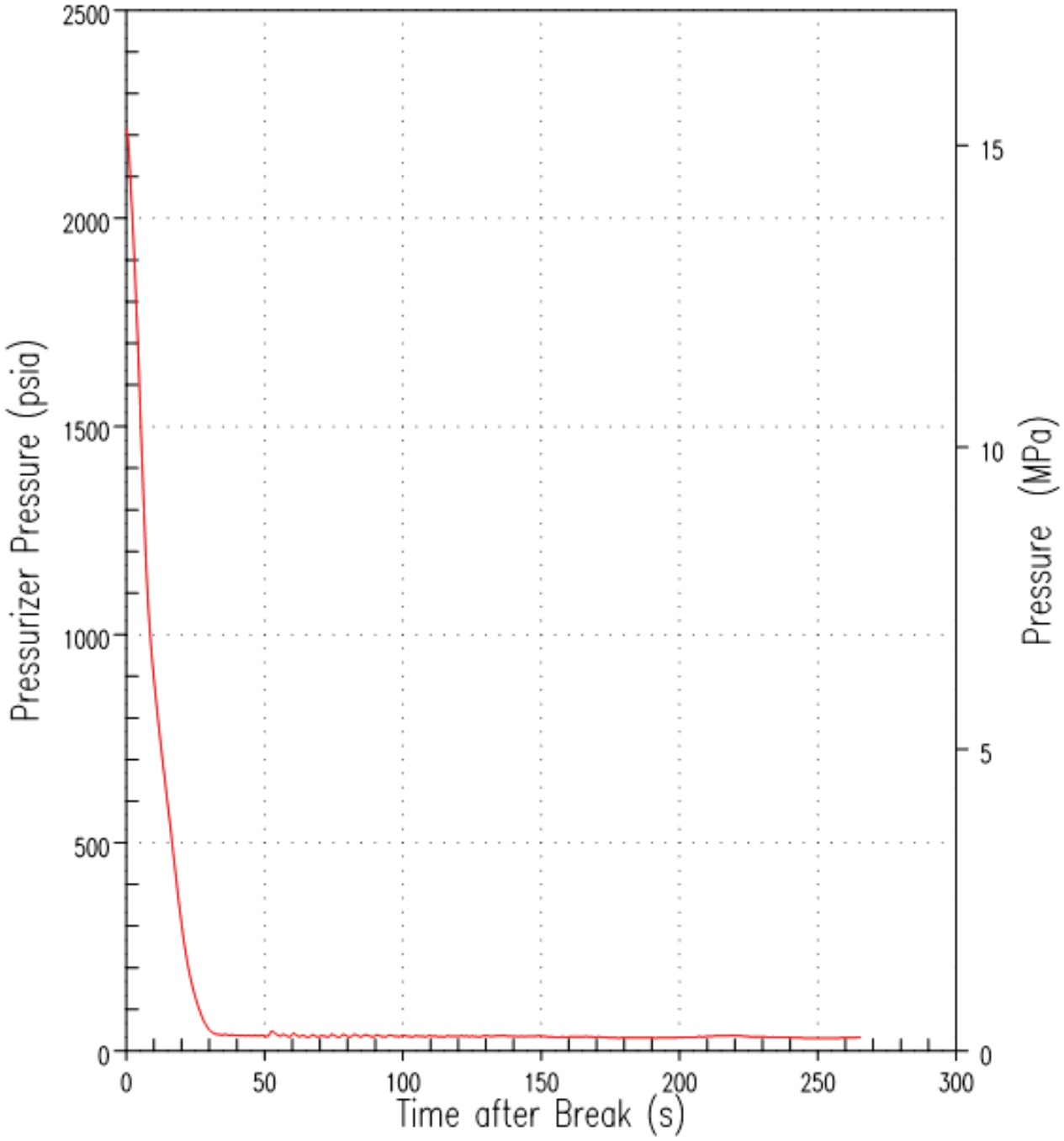


Figure 9.6.4-4. Pressuriser Pressure for 95th Percentile Estimator PCT Case

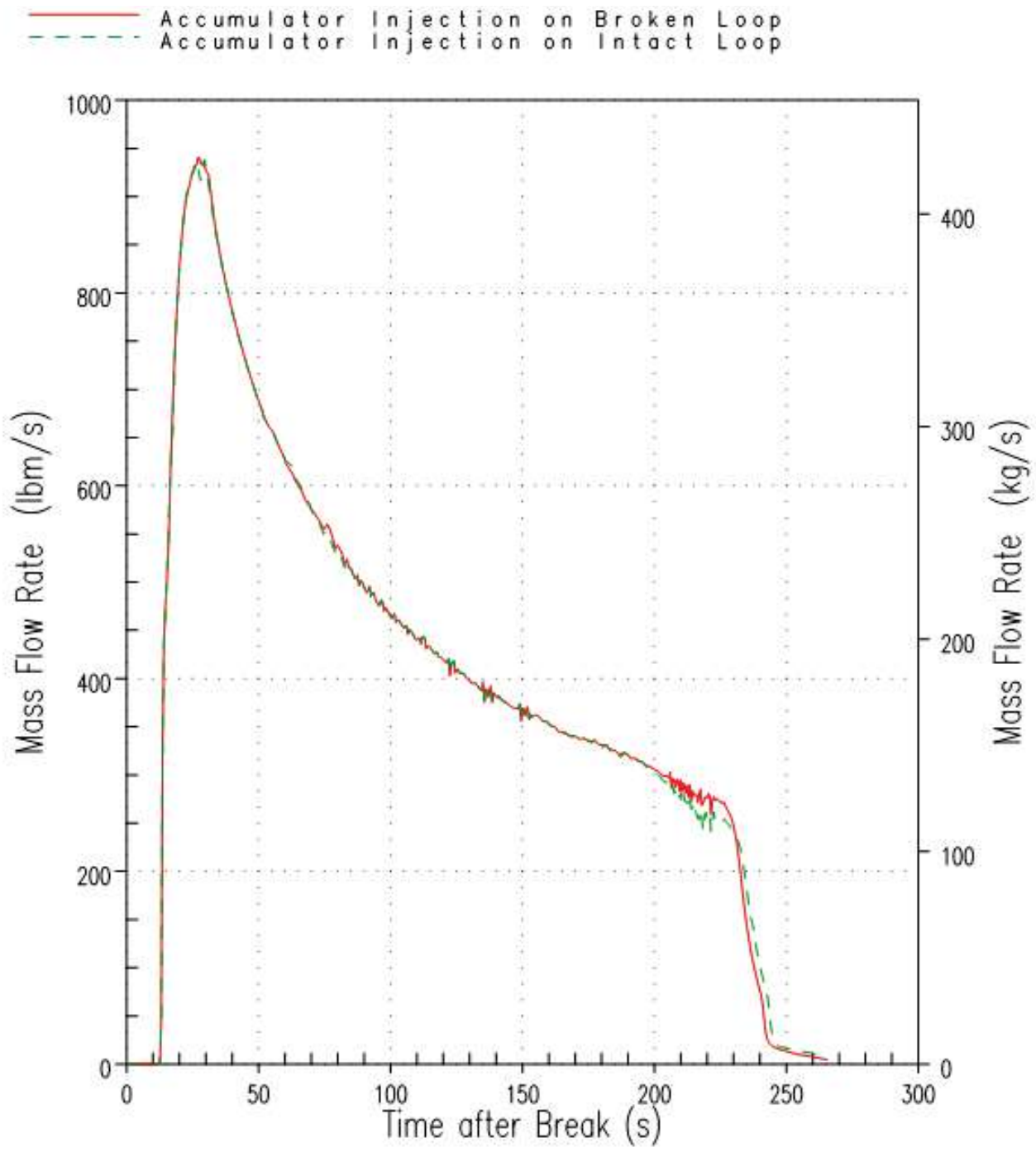


Figure 9.6.4-5. Accumulator Injection Flow for 95th Percentile Estimator PCT Case

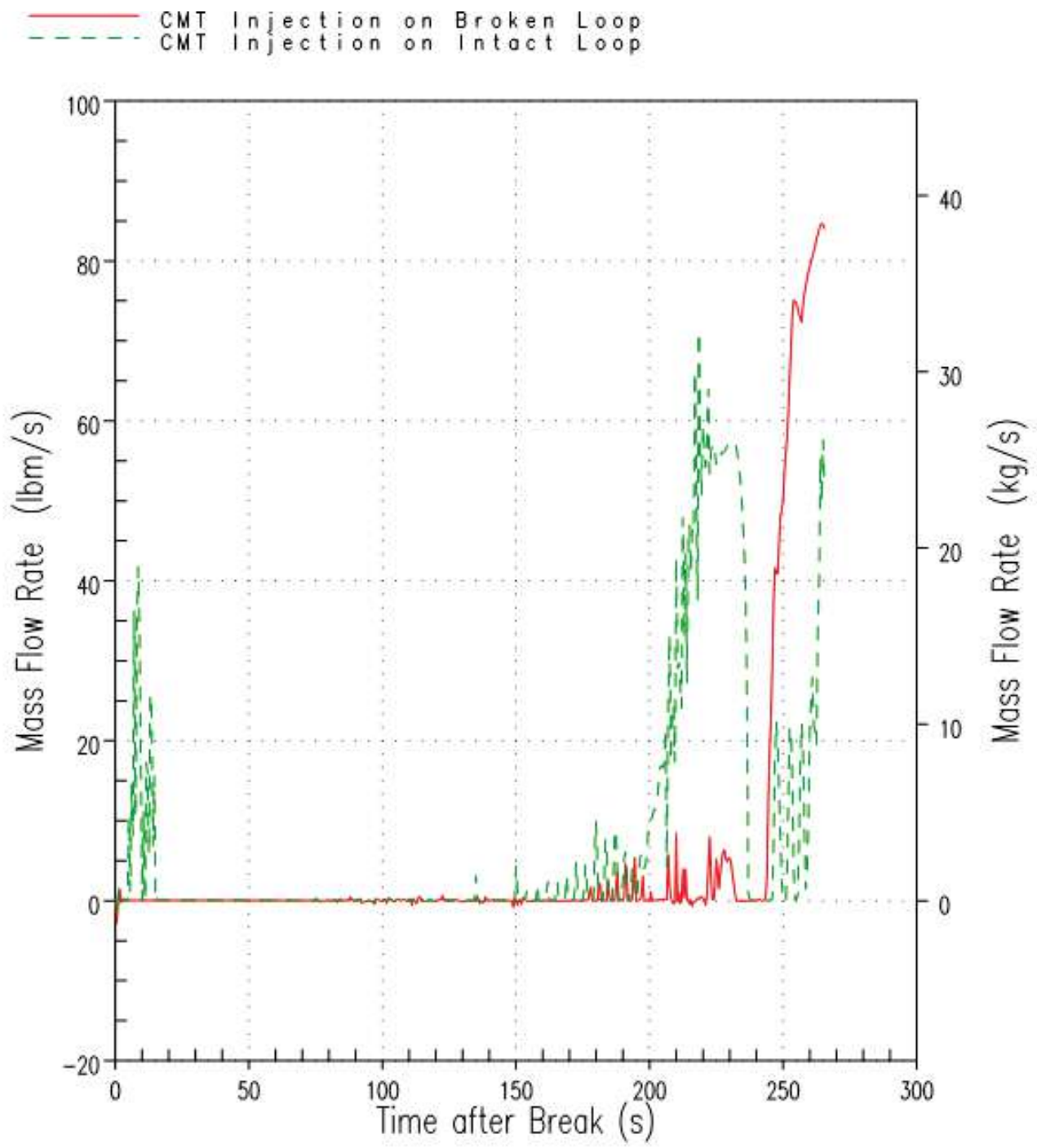


Figure 9.6.4-6. Core Makeup Tank Injection Flow for 95th Percentile Estimator PCT Case

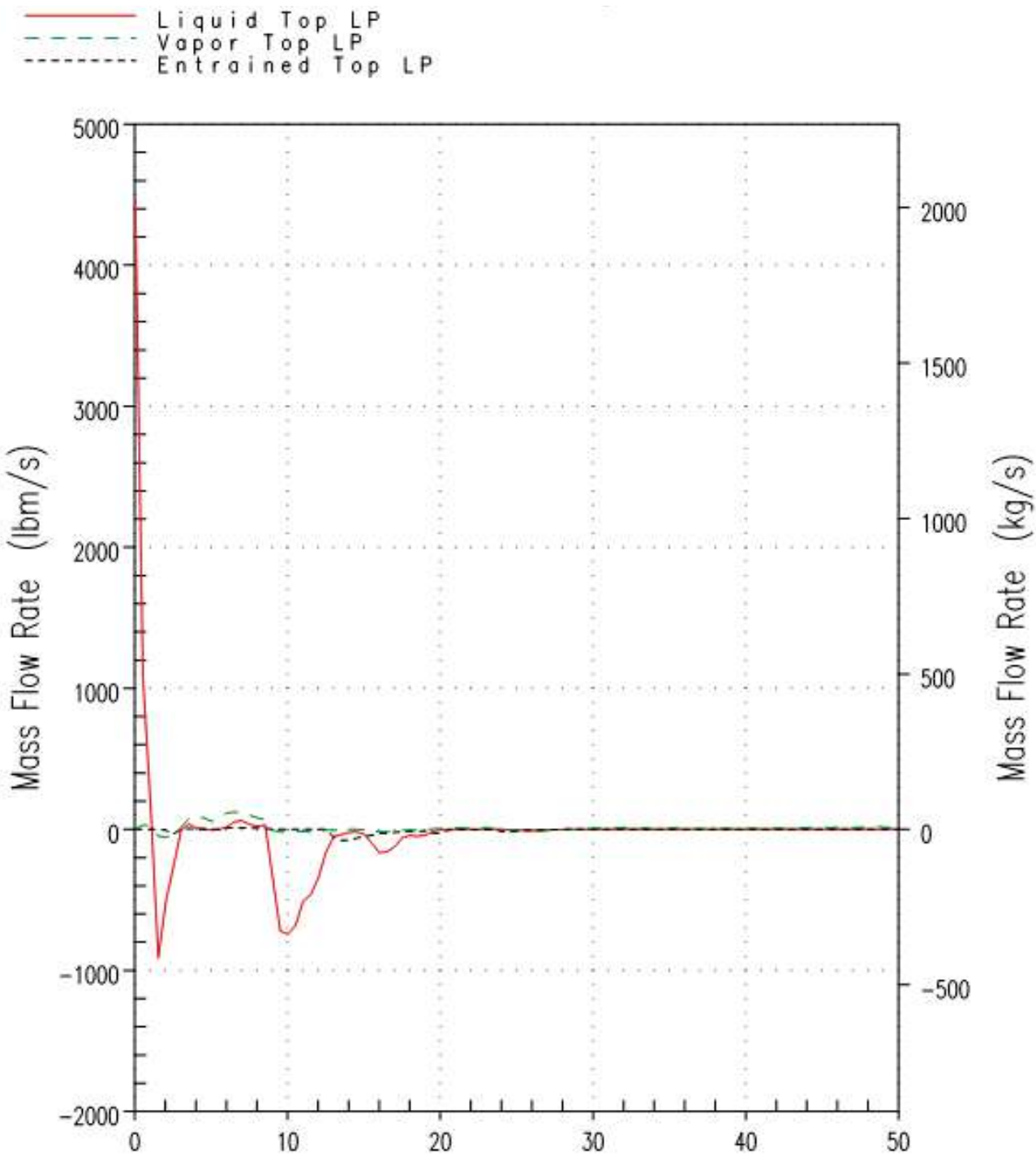


Figure 9.6.4-7. Mass Flow at Top of Peripheral Assemblies Channel for 95th Percentile Estimator PCT Case

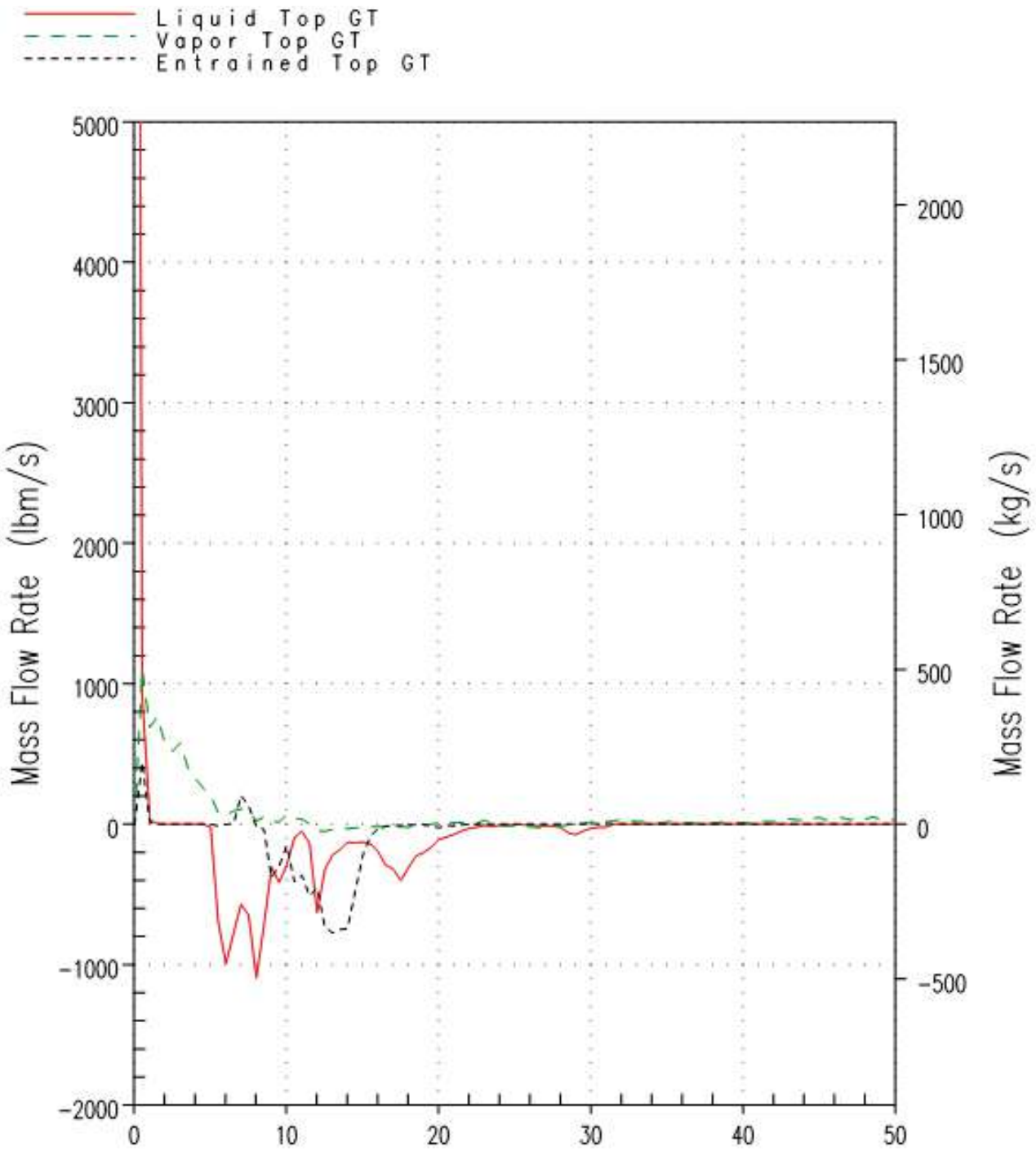


Figure 9.6.4-8. Mass Flow at Top of Guide Tube Assemblies Channel for 95th Percentile Estimator PCT Case

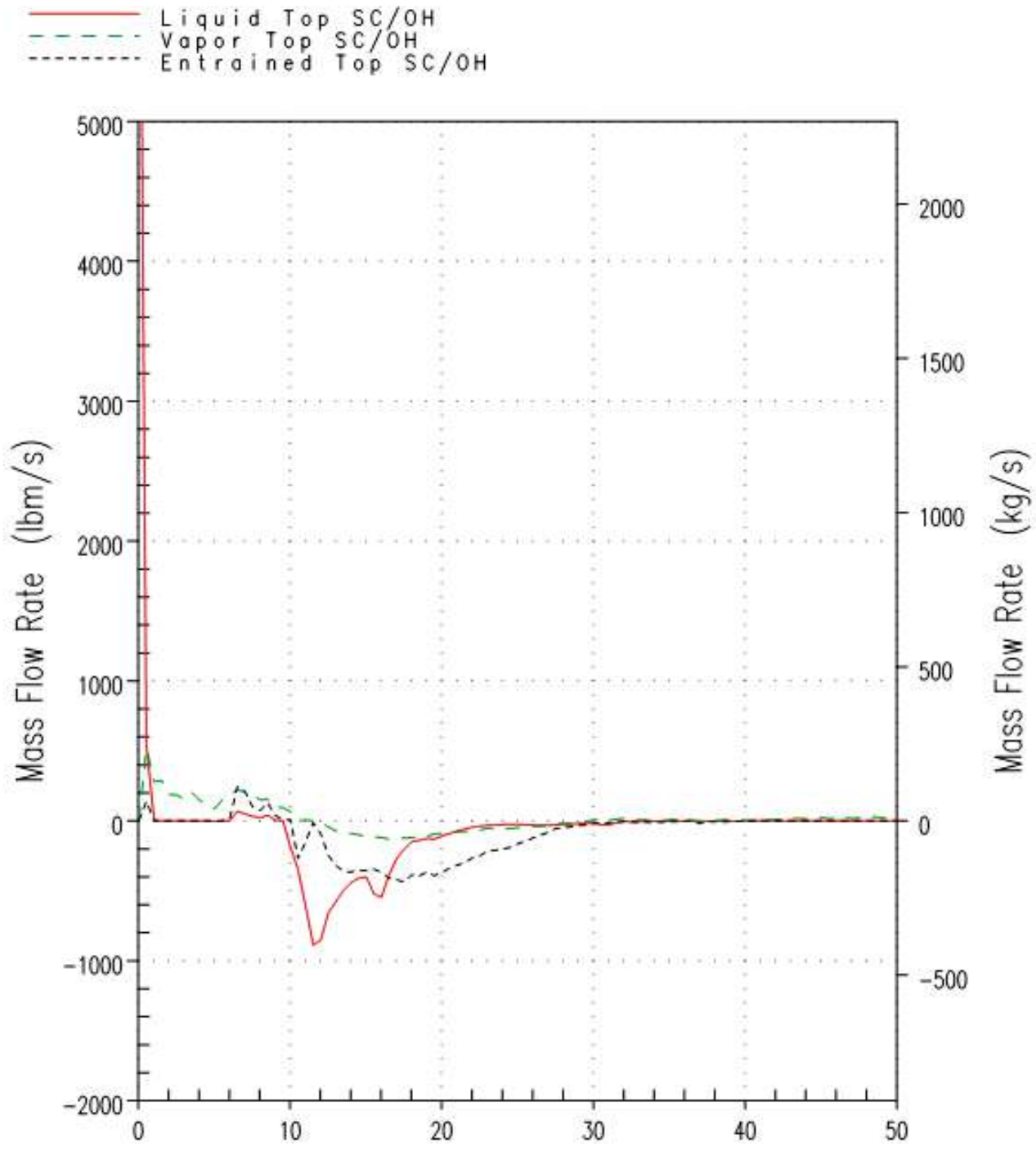


Figure 9.6.4-9. Mass Flow at Top of Support Column/Open Hole Assemblies Channel for 95th Percentile Estimator PCT Case

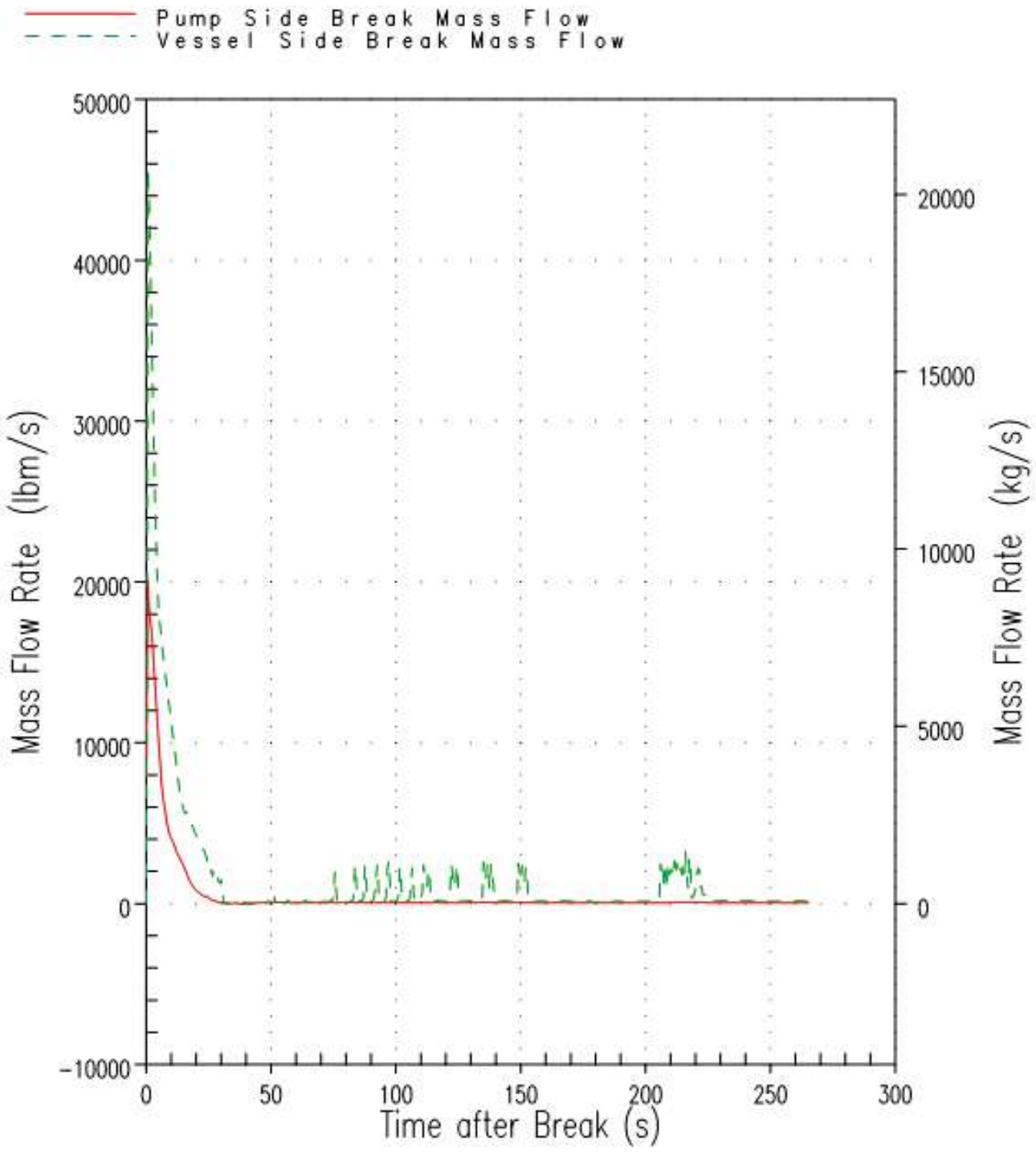


Figure 9.6.4-10. Break Mass Flow for 95th Percentile Estimator PCT Case

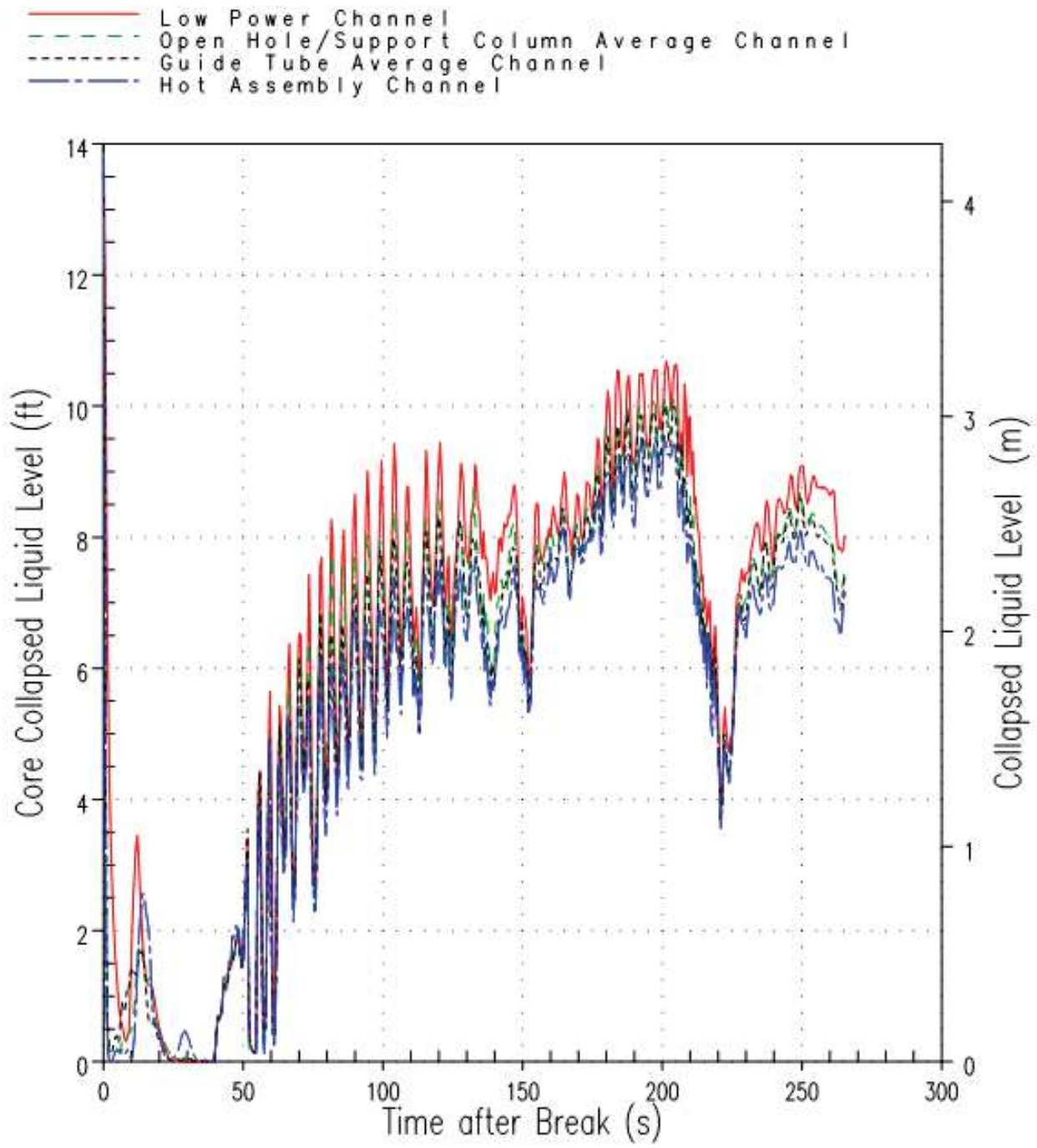


Figure 9.6.4-11. Core Channel Collapsed Liquid Levels for 95th Percentile Estimator PCT Case (Reference Point: Bottom of Active Fuel)

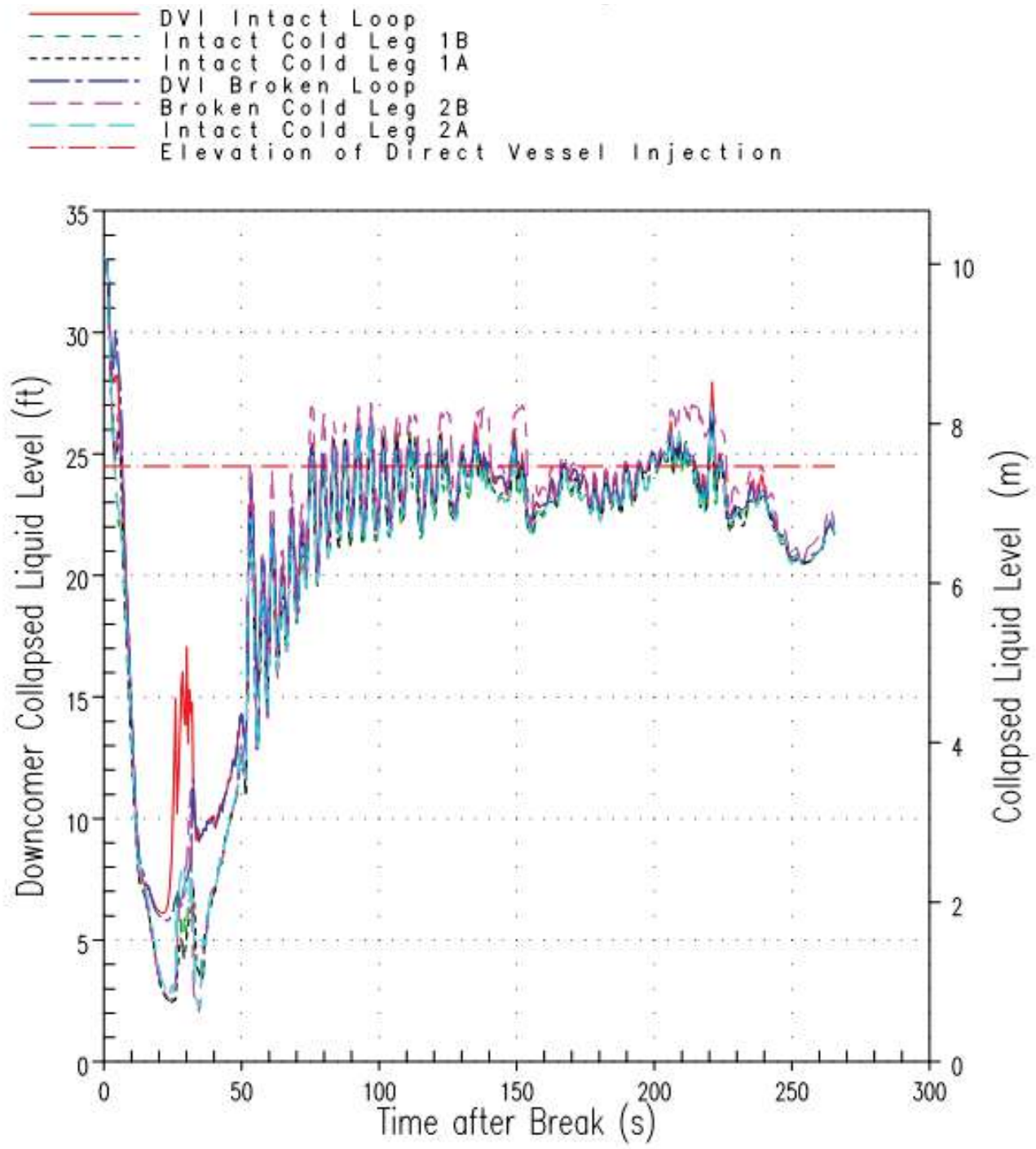


Figure 9.6.4-12. Downcomer Channel Collapsed Liquid Levels for 95th Percentile Estimator PCT Case (Reference Point: Inside Bottom of Vessel)

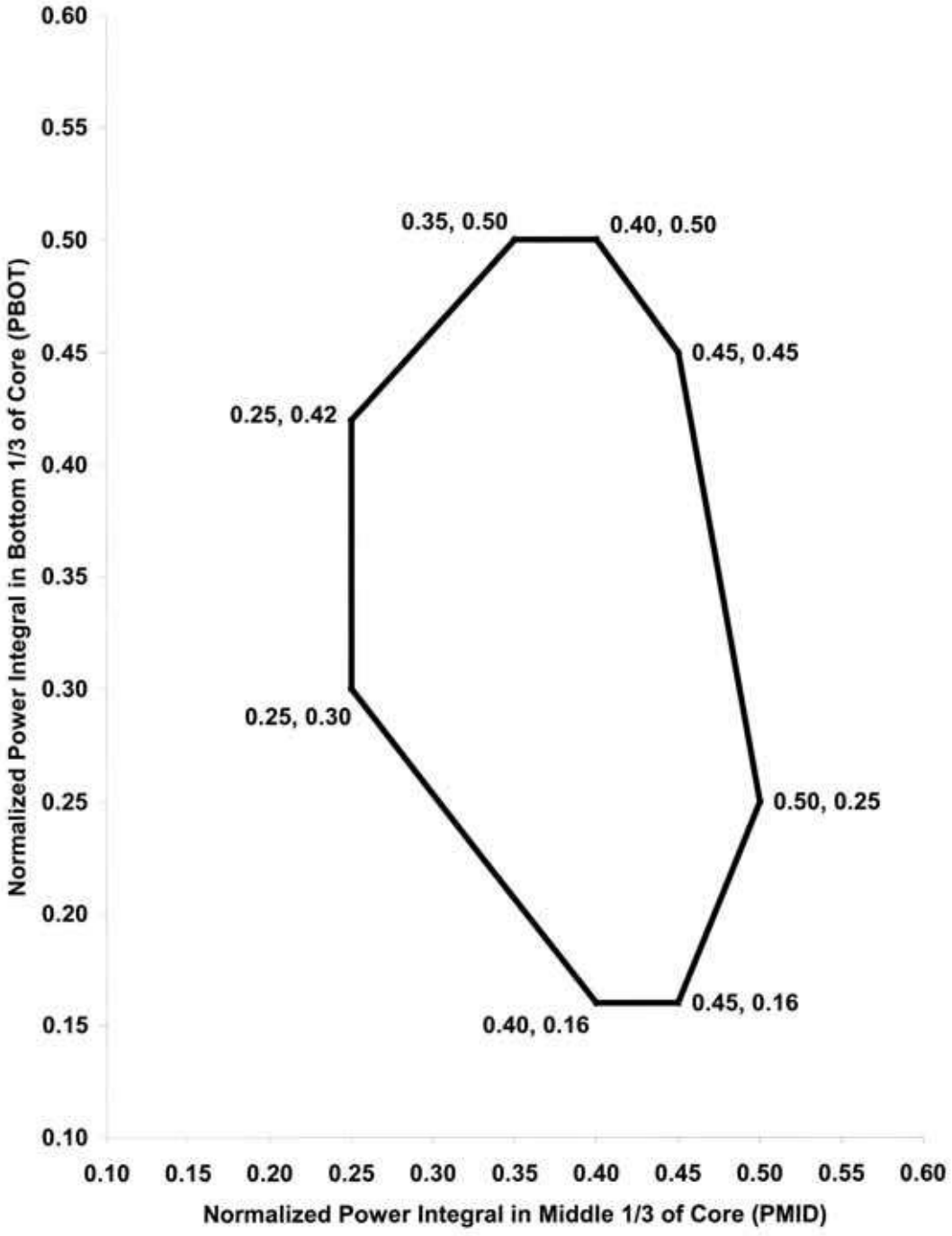


Figure 9.6.4-13. PBOT/PMID Box Supported by AP1000 ASTRUM Analysis

9.6.5 Medium and Small Break Loss-of-Coolant Accident Faults

A number of faults that could result in a decrease in reactor coolant inventory are postulated. The events smaller than a large break LOCA are discussed in this section. Detailed analyses are presented for the most limiting of the primary system coolant decrease events.

9.6.5.0 Introduction and Overview of Faults

A LOCA is the result of a rupture of the RCS pressure boundary. For the sake of convenience, this section addresses most LOCAs except LBLOCAs, since the phenomenology and methods of analysis are similar. The faults considered here, all of which result in leak paths to the containment, are as follows:

- MBLOCA, (Faults 1.4.1 – see Appendix 8A) including inadvertent opening of a pressuriser safety valve and inadvertent operation of ADS stages 1 to 3 (Fault 1.5.2 – see Appendix 8A)
- Safety injection (direct vessel injection [DVI]) line break (SI-LB) (Fault 1.7.1 – see Appendix 8A)
- CMT line break (CMTLB) (Fault 1.6.1 – see Appendix 8A)
- SBLOCA (Faults 1.8.1 and 1.8.2 – see Appendix 8A)
- PRHR system tube rupture (Fault 1.10.1 – see Appendix 8A)
- Reactor coolant leakage (Fault 1.9.1 – see Appendix 8A)

SGTR and leakage through sample and instrumentation lines are addressed separately because they may yield leak paths from the RCS that bypass the containment.

The AP1000 plant design includes passive safety features to prevent or minimise core uncovery during MBLOCAs and SBLOCAs (see the fault schedule in Appendix 8A). The passive safety design approach of the AP1000 plant is to depressurise the RCS if the break or leak is greater than the capability of the makeup system or if the normal makeup system fails to perform. By depressurising the reactor system, large volumes of borated water in the accumulators and IRWST become available for cooling the core. The CMT injection is available at any RCS pressure and its level is used to actuate the depressurisation system. The analysis presented herein demonstrates that, with a single failure, the passive systems are capable of depressurising the RCS while maintaining acceptable core conditions and establishing stable delivery of cooling water from the IRWST.

The spectrum of breaks analysed for the AP1000 design represents a range of expected break sizes in the RCS and PXS, and expected system response. It should be noted that a pipe break can consist of the following types:

1. Full or partial breaks across the diameter of a pipe
2. Split breaks of various orientations and configurations
3. Non-breaks consisting of the inadvertent opening of valves that form the pressure boundary.

A double-ended pipe break depends on the pipe diameter. For example, a double-ended break of a primary loop piping is a large LOCA, while a double-ended break of an instrument line is a small LOCA. Split breaks can be any size depending on the length and width of the crack. In general, if a split break is larger than the pipe flow area, the break flow will choke at the pipe diameter. Choked flow dominates the flow through the break until the upstream pressure is roughly twice the containment pressure. After the upstream pressure falls below this level, the flow is no longer choked and the size of the break has a large influence on the break flow.

A DBA of the bounding fault is presented, aspects of the fault progression are described, the methods and assumptions adopted for the DB analysis are reviewed, and the Class 1 systems assumed to be available for that analysis are summarised. The DB analyses are summarised, and the radiological consequences are compared with the relevant SAPs targets.

The discussion of each fault concludes with an ALARP assessment and a summary of the safety designations that follow from the assessment.

Design Basis Requirements

The acceptance criteria for all of the DB analyses for MBLOCAs and SBLOCAs are consistent, and are described below:

- The calculated maximum fuel element cladding temperature shall not exceed 1204.4°C (2200°F).
- Localised cladding oxidation shall not exceed 17 percent of the total cladding thickness before oxidation.
- The amount of hydrogen generated from fuel element cladding reacting chemically with water or steam shall not exceed 1 percent of the total amount if all metal cladding were to react.
- The core remains amenable to cooling for any calculated change in core geometry.
- The core temperature is maintained at a low value, and decay heat is removed for the extended period of time required by the long-lived radioactivity remaining in the core.

Each individual fault analysis shows that these criteria are met. These criteria are established to provide significant margin in ECCS performance following a LOCA.

The faults listed below are considered in turn in the sections below. Each fault is first described; the initial event frequency and the design basis class are provided and the bounding fault or faults are identified (if needed). The analysed faults are presented individually in Table 8A-2.

The analysed fault(s) are described in additional detail in the subsequent sections to complete the safety case for each fault, including:

- Identification of Causes and Accident Description
- Design Basis Analysis of Effects and Consequences
- Assessment of the Radiological Consequences for the DBA
- Diverse Mitigation and ATWT for Frequent Faults
- ALARP Assessment

- Conclusions

9.6.5.0.1 Medium Break Loss-of-Coolant Accident (Fault 1.4.1)

Description

The MBLOCA events are defined as all RCS ruptures with break sizes insufficient to depressurise the RCS to the RNS operating pressure without operation of the ADS, but sufficient to allow the automatic actuation of the ADS stage 4 without operation of the ADS stages 1, 2, and 3. This includes RCS pressure boundary breaks of less than 229 mm (9 inches) and greater than or equal to 101.6 mm (4 inches) equivalent diameter. Because these faults involve a leak path to the containment and may lead to core uncovery and heat-up, they are considered to have the potential to release radioactivity to the environment.

Stuck-open pressuriser safety valves and ADS spurious actuation events, which result in a consequential MBLOCA event, are included in the MBLOCA fault, since the pathways to the containment lie in the MBLOCA size range, but are discussed in a separate section.

On the basis of piping size, the range of this category includes SI-LBs and CMTLBs. However, because the mitigating systems response for these break categories is different than for an MBLOCA, they are evaluated separately.

Initiating Event Frequency[1]

The AP1000 design PSA gives the summed IEF for an MBLOCA resulting from a pipe break as 6.8E-06/yr (Table 8A-2). The summed frequency for the fault, which includes spurious operation of ADS stages 1 to 3 and stuck-open pressuriser valve events, is 3.9E-04/yr (Table 8A-2), which makes the fault an infrequent fault. See also a discussion under the SBLOCA section on IEF for further clarification of the correct interpretation of this frequency.

Design Basis Class

The unmitigated consequences of an MBLOCA are assumed to be greater than Target 4 BSL for frequent faults (1 mSv offsite and 20 mSv onsite). These LOCAs (152 mm [6 inch] equivalent piping diameter and larger) are DBL due to historical LOCA experience, the AP1000 design approach (reduced amount of piping, use of bent pipe to reduce number of welds, and better materials), and the piping analysis approach used for the AP1000 (i.e., leak before break). The core cooling response is conservatively analysed with DB1 assumptions (bounding analysis). The reactor internals/fuel structural analysis for these medium LOCAs is bounded by the large break LOCA analysis.

1. As discussed in Chapter 8, the frequency for initiating events from the PSA is used in both Chapters 8 and 9 with the sole purpose of supporting the categorisation of the fault to a specific DB category. As noted in Chapter 8, these probabilities should not be considered to be representative of actual frequency of the events, and for several events they can be significantly conservative. Detailed PSA results and their basis are discussed in Chapter 10.

9.6.5.0.2 Spurious Actuation of Automatic Depressurisation System or Opening of a Pressure Relief Valve (Fault 1.5.2)

Description

Two types of inadvertent depressurisation are discussed in this section: inadvertent operation of ADS valves leading to an MBLOCA, and inadvertent opening of a pressuriser safety valve. These faults are included in the MBLOCA fault; however, their analysis is described separately here for completeness.

Spurious actuation of the ADS is defined as an inadvertent valve-opening event. Depending on the number of the ADS lines spuriously opening, the frequency of ADS spurious actuation can be classified as MBLOCA or LBLOCA. Spurious ADS actuation leading to an LBLOCA is addressed in Section 9.6.4.

Spurious actuation of ADS consisting of one line of the ADS stage 1, 2, 3, or 4 opening is categorised and analysed as a medium LOCA. Spurious ADS consisting of the opening two lines of the ADS stage 4 or one line of the ADS stage 4 with all lines of the ADS stages 1, 2, and 3 may be categorised as a large LOCA.

The ADS system consists of four stages of depressurisation valves. The ADS stages are interlocked; for example, stage 1 is initiated first, and subsequent stages are not actuated until previous stages have been actuated. Each stage includes two redundant parallel valve paths, so that no single failure prevents operation of the ADS stage when it is called upon to actuate, and the spurious opening of a single ADS valve does not initiate ADS flow. To actuate the ADS manually from the MCR, the operators actuate two separate controls positioned at some distance apart on the main control board. Therefore, one unintended operator action does not cause ADS actuation (Section 9.6.1.1).

Initiating Event Frequency

The fault schedule (Appendix 8A) gives a frequency of <1E-08/yr for spurious ADS operation leading to an MBLOCA and a frequency of 3.9E-04/yr for a stuck-open pressuriser valve event. The latter is the dominant contributor to the overall MBLOCA frequency of 6.8E-06/yr. Given the frequency, the fault is an infrequent fault (DB1) in the UK definition.

Design Basis Class

As noted in the MBLOCA assessment, given that the unmitigated consequences of an MBLOCA are assumed to be greater than 1 mSv offsite and 20 mSv onsite and given the IEF, the event is in the DB1 class.

9.6.5.0.3 Small Break Loss-of-Coolant Accident (Faults 1.8.1 and 1.8.2)

Description

The SBLOCA is defined as all RCS ruptures with break sizes less than 102-mm (4-inch) equivalent diameter and greater than those producing leakage that can be made up by the CVS (about 9.5-mm (3/8-inch) equivalent diameter, which corresponds to a break flow rate within the capability of CVS makeup). Note that this fault is divided into two different faults, fault 1.8.1 includes larger breaks that are infrequent and fault 1.8.2 includes smaller breaks that are frequent.

The SBLOCA event differs from the MBLOCA event in that the operation of the PRHR system or the ADS stages 1, 2, and 3 is required to allow the actuation of the ADS stage 4 within its design basis RCS pressure.

Initiating Event Frequency

The more frequent small LOCAs are listed in the fault schedule (appendix 8A) as less than 102 mm (2 inch) with a frequency that is greater than 1E-4 pa. Since this frequency is greater than the cliff edge frequent fault, they are classified as DB2 events.

The less frequent small LOCAs are listed in the fault schedule (appendix 8A) as greater than 102 mm (2 inch) with a frequency that is less than 1E-4 pa. As a result, these faults are classified as DB1 events.

Design Basis Class

The unmitigated consequences of an SBLOCA are assumed to be greater than the Target 4 BSL for frequent faults (1 mSv offsite and 20 mSv onsite). Given the IEFs listed above, the event classification is DB1 for small LOCAs ≥102 mm (2 inch) and DB2 for small LOCAs <102 mm (2 inch).

9.6.5.0.4 Direct Vessel Injection (DVI) Line Break (Fault 1.7.1)

Description

The DVI line break event is defined as any rupture occurring in one of the safety injection (SI) lines (including the DVI and the line that connects the CMT, accumulator, or IRWST to the DVI).

On the basis of break size, these faults are classified as medium LOCAs, but they differ from the MBLOCA because one CMT, one accumulator, one gravity injection line, and one recirculation line are unavailable.

Initiating Event Frequency

The AP1000 design PSA gives the IEF for a DVI line pipe break of 1.4E-06/yr (Table 8A-2), which makes the fault an infrequent fault in the UK definition. It is noted that, depending on the size of the break, this fault is already included in the MBLOCA or SBLOCA faults discussed in previous sections.

Design Basis Class

The unmitigated consequences of an SI-LB are assumed to be greater than the Target 4 BSL for frequent faults (1 mSv offsite and 20 mSv onsite). Given the IEF above, the event is in the DB1 class.

9.6.5.0.5 Core Makeup Tank Line Break (Fault 1.6.1)

Description

The CMTLB event is defined as all ruptures occurring in one of the lines connecting the CMTs to the reactor coolant cold legs.

On the basis of break size, this category is classified as an MBLOCA but is different from the MBLOCA because one of the CMTs is unavailable, with no other systems being impacted.

Initiating Event Frequency

The AP1000 design PSA gives the IEF for a CMTLB of 5.4E-07/yr (Table 8A-2), which makes the fault an infrequent fault. It is noted that, depending on the size of the break, this fault is already included in the MBLOCA or SBLOCA faults discussed in previous sections.

Design Basis Class

The unmitigated consequences of a CMTLB are assumed to be greater than the Target 4 BSL for frequent faults (1 mSv offsite and 20 mSv onsite). Given the IEF above, the event is in the DB1 class.

9.6.5.0.6 Passive Residual Heat Removal Tube Rupture (Fault 1.10.1)

Description

This fault includes events in which a complete, circumferential tube rupture occurs in the PRHR HX. Note that this break could be isolated if the operators close the inlet MOV and the outlet AOVs. For the purposes of this evaluation, it is assumed that isolation of the PRHR does not occur. In this case, the progression of a PRHR tube rupture event is similar to that of an SBLOCA.

Initiating Event Frequency

The probability of this event is listed as 1.1E-04/yr in Table 8A-2, which makes the fault an infrequent fault. The size of the break is bounded by the SBLOCA faults discussed in previous sections.

Design Basis Class

The unmitigated consequences of a PRHR system tube rupture are assumed to be greater than the Target 4 BSL for frequent faults (1 mSv offsite and 20 mSv onsite). Given the IEF above, the event is in the DB1 class.

9.6.5.0.7 Reactor Coolant Leakage (Fault 1.9.1)

Description

For the purpose of this analysis, the RCS leakage category is defined as primary coolant leakage with a leak rate between 0.0631 (1 gpm) and 6.31 L/s (100 gpm). The break size corresponding to a 6.31 L/s flow rate is approximately a 9.5-mm (3/8-inch) break.

The CVS is designed to provide makeup for RCS leaks of 6.31 L/s or less. As long as the RCS inventory is replenished by the CVS, the plant will remain at power and in a safe condition. If the CVS fails, the pressuriser water level will decrease and the event will proceed as an SBLOCA. Thus, the initiating event for this fault is loss of CVS.

For the 0 to 0.0631 L/s leak range with failure of the CVS, it takes more than 60 hours to empty the pressuriser and more than 190 hours to drain each CMT to the ADS actuation water level setpoint. That is, with both CMTs operating, it would take more than 18 days to get to the ADS actuation setpoint.

This event is bounded by the small LOCA and analysis is not presented in this section.

Initiating Event Frequency

The AP1000 design PSA gives the IEF for reactor coolant leakage fault of 1.4E-03/yr (Table 8A-2), which makes the fault a frequent fault.

Design Basis Class

The unmitigated consequences of a reactor coolant leak are assumed to be greater than the Target 4 BSL for frequent faults (1 mSv offsite and 20 mSv onsite). Given the IEF above, the event is in the DB2 class.

9.6.5.1 Medium and Small Break LOCA Analyses

Should a medium or small-break LOCA occur, depressurisation of the reactor coolant system results in a pressure decrease in the pressuriser. The reactor trip signal occurs when the pressuriser low-pressure trip setpoint is reached. An "S" signal is generated when the appropriate setpoint is reached. These measures limit the consequences of the accident in two ways:

- Reactor trip leads to a rapid reduction of power to a residual level corresponding to fission product decay heat by the insertion of control rods to shut down the reactor.
- Injection of borated water provides core cooling and prevents excessive cladding temperatures.

9.6.5.1.1 Description of MBLOCA and SBLOCA Transients

The AP1000 plant design includes passive safety features to prevent or minimize core uncovery during small-break LOCAs. The passive safety design approach is to depressurise the reactor coolant system if the break or leak is greater than the capability of the makeup system or if the non-Class 1 makeup system fails to perform. By depressurising the reactor coolant system, large volumes of borated water in the accumulators and in the IRWST become available for cooling the core. The small-break analyses demonstrate that with a single failure of one of the ADS Stage 4 valves located off the non-pressuriser loop, the passive systems are capable of depressurising the reactor coolant system while maintaining acceptable core conditions and establishing stable delivery of cooling water from the IRWST.

During MBLOCAs and SBLOCAs, the reactor coolant system depressurises to the pressuriser low-pressure setpoint, actuating a reactor trip signal. The passive core cooling system is aligned for delivery following the generation of an "S" signal when the pressuriser low-pressure setpoint is reached. The passive core cooling system includes two core makeup tanks, two accumulators, a large IRWST, and the PRHR heat exchanger.

The core makeup tanks operate at reactor coolant system pressure. They provide high-pressure safety injection in the event of an MBLOCA or SBLOCA and are filled with borated water to provide core shutdown margin. The core makeup tanks share a common discharge line with the accumulators and IRWST. Gravity head of the colder water in the core makeup tanks provides the injection of the core makeup tanks. The core makeup tanks are located above the reactor coolant loops, and each is equipped with a pressure balancing line from a cold leg to the top of the tank.

The pressurised accumulators provide additional borated water to the reactor coolant system in the event of a LOCA. Nominally, these 57.2 m^3 (2020 ft^3) tanks are filled with 48.1 m^3 (1700 ft^3) of water and nitrogen cover gas at an initial gauge pressure of 4.83 MPa (700 psig). Once sufficient reactor coolant system depressurisation occurs, either as a result of a LOCA or the actuation of the ADS, accumulator injection begins.

The IRWST provides an additional source of water for core cooling. To attain injection from the IRWST, the reactor coolant system pressure must be lowered to approximately 0.0896 MPa (13 psi) above containment pressure. For this pressure to be achieved during a small-break LOCA, the actuation of the ADS valves is required.

The ADS consists of a series of valves, connected to the pressuriser and hot legs, which provide a phased depressurisation of the reactor coolant system. As the reactor coolant system loses inventory through the break, the core makeup tanks provide flow to the reactor vessel. When the inventory level in one core makeup tank drops to 67.5-percent volume, the ADS valves begin opening to accelerate the reactor coolant system depressurisation rate. The ADS Stage 1 valves open at the 67.5-percent volume setpoint; the Stage 2 and the Stage 3 valves open in a timed sequence thereafter. The flow from the first three stages of the ADS is discharged into the IRWST through a sparger system. The fourth stages of the ADS are connected to the reactor coolant system hot legs and discharge to containment atmosphere. The ADS Stage 4 valves are activated when one core makeup tank reaches 20-percent volume and a delay has elapsed after ADS Stage 3 actuation. A list of the ADS parameters is given in Table 9.6.5-10.

As the reactor system depressurises and mass is lost out of the break, mass is added to the reactor vessel from the core makeup tanks and the accumulators. When the system is depressurised below the IRWST delivery pressure, flow from the IRWST continues to maintain the core in a coolable state. Calculations described in this section indicate that acceptable core cooling is provided for the medium and small-break LOCA transients.

9.6.5.2 Medium and Small Break LOCA Analysis Methodology

Medium and Small-break LOCA responses are evaluated for the AP1000 plant with a deterministic evaluation model. The elements of the AP1000 plant small-break LOCA evaluation model are the following:

- NOTRUMP computer code
- NOTRUMP homogeneous sensitivity model
- Critical heat flux assessment during accumulator injection
- SBLOCTA computer code

Note that the cliff edge small-break LOCA diversity analyses are evaluated using the RELAP computer code. In the site specific phase, this analysis will be repeated using the NOTRUMP computer code. For this cliff edge small-break LOCA diversity analsyes, the use of the NOTRUMP computer code will use realistic inputs and assumptions and with acceptance criteria that are appropriate for such events (cliff edge faults with a common cause failure); refer to Section 8.2.3.

9.6.5.2.1 NOTRUMP Computer Code

The NOTRUMP computer code is used in the analysis of LOCAs due to medium and small-breaks in the reactor coolant system. The NOTRUMP computer code is a one-dimensional, general network code, which includes a number of advanced features. Among these features

are the calculation of thermal non-equilibrium in all fluid volumes, flow regime-dependent drift flux calculations with counter-current flooding limitations, mixture level tracking logic in multiple-stacked fluid nodes, and regime-dependent heat transfer correlations. The version of NOTRUMP used in AP1000 medium and small-break LOCA calculations has been validated against applicable passive plant test data (References 9.6.5-8 and 9.6.5-9). The code has limited capability in modelling upper plenum and hot leg entrainment and did not predict the core collapsed level during the accumulator injection phase adequately. The NOTRUMP homogeneous sensitivity model (discussed in Section 9.6.5.2.2) and the critical heat flux assessment during the accumulator injection phase (discussed in Section 9.6.5.2.3) supplement the base NOTRUMP analysis to demonstrate the adequacy of the design.

In NOTRUMP, the reactor coolant system is nodalised into volumes interconnected by flow paths. The transient behaviour of the system is determined from the governing conservation equations of mass, energy, and momentum applied throughout the system. A description of NOTRUMP is given in References 9.6.5-5 and 9.6.5-6. The AP600 modelling approach, described in Reference 9.6.5-7, is also used to develop the AP1000 model; NOTRUMP's applicability to the AP1000 design is documented in Reference 9.6.5-9.

The use of NOTRUMP in the analysis involves the representation of the reactor core as heated control volumes with an associated bubble rise model to permit a transient mixture height calculation. The multi-node capability of the program enables an explicit and detailed spatial representation of various system components. Table 9.6.5-9 lists important initial conditions of the analysis.

A steady-state input deck was set up to comply, where appropriate, with the standard small-break LOCA Evaluation Model methodology. Major features of the modelling of the AP1000 plant follow:

- Accumulators are modelled at an initial pressure of 4.9 MPa (715 psia).

- The flow through the ADS links is modelled using the Henry-Fauske and the homogeneous equilibrium (HEM) critical flow models. The Henry-Fauske subcooled correlation is used for subcooled flow, and the HEM correlation is used for superheated flow. For saturated donor conditions above the transition static quality of 10 percent, the HEM correlation is used. Below the transition quality, the flow is transitioned between the HEM correlation and the Henry-Fauske saturated correlation.

- Isolation and check valves used in the passive safety systems are modelled.

- The IRWST is modelled as two connected fluid nodes. The lower node is connected to the direct vessel injection line and is the source of injection water to the DVI lines driven by gravity head. The upper node acts as a sink for the ADS flow from the pressuriser and as a heat sink for the PRHR heat exchanger. These nodes are modelled as having an initial temperature of 48.9°C (120°F), a pressure reflective of containment conditions, and the minimum full-power operation level of 8.72 m (28.6 feet). Therefore, the minimum head for IRWST injection is assumed. For the double-ended, direct vessel injection (DEDVI) line break simulations, a conservatively low 0.138-MPa (20 psia) containment pressure was used based on containment pressurisation calculations performed with the WGOTHIC containment model. In addition, the inadvertent ADS actuation and the 50.8 mm (2-inch) cold leg break simulations each used a conservatively low, time-dependent containment pressure response also based on containment pressurisation calculations performed with the WGOTHIC minimum

containment pressure model as described in Section 13.8 of WCAP-15846 (Reference 9.6.5-3).

- The PRHR system is modelled in accordance with the guidance provided in References 9.6.5-8 and 9.6.5-9. The PRHR isolation valve is modelled as opening with the maximum delay after the generation of an "S" signal to conservatively deny the cooling capability of the heat exchanger to the reactor coolant system for an extended period.

- The core power is initially set to 101 percent of the nominal core power. The reactor trip signal occurs when the pressuriser pressure falls below 12.41 MPa (1800 psia). A conservative delay time is modelled between the reactor trip signal and reactor trip. Decay heat is modelled according to the ANS 5.1-1971 (Reference 9.6.5-1) standard, with 20-percent uncertainty added.

- The "S" signal is generated when the pressuriser pressure falls below 11.72 MPa (1700 psia). The isolation valves on the core makeup tank injection lines begin to open after the signal setpoint is reached; the valves are then assumed to open linearly. The main feedwater isolation valves are ramped closed between 2 and 7 seconds after the "S" signal. The reactor coolant pumps are tripped 7 seconds after the "S" signal.

- The ADS actuation signals are generated on low core makeup tank levels and the ADS timer delays. A list of the ADS parameters is given in Table 9.6.5-10. Note that the medium and small-break LOCA transients model the minimum valve flow area given in Table 9.6.5-10. ADS Stages 1, 2, and 3 are modelled as discharging through spargers submerged in the IRWST at the appropriate depth.

- The inadvertent ADS actuation and 50.8 mm (2-inch) cold leg break NOTRUMP simulations use a time-dependent containment pressure in the boundary node modelling containment. These containment conditions were generated by providing mass and energy releases from these breaks to the AP1000 plant WGOTHIC minimum containment pressure model (described in Section 13.8 of Reference 9.6.5-3). The WGOTHIC code calculates the containment pressure response. The inadvertent ADS actuation and 50.8 mm (2-inch) cold leg break NOTRUMP simulations then used the time-dependent pressure history curves as generated by WGOTHIC. The 254 mm (10-inch) cold leg break case models a constant containment pressure of 0.101 MPa (14.7 psia) and the DEDVI line break models a constant containment pressure of 0.138 MPa (20 psia).

- The steam generator secondary is isolated immediately after the reactor trip signal, due to closure of the turbine stop valves. The main steam safety valves actuate and remove energy from the steam generator secondary when pressure reaches approximately 8.34 MPa (1210 psia).

A single failure of the passive ESF systems is considered. The limiting failure is one out of four ADS Stage 4 valves failing to open on demand, which is the failure that most severely impacts depressurisation capability. The safety design approach of the AP1000 plant is to depressurise the reactor coolant system to the containment pressure in an orderly fashion such that the large reservoir of water stored in the IRWST is available for core cooling. The mass inventory plots provided for the breaks show the minimum inventory condition generally occurs at the start of IRWST injection. Penalizing the depressurisation is the most conservative approach in postulating the single failure for such breaks.

The analysed medium and small-break LOCA break spectrum includes breaks that exhibit a minimum reactor vessel inventory early in the transient, before the ADS Stage 4 depressurisation phase: the DEDVI line break at 0.138-MPa (20 psia) containment backpressure and 254 mm (10 inch) cold leg break transients. In these transients, the early mass inventory decrease is terminated by injection flow from the accumulators. For consistency, and because the transition to IRWST injection is still a tenuous period of the transients, the conservative failure of one of the ADS Stage 4 valves located off of the non-pressuriser loop is assumed in all cases.

9.6.5.2.1.1 AP1000 Model-Detailed Noding

The AP1000 plant NOTRUMP model was developed in the same fashion as the AP600 NORTUMP model (details of the AP600 NOTRUMP model are provided in Reference 9.6.5-7). Modifications to the AP600 model to create the AP1000 plant model include the following:

- The addition of two core nodes, one foot each in length, to reflect the added active fuel length of this design.
- The ADS-4 flow path resistances were increased to accommodate shortcomings in NOTRUMP identified during the integral test facility simulations, namely, the lack of a detailed momentum flux model in the ADS-4 discharge paths. A detailed calculation of the energy and momentum equations is performed for the ADS-4 piping over a range of flow and pressure conditions to provide a benchmark for the NOTRUMP ADS-4 flow path resistance. The methodology used to determine the resistance increase is described in Reference 9.6.5-9. By increasing the ADS-4 resistances, the onset of IRWST injection is more appropriately calculated. This methodology directly addresses the effect of momentum flux in ADS-4. The ADS-4 resistance increase utilized is computed for the NOTRUMP analyses in this section to be a 79-percent ADS-4 flow path resistance increase.

The AP1000 plant NOTRUMP model noding diagram is provided as Figure F-10 of Reference 9.6.5-9.

9.6.5.2.1.2 Plant Initial Conditions/Steady-State

Steady-state calculations are performed prior to initiating the transient portion of the calculations.

Table 9.6.5-9 contains the most important initial conditions for the transient calculations. The behaviours of the primary pressure and pressuriser level, steam generator pressures, and the core flow rate are stable at the end of the 100-second steady-state calculation.

9.6.5.2.2 NOTRUMP Homogeneous Sensitivity Model

In order to address the uncertainties associated with entrainment in the upper plenum and hot leg following ADS-4 operation, a sensitivity study is performed with the limiting break with respect to these phenomena, effectively maximizing the amount of entrainment downstream of the core. This methodology is described and the original results are presented for the DEDVI line break in detail in Reference 9.6.5-9.

In order to maximize the entrainment downstream of the core for the limiting break with respect to entrainment, NOTRUMP is run with the regions of the upper plenum, hot leg, and ADS-4 lines in a homogeneous fluid condition, with slip = 1, to demonstrate that even with maximum entrainment, the design basis requirements are met.

9.6.5.2.3 Critical Heat Flux Assessment During Accumulator Injection

An assessment is performed of the peak core heat flux with respect to the critical heat flux during the later ADS depressurisation time period for a double-ended rupture of the direct vessel injection line. This time period corresponds to the accumulator injection phase of the transient. The predicted average mass flux at the core inlet and the reactor pressure from the NOTRUMP computer code base model analysis are used as input parameters to critical heat flux correlation as described in Reference 9.6.5-10. The design basis requirements are met provided the maximum heat flux is less than the critical heat flux calculated by the correlation. NOTRUMP has been shown (Reference 9.6.5-9) to adequately predict mass flux and pressure for integral systems tests. The predicted mass flux at the core inlet is on the average constant and corresponds to 35 kg m^{-2} s^{-1} (7.2 lbm ft^{-2} s^{-1}). The key thermal-hydraulic parameters at different times during the ADS depressurisation time period are summarized in the following table.

Time (sec)	UP Pressure (kPa)	UP Pressure (psia)	Mass Flux (kg/m^2s)	Hot Channel Heat Flux (kW/m^2)
400	1196	173.4	35	48.6
450	903	131.0	35	47.2
500	581	84.3	35	46.0
570	314	45.5	35	44.5

For the critical heat flux assessment, the peak core heat flux is applied to simulate the hot channel condition in a conservative manner. No credit is taken for increased flow in the hot channel that is known to occur in rod bundles.

The correlation applied for this assessment is from vertical tube data (Reference 9.6.5-10) and recognizes two regimes depending on the mass flux. The main difference between the two is the mass flux dependence. The equations for the two regimes are as follows:

$$q^*_{CL} = q^*_{CF} + 0.01351\left(D^*\right)^{-0.473}\left(L/D\right)^{-0.533}\left|G^*\right|^{1.45} \quad \text{for low G*}$$

and,

$$q^*_{CH} = q^*_{CF} + 0.05664\left(D^*\right)^{-0.247}\left(L/D\right)^{-0.501}\left|G^*\right|^{0.77} \quad \text{for high G*}$$

The first term of above correlations is,

$$q^*_{CF} = 1.61\left(\frac{A}{Ah}\right)\frac{\left(D^*\right)^{0.5}}{\left[1+\left(\frac{\rho_g}{\rho_l}\right)^{0.25}\right]^2}$$

where A is the flow area and Ah is the heated area.

The dimensionless CHF is calculated as,

$$q^*_{CHF} = \min(q^*_{CL}, q^*_{CH})$$

Dimensionless CHF, G, and D are defined as,

$$q^*_{CHF} = \frac{q''_{CHF}}{h_{fg}\sqrt{\lambda \rho_g g \Delta\rho}}$$

$$G^* = \frac{G}{\sqrt{\lambda \rho_g g \Delta\rho}}$$

$$D^* = \frac{D}{\lambda}$$

where λ is the length scale of the Taylor instability:

$$\lambda = \sqrt{\frac{\sigma}{g\Delta\rho}}$$

Conservative application of this correlation with the AP1000 parameters indicates that the peak AP1000 heat flux during this period is approximately 30 percent or more below the predicted critical heat flux.

This CHF assessment addresses core cooling during a time period where the NOTRUMP computer code may not conservatively predict the core average void fraction. The design basis requirements are met during this period since this CHF assessment indicates peak core heat flux is less than critical heat flux. Cladding temperatures will remain near the coolant saturation temperature, well below the peak cladding temperature limit.

9.6.5.2.4 SBLOCTA Computer Code

The LOCTA-IV computer code (Reference 9.6.5-2) was modified as described in WCAP-10054-P-A (Reference 9.6.5-6) to form SBLOCTA, a small-break LOCA specific version of the LOCTA-IV code. The SBLOCTA code calculates the cladding temperature and oxidation transients for the hot rod and hot assembly average rod, which represent the highest power rod and the average of the highest power fuel assembly in the core. PCT calculations are performed with the SBLOCTA code using boundary conditions from the NOTRUMP calculation. In addition to PCT, SBLOCTA also calculates the maximum local and axial average zirconium-water oxidation reaction based on the Baker-Just oxidation model. In the event that the NOTRUMP code predicts core uncovery in the core average channel, the NOTRUMP boundary conditions will be transferred to the SBLOCTA code to perform fuel rod heatup calculations.

9.6.5.3 Medium and Small Break LOCA Analysis Results

Several medium and small break LOCA transients are analysed using NOTRUMP, and the results of these calculations are presented. The transients documented herein analyse a single failure of one ADS Stage 4 valve on the non-pressuriser side. The results demonstrate that the minimum reactor vessel mixture mass inventory condition occurs for the relatively small system pipe breaks. Larger breaks exhibit a greater margin-to-core uncovery.

9.6.5.3.1 Introduction

The small-break LOCA safety design approach for the AP1000 design is to provide for a controlled depressurisation of the primary system if the break cannot be terminated, or if the non-Class 1 CVS makeup system is postulated to be lost or cannot maintain acceptable plant conditions. Non-Class 1 systems are not modelled in this design basis analysis; the testing conducted in the SPES-2 facility has indicated that the mass inventory condition during small LOCAs is significantly improved when these non-Class 1 systems operate. The core makeup tank level activates primary system depressurisation through the actuation of the ADS. The core makeup tank provides makeup to help compensate for the postulated break in the reactor coolant system. As the core makeup tank level drops, Stages 1 through 4 of the ADS valves are ramped open in sequence. The ADS valve parameters used in the small-break analysis are presented in Table 9.6.5-10. Note that the small-break LOCA transients model the minimum valve flow area. The reactor coolant system depressurises due to the break and the ADS valves, while subcooled water from the core makeup tanks and accumulators enters the reactor vessel downcomer to maintain system inventory. Design basis maximum values of passive core cooling system resistances are applied to obtain a conservative prediction of system behaviour during the small LOCA events.

During controlled depressurisation via the ADS, the accumulators and core makeup tanks maintain system inventory for small-break LOCAs. Once the reactor coolant system depressurises, injection from the IRWST maintains core cooling. For continued injection from the IRWST, the reactor coolant system must remain depressurised. To conservatively model this condition, design maximum resistance values are specified for the IRWST delivery lines.

A series of small-break LOCA calculations are performed to assess the passive core cooling system design performance. In the DBA calculations, the decay heat used is the ANS 5.1-1971 standard (Reference 9.6.5-1) plus 20 percent for uncertainty. This maximizes the core steam generation to be vented. Note that for diverse mitigation analysis, margin is not added to the decay heat because of the low probability of the event combined with a CCF.

Additional detail about some of the breaks analysed in this section are provided as follows:

Inadvertent ADS Actuation

A “no-break” small-break LOCA calculation that uses an inadvertent opening of the 101.6 mm (4 inch) nominal size ADS Stage 1 valves is a situation that minimizes the venting capability of the reactor coolant system. Only the ADS valve vent area is available; no additional vent area exists due to a break. This case demonstrates that sufficient ADS vent area is available to completely depressurise the reactor coolant system and achieve adequate injection from the IRWST as well as long term core cooling by natural circulation containment cooling. The worst single failure for this situation is a failure of one of two ADS Stage 4 valves connected to the non-pressuriser side hot leg. The ADS Stage 4 valves are the largest ADS valves, and they vent directly to the containment with no additional backpressure from the spargers being submerged in the IRWST. The containment pressure is a

conservative, time-dependent containment pressure response. This pressure response is based on iterative execution of the NOTRUMP and WGOTHIC codes. The NOTRUMP code generates the mass and energy releases from the inadvertent ADS actuation simulation, which are then input into the WGOTHIC minimum containment pressure model, which calculates the containment pressure response.

50.8 mm (2 inch) Break in a Cold Leg

A 50.8 mm (2 inch) equivalent diameter break is analysed as a representative break, not specific to a particular pipe connection. The small size of the break leads to a long period of recirculatory flow from the cold leg into the core makeup tanks. This delays the formation of a vapour space in the core makeup tank and therefore the actuation of the ADS. The containment pressure is a conservative, time-dependent containment pressure response. This pressure response is based on iterative execution of the NOTRUMP and WGOTHIC codes. The NOTRUMP code generates the mass and energy releases from the 50.8mm (2-inch) cold leg break simulation, which are then input into the WGOTHIC minimum containment pressure model, which calculates the containment pressure response. Note that both DBA and diverse analyses are presented for this break size. In addition, the diverse analysis assumes nominal initial RCS conditions, PXS performance, and decay heat; these assumptions are appropriate for these events because of the probability of the event and a CCF is low.

Double-Ended Rupture of the Direct Vessel Injection Line

The DEDVI line break evaluates the ability of the plant to recover from a moderately sized break with only half of the total passive core cooling system capacity available. The vessel side of the break of the DEDVI line break is 101.6 mm (4 inches) in equivalent diameter. The double-ended nature of this break means that there are effectively two breaks modelled:

- Downcomer to containment. The direct vessel injection nozzle includes a venturi, which limits the available break area.

- Direct vessel injection line into containment from the cold leg balance line and the broken line core makeup tank.

The containment pressure is conservatively assumed to be 0.138 MPa (20 psia) based on iterative execution of the NOTRUMP and WGOTHIC codes. The NOTRUMP code generates the mass and energy releases from the DEDVI line break, which are input into the WGOTHIC minimum containment pressure model, which calculates the containment pressure response used to confirm the NOTRUMP containment pressure assumption remains conservative.

The peak core heat flux during the accumulator injection period is assessed relative to the predicted critical heat flux as discussed in Section 9.6.5.2.3.

Double-Ended Rupture of the Direct Vessel Injection Line Entrainment Sensitivity

The sensitivity case is performed to assess the effect of higher than expected entrainment in the upper plenum and hot legs on the overall system response and core cooling.

254 mm (10 inch) Break in a Cold Leg

The 254 mm (10 inch) equivalent diameter break models a break size at the upper limit for MBLOCAs.

9.6.5.3.2 Not Used

9.6.5.3.3 DBA Spurious Actuation of Automatic Depressurisation System or Opening of a Pressure Relief Valve Results

This section evaluates the consequences of a spurious ADS or spurious opening of a pressuriser safety valve fault. This evaluation focuses on the ability of the plant safety systems to cope with the associated depressurisation due to a loss of coolant event. The evaluation of short term effects of this fault, such as DNB criteria, is presented in Section 9.6.1.

9.6.5.3.3.1 DBA Credited SSCs

For the DBA LOCA for spurious ADS actuation scenarios, only the Class 1 systems listed in Table 9.6.5-3 are credited, and the same performance requirements discussed in Section 9.6.5.2.1 apply. In addition to the accumulators, the PMS provides the following:

- RT on:
  - Low-2 pressuriser pressure
  - Overtemperature ΔT
- PRHR on Low-2 steam generator narrow range level coincident with Low-2 startup feedwater flow
- CMTs and containment isolation on Low-2 cold leg temperature
- ADS 1-4 on Low CMT level
- IRWST injection on Low CMT level (via ADS stage 4 signal)
- Containment recirculation on Low IRWST level
- PCS on High-2 containment pressure

9.6.5.3.3.2 DBA Results

An ADS actuation signal is spuriously generated and the ADS Stage 1 valves open. The plant is depressurised via the ADS alone. Only safety-related systems are assumed to operate in this and other small-break LOCA cases. The ADS Stage 2 and 3 valves open in sequence after the ADS Stage 1 valves open (Table 9.6.5-11 (sheet 1)). At the 20-percent core makeup tank volume, the operating ADS Stage 4A valve, which is connected to the PRHR inlet pipe, receives a signal to open. After a 60-second delay, both Stage 4B valves (one connected to the non-pressuriser hot leg and the other connected to the PRHR inlet pipe) open. The path that fails to open as the assumed single active failure is the Stage 4A valve connected to the hot leg. The assumed reactor steady-state initial conditions can be found in Table 9.6.5-9. The sequence of events for the transient is given in Table 9.6.5-11.

This case uses a containment backpressure based on the containment pressure history that occurs as a result of the inadvertent ADS actuation. It represents a conservatively low estimate of the expected containment pressure response during the transient. The containment pressurises for an inadvertent ADS actuation as a result of the ADS Stage 4 discharge paths that vent directly to the containment atmosphere. The time-dependent containment pressure curve (Figure 9.6.5-1(c)) was calculated using the mass and energy releases from the NOTRUMP small-break LOCA code, which were used as inputs in the WGOTHIC containment model.

Transient results are shown in Figures 9.6.5-1(a) through 9.6.5-16(b).The transient is initiated by the opening of the two ADS Stage 1 paths. Reactor trip, reactor coolant pump trip, and safety injection signals are generated via pressuriser low-pressure signals with appropriate delays. After generation of the reactor trip signal, the turbine stop valves close. The main feedwater isolation valves begin to close 2 seconds after the "S" signal pressure setpoint is reached. The opening of the ADS valves and the reduction in core power due to reactor trip causes the primary pressure to fall rapidly (Figure 9.6.5-1(a)). Flow of fluid toward the open ADS paths causes the pressuriser to fill rapidly (Figure 9.6.5-2), and the ADS flow becomes two-phase (Figures 9.6.5-3 and 9.6.5-4(a)). The safety injection signal opens the valves isolating the core makeup tanks and circulation of cold water begins (Figures 9.6.5-5 and 9.6.5-6). The core makeup tanks begin to drain (Figures 9.6.5-7 and 9.6.5-8) during the accumulators injection period (Figures 9.6.5-10 and 9.6.5-11). The reactor coolant pumps begin to coast down due to an automatic trip signal following a 7-second delay from the "S" signal.

Continued mass flow through the ADS Stage 1, 2, and 3 valves drains the upper parts of the reactor coolant system (Figure 9.6.5-4(b)). The cold leg sides of the steam generator tubes start to drain, followed by the drop in mixture levels in the hot leg sides. As the ADS Stage 2 and 3 paths begin to open, increased ADS flow causes the primary pressure to continue falling rapidly (Figures 9.6.5-1(a)). As the cold leg sides of the steam generator tubes empty, the cold legs drain and a mixture level forms in the downcomer (Figure 9.6.5-9).

The primary pressure falls below the pressure in the accumulators thus causing the accumulator check valves to open and accumulator delivery to begin (Figures 9.6.5-10 and 9.6.5-11). The accumulators, and then the core makeup tanks inject until they empty. The ADS flow falls off (Figures 9.6.5-3, 9.6.5-4(a), and 9.6.5-4(b)) as the primary pressure decreases. The flow from the accumulators raise the mixture levels in the upper plenum and downcomer (Figures 9.6.5-16(a) and 9.6.5-9).

As the levels in the core makeup tanks reach the ADS Stage 4 actuation setpoint, the ADS Stage 4 valves open as described earlier. Activating the Stage 4 paths (Figures 9.6.5-12(a), 9.6.5-12(b), and 9.6.5-12(c)) leads to reduced flow through ADS Stages 1, 2, and 3 (Figures 9.6.5-3, 9.6.5-4(a), and 9.6.5-4(b)). The reduced flow allows the pressuriser mixture level to fall (Figure 9.6.5-2), and these stages begin to discharge only steam. After the CMTs are empty (Figures 9.6.5-7 and 9.6.5-8), IRWST injection (Figures 9.6.5-13 and 9.6.5-14) does not begin until the pressure in the DVI line drops below the IRWST injection pressure, creating an injection gap (Table 9.6.5-11 and Figures 9.6.5-5, 9.6.5-6, 9.6.5-13, and 9.6.5-14). The overall decrease in reactor vessel mixture inventory (Figure 9.6.5-15(b)) is large enough to result in a core uncovery (Figure 9.6.5-16(a)). At 4000 seconds, the calculation is considered complete; IRWST delivery exceeds the ADS flows (which are removing the decay heat), and the reactor coolant system inventory and reactor vessel mixture inventory are slowly rising (Figure 9.6.5-15(a) and 9.6.5-15(b))

The inadvertent opening of the ADS Stage 1 transient confirms the capability of the minimum venting area to depressurise the reactor coolant system to the IRWST pressure. The analysis indicates that the ADS sizing is sufficient to depressurise the reactor coolant system assuming the worst single failure as the failure of a Stage 4 ADS path to open and the decay heat based on the ANS 5.1-1971 Standard (Reference 9.6.5-1) plus 20 percent, which leads to over estimation of the core steam generation rate. Even under these limiting conditions, IRWST injection is obtained, and the core mixture level recovers, which terminates the cladding heatup transient (Figure 9.6.5-16(b)).

9.6.5.3.3.3 Radiological Consequences

For the purposes of comparison of radiological dose with SAPs Target 4, the spurious activation of the ADS and opening of the pressuriser relief valve are included in the assessment for the MBLOCA scenario presented in Section 9.6.5.3.6.3. This is a conservative assumption, as the analysis described above shows that there is no core heatup during these events.

9.6.5.3.3.4 As Low As Reasonably Practicable Assessment

First of all extensive efforts have been applied to the AP1000 to prevent spurious ADS stage 1, 2, 3 actuation and as a result its probability of occurrence is so low that it is a DBD event. These features and the event classification are summarized in Table 8A-2.

The spurious activation of the ADS and opening of the pressuriser relief valve are included in the ALARP assessment for the MBLOCA scenario, as discussed in Section 9.6.5.3.6.5.

9.6.5.3.3.5 Spurious ADS or Pressuriser Relief Valve Conclusions

The conclusion from the MBLOCA fault applies (Section 9.6.5.3.6.5).

9.6.5.3.4 SBLOCA – 50.8 mm (2-inch) Cold Leg Break Results

This size small LOCA represents the maximum small LOCA that is considered a cliff edge frequent fault. As a result, diverse mitigation needs to be demonstrated.

Two different types of diverse mitigation analysis are provided in the following sections. One demonstrates the reactor can be shut down when considering a CCF that prevents control rod insertion. Such an event is defined as an ATWT. The other demonstrates that adequate core cooling can be provided when analysis considers a CCF the affects the core cooling credited in the DBA. In the diverse core cooling case rod insertion via RT is assumed to occur.

This section contains analysis results for:

- DBA case, where all installed Class 1 SSCs are credited (Section 9.6.5.3.4.1)
- Diverse core cooling cases, where several different sets of SSCs are credited (Section 9.6.5.3.4.2)
- Diverse reactor shutdown cases (ATWT), where a diverse set of SSCs is credited (Section 9.6.5.3.4.3)

9.6.5.3.4.1 DBA Small LOCA Results

9.6.5.3.4.1.1 DBA Credited SSCs

For the DBA of the SBLOCA, only the Class 1 systems listed in Table 9.6.5-3 are credited, and the performance parameters described in Section 9.6.5.2.1 apply. In addition to the accumulators, the PMS provides the following:

- RT, PRHR, CMTs and containment isolation on Low-2 pressuriser pressure
- ADS 1-4 on Low CMT level
- IRWST injection on Low CMT level (via ADS stage 4 signal)
- Containment recirculation on Low IRWST level
- PCS on High-2 containment pressure

9.6.5.3.4.1.2 DBA Analysis Results

This case models a 50.8 mm (2 inch) break occurring in a cold leg on the pressuriser side of the RCS. The reactor steady-state initial conditions assumed for this transient can be found in Table 9.6.5-9. The event times for this transient are given in Table 9.6.5-11 (sheet 2).

This case uses a containment backpressure based on the containment pressure history that occurs as a result of the 50.8 mm (2 inch) cold leg break. It represents a conservatively low estimate of the expected containment pressure response during the transient. The containment pressurises for a 50.8 mm (2 inch) cold leg break as a result of the break and the ADS Stage 4 discharge paths that vent directly to the containment atmosphere. The time-dependent containment pressure curve (Figure 9.6.5-17(c)) was calculated using the mass and energy releases from the NOTRUMP small-break LOCA code, which were used as inputs in the WGOTHIC containment model.

The transient results are shown in Figures 9.6.5-17(a) through 9.6.5-35. The break opens at time zero, and the pressuriser pressure begins to fall as shown in Figure 9.6.5-17(a) as mass is lost out the break. The pressuriser mixture level initially decreases as given in Figure 9.6.5-18. The liquid and vapour flow out of the break is shown in Figures 9.6.5-32 and 9.6.5-33. The pressuriser pressure falls below the reactor trip set point, causing the reactor to trip (after the appropriate time delay) and causing isolation of the steam generator main steam lines. The core makeup tank discharge isolation valves for both core makeup tanks and the PRHR delivery line isolation valve open after an “S” signal occurs (with appropriate delays); the reactor coolant pumps trip after an “S” signal with a 7-second delay. The reactor coolant system is cooled by natural circulation with decay heat being removed by the steam generators through their safety valves, through the break, and via the PRHR. The PRHR heat removal and integrated heat removal are shown in Figure 9.6.5-34 and Figure 9.6.5-35. Once the core makeup tank isolation valves open, the core makeup tanks begin to inject borated water into the reactor coolant system as shown in Figures 9.6.5-22 and 9.6.5-23.

As time proceeds, the loops drain to the reactor vessel. The mixture level in the downcomer begins to drop as seen in Figure 9.6.5-21. The core makeup tank reaches the 67.5-percent volume, and after an appropriate delay, the ADS Stage 1 valves open. When the ADS is actuated, the mixture level increases in the pressuriser (Figure 9.6.5-18) because an opening has been created at the top of the pressuriser. After these valves open, a rapid depressurisation occurs as seen in Figure 9.6.5-17(a); the accumulator gas cover pressure is reached and the

accumulators begin to inject. The injection flow from the core makeup tanks are shown in Figures 9.6.5-22 and 9.6.5-23, and from the accumulators, in Figures 9.6.5-24 and 9.6.5-25.

As Figures 9.6.5-22 and 9.6.5-23 indicate, when the accumulators begin to inject, the flow from both core makeup tanks is reduced, and the flow is temporarily reversed due to the pressurisation of the DVI line and core makeup tanks injection lines by the accumulators.

The ADS Stage 2 valves open, continuing the RCS depressurisation as shown in Figure 9.6.5-17(a). ADS Stage 3 valves open, thereby increasing the system venting capability. Figures 9.6.5-31(a), 9.6.5-31(b), and 9.6.5-31(c) indicate the instantaneous liquid, instantaneous vapour, and integrated total mass discharged from the ADS Stage 1-3 valves. The ADS Stage 4 valves open when the core makeup tank water volume is reduced to 20 percent. Figures 9.6.5-28(a), 9.6.5-28(b), and 9.6.5-28(c) indicate the instantaneous liquid, instantaneous vapour, and integrated total mass discharged from the ADS Stage 4 valves. After the ADS Stage 4 paths open, the pressuriser begins to drain mixture into the hot legs as seen in Figure 9.6.5-18. After the CMTs are empty, IRWST injection does not begin until the pressure in the DVI line drops below the IRWST injection pressure, creating an injection gap (Table 9.6.5-11 and Figures 9.6.5-22, 9.6.5-23, 9.6.5-26, and 9.6.5-27). The mass inventory shown in Figure 9.6.5-29(a) considers the primary inventory to be the reactor coolant system proper, including the pressuriser; the mass present in the passive safety system components is not included. The mass inventory shown in Figure 9.6.5-29(b) considers the reactor vessel mixture inventory, including the downcomer, lower plenum, core fluid channel, upper plenum, and upper head, and clearly shows the decrease in the inventory during the injection gap period. Once the pressures in the DVI lines drop below the IRWST injection pressure, flow enters the reactor vessel from the IRWST. The mixture level in the reactor vessel is approximately at the hot leg elevation as shown in Figure 9.6.5-30(a) for the majority of the transient; however, the upper plenum mixture level drops during the injection gap period and the core uncovers as the mixture level drops below the top of the active fuel. The 50.8 mm (2-inch) break case exhibits a cladding heatup transient as a result of the core uncovery as shown in Figure 9.6.5-30(b).

Section 9.6.6 describes the analysis that has been performed to demonstrate long-term safe shutdown is achieved following LOCAs.

9.6.5.3.4.1.3 Radiological Consequences

The consequences of an SBLOCA are conservatively estimated based on the consequences of an MBLOCA. With limited fuel damage (less than 1 percent predicted for SBLOCA) and a concurrent release to containment, the releases are less than 10 percent of those considered in the MBLOCA doses presented in Section 9.6.5.3.6.3 which considered up to 10 percent fuel damage. Therefore, doses that are ten percent of the MBLOCA doses listed in Section 9.6.5.3.6.3 are presented herein. The calculated maximum doses for all relevant pathways (inhalation, cloudshine, and groundshine) are as follows:

Offsite dose: 0.26 mSv Worker dose: 0.60 mSv

These doses are within the Target 4 BSL for these frequent faults (1 mSv offsite and 20 mSv onsite).

9.6.5.3.4.2 Diverse Core Cooling SBLOCA Mitigation

This section describes the diverse mitigation of this cliff edge frequent fault small LOCA (Reference 9.6.5-13). This diverse analysis focuses on the cliff-edge SBLOCA size of up to a

50.8 mm (2-inch) equivalent break diameter. Above this size is considered DB1 and does not require diverse mitigation.

The primary design basis analysis presented in Section 9.6.5.3.4.1 for the SBLOCA assumes the full suite of Class 1 equipment is available for mitigation including a worst-case single failure. In order to show diverse core cooling mitigation, three additional cases are presented. Three diversity cases are analysed using different combinations of Class 1 SSCs, and in some cases Class 2 SSCs. The SSCs credited in these cases are listed in Table 9.6.5-4.

For diverse core cooling the following 3 diverse cases are provided. Diversity Case 1 utilises a subset of the Class 1 SSCs noted for the primary DB case, including the PMS, PRHR, CMTs, ADS 4 and IRWST. Diversity Case 2 utilises a different set of Class 1 SSCs, including the PMS, CMTs, ADS 1, 2, 3, and 4 and IRWST. Diversity Case 3 utilises both Class 1 and Class 2 SSCs, including DAS, PRHR, Accumulator, ADS 1, 2, and 3, RNS. For Diversity Cases 1 and 2, core cooling is provided by Class 1 SSCs including actuation from the Class 1 PMS. For Diversity Case 3, core cooling is also provided by Class 1 SSCs except pumped injection by the Class 2 RNS, and actuation by the Class 2 DAS.

Table 9.6.5-4 lists the SSCs credited in these different cases. As this is a frequent fault, diverse means of providing the Category A safety functions is provided.

The next three sections discuss core cooling analysis of an SBLOCA using diverse mitigation.

For Diversity Cases 1 and 2, Section 9.6.6 describes the analysis that has been performed to demonstrate long-term safe shutdown is achieved following LOCAs. For Diversity Case 3, long-term safe shutdown is achieved by switching suction sources (RNS and IRWST).

9.6.5.3.4.2.1 Diverse Core Cooling Mitigation SBLOCA Event, Case 1

The Diversity Case 1 credited SSCs include the PMS, PRHR, CMTs, ADS 4, IRWST injection, and containment recirculation. Table 9.6.5-11 (sheet 3) shows the sequence of events. Figures 9.6.5-95 through 98 show the plant behaviour. The PMS provides the following:

- RT on Low-2 pressuriser pressure
- PRHR, CMTs, and containment isolation on Low-2 pressuriser pressure
- ADS stage 4 on Low CMT level
- IRWST injection on Low CMT level (via ADS stage 4 signal)
- Containment recirculation on Low IRWST level
- PCS on High-2 containment pressure

The PRHR HX and the break cause the RCS pressure to decrease, such that even without credit for ADS stages 1, 2, and 3, the RCS pressure has dropped to 2.15 MPa (313 psig) when ADS stage 4 is actuated at about 3400 sec. Note that the ADS stage 4 valves and piping are designed to actuate with an RCS pressure of 1.4 MPa (200 psig) and have been shown to remain operable up to pressures of 4.14 MPa (600 psig) for use in PSA sequences. This analysis shows that the RCS pressure at the time of ADS stage 4 actuation is 2.15 MPa (313

psia) which is somewhat above the design actuation pressure but is significantly below the pressure assumed in the PSA.

This analysis shows that adequate core cooling is provided with no core uncovery.

9.6.5.3.4.2.2 Diverse Core Cooling Mitigation SBLOCA Event, Case 2

The Diversity Case 2 credited SSCs include the PMS, CMTs, ADS 1-4, IRWST injection, and containment recirculation. Table 9.6.5-11 (sheet 4) shows the sequence of events. Figures 9.6.5-99 through 101 show the plant behaviour. The PMS provides the following:

- RT on Low-2 pressuriser pressure
- CMTs and containment isolation on Low-2 pressuriser pressure
- ADS 1-4 on Low CMT level
- IRWST injection on Low CMT level (via ADS stage 4 signal)
- Containment recirculation on Low IRWST level
- PCS on High-2 containment pressure

This case shows that the initial SG secondary side inventory is sufficient to limit the RCS pressure and allow for adequate ADS performance even though without the PRHR the RCS pressure is somewhat higher.

This analysis shows that adequate core cooling is provided with no core uncovery. In addition, it shows that the ADS stage 1 actuation at an elevated pressure due to PRHR being out of service still leads to successful event mitigation.

9.6.5.3.4.2.3 Diverse Core Cooling Mitigation SBLOCA Event, Case 3

The Diversity Case 3 credited SSCs include the DAS, PRHR, accumulators, ADS 1-3, RNS pumped injection, and containment recirculation. Table 9.6.5-11 (sheet 5) shows the sequence of events. Figures 9.6.5-102 through 105 show the plant behaviour. Manual RNS injection is credited via the plant control system (PLS). DAS provides:

- RT and PRHR on Low-2 pressuriser level
- Manual ADS 1-3 and containment recirculation
- PCS and containment isolation on High containment temperature

In this case, the PRHR and the accumulators keep the core cooled and covered until the operator take action to align and start the RNS pumps and actuate ADS stages 1, 2, and 3. The PRHR assists by condensing steam and draining the condensate into the RV through the CLs. The break location is placed on the bottom of one of the CLs on the PRHR side to minimize this benefit. If the break were on the other loop or on the top of the CL it would extend the time available for operator action.

This analysis shows that adequate core cooling is provided with no core uncovery. In addition, it shows that the operators have ample time to perform the required manual actions, more than 1 hour.

Note that Reference 9.6.5-13 contains a sensitivity case from Case 3 which credits the same SSCs except for ADS stages 1, 2, and 3. This case shows that a limited amount of nitrogen gas is injected from the accumulators because the RCS pressure only drops slightly below the accumulator empty pressure. This nitrogen is expected to result in a small degradation of the PRHR HX performance however the PRHR HX is predicted to maintain this RCS pressure and allow for adequate RNS pumped injection. This case credits operator action at one hour. An additional sensitivity case was also performed assuming operator action at two hours. For this case, the core would still be adequately cooled however there would be a core uncovery resulting in a heat-up significantly below the peak cladding temperature limit.

9.6.5.3.4.3 Diverse ATWT for SBLOCA

Two additional cases are provided to demonstrate diverse ATWT mitigation for SBLOCAs in Table 9.6.5-4.

For diversity Case 4, an SBLOCA with a PMS CCF, the credited SSCs include both Class 1 and Class 2 SSCs; DAS, RCCAs, PRHR, CMTs, ADS 1-4, IRWST injection, and containment recirculation are all utilised. The DAS provides:

- RT on High hot leg temperature
- PRHR and CMTs on Low-2 pressuriser level
- Manual ADS 1-4, IRWST injection, and containment recirculation
- PCS and containment isolation on High containment temperature

For Case 4, the RCS will lose coolant which will cause the pressuriser level to decrease. Assuming that the PMS does not respond, DAS will sense the low pressuriser level and generate signals to automatically trip the reactor, turbine, RCPs, and start the PRHR and CMTs. Actuation of those features will shut down the reactor core and provide short-term core cooling. Later on, due to the LOCA causing continued loss of coolant, the operators would manually actuate ADS, IRWST injection, and containment recirculation through DAS to maintain core cooling.

For diversity Case 5, an SBLOCA with a mechanical CCF of the control rods, the Class 1 credited SSCs include PMS, PRHR, CMTs, ADS 1-4, IRWST injection, and containment recirculation. The PMS provides:

- No reactor trip due to mechanical failure
- PRHR, CMTs, and containment isolation on Low-2 pressuriser pressure
- ADS 1-4 on Low CMT level
- IRWST injection on Low CMT level (via ADS stage 4 signal)
- Containment recirculation on Low IRWST level
- PCS isolation on High-2 containment pressure

For Case 5, the rods fail to insert due to a CCF mechanical failure. The PMS trip of the RCPs together with the loss of coolant causes voiding in the core which results in a rapid power

reduction. With PMS also actuating the CMTs the core would be completely shut down by the boron addition. Such an ATWT case is less limiting than others because main feedwater is not lost as the initiating event and the LOCA drains the pressuriser which increases its steam space; both of these factors reduce the peak RCS pressure. In this case, PMS also automatically starts the PRHR, which would provide short-term decay heat removal. Later on, due to the LOCA causing continued loss of coolant, the PMS would automatically actuate ADS, IRWST injection and containment recirculation to maintain core cooling.

9.6.5.3.4.4 Diverse Radiological Consequences

The diverse core cooling scenarios demonstrate that there is no significant fuel damage. For a diverse mitigation radiological consequences analysis better estimate assumptions would be credited. This would include reactor coolant system activity levels significantly lower than those modelled for the DBA and better activity retention in containment. In addition better estimate atmospheric dispersion factors would be used. Therefore, a diverse mitigation radiological consequences analysis would show that the doses for the diverse core cooling scenario would be much less than for the design basis LOCA. The diverse mitigation analyses would not have to meet the Target 4 BSL for frequent faults and would meet the Target 4 BSL for infrequent faults. Further, while consideration of a containment isolation failure (if required) would result in higher doses, the results would be much less than those presented in Section 9.8.5.2.3.3 for a design basis RNS break outside containment, which are within the Target 4 BSL for infrequent faults with IEF < 1E-04 (100 mSv offsite and 500 mSv onsite).

9.6.5.3.4.5 As Low As Reasonably Practicable Assessment

For this event, the identification of the primary safety functions as Class 1 SSCs has been shown to be adequate to meet DB requirements.

In addition, since smaller SBLOCAs are frequent faults, diverse core cooling has been demonstrated in three cases using different sets of SSCs. For the small-break loss of coolant accident, the two diversity cases that credit the Class 1 SSCs were shown to be adequate to meet DB requirements.

The third diversity case which includes other Class 1 safety functions as well as RNS and the DAS functions, which are Class 2, are also shown by analysis to meet the corresponding requirements for this event. See Reference 9.6.5-12 for additional discussions on these diverse mitigation features.

It was determined that an increase in the RNS pump head would not significantly increase the plant safety for this event.

A detailed ALARP assessment is documented in Reference 9.6.5-13. The following information developed in this assessment supports the justification of the use of the RNS for RCS injection as the diverse mitigation of frequent SBLOCA faults:

- The upper range ‘cliff edge’ small break LOCA was analysed only crediting the equipment identified for the diverse mitigation, including the PRHR HX, accumulators, ADS Stage 1, 2, and 3, and the RNS pumps. The accident was successfully mitigated even with delayed operator actions times (up to 2 hours) to align the RNS for injection and manually actuate ADS. This analysis shows large margin to the operator action time expected when the emergency operating procedures are followed.

- The benefit of increasing the RNS pump injection pressure for the diverse mitigation case is insignificant because the PRHR and ADS Stage 1, 2 and 3 are able to reduce the RCS pressure to the RNS pump cut-in pressure. Note that the increased RNS pump pressure does not change / eliminate the need for the operator to take manual action (to align and start the RNS pumps). Changing the RNS pump injection and the related system impacts would result in potential reductions in RNS pump reliability without a significant increase in safety benefits.
- The benefit of adding a new water storage tank to replace the cask loading pit (CLP) option has essentially no safety benefit. Adding a new tank results in significant cost impacts without a meaningful increase in safety benefits.
- The benefit of automatically aligning and starting injection from the RNS has essentially no safety benefit and may even reduce safety because of the potential of failures for such a complex interlock. The number of different RNS operating alignments as well as the use of two different suction supplies (IRWST or CLP) results in the complexity of automatic control. Given the long-time available for operator action, the reliability of the operator actions will only contribute a small amount to the RNS unreliability. The cost of adding and maintaining the automatic controls would not be so large; however, the safety benefit is negligible.
- The benefit of automatically actuating PRHR on a low pressuriser level DAS signal does have some safety benefit to prevent PCT excursions and to provide some additional time for operator actions. The impact to the plant would be minor, since DAS already has pressuriser level sensors as well as PRHR valve controls. However, as the effort to implement is not considered to be overly arduous; this DAS function is incorporated into the AP1000 design.

Providing further means of removing decay heat or tripping the reactor in addition to these functions would not be significantly reduce the PSA risk for this event.

9.6.5.3.4.6 SBLOCA Conclusions

The DB analysis shows that for the SBLOCA fault, the acceptance criteria defined in Section 9.6.5.0 are met. Two diversity cases were analysed to show that different combinations of Class 1 SSCs result in successful mitigation, and a third case showed that a combination of Class 1 and Class 2 SSCs also meet the LOCA acceptance criteria.

DBA radiological consequences are within the Target 4 BSL for frequent faults (1 mSv offsite and 20 mSv onsite). Thus, the identification of necessary Class 1 SSCs is adequate to meet DB requirements for this fault.

It has been shown that the AP1000 plant includes adequate systems for the protection of the fault, which limit the radiological consequences such that they are compliant with the SAPs targets and the risks have been reduced to be ALARP.

9.6.5.3.5 Direct Vessel Injection Line Break Results

9.6.5.3.5.1 DBA Credited SSCs

For the DBA of the DVI scenarios, only the Class 1 systems listed under the MBLOCA event are available (See Section 9.6.5.3.6.1) with the exception of only one accumulator, one CMT,

and one IRWST direct injection line being available since the others spill as a result of the initiating fault. The same performance requirements discussed in Section 9.6.5.2.1 apply.

9.6.5.3.5.2 Results of Design Basis Analysis

This case models the double-ended rupture of the DVI line at the nozzle into the downcomer. The broken loop injection system (consisting of an accumulator, a core makeup tank, and an IRWST delivery line) is modelled to spill completely out of the DVI line side of the break into containment. The steady-state reactor coolant system conditions for this transient are shown in Table 9.6.5-11 (sheet 6). Minimum resistances are applied to the broken loop IRWST injection line to maximize the spill to containment, thus minimizing the reactor coolant system mass inventory. The containment pressurisation is calculated using the mass and energy releases from the NOTRUMP small-break LOCA code in the WGOTHIC minimum containment pressure model and demonstrates that the 0.138 MPa abs (20 psia) containment backpressure assumption is conservative.

This case uses a containment backpressure defined to be a constant 0.138 MPa abs (20 psia). While not exactly reflecting the containment pressure history that occurs as a result of the DVI line break, it represents a conservatively low estimate of the expected containment pressure response during a DEDVI transient. The containment pressurises for a DEDVI line break as a result of the break mass and energy releases in addition to the ADS-4 discharge paths that vent directly to the containment atmosphere.

The event times for this transient are shown in Table 9.6.5-11 (sheet 6). Transient results are shown in Figures 9.6.5-36 through 9.6.5-55. The break is assumed to open instantaneously at 0 seconds. The accumulator on the broken loop starts to discharge via the DVI line to the containment. Figure 9.6.5-36 shows the subcooled discharge from the downcomer nozzle, which causes a rapid RCS depressurisation (Figure 9.6.5-38(a)). A reactor trip signal is generated, followed by generation of the “S” signal. Following a delay, the isolation valves on the core makeup tank and PRHR delivery lines begin to open. The PRHR heat removal and integrated heat removal are shown in Figure 9.6.5-54 and Figure 9.6.5-55. The “S” signal also causes closure of the main feedwater isolation valves after a 2-second delay and trips the reactor coolant pumps after a 7-second delay. The opening of the core makeup tank isolation valves allows the broken loop core makeup tank to discharge directly to the containment (Figure 9.6.5-39), and a small circulatory flow develops through the intact loop core makeup tank (Figure 9.6.5-40).

As the pressure falls, the reactor coolant system fluid saturates, and a mixture level forms in the upper plenum and then falls to the hot leg elevation (Figure 9.6.5-41). The upper parts of the reactor coolant system start to drain, and a mixture level forms in the downcomer (Figure 9.6.5-42) and falls below the elevation of the break. Two-phase discharge, then vapour flow occurs from the downcomer side of the break (Figure 9.6.5-37).

In the core makeup tank connected to the broken loop, a level forms and starts to fall. The ADS Stage 1 setpoint is reached, and the ADS Stage 1 valves open after the signal delay time elapses. The ensuing steam discharge from the top of the pressuriser (through the ADS valves; Figures 9.6.5-43(a), 9.6.5-43(b), and 9.6.5-43(c)) increases the reactor coolant system depressurisation rate. The depressurisation rate is also increased due to the steam discharge from the downcomer to the containment (Figure 9.6.5-37) as the downcomer mixture level falls below the DVI nozzle (Figure 9.6.5-42).

During the initial portion of the DEDVI line break, only liquid flows out the top of the core (Figure 9.6.5-45). Soon, steam flow follows (Figure 9.6.5-46) correlating with the void fraction increase in the core (Figure 9.6.5-44). The break in the downcomer stalls fluid flow

into the bottom of the core (Figure 9.6.5-47) leaving insufficient liquid in the upper plenum. The mixture level, therefore, starts to decrease (Figure 9.6.5-41). The mixture level falls early in the transient and then recovers slightly as flow slowly re-enters the core from the downcomer (Figure 9.6.5-41 compared to Figure 9.6.5-47).

The ADS Stage 2 valves open after the appropriate time delay following the actuation of ADS Stage 1. The intact loop accumulator starts to inject into the downcomer (Figure 9.6.5-50) causing the mixture level in the downcomer to slowly rise (Figure 9.6.5-42). The mixture level also increases slightly within the upper plenum.

The ADS Stage 3 valves open upon completion of the time delay of 120 seconds following the actuation of ADS Stage 2. The broken loop core makeup tank level reaches the ADS Stage 4 setpoint, but the ADS Stage 4 valves do not open until the minimum time delay between the actuation of ADS Stages 3 and 4 occurs. Two-phase discharge ensues through three of the four Stage 4 paths (Figures 9.6.5-48(a), 9.6.5-48(b), and 9.6.5-49). During the same time frame, the broken loop core makeup tank and accumulator empty rapidly.

The fluid level at the top of the intact loop core makeup tank starts to decrease slowly (Figure 9.6.5-52) because injection from the tank has begun (Figure 9.6.5-40). The intact loop core makeup tank injection is temporarily reduced and then reversed as the intact loop accumulator injects (Figure 9.6.5-50). Following accumulator injection, the core makeup tank injects continuously until empty.

During the period of accumulator injection, the downcomer mixture level rises slowly (Figure 9.6.5-42). Figure 9.6.5-53(a) presents the RCS mass inventory, and Figure 9.6.5-53(b) presents the reactor vessel mixture inventory, which includes the downcomer, lower plenum, core fluid channel, upper plenum, and upper head. Both figures also show the increase in inventory due to the accumulator injection. With injection available only from the intact loop core makeup tank, the downcomer level remains fairly constant; however, reactor vessel mixture coolant system inventory depletion continues until sufficient IRWST injection flow can be introduced. The level in the upper plenum is maintained near the hot leg elevation (Figure 9.6.5-41) throughout the remainder of the transient.

Once the pressure in the broken DVI line falls below that in the IRWST discharge piping, the water from the tank begins spilling to containment.

Stable, but decreasing, injection continues from the intact loop core makeup tank as the inventory slowly depletes; the reactor coolant system pressure declines slowly. The reactor coolant system pressure continues to fall until it drops below that of the IRWST and injection begins (Figure 9.6.5-51). With the reduced initial RCS inventory recovery from a single accumulator, CMT, and IRWST injection path available for the DEDVI line break, the minimum RCS inventory occurs after the initiation of continuous IRWST injection flow. After injection flow greater than the sum of the break and ADS flows exists, a slow rise in the reactor vessel mixture inventory (Figure 9.6.5-53(b)) occurs. Since no core uncovery is predicted for this scenario, no cladding heatup occurs.

The critical heat flux (CHF) assessment described in Section 9.6.5.2.3 addresses core cooling during a time period where the NOTRUMP computer code may not conservatively predict the core average void fraction. The design basis requirements are met during this period since this CHF assessment indicates peak core heat flux is less than critical heat flux. Cladding temperatures will remain near the coolant saturation temperature, well below the peak cladding temperature limit.

Section 9.6.6 describes the analysis that has been performed to demonstrate long-term safe shutdown is achieved following LOCAs.

9.6.5.3.5.2.1 Direct Vessel Injection Line Break (Entrainment Sensitivity) Results

In order to assess the potential impact of higher than expected entrainment in the upper plenum and hot legs on the overall system response and core cooling, an AP1000 plant sensitivity run was performed. The simulation utilizes the same initial conditions as the base DEDVI line break case presented in Section 9.6.5.3.5. The transient response is essentially identical until ADS-4 actuation, at which time the bounding entrainment conditions are included in the analysis by assuming homogenous conditions in the regions downstream of the core (upper plenum, hot leg, and PRHR inlet). In addition, since homogenous treatment of these regions will eliminate the pressure drop effect of the accumulated mass stored in the upper plenum, the NOTRUMP model was conservatively adjusted to account for this effect following the transition of the ADS-4 flow paths to noncritical conditions.

The event times for this transient are shown in Table 9.6.5-11 (Sheet 8). Transient results are shown in Figures 9.6.5-79(a) through 9.6.5-90. Figures 9.6.5-79(a) and 9.6.5-79(b) present comparisons of the pressure in the upper portion of the downcomer between the base and sensitivity cases. The sensitivity case results in higher pressure in the upper portion of the downcomer and subsequently results in delayed IRWST injection (Figure 9.6.5-80). This can also be observed in the intact DVI line flow, which comprises all intact injection flow components (accumulator, CMT, and IRWST) per Figure 9.6.5-81, and the pressuriser mixture level response (Figure 9.6.5-90), which follows the change in pressure response. As expected, the initial ADS-4 liquid discharge is much higher (Figure 9.6.5-82) until the upper plenum and hot leg region inventory is depleted (Figure 9.6.5-83). The net effect is a decrease in the ADS-4 vapour discharge rate (Figure 9.6.5-84) and subsequently higher RCS pressure.

Due to the elimination of the inventory stored in the upper plenum, the downcomer mass is also reduced (Figure 9.6.5-85). Since the static head that existed in the upper plenum is eliminated when the model is made homogenous, the downcomer mixture is subsequently driven into the core as the static heads equilibrate. This results in the core region mass increasing initially due to the introduction of cold downcomer fluid to the core region (Figure 9.6.5-86(a) and 9.6.5-86(b)). The net effect of the sensitivity case is that the vessel inventory is substantially decreased over the base model simulation (Figure 9.6.5-87); however, this inventory is sufficient to provide adequate core cooling because the ADS-4 continually draws liquid flow through the core (Figure 9.6.5-82). Even though there is no liquid storage in the upper plenum for the homogenous case (Figure 9.6.5-88), the core collapsed liquid level (Figure 9.6.5-89(a) and 9.6.5-89(b)) is not impacted significantly.

This sensitivity demonstrates that the AP1000 plant response is relatively insensitive to upper plenum and hot leg entrainment. Even with the assumption of homogenous fluid nodes above the core, adequate core cooling is demonstrated. No significant core uncovery/heatup is predicted for this scenario.

9.6.5.3.5.3 Radiological Consequences

The consequences of a DVI line break are bounded by those of an MBLOCA. With limited fuel damage and a concurrent release to containment, the releases are the same as those considered in the medium break LOCA doses presented in Section 9.6.5.3.6.3. Therefore, the medium break LOCA doses from Section 9.6.5.3.6.3 are presented. The calculated maximum doses for all relevant pathways (inhalation, cloudshine, and groundshine) are as follows:

Offsite dose: 2.6 mSv Worker dose: 6.0 mSv

These doses are within the Target 4 BSL for infrequent faults (10 mSv offsite and 200 mSv onsite).

9.6.5.3.5.4 Diverse Mitigation

Diverse mitigation for this event is not required as it is an infrequent fault classified as DB1.

9.6.5.3.5.5 As Low As Reasonably Practicable Assessment

The ALARP assessment for the MBLOCA fault applies with the exception that only one accumulator and one CMT are available. Refer to Section 9.6.5.3.6.5.

9.6.5.3.5.6 DVI Line Break Conclusions

The DB analysis shows that for the DVI line break fault, the acceptance criteria defined in Section 9.6.5.0 are met.

DBA radiological consequences are within the Target 4 BSL for frequent faults (1 mSv offsite and 20 mSv onsite). Thus, the identification of necessary Class 1 SSCs is adequate to meet DB requirements for this fault.

It has been shown that the AP1000 plant includes adequate systems for the protection of the fault, which limit the radiological consequences such that they are compliant with the SAPs targets and the risks have been reduced to be ALARP.

9.6.5.3.6 MBLOCA – 254 mm (10-inch) Cold Leg Break Results

9.6.5.3.6.1 DBA Credited SSCs

As the MBLOCA event is classified as an infrequent fault (DB1), a diverse means of providing the required Category A safety functions are not required. For the MBLOCA fault, the available Class 1 SSCs are shown below.

In addition to the accumulators, the PMS provides the following:

- RT, PRHR, CMTs and containment isolation on Low-2 pressuriser pressure
- ADS 1-4 on Low CMT level
- IRWST injection on Low CMT level (via ADS stage 4 signal)
- Containment recirculation on Low IRWST level
- PCS on High-2 containment pressure

9.6.5.3.6.2 Results of Design Basis Analysis

This case models a 254 mm (10-inch) break occurring in the cold leg connected to the balance line of CMT-1. The reactor steady-state initial conditions assumed for this transient are found in Table 9.6.5-9. The event times for this transient are given in Table 9.6.5-11 (Sheet 7).

Transient results are shown in Figures 9.6.5-56(a) through 9.6.5-78. The break opens at time zero, and the pressuriser pressure begins to fall, as shown in Figures 9.6.5-56(a), as mass is lost out the break. The pressuriser mixture level initially decreases as given in Figure 9.6.5-57. The break fluid flow is shown in Figures 9.6.5-75 and 9.6.5-76 for the liquid and vapour components respectively. The pressuriser pressure falls below the reactor trip set point, which causes the reactor to trip (after the appropriate time delay) and isolation of the steam generator main steam lines. The core makeup tank discharge isolation valves for both CMTs and the PRHR delivery line isolation valves open after an "S" signal occurs (with appropriate delays); the reactor coolant pumps trip after an "S" signal with a 7-second delay. The reactor coolant system is cooled by natural circulation with energy being removed by the steam generator safety valves, the core makeup tanks, and the PRHR heat exchanger. The PRHR heat removal rate and integrated heat removal are shown in Figure 9.6.5-77 and Figure 9.6.5-78. Once the core makeup tank isolation valves open, the core makeup tanks begin to inject borated water into the reactor coolant system as shown in Figures 9.6.5-61 and 9.6.5-62.

As time proceeds, the loops drain to the reactor vessel. The mixture level in the downcomer begins to drop as seen in Figure 9.6.5-60, and the core remains completely covered with the exception of a few short oscillatory time intervals in which the mixture level drops below the active fuel (Figure 9.6.5-69). Due to the size and location of the break involved, the accumulator setpoint is reached prior to the core makeup tanks transitioning from recirculation to injection mode. The flows from the core makeup tanks are shown in Figures 9.6.5-61 and 9.6.5-62, and from the accumulators, in Figures 9.6.5-63 and 9.6.5-64. Core makeup tank 2 reaches the 67.5-percent volume first, and after an appropriate delay, the ADS Stage 1 valves open. When the ADS is actuated, the mixture level increases in the pressuriser (Figure 9.6.5-57) because an opening has been created at the top of the pressuriser. After these valves open, a more rapid depressurisation occurs as seen in Figure 9.6.5-56(a).

During the initial portion of the 254 mm (10-inch) break, both liquid and steam flow out the top of the core (Figures 9.6.5-71 and 9.6.5-72) as the void fraction in the core increases (Figure 9.6.5-73). The break in the cold leg draws fluid from the bottom of the core, leaving insufficient liquid in the upper plenum. The mixture level, therefore, starts to decrease (Figure 9.6.5-69). The mixture level falls until accumulator flows enter the downcomer (Figures 9.6.5-63 and 9.6.5-64).

As Figures 9.6.5-61 and 9.6.5-62 indicate, when the accumulators begin to inject, the flow from both core makeup tanks is reduced and briefly reversed due to the pressurisation of the CMT injection lines by the accumulators. The opening of ADS Stage 2 valves maintains the depressurisation rate as shown in Figure 9.6.5-56(a). ADS Stage 3 valves subsequently open. This increases the system venting capability. Figures 9.6.5-70(a), 9.6.5-70(b), and 9.6.5-70(c) indicate the instantaneous liquid, instantaneous vapour, and integrated total mass discharge from the ADS Stage 1-3 valves respectively. The ADS Stage 4 valves open when the core makeup tank water volume is reduced to 20 percent. Figures 9.6.5-67(a), 9.6.5-67(b), and 9.6.5-74 indicate the instantaneous liquid, instantaneous vapour, and integrated total mass discharged from the ADS Stage 4 valves. After the ADS Stage 4 path opens, the pressuriser begins to drain mixture into the hot legs as seen in Figure 9.6.5-57. The Figure 9.6.5-68(a) mass inventory plot considers the primary inventory to be the reactor coolant system proper, including the pressuriser; the mass present in the passive safety system components is not included. The Figure 9.6.5-68(b) mass inventory plot considers the reactor vessel mixture inventory, including the downcomer, lower plenum, core fluid channels, upper plenum, and upper head. Once the downcomer pressure drops below the IRWST injection pressure, flow enters the reactor vessel from the IRWST. The mixture level in the reactor vessel is

approximately at the hot leg elevation as shown in Figure 9.6.5-69 throughout this transient; core uncovery does not occur for any prolonged period of time and may be deemed negligible. As such, the 254 mm (10-inch) break case exhibits large margins to the peak cladding temperature acceptance criteria of 1204.4°C (2200°F).

9.6.5.3.6.3 Radiological Consequences

The evaluation of the radiological consequences of a postulated MBLOCA assumes that as a result of the accident, 10 percent of the fuel rods are damaged such that the activity contained in the fuel-cladding gap is released to the reactor coolant. Activity is released to the containment via the break. The dose calculations take into account the release of activity by way of the containment purge line prior to its isolation near the beginning of the accident and the release of activity resulting from containment leakage. Purge of the containment for hydrogen control is not an intended mode of operation and is not considered in the dose analysis. While the normal residual heat removal system is capable of post-LOCA cooling, it is not a safety-related system and may not be available following the accident. If it is operable, it would be used only if the source term is not far above the normal shutdown primary coolant source term. It is assumed that core cooling is accomplished by the passive core cooling system, which does not pass coolant outside of containment. Thus, there is no recirculation leakage release path to be modelled.

9.6.5.3.6.3.1 Source Term

The most significant radionuclide releases are the noble gases, alkali metals, and iodines. The release of activity to the containment consists of two parts. The initial release is the activity contained in the reactor coolant system. This is followed by the release of core activity.

All activity in the fuel rod gap of the damaged fuel is assumed to be released to the coolant. Based on Table 7.3 of Reference 9.6.5-4, the gap fraction is assumed to be 3 percent of the core inventory for iodines, 10 percent for noble gases, and 4 percent for alkali metals. To address the fact that the failed fuel rods may have been operating at power levels above the core average, the source term is increased by a lead rod radial peaking factor of 1.75 which bounds the COLR limit of 1.72.

The core is assumed to remain covered by water post-accident. Therefore, the modelling is consistent with the wet phase described in Reference 9.6.5-4.

The release from the fuel is assumed to begin at 120 seconds. The fraction of gap activity released is 1.0 for noble gases, 1.0 for iodines, and 1.0 for alkali metals. The water covering the core is assumed to retain some of the radionuclides released from the core. The iodine activity is all assumed to enter into solution with 60 percent of the iodine assumed to convert to the elemental form and then enter the containment atmosphere, consistent with Section 2.2.1 of Chapter IX of Reference 9.6.5-4. It is assumed that 1% of the iodine released converts to the organic form while the other 99% stays in the elemental form. In practice, the iodine activity released from the fuel would initially enter into solution and is anticipated to be gradually released to the containment atmosphere over an indefinite period of time. However, it is conservatively assumed that all of the iodine releases to the containment atmosphere occur over 60 seconds. This assumption makes the activity quickly available for release to the environment by way of containment leakage. The alkali metals activity is assumed to be retained in the primary coolant and none of it is assumed to enter the containment atmosphere

The AP1000 does not include active systems for the removal of activity from the containment atmosphere. The containment atmosphere is depleted of elemental iodine and of particulates as a result of natural processes within the containment.

Elemental iodine is removed by deposition onto surfaces. Particulates are removed by sedimentation, diffusiophoresis (deposition driven by steam condensation), and thermophoresis (deposition driven by heat transfer). No removal of organic iodine is assumed.

If the post-LOCA cooling solution has a pH of less than 6.0, part of the caesium iodide may be converted to the elemental iodine form. The passive core cooling system provides sufficient trisodium phosphate to the post-LOCA cooling solution to maintain the solution pH at 7.0 or greater following a LOCA.

9.6.5.3.6.3.2 Release Pathways

The release pathways are the containment purge line and containment leakage. The activity releases are assumed to be ground level releases.

During the initial part of the accident, before the containment is isolated, it is assumed that containment purge is in operation and that activity is released through this pathway until the purge valves are closed. No credit is taken for the filters in the purge exhaust line.

The majority of the releases due to the LOCA are the result of containment leakage. The containment is assumed to leak at its design leak rate for the first 24 hours and at half that rate for the remainder of the analysis period.

9.6.5.3.6.3.3 Dose Calculation Models

The models used to calculate doses are provided in Appendix 9A.

9.6.5.3.6.3.4 Analytical Assumptions and Parameters

The assumptions and parameters used in the analysis are listed in Table 9.6.5-1.

9.6.5.3.6.3.5 Doses

The calculated maximum doses for all relevant pathways (inhalation, cloudshine, and groundshine) are as follows:

- Offsite dose: 2.6 mSv Worker dose: 6.0 mSv

These doses are within the Target 4 BSL for these infrequent faults (100 mSv offsite and 500 mSv onsite).

The limiting conditions for operation of the Technical Specifications used in the dose assessment are provided in Table 9.6.5-2. The Table 9.6.5-2 values ensure the Target 4 BSL is met.

9.6.5.3.6.4 Diverse Mitigation

Diverse mitigation for this event is not required as it is an infrequent fault classified as DB1.

9.6.5.3.6.5 As Low As Reasonably Practicable Assessment

For the medium-break loss of coolant accident, the identification of the primary safety functions as Class 1 SSCs has been shown to be adequate to meet DB requirements.

As shown in the PSA (Chapter 10), the AP1000 has diverse MBLOCA features including:

- CMTs or Accumulator provide high pressure injection
- ADS Stage 4 with IRWST gravity injection and recirculation or ADS Stage 1, 2, and 3 with RNS pumps providing IRWST injection and containment recirculation.
- PMS or DAS provide C&I. There is sufficient time available for the operators to manually actuate ADS and align the RNS if PMS is unavailable and DAS is credited.

Providing further means of removing decay heat or tripping the reactor in addition to these functions would not be significantly reduce the PSA risk for this event.

9.6.5.3.6.6 MBLOCA Conclusions

The DB analysis shows that for the MBLOCA fault, the acceptance criteria defined in Section 9.6.5.0 are met.

DBA radiological consequences are within the Target 4 BSL for infrequent faults (10 mSv offsite and 200 mSv onsite). Thus, the identification of necessary Class 1 SSCs is adequate to meet DB requirements for this fault.

It has been shown that the AP1000 plant includes adequate systems for the protection of the fault, which limit the radiological consequences such that they are compliant with the SAPs targets and the risks have been reduced to be ALARP.

9.6.5.3.7 Not Used

9.6.5.3.8 Core Makeup Tank Line Break Results

The general description of MBLOCA fault applies (See Section 9.6.5.3.6). However, with the break located in one of the lines between the CMT and the cold leg, only one of the CMTs is available.

For the DBA of the DVI line break scenarios, only the Class 1 systems listed under the MBLOCA event are available, but additionally, only one CMT is available. The same performance requirements apply.

A break in a balance line between a CMT and a cold leg is bounded by both of the following:

- The DVI line break scenario, which involves a similar break size but in which not only one CMT but also one accumulator and one IRWST injection line are unavailable, so that less emergency cooling water is available to replenish that lost from the break

- The limiting MBLOCA, which involves a larger-size break in the cold leg so that more water is lost from the break, placing greater demands on the emergency cooling water systems

Therefore, no additional analyses have been performed for the CMTLB; for the purpose of the DB analyses, the consequences have been assumed to be those associated with the DVI line break.

9.6.5.3.8.1 As Low As Reasonably Practicable Assessment

The ALARP assessment for the MBLOCA fault applies with the exception that only one CMT is available. Refer to Section 9.6.5.3.6.5.

9.6.5.3.8.2 CMT Line Break Conclusions

A separate analysis for this fault is not required as it is bounded by the DVI line break and MBLOCA faults as described above.

It has been shown that the AP1000 plant includes adequate systems for the protection of the fault, which limit the radiological consequences such that they are compliant with the SAPs targets and the risks have been reduced to be ALARP.

9.6.5.3.9 Passive Residual Heat Removal Tube Rupture Results

The general descriptions of SBLOCAs apply (See Section 9.6.5.3.4). However, with the break located in one of the PRHR system tubes, the PRHR performance would be degraded.

For the DBA of the PRHR system tube rupture, only the Class 1 systems listed for SBLOCA events would be credited, except that the PRHR system is conservatively assumed to be unavailable. In reality, the PRHR heat exchanger would be expected to be functional, albeit at a reduced capacity. A rupture of one of the PRHR tubes (inner diameter 15.7 mm (0.62 inch) results in a LOCA that is smaller than the limiting frequent fault SBLOCA, which has an equivalent break diameter of 50.8 mm (2 inch). The PRHR performance for SBLOCAs is not very important because the initial SG secondary side inventory is capable of removing heat for an extended time. During this time the RCS pressure would be reduced to the SG secondary side pressure of 8.34 MPa (1210 psia) due to steam relief from the SGs and the break. The RCS pressure at the time of ADS 1, 2, and 3 actuation would be higher if the PRHR was assumed unavailable. However, the spurious ADS actuation case discussed in this section bounds this case with respect to RCS pressure at the time of ADS 1, 2, and 3 actuation (normal RCS pressure, 15.9 MPa (2300 psig)) and has much higher decay heat levels since the ADS actuation time is much earlier.

Also note that in the DBA SBLOCA analysis, the PRHR is assumed to stop functioning when the accumulators empty and nitrogen enters the RCS. Therefore, no additional analyses have been performed for the PRHR system tube rupture; for the purpose of the DB analyses, the consequences have been assumed to be those associated with the limiting infrequent SBLOCA.

9.6.5.3.9.1 As Low As Reasonably Practicable Assessment

The ALARP assessment for the SBLOCA fault applies with the exception that the PRHR system is not available. Refer to Section 9.6.5.3.4.4.

9.6.5.3.10 Reactor Coolant Leakage Results

The general descriptions of SBLOCAs apply to the reactor coolant leakage fault, noting that time scales are extended.

The analysis methods and assumptions described for the SBLOCA apply for the analysis of reactor leaks. The plant conditions from transient analysis of the SBLOCA scenario are assumed to be bounding.

9.6.5.3.10.1 DBA Credited SSCs

For the DBA of the reactor coolant leakage, only the Class 1 systems listed under the SBLOCA event are available (See Section 9.6.5.3.4.1.1), and the same performance requirements discussed in Section 9.6.5.2.1 also apply. As the RCS Leak event is classified as a high frequency, low consequence fault, a diverse means of providing the required Category A safety functions is also required.

9.6.5.3.10.2 Results of Design Basis Analysis

Since the behaviour associated with the reactor coolant leakage fault is bounded by the limiting SBLOCA, only sensitivity transient analyses have been performed for the RCS leakage fault in order to demonstrate diverse mitigation for this frequent fault.

9.6.5.3.10.3 Radiological Consequences

The consequences of a reactor coolant leakage fault are bounded by the consequences from an SBLOCA. The consequences of an SBLOCA are conservatively estimated based on those of an MBLOCA (see Section 9.6.5.3.4.3). With limited fuel damage (less than 1 percent predicted for SBLOCA) and a concurrent release to containment, the releases are less than 10 percent of those considered in the MBLOCA doses (see Section 9.6.5.3.6.3) which considered up to 10 percent fuel damage. Therefore, doses that are ten percent of the MBLOCA doses from Section 9.6.5.3.6.3 are presented. The calculated maximum doses for all relevant pathways (inhalation, cloudshine, and groundshine) are as follows:

Offsite dose: 0.26 mSv Worker dose: 0.60 mSv

These doses are within the Target 4 BSL for frequent faults (1 mSv offsite and 20 mSv onsite).

9.6.5.3.10.4 Diverse Mitigation

The available diverse mitigation for the SBLOCA fault applies to the RCS leak event.

9.6.5.3.10.5 Diverse Mitigation Analysis

Depressurisation of Reactor Coolant System

This section deals with inadvertent pressuriser spray, even though it is not a loss of RCS coolant inventory. Pressuriser spray draws subcooled water from a scope in the RCS cold leg and sprays it into the top of the pressuriser (the steam space). The subcooled spray condenses steam, thereby lowering the RCS pressure. The spray valve is controlled by the PLS pressure control system.

Inadvertent spray could result from either a spray valve failure causing it to go open when not needed, or by a failure in the pressure control system demanding spray when it is not needed.

The PMS will protect the core DNB design limits with reactor trip on low pressuriser pressure and overtemperature ΔT. The PLS will initiate alarms and control withdrawal blocks based on low margin to the overtemperature ΔT reactor trip.

For ATWS assessment of this event, the pressuriser spray valves was assumed to go wide open and stay there, and the pressuriser heaters were not energised (as they would be on low pressure).

Figures 9.6.5-91 to 9.6.5-94 illustrate the transient with no action by either reactor trip or ESF actuation from the PMS (i.e., it applies to assumed PMS CCF.)

Initially, the spray will reduce pressure and increase pressuriser water level as steam is condensed. The reduction in pressure will tend to cause a small decrease in core power. The automatic reactor power control system will withdraw control rods as needed to maintain RCS average temperature.

In this calculation, the PLS overtemperature ΔT rod stop (on low margin to overtemperature ΔT reactor trip) was arbitrarily assumed to be reached 5 minutes after start of spray. (It makes little difference in the course of events when that event occurs. Five minutes was an arbitrary selection and is not intended to represent an actual setpoint.) Its effect is so small that there is no noticeable change at that time in the figures.

In this illustration, saturation of the average core outlet fluid is reached at approximately 375 seconds. At that time, core power begins to decrease noticeably, causing reduction in RCS temperatures and steam pressure. The turbine control valves will open automatically to maintain constant turbine power until they reach their full open position. (A 5 percent margin is assumed in the turbine control valves, such that they are able to maintain flow turbine load until pressure drops to 5.45 MPa-abs (790 psia). At that point, turbine steam flow begins to decrease.

As the pressuriser pressure and saturation temperature decrease, the liquid region cools and becomes more dense, causing a slow decrease in pressuriser water volume. This water volume decrease accelerates as temperature decreases in the cold leg (and its density increases).

RCS pressure continues to decrease as pressuriser steam continues to be condenses by the continually cooling cold-leg fluid. The core reactivity balance dictates that the core exit conditions stay near boiling, with low void content in the top of the core. Lower RCS temperatures and steam pressures cause a decrease in turbine steam flow. Basically, the reactor core continues to meet the steam load demand, with the reactivity balance forcing the power to stay near the saturation line in the hot leg.

For simplicity, these calculations neglected the decrease in feedwater temperature that would accompany a reduction in turbine steam flow. Cooler feedwater would cause a somewhat higher steam thermal load, causing core power to decrease somewhat more slowly than is shown in the figures. The inherent behaviour and sequence of events would not be significantly affected.

These calculations were based on BOC reactivity feedback described in Section 9D.6.1.1. There would be little difference with EOC feedback. In either case, the core reactivity will force low void content in the upper part of the core.

Unless a PMS CCF is assumed, the PMS reactor trip signal will trip the turbine. In that case, the transient is dominated by the loss of steam load and the course of events would be similar to those shown for turbine trip. Whatever voids were formed as a result of depressurisation would aid in reducing core power.

Loss of Reactor Coolant System Inventory – Reactor Coolant System Leaks

This section deals with RCS leaks that are greater than the capacity of the makeup system or when the makeup system is unavailable. Therefore, they represent a loss of RCS inventory that eventually requires automatic or manual action to maintain effective core cooling.

A leak will drain the pressuriser. Assuming no PMS reactor trip or actuations of ESFs, the system response will be similar to that shown for inadvertent pressuriser spray, with one important difference: Since fluid inventory is being lost from the RCS, the pressuriser level will decrease much more than is shown in Figure 9.6.5-94. The rate of depressurisation will depend upon the size of the leak.

In the absence of manual or automatic PMS action, the pressuriser will drain, leading to DAS low pressuriser level actuation of reactor trip, turbine trip, RCP trips, CMT, and PRHR. Actuation of those features will shut down the reactor core and maintain core cooling.

If mechanical failure of control rods to insert is postulated, then the PMS would still actuate turbine trip, RCP trips, CMT, and PRHR. Trip of RCPs will cause a rapid core power reduction, and boration by the CMT will provide shutdown reactivity.

9.6.5.3.10.6 As Low As Reasonably Practicable Assessment

The ALARP assessment for this event is the same as for small LOCAs as discussed in Section 9.6.5.3.4.4.

9.6.5.3.10.7 RCS Leak Conclusions

The DB analysis shows that for the SBLOCA fault, which bounds the RCS leak fault, the acceptance criteria defined in Section 9.6.5.0 are met.

This event has also been adequately assessed with respect to ATWT considerations. This event was explicitly analysed for the change in the current design reference point in the UK as described in Reference 9.6.5-14. Reference 9.6.5-11 demonstrated that there is little impact on the key analysis trends, results, and margin to the applicable acceptance criteria. Therefore, the change in design reference point would not invalidate the conclusions presented for this event.

DBA radiological consequences are within the Target 4 BSL for frequent faults (1 mSv offsite and 20 mSv onsite). Thus, the identification of necessary Class 1 SSCs is adequate to meet DB requirements for this fault.

It has been shown that the AP1000 plant includes adequate systems for the protection of the fault, which limit the radiological consequences such that they are compliant with the SAPs targets and the risks have been reduced to be ALARP.

9.6.5.4 MBLOCA and SBLOCA Overall Conclusions

The small-break and medium-break LOCA analyses performed show that the passive safeguards systems are sufficient to mitigate small-break and medium-break LOCAs. Specifically, it is concluded that:

- The primary side can be depressurised by the ADS to allow stable injection into the core.
- Injection from the core makeup tanks, accumulators, and IRWST prevents excessive cladding heatup for small-break and medium-break LOCAs analysed, including double-ended ruptures in the passive safeguards system lines. The peak heat flux during the DEDVI line break accumulator injection period is below the predicted critical heat flux.
- The effect of increasing upper plenum/hot leg entrainment does not significantly affect plant safety margins.

The analyses performed demonstrate that the acceptance criteria provided in the design basis requirements are met. Summarizing the small-break and medium-break LOCA spectrum:

Break Location/Diameter	Minimum Reactor Vessel Mixture Inventory	Peak Cladding Temperature
DBA Inadvertent ADS	24,717 kg (54,491 lbm)	504°C (938.5°F)
DBA 50.8 mm (2-inch) cold leg break	24,557 kg (54,139 lbm)	434°C (813.5°F)
DBA 254 mm (10-inch) cold leg break	35,978 kg (79,319 lbm)	(1)
DBA DEDVI	33,234 kg (73,268 lbm)	(1)
DBA DEDVI (Entrainment Study)	25,817 kg (56,916 lbm)	(1)

(1) There is no core heatup as a result of these transients; PCT occurs at transient initiation.

The 50.8 mm (2-inch) cold leg break exhibits the limiting minimum reactor vessel mixture inventory conditions, and the inadvertent ADS actuation transient has the limiting peak cladding temperature. The AP1000 design is such that the minimum reactor vessel mixture inventory occurs around the time of IRWST injection for the limiting breaks. All breaks simulated in the break spectrum produce results that demonstrate significant margin to the design basis requirements.

In addition, a selection of appropriate diversity cases is presented to demonstrate the diverse capabilities for all frequent fault small-break LOCAs (those up to 2" in diameter).

As noted in Section 9.6.4.6, an additional assessment was carried out to assess the potential for grid crush to extend beyond the assemblies in the low power channel as a result of a depressurisation of the primary circuit due to a double-ended guillotine (DEG) break of the RCS cold leg. This assessment concluded that no grid crushing will occur outside of the low power assemblies due to the depressurisation and therefore coolable geometry will be maintained. These limited impacts for LBLOCAs are further reduced when considering smaller breaks; therefore, the analysis results presented in this section are not impacted.

9.6.5.5 References

9.6.5-1 ANS 5.1-1971, "Decay Energy Release Rates Following Shutdown of Uranium-Fueled Thermal Reactors," American Nuclear Society, October 1971.

9.6.5-2 Westinghouse Document WCAP-8301 (Proprietary), "LOCTA-IV Program: Loss-of-Coolant Transient Analysis," June 1974.

9.6.5-3 Westinghouse Documents WCAP-15846, Rev. 5 (Proprietary), and WCAP-15862, Rev. 5 (Non-Proprietary), "WGOTHIC Application to AP600 and AP1000," September 2016.

9.6.5-4 European Commission Report EUR 19841 EN, "Determination of the in-containment source term for a large-break loss of coolant accident," April 2001.

9.6.5-5 Westinghouse Documents WCAP-10079-P-A, Rev. 0 (Proprietary) and WCAP-10080-A, Rev. 0 (Non-Proprietary), "NOTRUMP A Nodal Transient Small Break and General Network Code," August 1985.

9.6.5-6 Westinghouse Documents WCAP-10054-P-A (Proprietary) and WCAP-10081-A (Non-Proprietary), "Westinghouse Small Break ECCS Evaluation Model Using the NOTRUMP Code," August 1985.

9.6.5-7 Westinghouse Documents WCAP-14601, Rev. 2 (Proprietary) and WCAP-15062, Rev. 2 (Non-Proprietary), "AP600 Accident Analyses - Evaluation Models," May 1998.

9.6.5-8 Westinghouse Documents WCAP-14807, Rev. 5 (Proprietary) and WCAP-14808, Rev. 2 (Non-Proprietary), "NOTRUMP Final Validation Report for AP600," August 1998.

9.6.5-9 Westinghouse Documents WCAP-15644-P, Rev. 2 (Proprietary) and WCAP-15644-NP, Rev. 2 (Non-Proprietary), "AP1000 Code Applicability Report," March 2004.

9.6.5-10 Chang, S. H. et al. "A study of critical heat flux for low flow of water in vertical round tubes under low pressure," Nuclear Engineering and Design, 132, 225-237, 1991.

9.6.5-11 Westinghouse Report UKP-SSAR-GLR-002, Rev. 0, "UK AP1000® Plant: Summary Report Supporting the Closure of Fault Studies Issue 03," May 2016.

9.6.5-12 Westinghouse Report UKP-GW-GL-067, Rev. 1, "AP1000 Assessment of Diverse Mitigation of Frequent Faults for the UK," December 2011.

9.6.5-13 Westinghouse Report UKP-GW-GL-797, Rev. 1, "AP1000 ALARP Assessment of Diverse Mitigation of 'Frequent Fault' Small Break LOCAs," July 2016.

9.6.5-14 Westinghouse Report UKP-SSAR-GLR-001, Rev. A, "UK Fault Studies Analysis Basis," July 2015.

Table 9.6.5-1. Parameters Used In Evaluating The Radiological Consequences Of Medium Break LOCA

(Page 1 of 2)

Reactor coolant iodine activity	Equal to the operating limit for reactor coolant activity of 9.25E6 Bq/kg (0.25 µCi/g) dose equivalent I-131 (see Table 9A-1)
Reactor coolant noble gas activity	Equal to the operating limit for reactor coolant activity of 2.6E9 Bq/kg (70 µCi/g) dose equivalent Xe-133 (see Table 9A-1)
Reactor coolant alkali metal activity	Design basis activity (see Table 9A-1)
Reactor coolant mass	1.99E5 kg (4.39E5lbm)
RCS Activity Airborne fractions Iodines Noble gases Alkali metals	 0.5 1.0 0.5
Containment Volume	5.83E4 m^3 (2.06E6 ft^3)
Containment Purge Modelling Flow Rate Isolation Timing	 2.72E4 m^3/hr (1.6E4 cfm) 30 sec
Fraction of fuel rods assumed to fail	0.1
Core activity	See Table 9A-3
Radial peaking factor (for determination of activity in failed fuel rods)	1.75
Fission product gap fractions Iodines Noble gases Alkali metals	 0.03 0.10 0.04
Activity Release from Fuel (120 seconds to 180 seconds)| Fraction of Gap Activity Released to RCS Iodines Noble gases Alkali metals Fraction of RCS Activity becoming airborne Iodines Noble gases Alkali metals Airborne Iodine Chemical Fractions Elemental Iodine Organic Iodine Particulate Iodine	 1.0 1.0 1.0 0.6 1.0 0.0 0.99 0.01 0.0

Table 9.6.5-1. Parameters Used In Evaluating The Radiological Consequences Of Medium Break LOCA

(Page 2 of 2)

Removal Coefficients(1) Elemental Iodine Organic Iodine Particulates	 1.7 (hr^{-1}) 0.0 (hr^{-1}) 0.5 (hr^{-1})
Containment Leakage Rate 0-24 hours 24-720 hours	 0.1 (%/day) 0.05 (%/day)
Offsite atmospheric dispersion factors	See Table 9A-5
Control room modelling	See Appendix 9A

Note:

1. Elemental iodine removal is modelled until a DF of 200 is reached. Particulate removal is modelled until a DF of 1.0E4 is reached.

Table 9.6.5-2. Medium Break LOCA Technical Specifications Used In Dose Analysis

Limit or Condition	Tech Spec Identification and Notes
Primary Containment Leakage Rate	3.6.1 (SR 3.6.1.1) within containment leakage acceptance criteria. 5.5.8 (Containment leakage rate testing program) defines maximum allowable primary containment leak rate to be less than or equal to 0.1 weight-% per day at the calculated peak containment internal pressure for the design basis LOCA.
Primary coolant specific activity	3.4.10 dose equivalent specific activity to be < 9.25E6 Bq/kg (0.25 μCi/g) for I-131 and < 2.6E9 Bq/kg (70 μCi/g) for Xe-133

Table 9.6.5-3 SSCs Available for DBA Mitigation of Small and Medium LOCA

Category A Safety Function	SSCs	Classification
Short-term reactivity control	Reactor trip Breakers (PMS)	1
Long-term reactivity control	Note 1	1
Decay heat removal	Note 1	1
RCS pressure control	Not required. - Small and Medium LOCAs result in RCS depressurisation	
RCS inventory control	Note 1	1
Containment cooling	PCS AOVs and MOV	1

Note: 1. Passive RCS injection and depressurisation is provided by PRHR HX, CMTs, accumulators, IRWST injection, containment recirculation, and ADS.

Table 9.6.5-4 SSCs Credited in Diverse Mitigation of Small Break LOCAs

Case	PMS	DAS	RCCA	PRHR	CMT	ACC	ADS123	ADS4	RNS	IRWST(2)	Notes
1	X	-	X	X	X	-	-	X	-	X	Core cooling
2	X	-	X	-	X	-	X	X	-	X	Core cooling
3	-	X	X	X	-	X	X(1,3)	-	X(3)	X(4)	Core cooling
4	-	X	X	X	X	-	X(3)	X(3)	-	X(3)	ATWT
5	X	-	-	X	X	-	X	X	-	X	ATWT

Notes (1) ADS 1, 2, and 3 is included in this 3rd diverse case to address potential concerns with non-condensable gas (nitrogen) entering the RCS from the accumulators and degrading the PRHR performance. Reference 9.6.5-12 provides analysis that shows that such degradation would not be severe and would allow for RNS injection without ADS 1, 2, and 3 actuation.

(2) "IRWST" means passive IRWST injection and Containment Recirculation capability.

(3) Manually actuated via DAS.

(4) Containment recirculation function only.

Tables 9.6.5-5 through 9.6.5-8 Not Used.

Table 9.6.5-9. Initial Conditions For AP1000 Small-Break And Medium-Break LOCA Analysis

Condition	Calculation	Nominal Steady-state
Pressuriser pressure (MPa [psia])	15.859 [2300.1]	15.858 [2300]
Vessel inlet temperature (°C [°F])	278.91 [534.03]	279.22 [534.59]
Vessel outlet temperature (°C [°F])	322.31 [612.16]	322.56 [612.61]
Vessel flow rate (kg/sec [lbm/sec])	14115 [31118]	14115 [31118]
Steam generator pressure (MPa [psia])	5.480 [794.76]	5.478 [794.59]

Table 9.6.5-10. ADS Parameters Utilised In LOCA Analyses

ADS Valve Actuation Signal (percentage of core makeup tank volume)		Actuation Time (seconds)	Minimum Valve Flow Area (for each path, in^2)	Maximum Valve Flow Area (for each path, in^2)	Number of Paths	Valve Opening Time (seconds)
Stage 1 – Control CMT Level – Low 3	67.5	32 after CMT Level-Low 3	4.6(4)	7(4)	2 out of 2	≤ 40
Stage 2 – Control		48 after Stage 1	21(4)	26(4)	2 out of 2	≤ 100
Stage 3 – Control		120 after Stage 2	21(4)	26(4)	2 out of 2	≤ 100
Stage 4A CMT Level – Low 6	20	128 after Stage 3(2)	67	NA	1 out of 2	≤ 4(3)
Stage 4B		60 after Stage 4A	67	NA	2 out of 2	≤ 4(3)

Notes:

1. Not used.
2. The interlock requires coincidence of CMT Level Low-6 as well as 128 seconds after the Stage 3 actuation signal is generated.
3. This includes “arm-fire” processing delay and the assumed valve opening time.
4. The areas listed above for the ADS Stage 1, 2, and 3 valves are an effective flow area.

Table 9.6.5-11 (Sheet 1 of 8) DBA Sequence Of Events, Inadvertent ADS Depressurisation

Event	Time (seconds)
Inadvertent opening of ADS Stage 1 valves	0.0
Reactor trip signal	47.4
Steam turbine stop valves close	47.4
ADS Stage 2	48.0
"S" signal	56.4
Main feed isolation valves close	63.4
Reactor coolant pumps start to coast down	63.4
ADS Stage 3	168.0
Accumulator injection starts	257.4
Accumulator tank empties (1 / 2)	676.9 / 676.5
ADS Stage 4	1578.0
Core makeup tank empties (1 / 2)	1933.7 / 1951.0
Core uncovery begins	2509.5
IRWST injection starts[1]	2738.0
Core uncover ends	2784.0

Note:
1. Continuous injection period

Table 9.6.5-11 (Sheet 2 of 8) DBA Sequence Of Events, Small LOCA (50.8 mm (2-Inch) Cold Leg Break)

Event	Time (seconds)
Break opens	0.0
Reactor trip signal	53.8
Steam turbine stop valves close	53.8
“S” signal	65.4
Main feed isolation valves begin to close	72.4
Reactor coolant pumps start to coast down	72.4
ADS Stage 1	1201.7
ADS Stage 2	1249.7
Accumulator injection starts	1306.2
ADS Stage 3	1369.7
Accumulators empty (1 / 2)	1714.4 / 1716.1
ADS Stage 4	2237.2
CMTs empty (1 / 2)	2584.7 / 2610.5
Core uncovery begins	2939.0
IRWST injection starts[1]	3126.1
Core uncovery ends	3179.3

Note:
1. Continuous injection period

Table 9.6.5-11 (Sheet 3 of 8) Diverse Core Cooling Sequence of Events, Small LOCA (50.8 mm (2-Inch) Cold Leg Break) Case 1

Event	Time (seconds)
Break opens	500
Reactor trip signal	566
Main feed isolation	570
Turbine trip	571
CMT injection	574
PRHR HX start	576
Steam line isolation	3385
ADS Stage 4 opens	3385
CMTs empty	3630
IRWST injection starts[1]	3593

Note:
1. Continuous injection period

Table 9.6.5-11 (Sheet 4 of 8) Diverse Core Cooling Sequence of Events, Small LOCA (50.8 mm (2-Inch) Cold Leg Break) Case 2

Event	Time (seconds)
Break opens	500
Reactor trip signal	566
Turbine trip	571
Main feed isolation	572
CMT injection	574
Steam line isolation	1399
ADS Stage 1 opens	3665
CMTs empty	4217
IRWST injection starts[1]	4178

Note:
1. Continuous injection period

Table 9.6.5-11 (Sheet 5 of 8) Diverse Core Cooling Sequence Of Events, Small LOCA (50.8 mm (2-Inch) Cold Leg Break) Case 3

Event	Time (seconds)
Break opens	500
Reactor trip signal	567
Main feedwater isolation	570
Turbine trip	571
PRHR HX start	576
Steam line isolation	967
Accumulator injection begins	2171
RNS pumps started(1)	4100
ADS Stage 1 opened[1]	4100
Accumulator empty[2]	4410
RNS injection begins[2]	4100

Note:
1. Operator manually actuates these components. They also actuate ADS stages 2 and 3 in sequence.
2. Shortly after the ADS stage 1 is opened the accumulators empty and RNS injection begins.

Table 9.6.5-11 (Sheet 6 of 8) DBA Sequence of Events, Double-Ended Direct Vessel Injection Line Break with 0.138 MPa abs (20 psia) Containment Backpressure

Event	Time (seconds)
Break opens	0.0
Reactor trip signal	13.4
Steam turbine valves close	13.4
"S" signal	19.8
Main feed isolation valves close	26.8
Reactor coolant pumps start to coast down	26.8
ADS Stage 1	181.7
ADS Stage 2	229.7
Accumulator injection starts	244.2
ADS Stage 3	349.7
ADS Stage 4	477.7
Accumulator empties (1 / 2)	443.1 / 573.6
Intact DVI line IRWST injection starts[1]	1778.6
Core makeup tank empties (1 / 2)	226.1 / 1866.0

Note:
1. Continuous injection period

Table 9.6.5-11 (Sheet 7 of 8) DBA Sequence of Events, 254 mm (10-Inch) Cold Leg Break

Event	AP1000 Time (seconds)
Break opens	0.0
Reactor trip signal	5.5
Steam turbine stop valves close	5.5
“S” signal	6.7
Main feed isolation valves begin to close	13.7
Reactor coolant pumps start to coast down	13.7
Accumulator injection starts	84.0
Accumulator tank empties (1 / 2)	500.8 / 503.3
ADS Stage 1	745.2
ADS Stage 2	793.2
ADS Stage 3	913.2
ADS Stage 4	1358.5
IRWST injection starts[1]	2660.8
Core makeup tank empties (1 / 2)	2106.9 / 1928.5

Note:
1. Continuous injection period

Table 9.6.5-11 (Sheet 8 of 8) DBA Sequence of Events, Double-Ended Direct Vessel Injection Line Break (Entrainment Sensitivity)

Event	AP1000 Time (seconds)
Break opens	0.0
Reactor trip signal	13.4
Steam turbine stop valves close	13.4
"S" signal	19.9
Main feed isolation valves close	26.8
Reactor coolant pumps start to coast down	26.8
ADS Stage 1	181.2
ADS Stage 2	229.2
Intact accumulator injection starts	293.4
ADS Stage 3	349.2
ADS Stage 4	477.2
Accumulator tank empties (1 / 2)	441.0 / 580.8
Intact DVI line IRWST injection starts[1]	1851.4
Core makeup tank empties (1 / 2)	225.2 / 1850.1

Note:
1. Continuous injection period

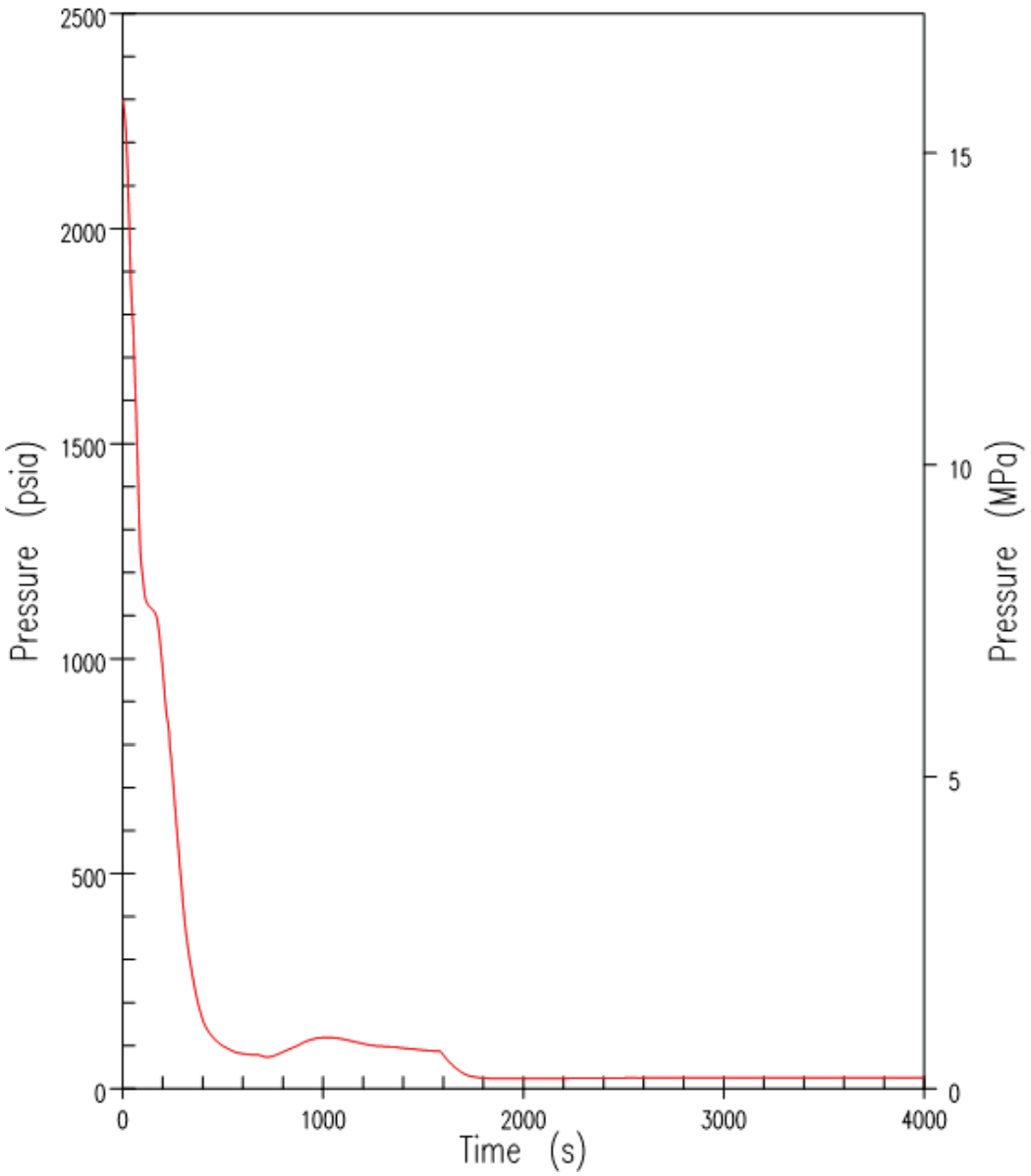


Figure 9.6.5-1(a). DBA Inadvertent ADS – RCS Pressure

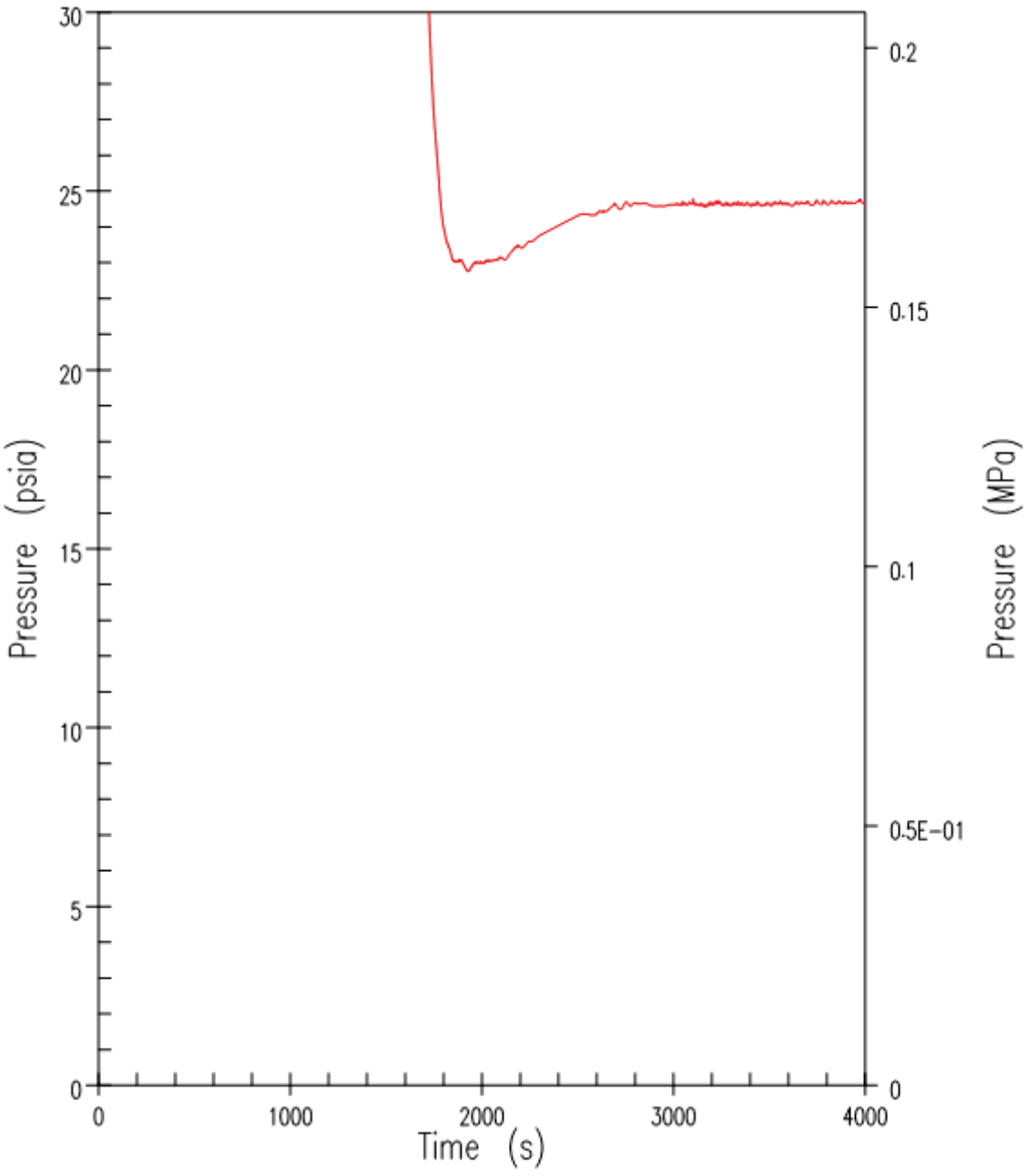


Figure 9.6.5-1(b). DBA Inadvertent ADS – RCS Pressure (Zoomed)

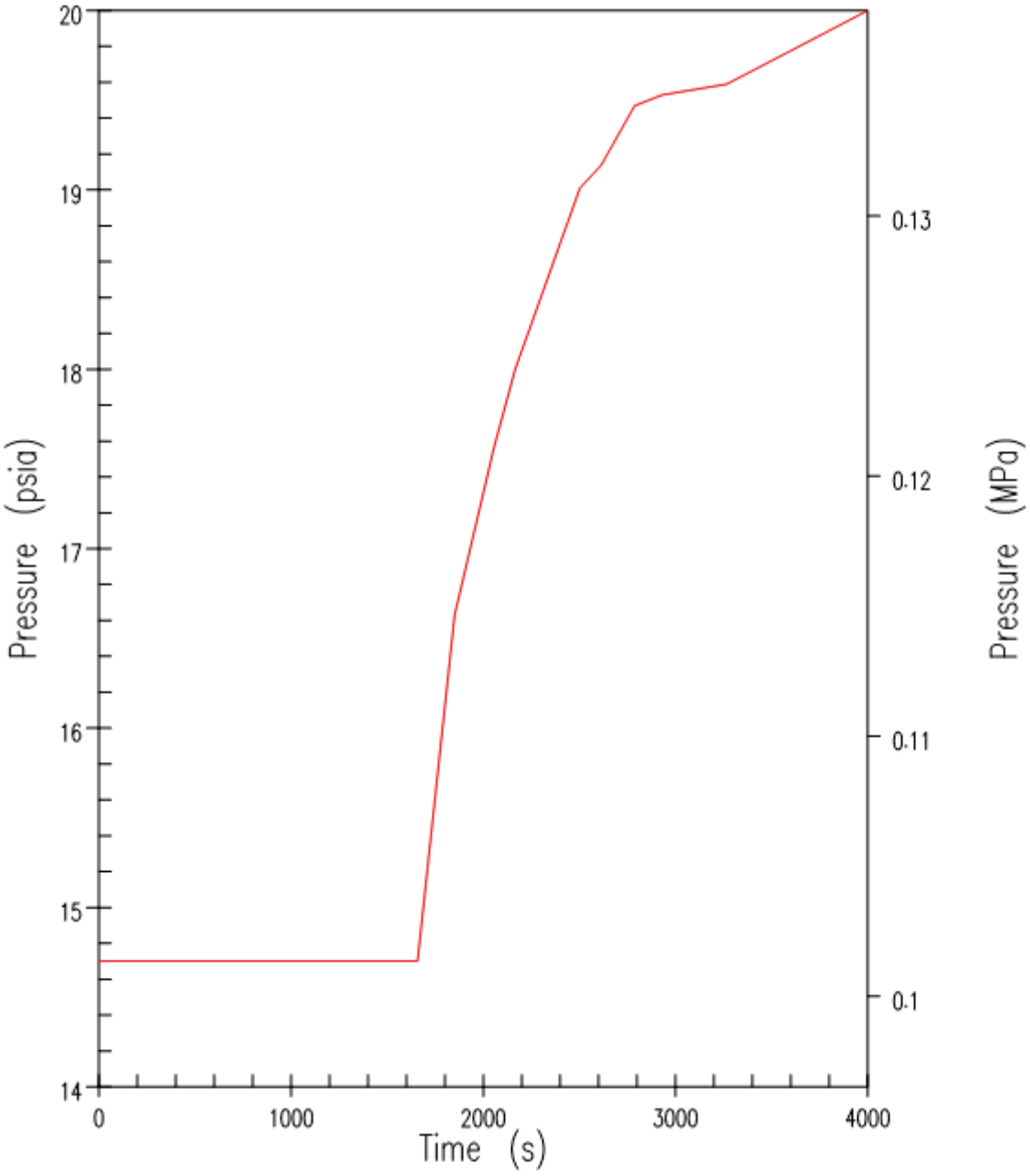


Figure 9.6.5-1(c). DBA Inadvertent ADS – Containment Pressure

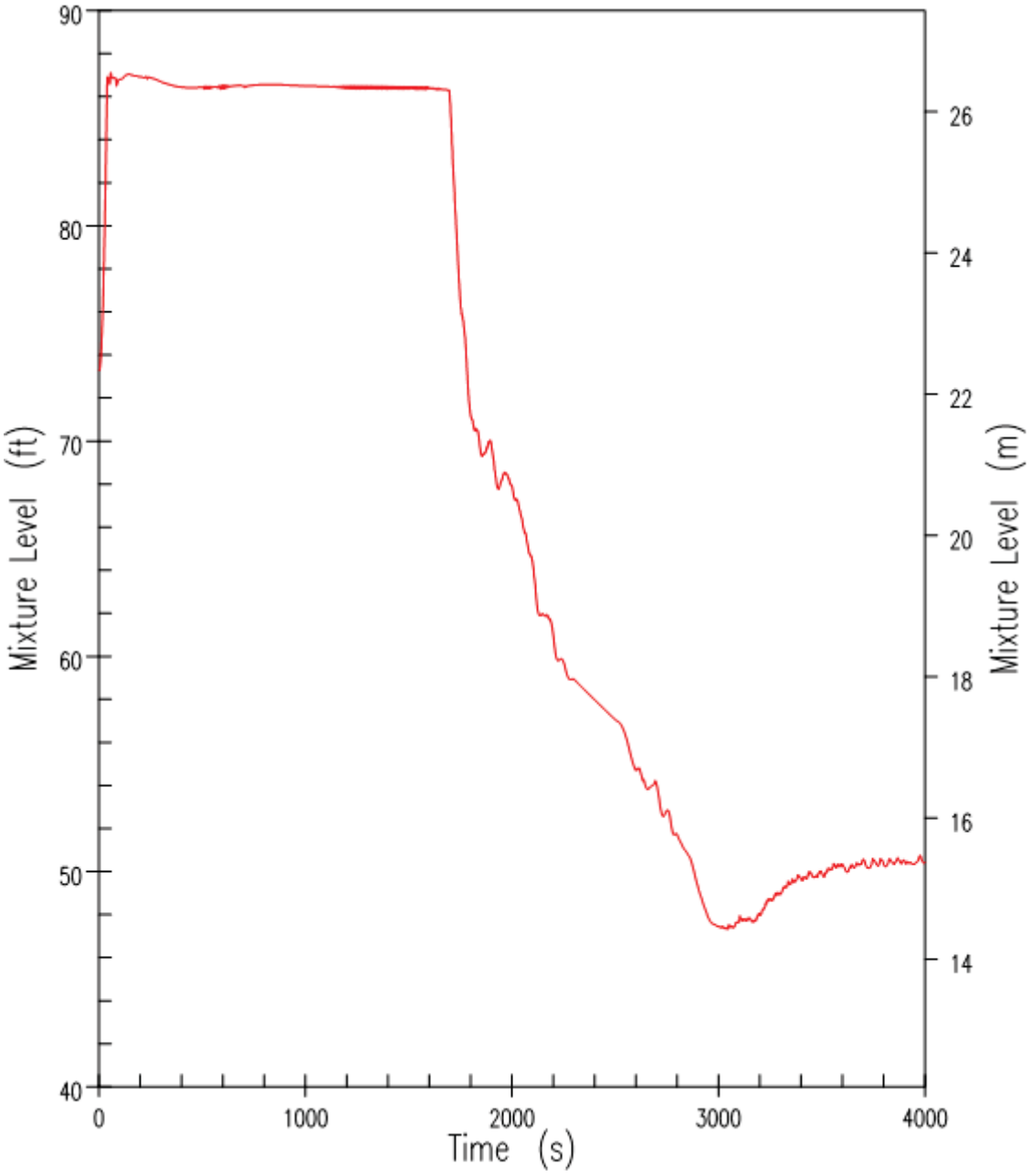


Figure 9.6.5-2. DBA Inadvertent ADS – Pressuriser Mixture Level

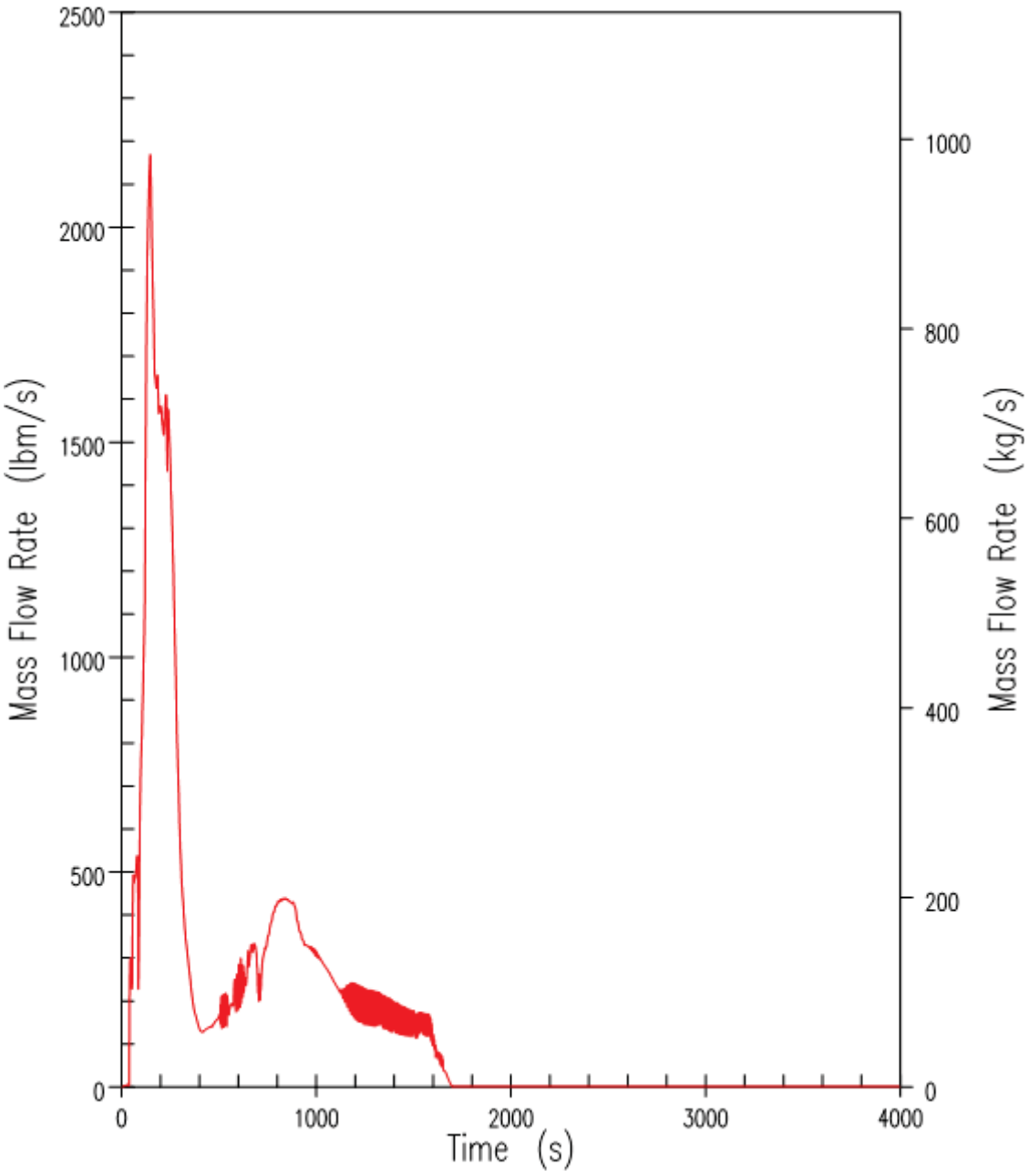


Figure 9.6.5-3. DBA Inadvertent ADS – ADS 1-3 Liquid Discharge

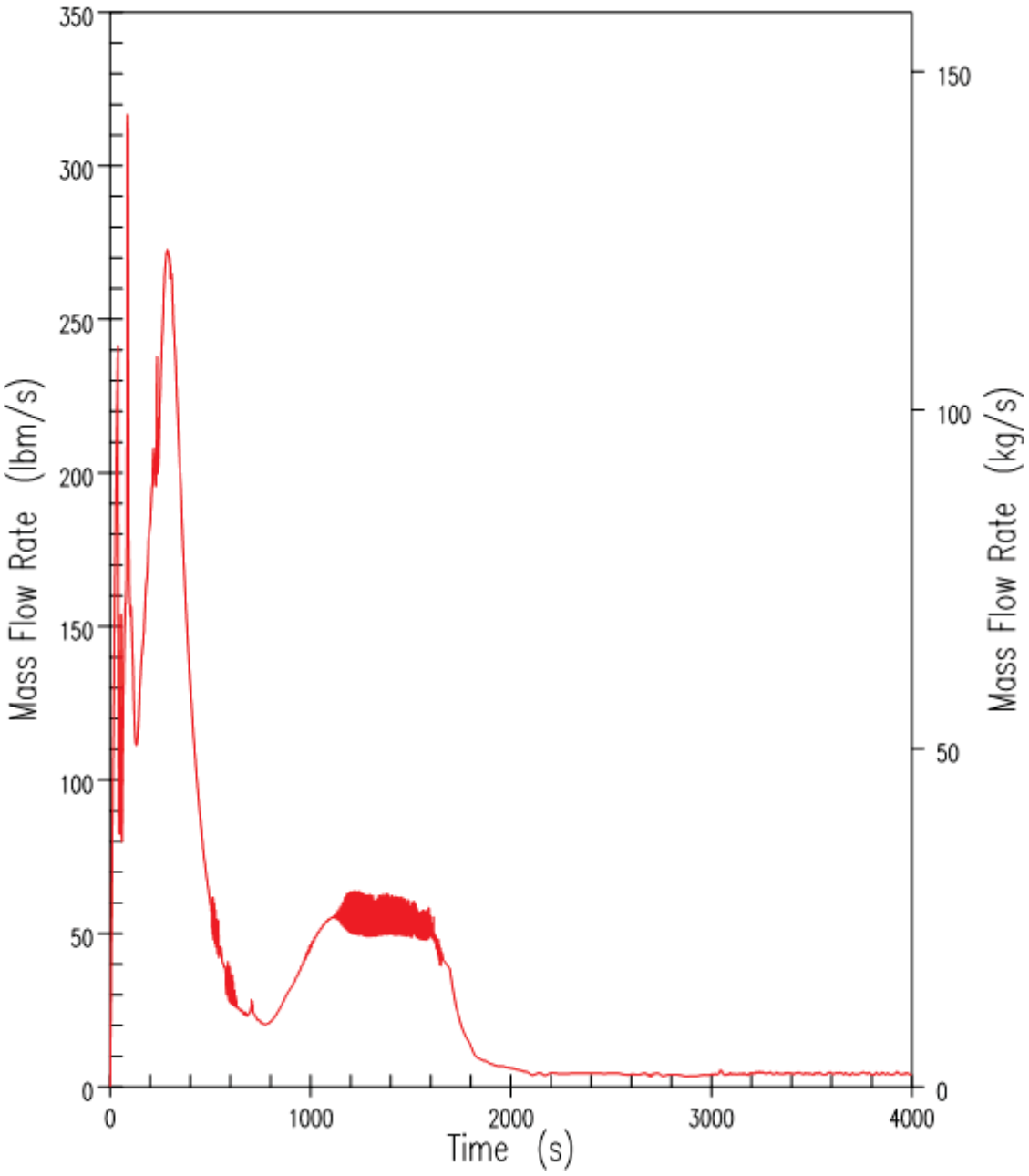


Figure 9.6.5-4(a). DBA Inadvertent ADS – ADS 1-3 Vapour Discharge

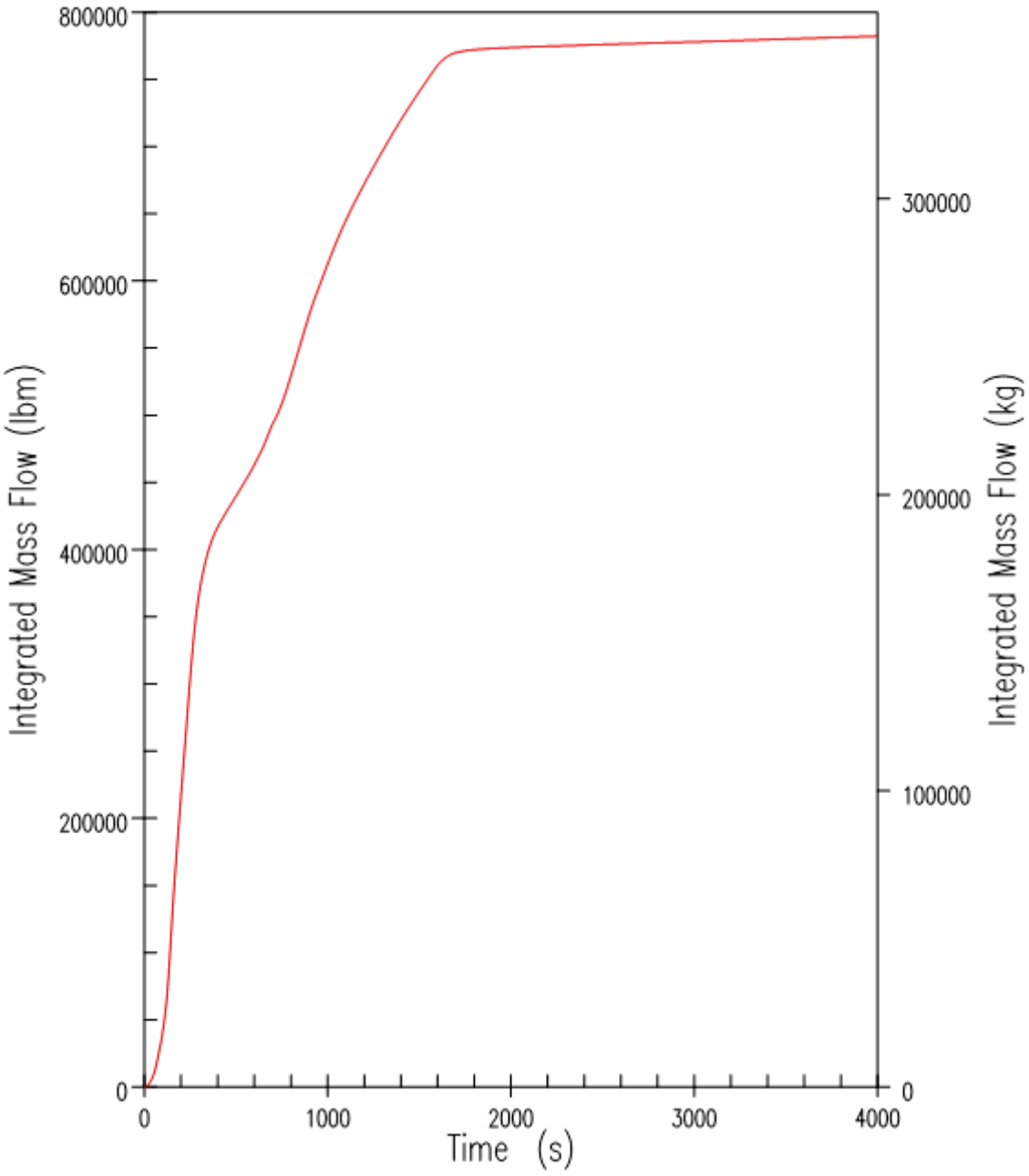


Figure 9.6.5-4(b). DBA Inadvertent ADS – ADS 1-3 Integrated Discharge

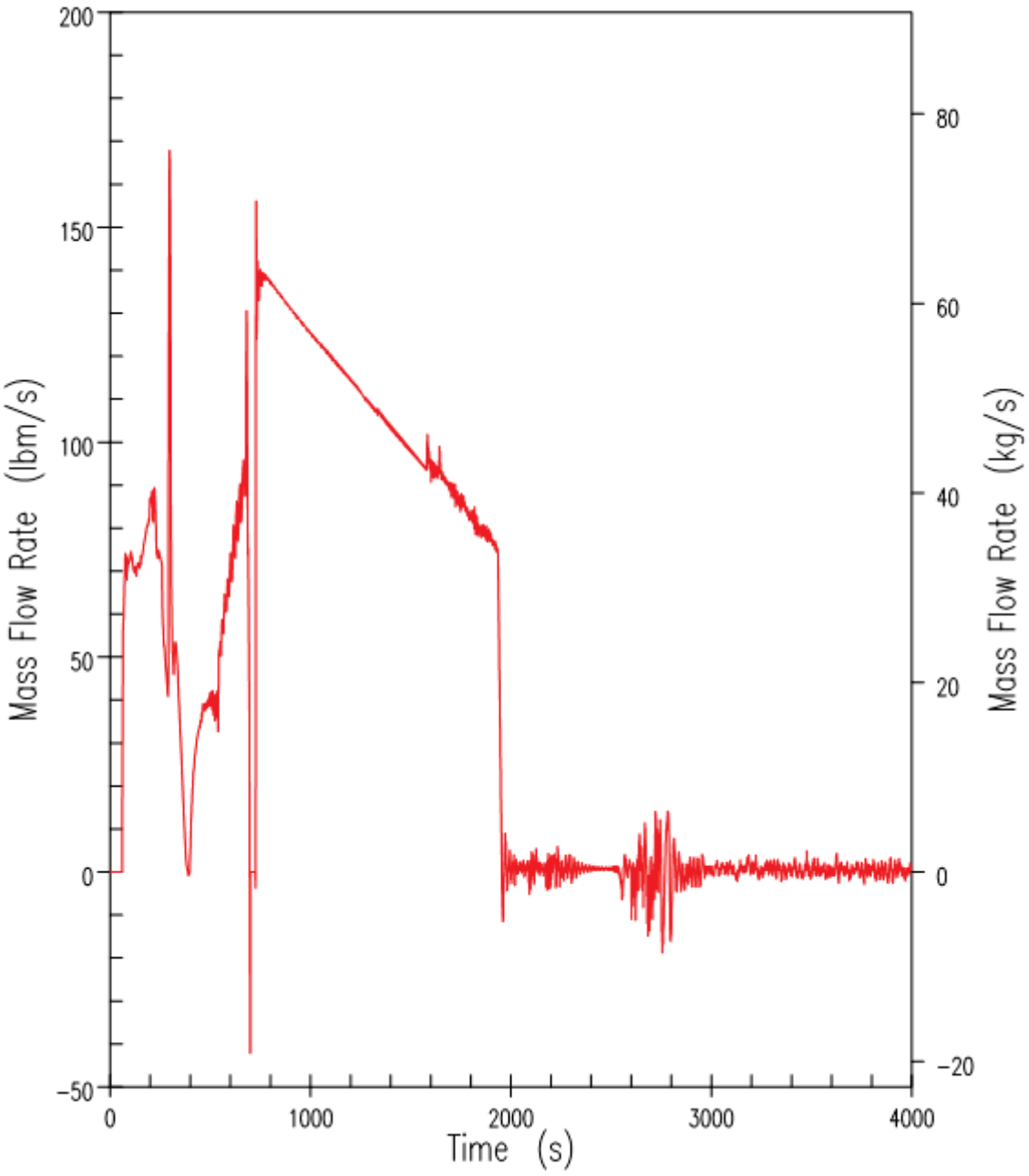


Figure 9.6.5-5. DBA Inadvertent ADS – CMT-1 Injection Rate

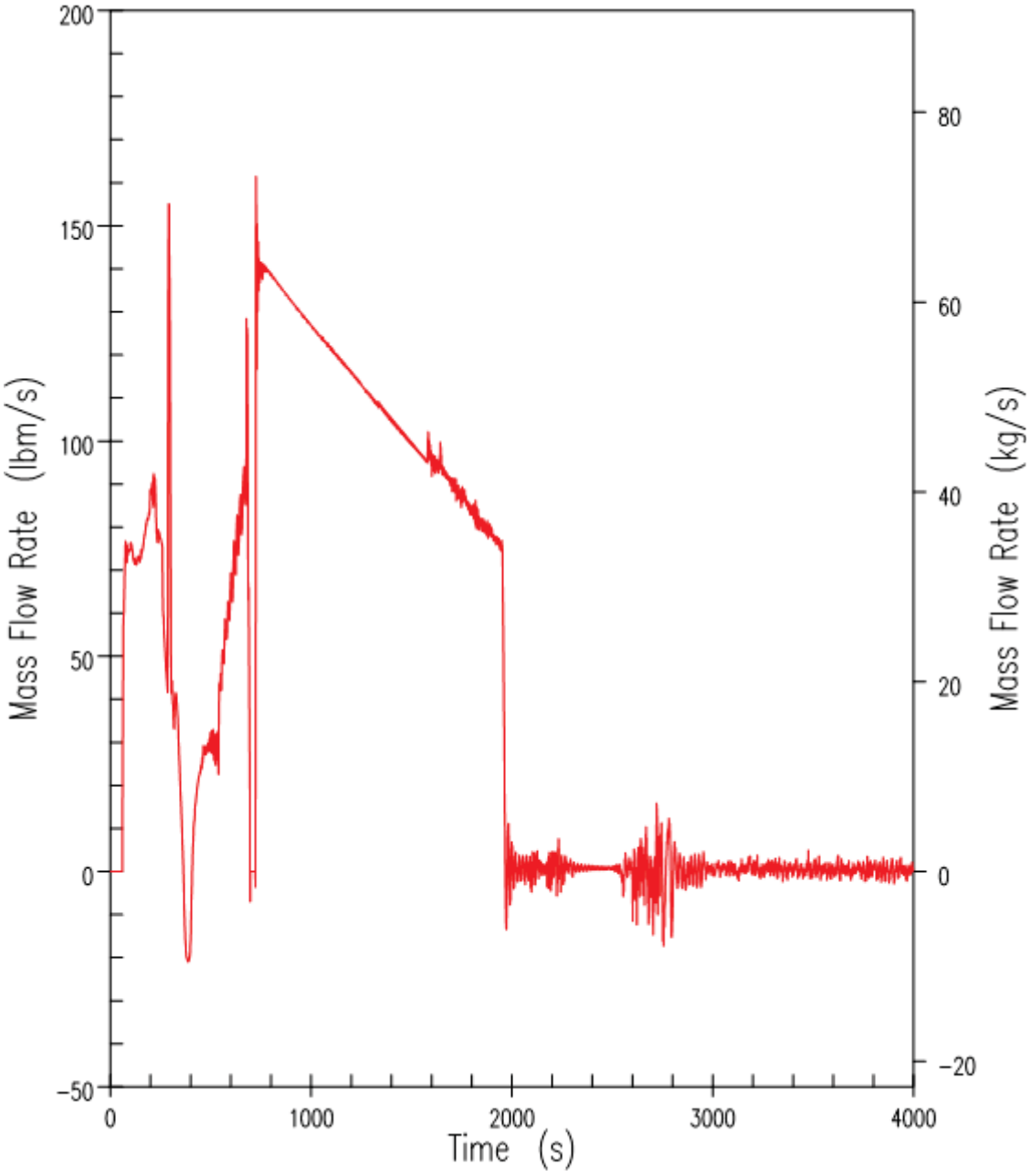


Figure 9.6.5-6. DBA Inadvertent ADS – CMT-2 Injection Rate

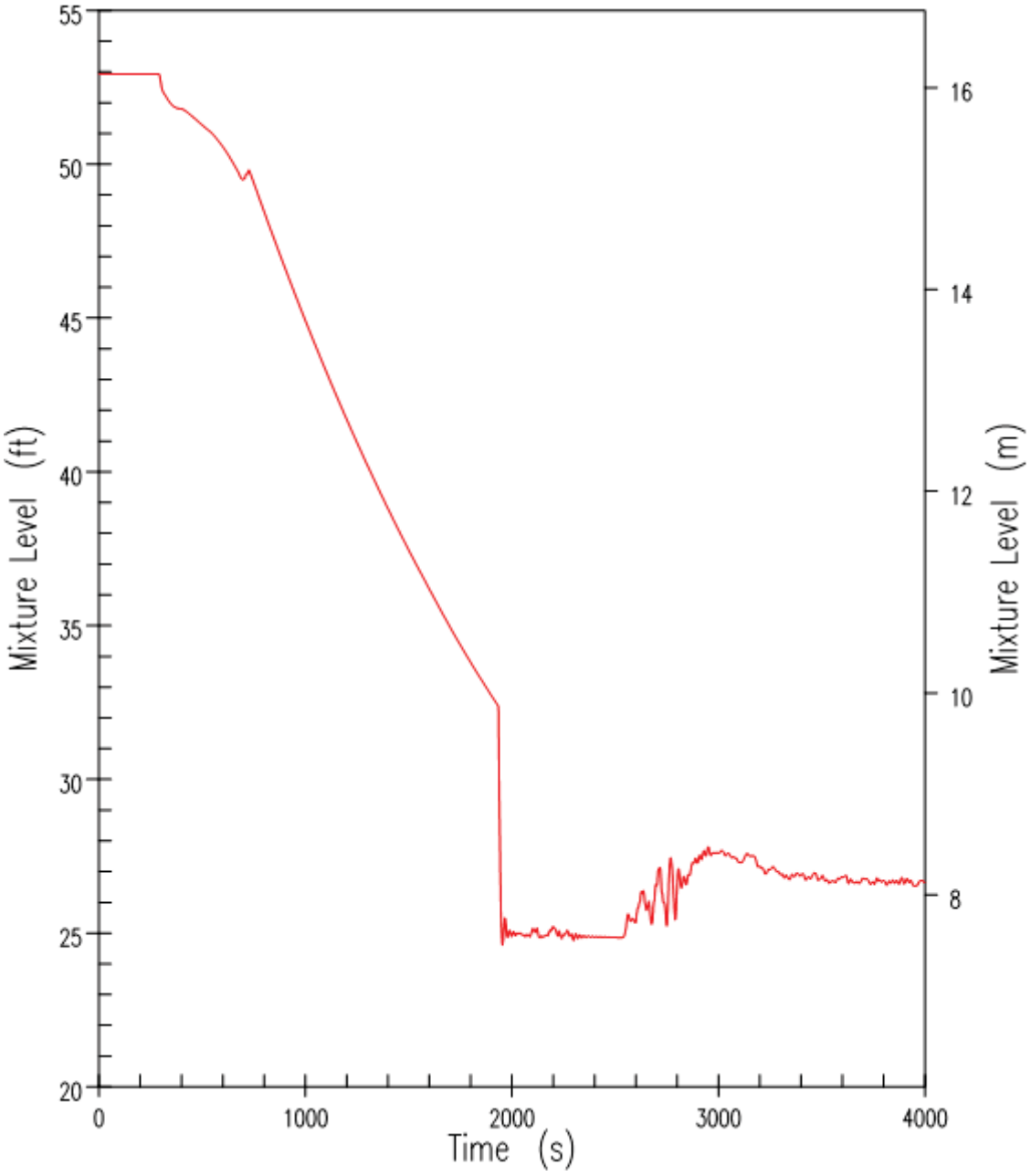


Figure 9.6.5-7. DBA Inadvertent ADS – CMT-1 Mixture Level

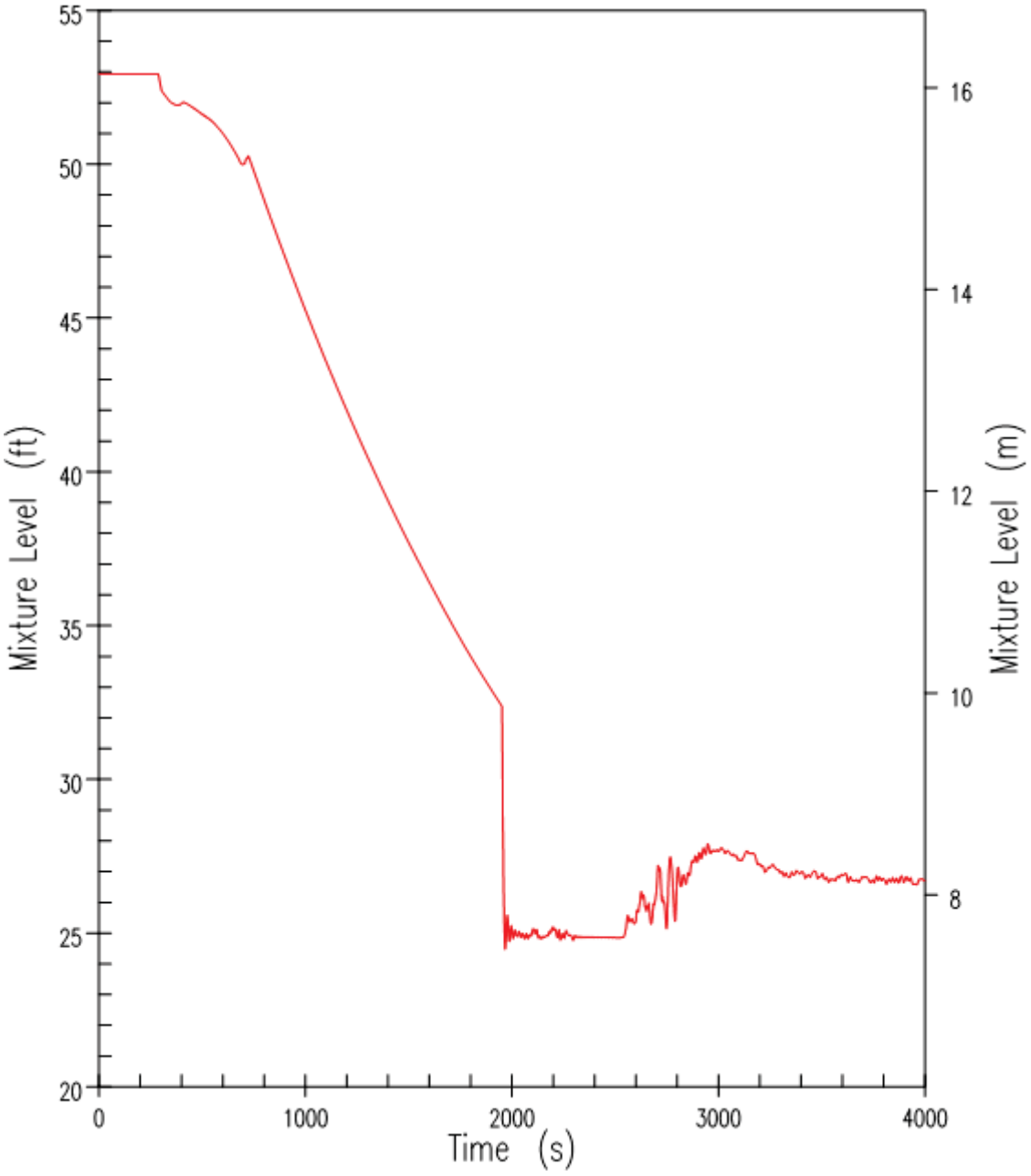


Figure 9.6.5-8. DBA Inadvertent ADS – CMT-2 Mixture Level

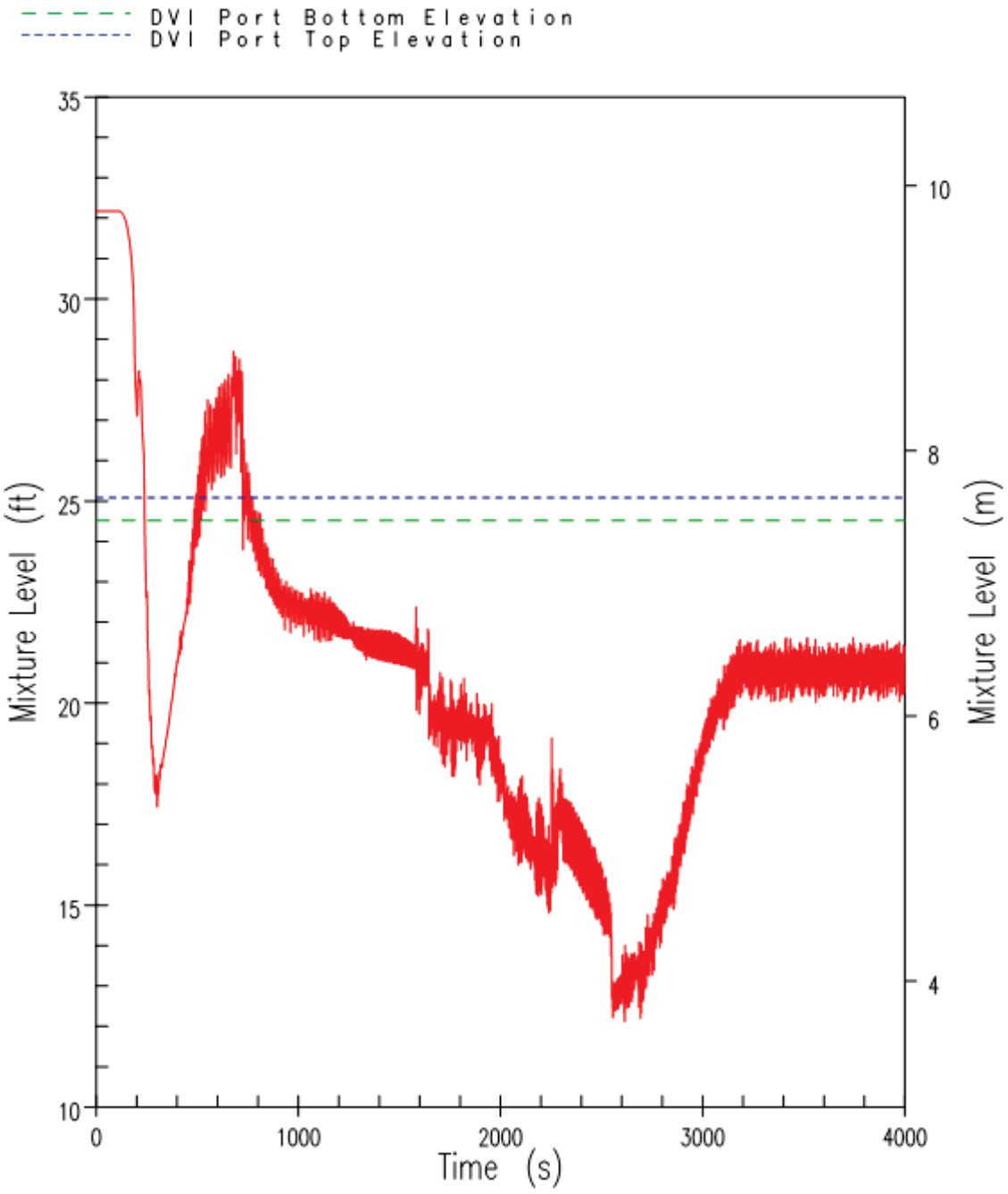


Figure 9.6.5-9. DBA Inadvertent ADS – Downcomer Mixture Level

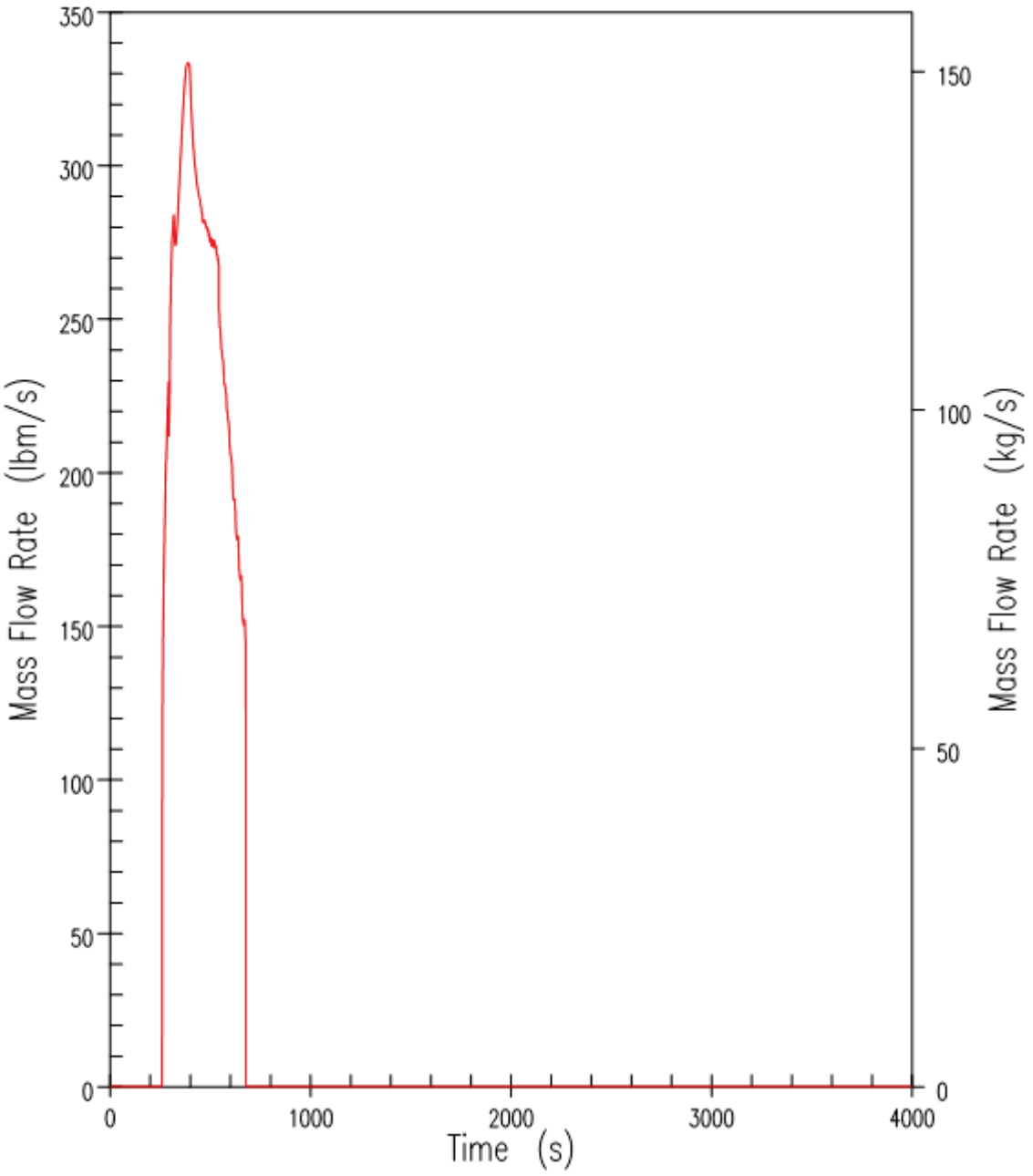


Figure 9.6.5-10. DBA Inadvertent ADS – Accumulator-1 Injection Rate

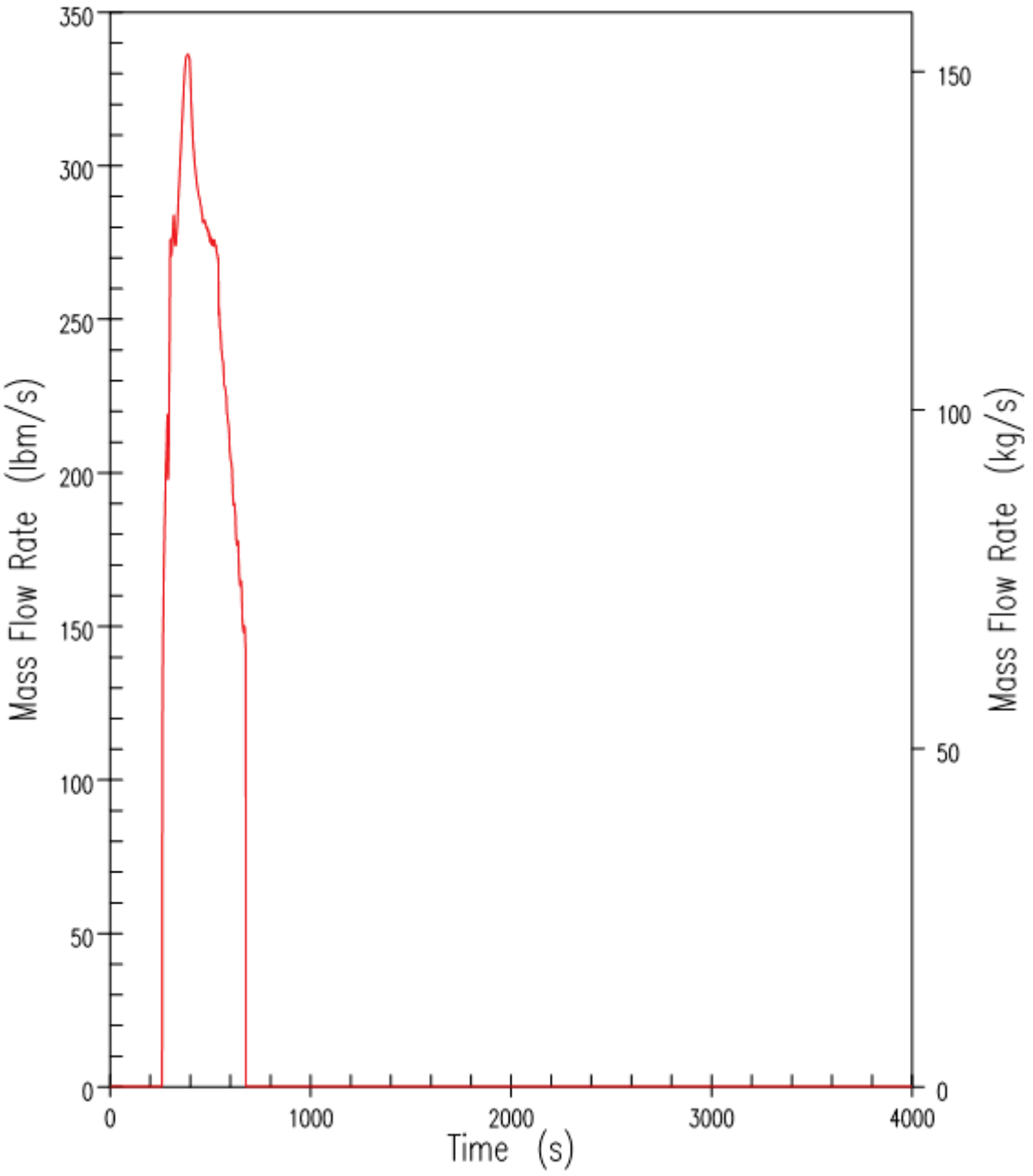


Figure 9.6.5-11. DBA Inadvertent ADS – Accumulator-2 Injection Rate

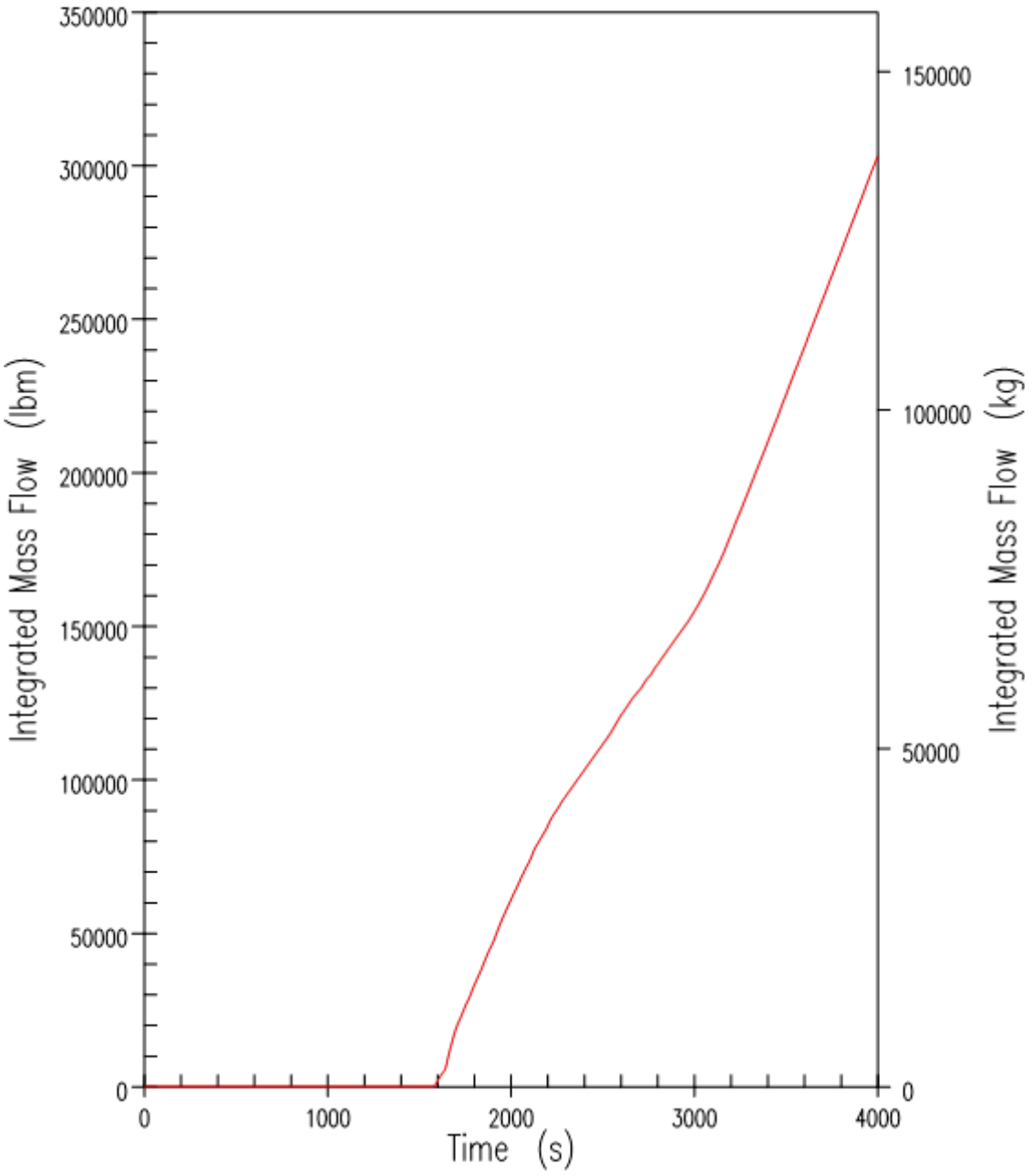


Figure 9.6.5-12(a). DBA Inadvertent ADS – ADS-4 Integrated Discharge

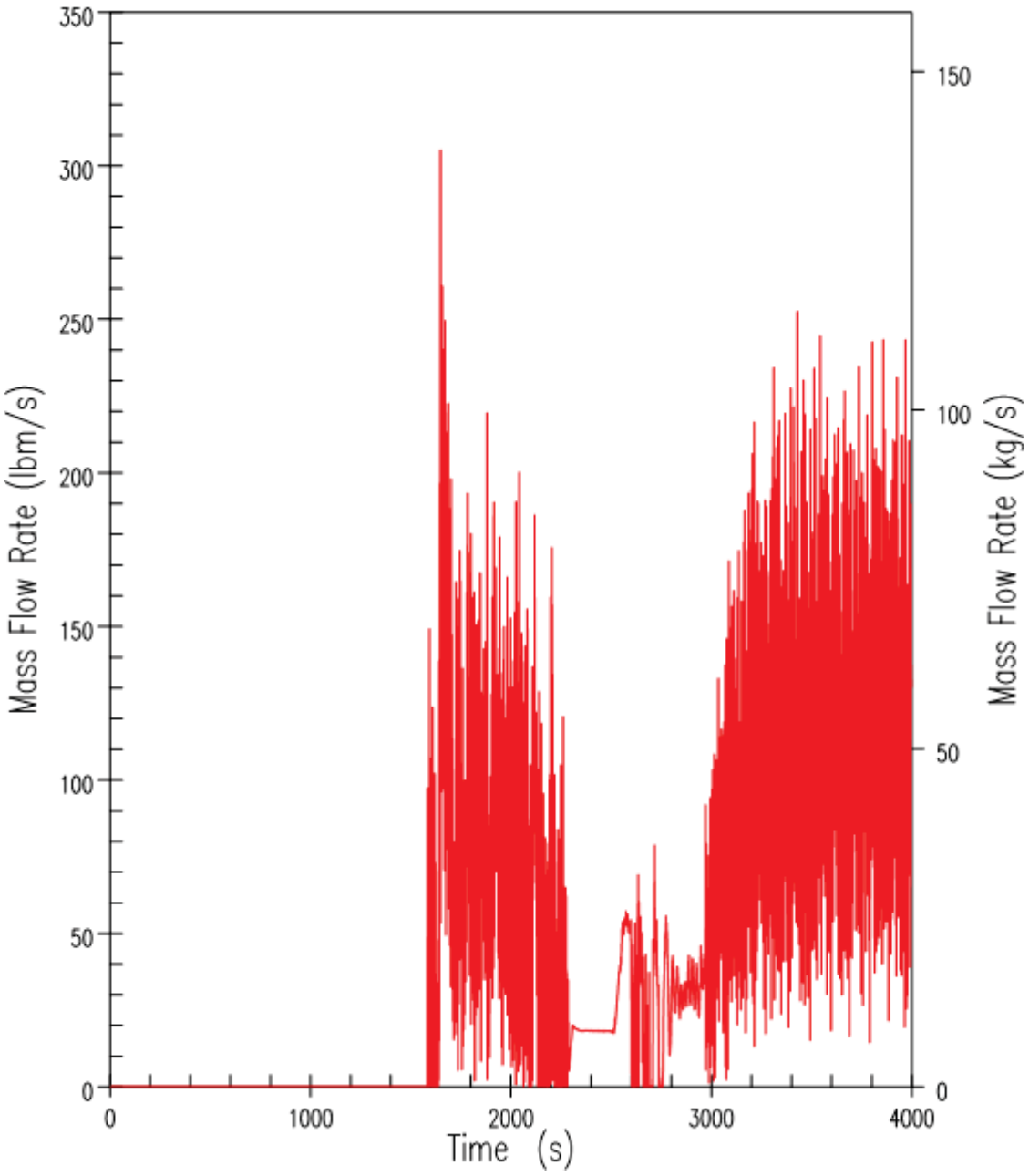


Figure 9.6.5-12(b). DBA Inadvertent ADS – ADS-4 Liquid Discharge

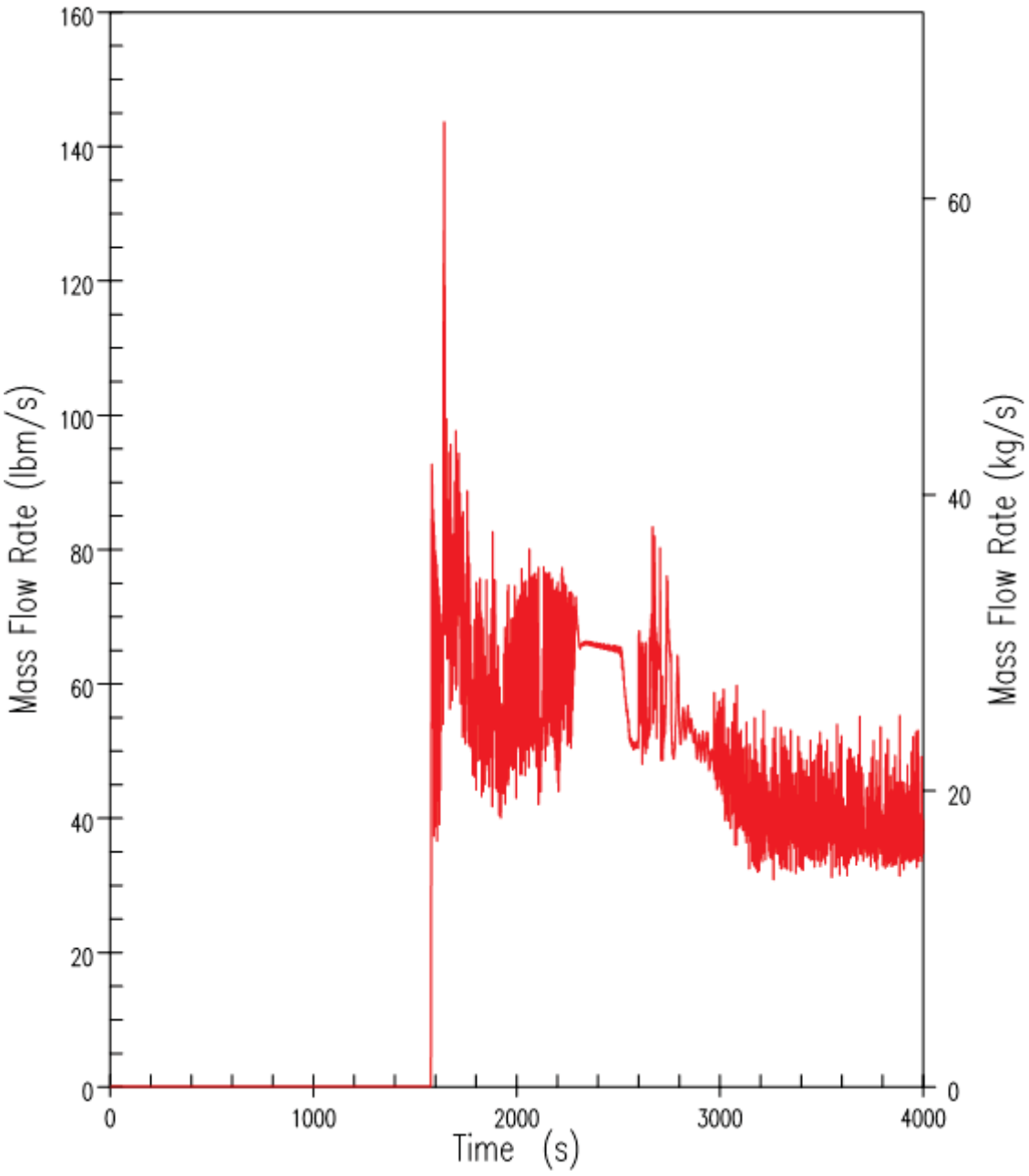


Figure 9.6.5-12(c). DBA Inadvertent ADS – ADS-4 Vapour Discharge

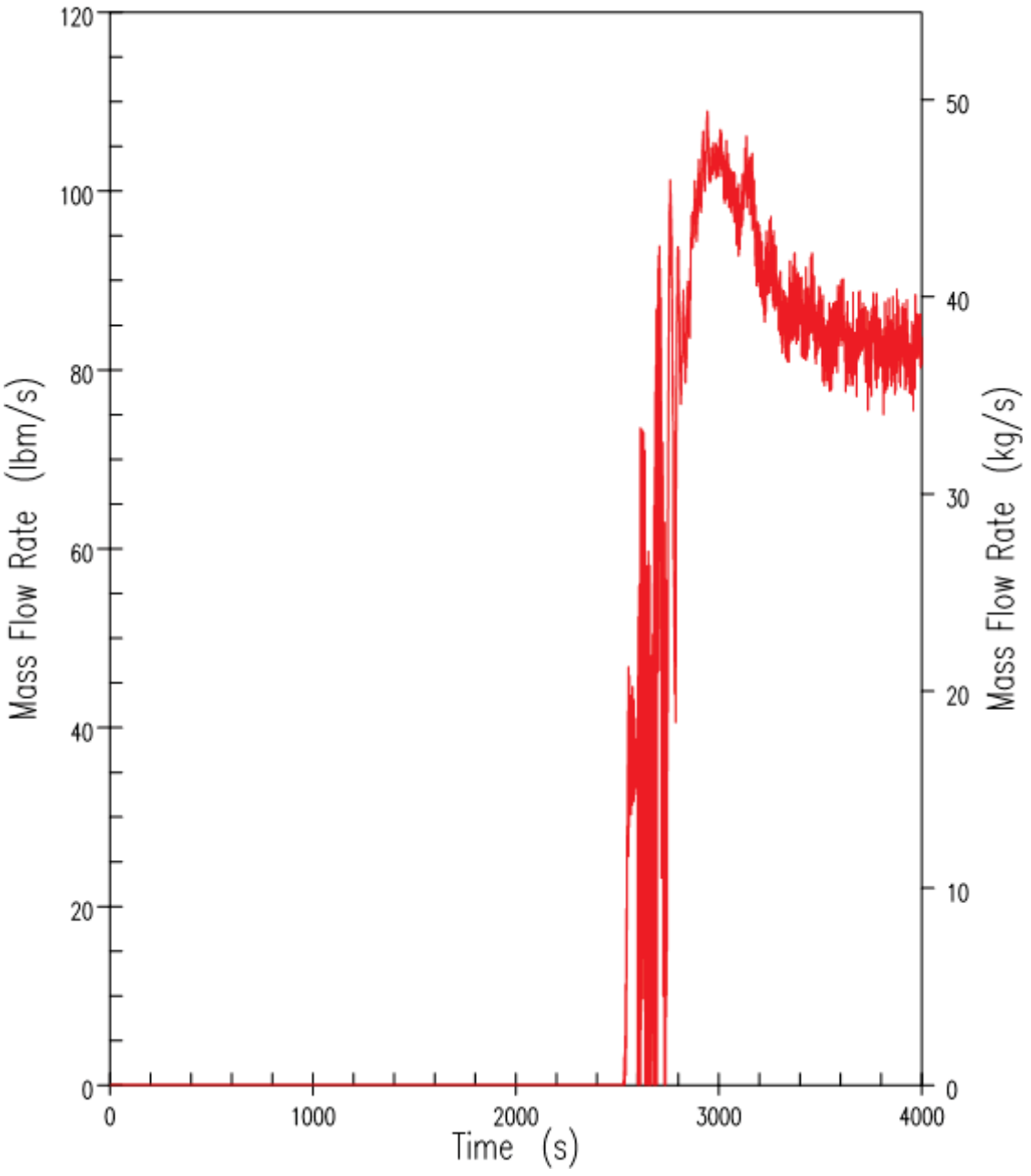


Figure 9.6.5-13. DBA Inadvertent ADS – IRWST-1 Injection Rate

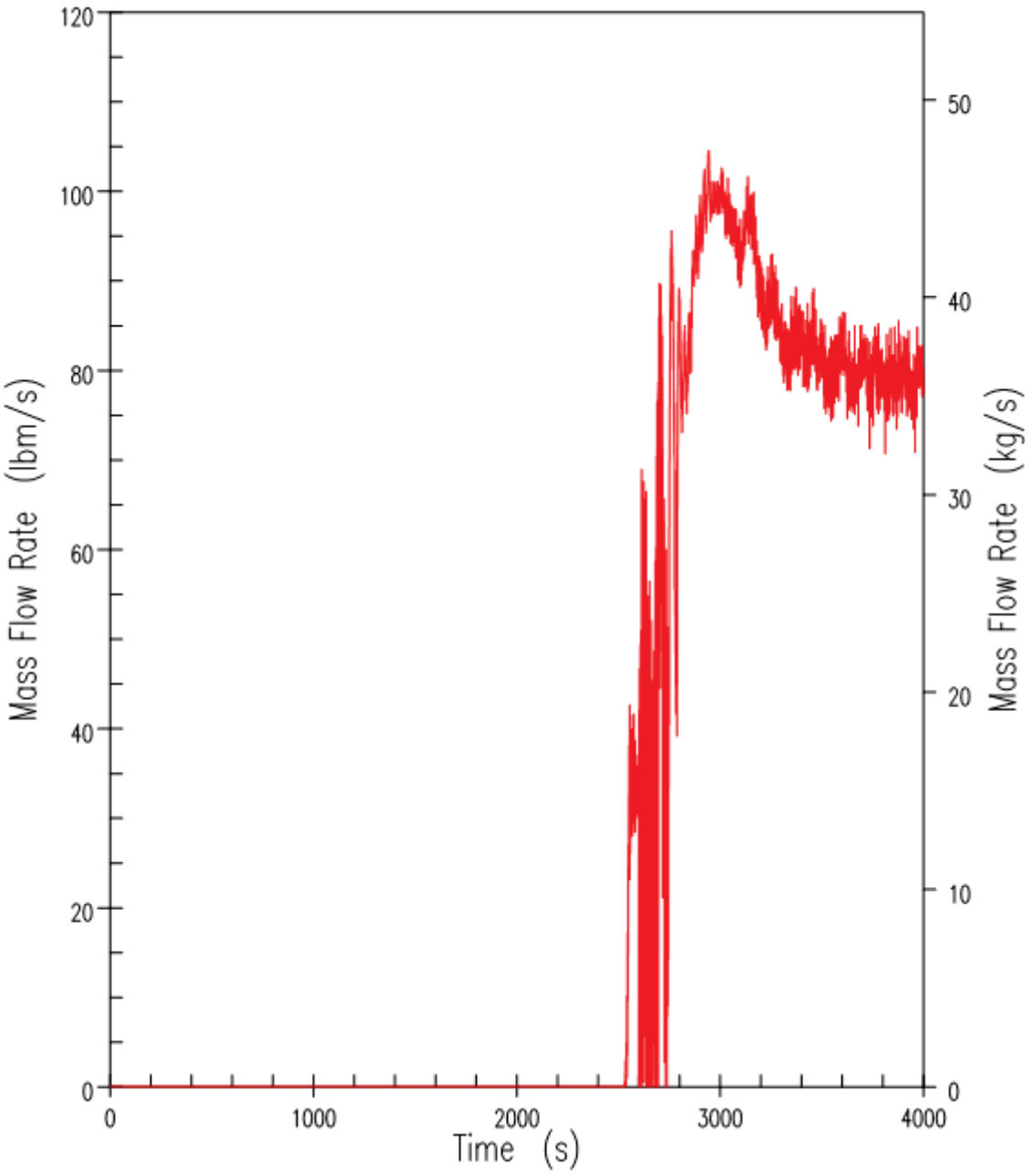


Figure 9.6.5-14. DBA Inadvertent ADS – IRWST-2 Injection Rate

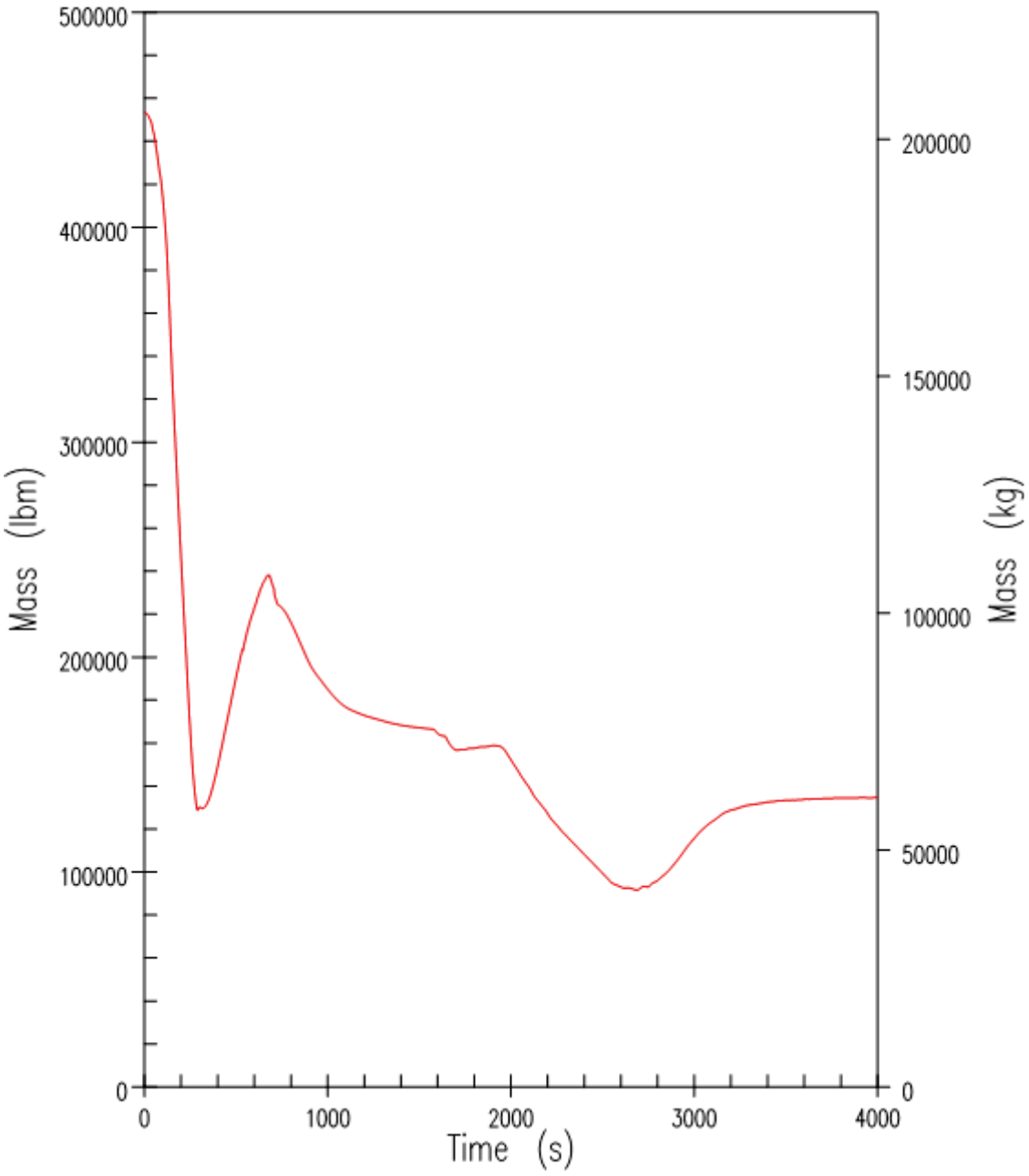


Figure 9.6.5-15(a). DBA Inadvertent ADS – RCS System Inventory

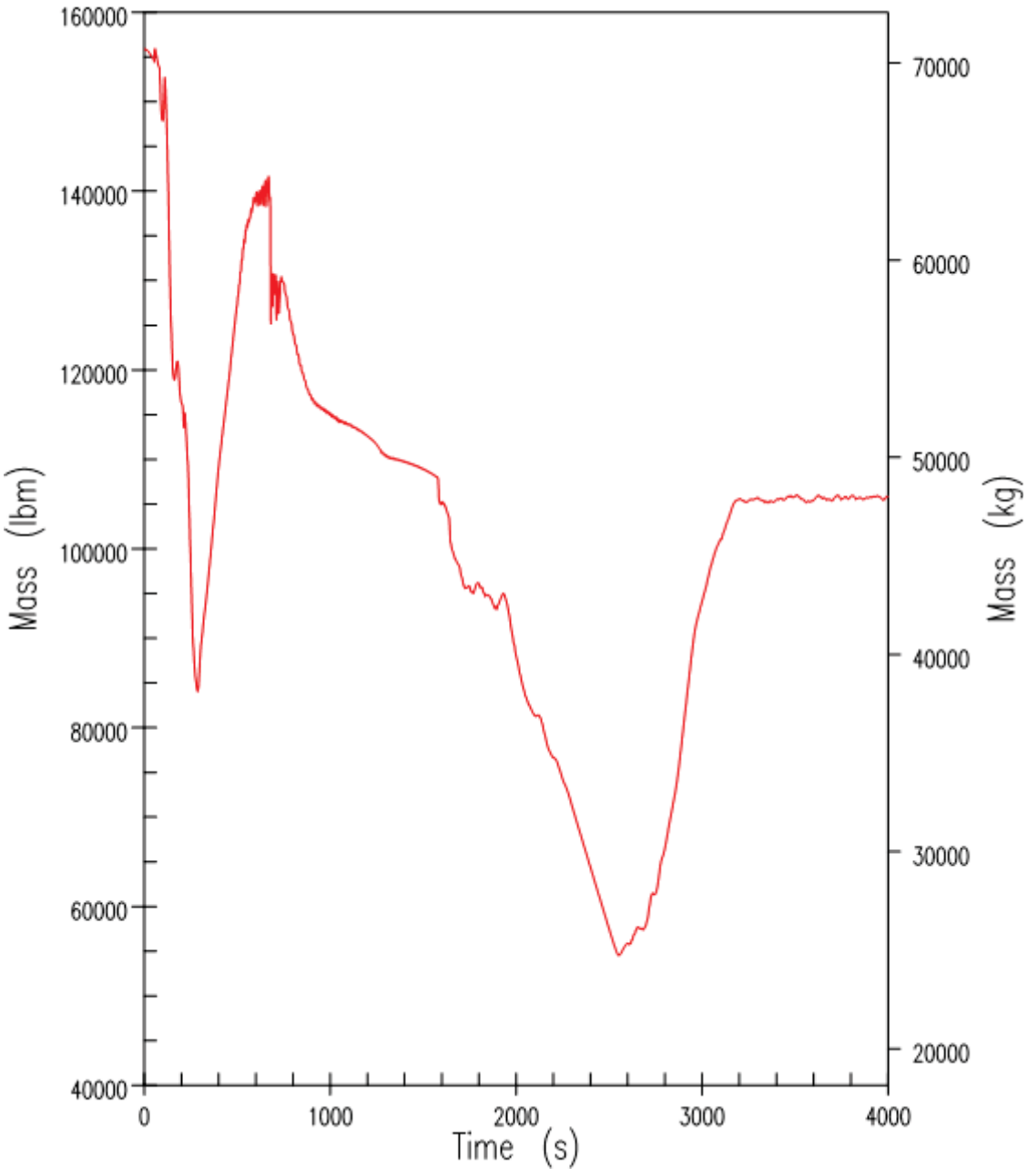


Figure 9.6.5-15(b). DBA Inadvertent ADS – Reactor Vessel Mixture Inventory

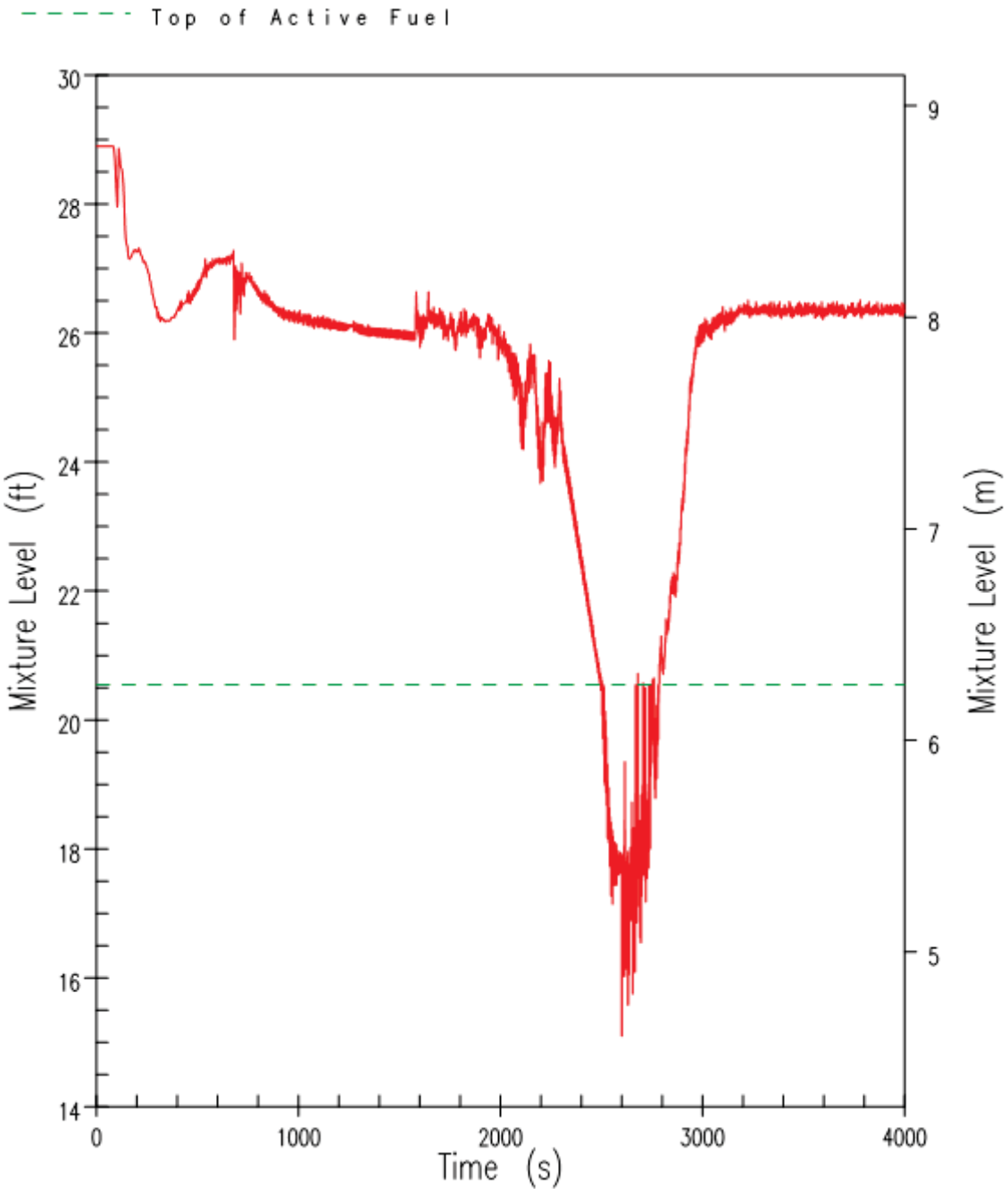


Figure 9.6.5-16(a). DBA Inadvertent ADS – Core/Upper Plenum Mixture Level

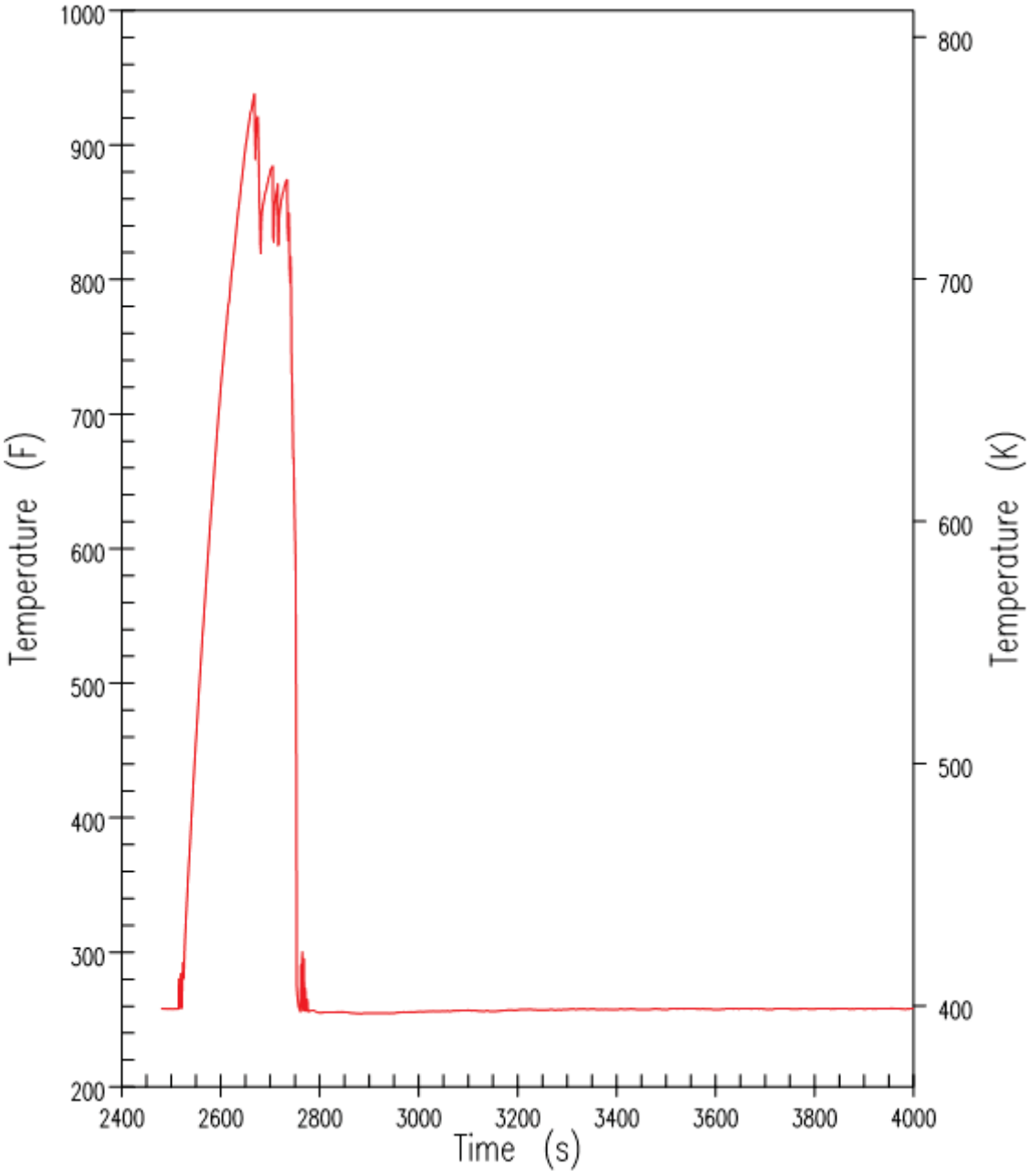


Figure 9.6.5-16(b). DBA Inadvertent ADS – Peak Cladding Temperature

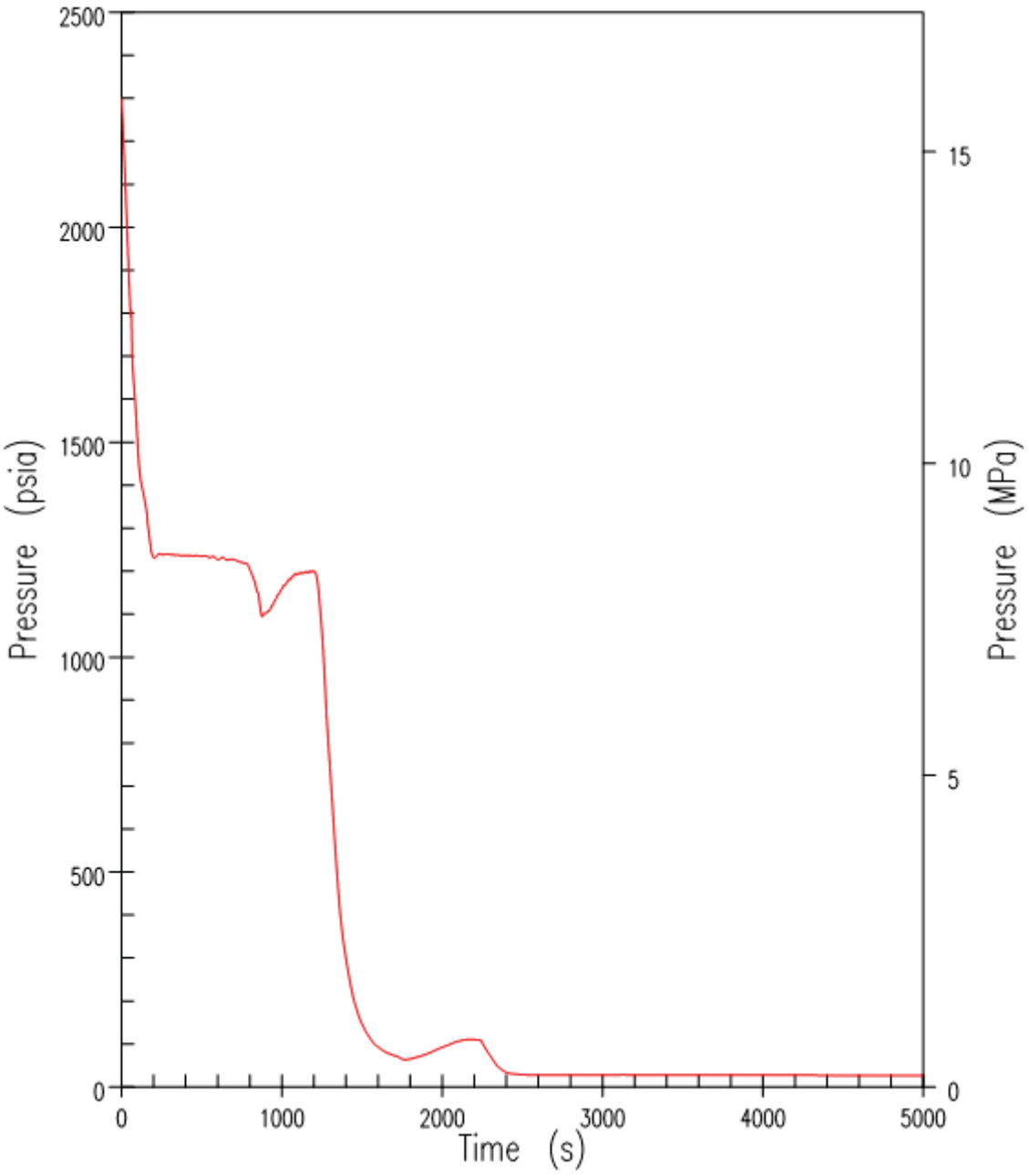


Figure 9.6.5-17(a). DBA 50.8 mm (2-Inch) Cold Leg Break – RCS Pressure

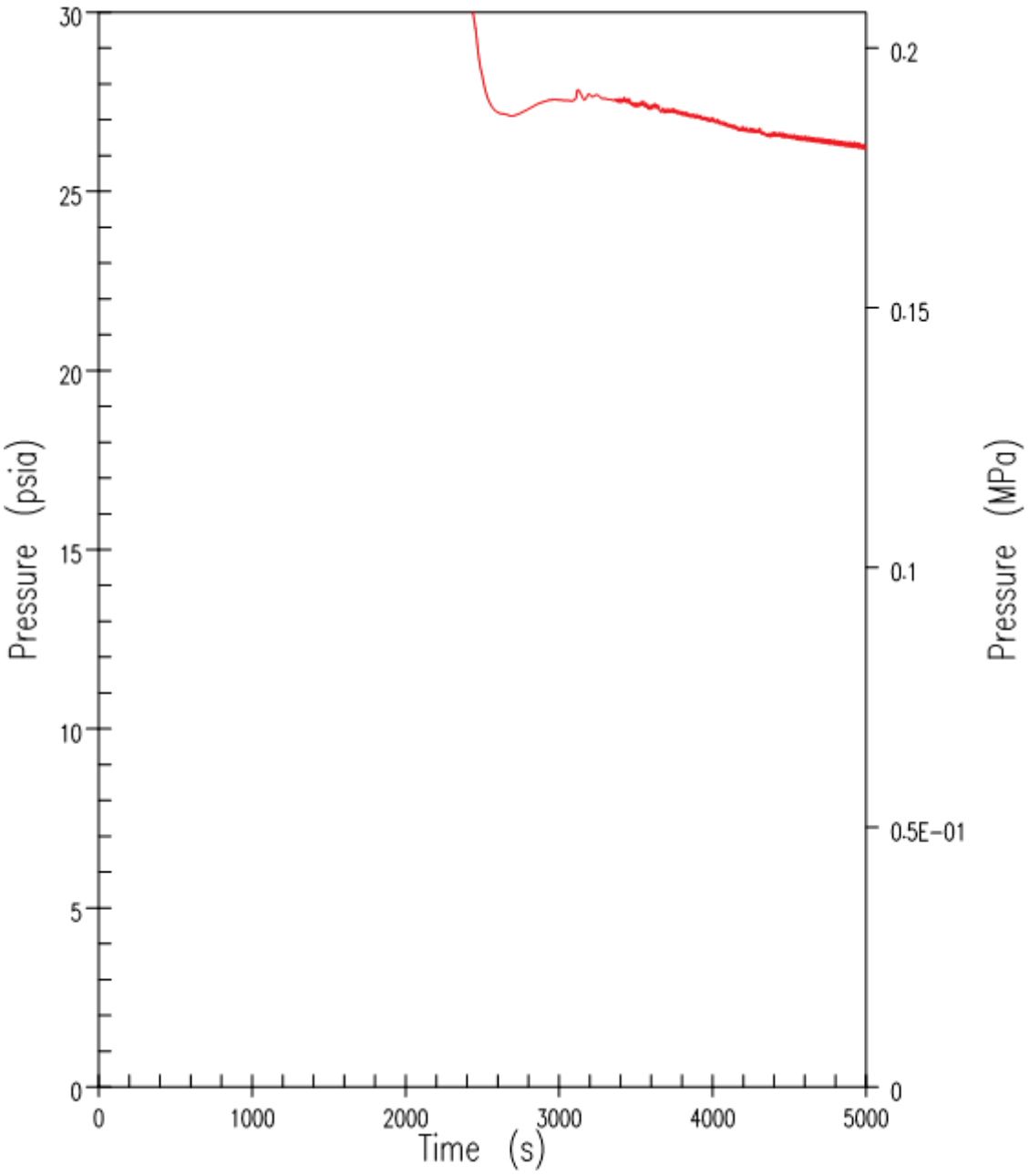


Figure 9.6.5-17(b). DBA 50.8 mm (2-Inch) Cold Leg Break – RCS Pressure (Zoomed)

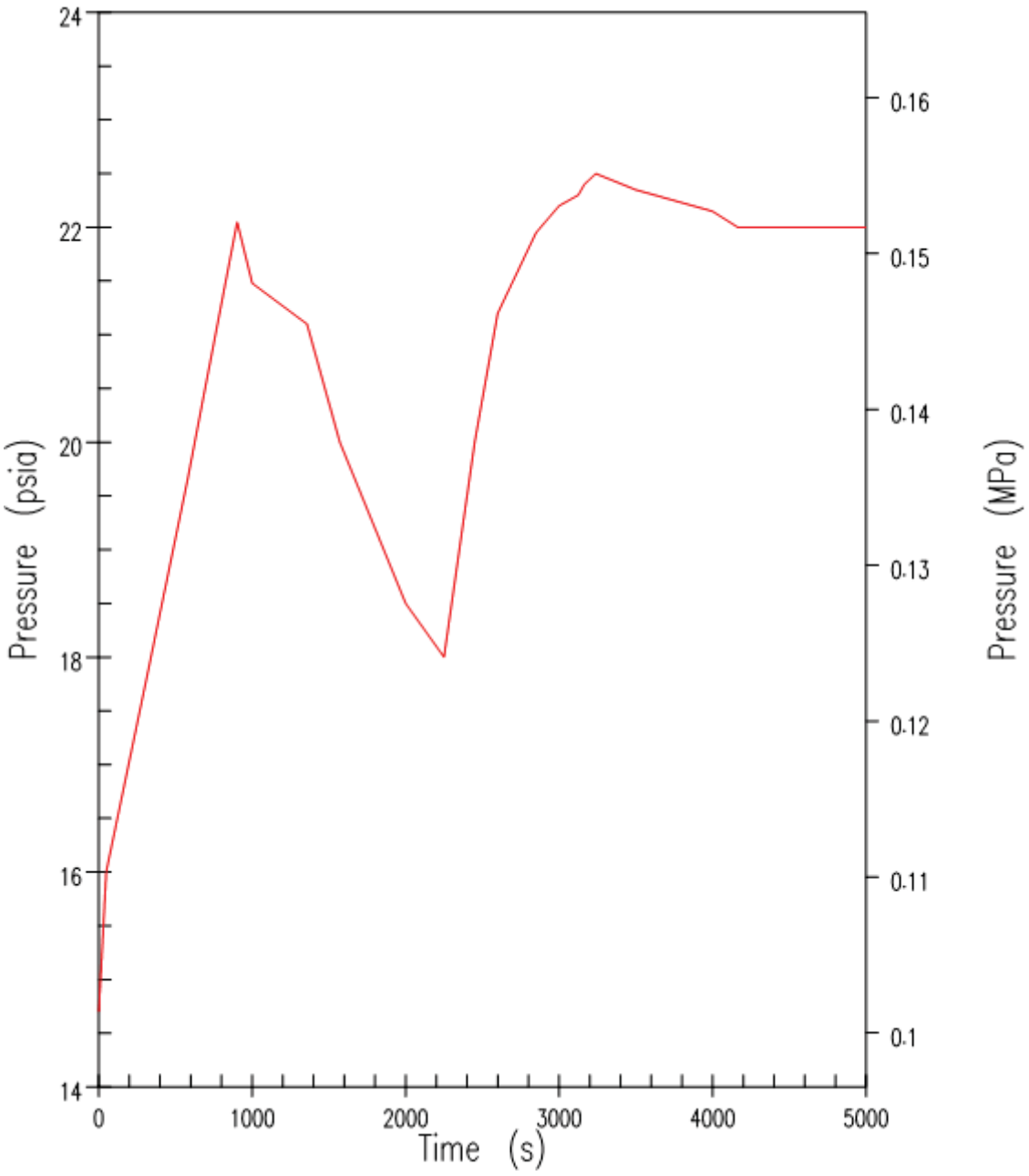


Figure 9.6.5-17(c). DBA 50.8 mm (2-Inch) Cold Leg Break – Containment Pressure

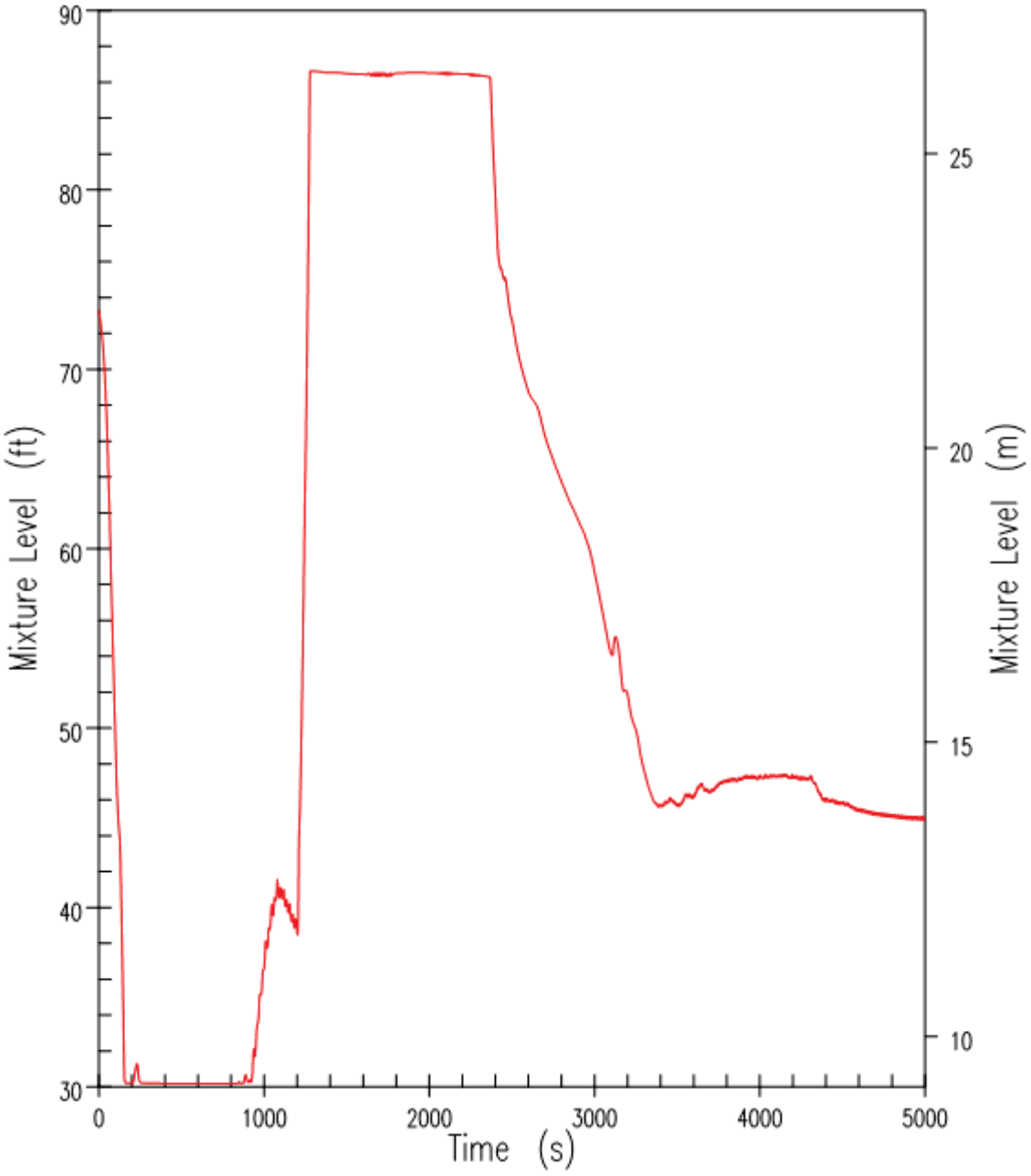


Figure 9.6.5-18. DBA 50.8 mm (2-Inch) Cold Leg Break – Pressuriser Mixture Level

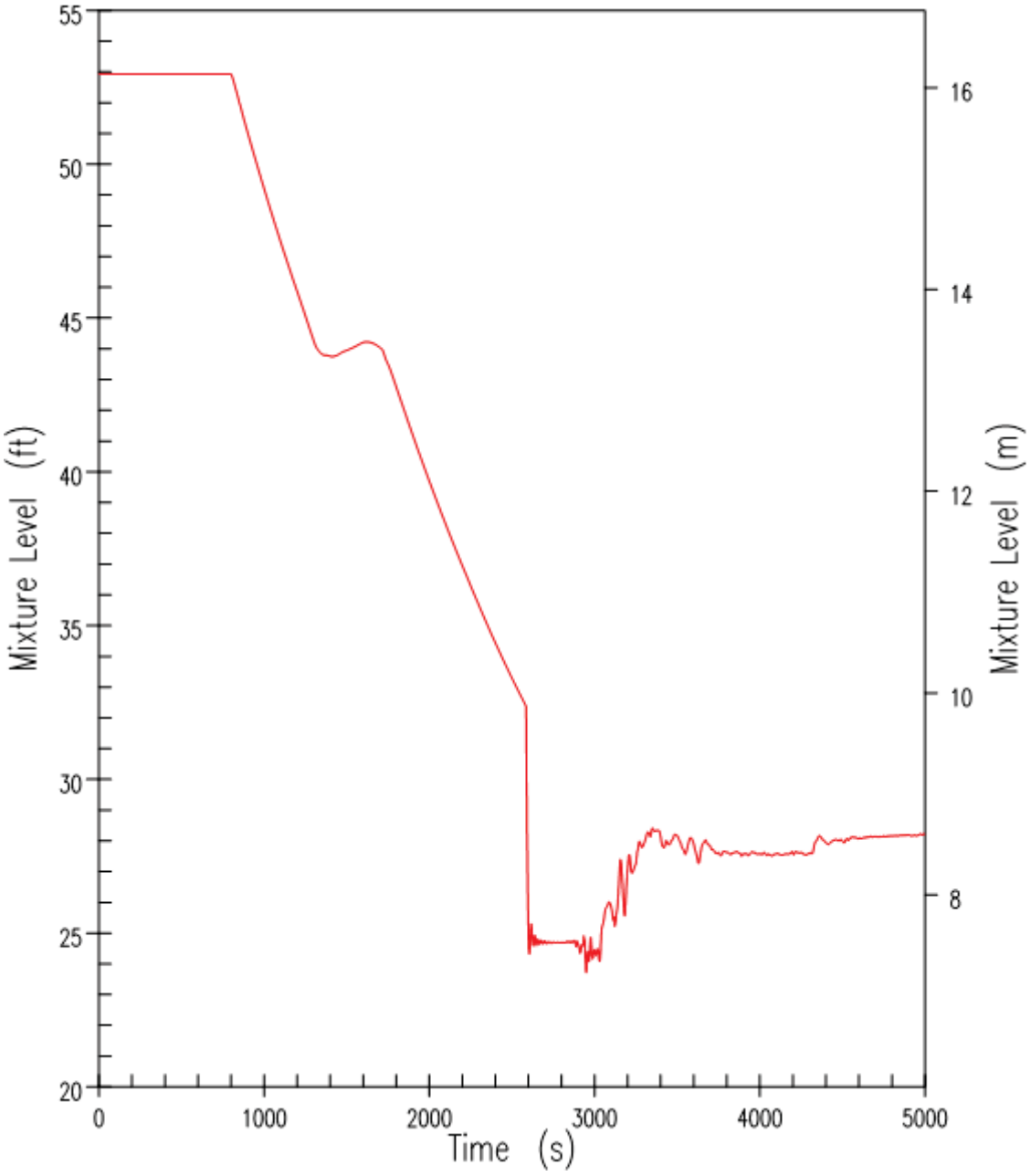


Figure 9.6.5-19. DBA 50.8 mm (2-Inch) Cold Leg Break – CMT-1 Mixture Level

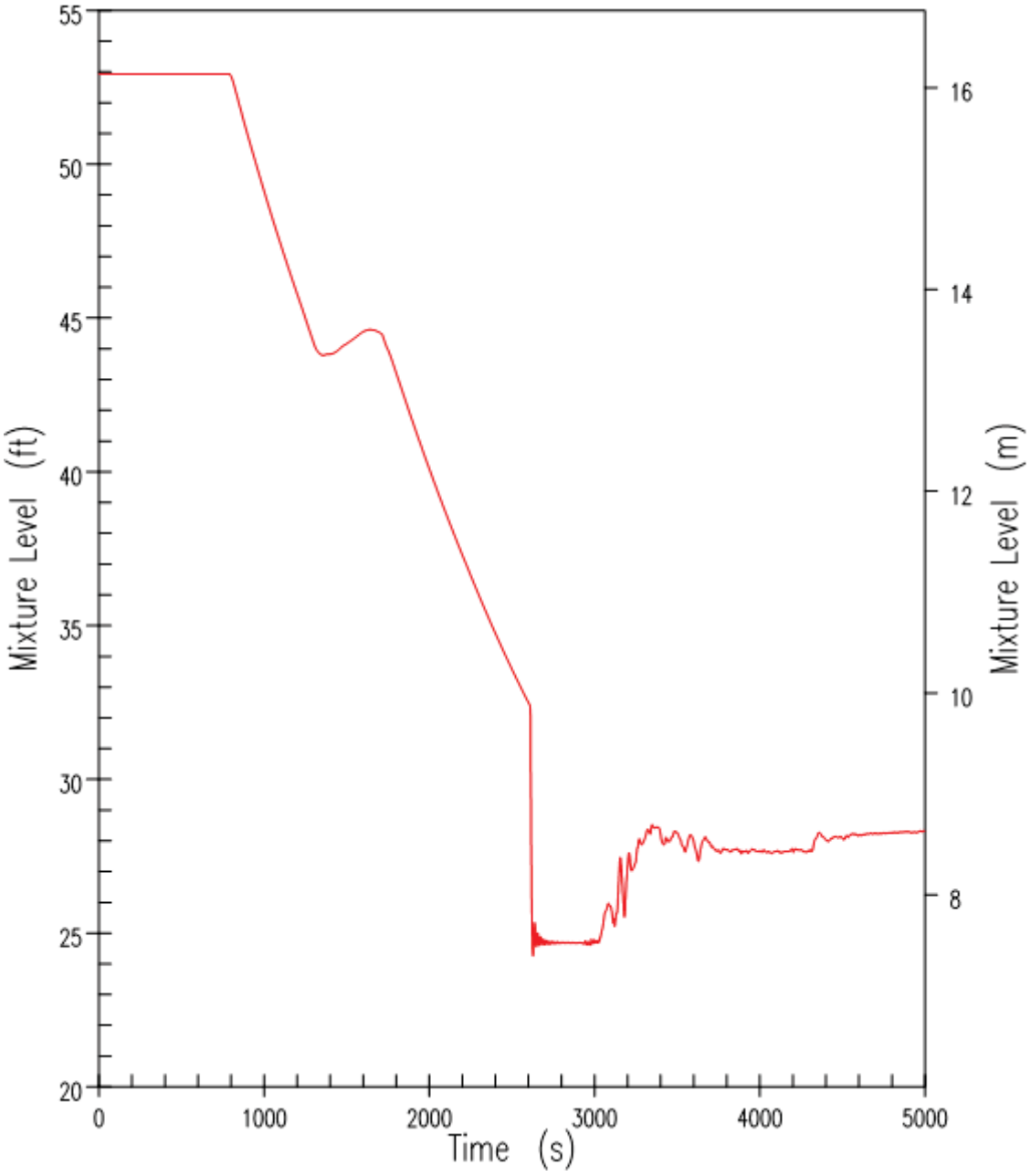


Figure 9.6.5-20. DBA 50.8 mm (2-Inch) Cold Leg Break – CMT-2 Mixture Level

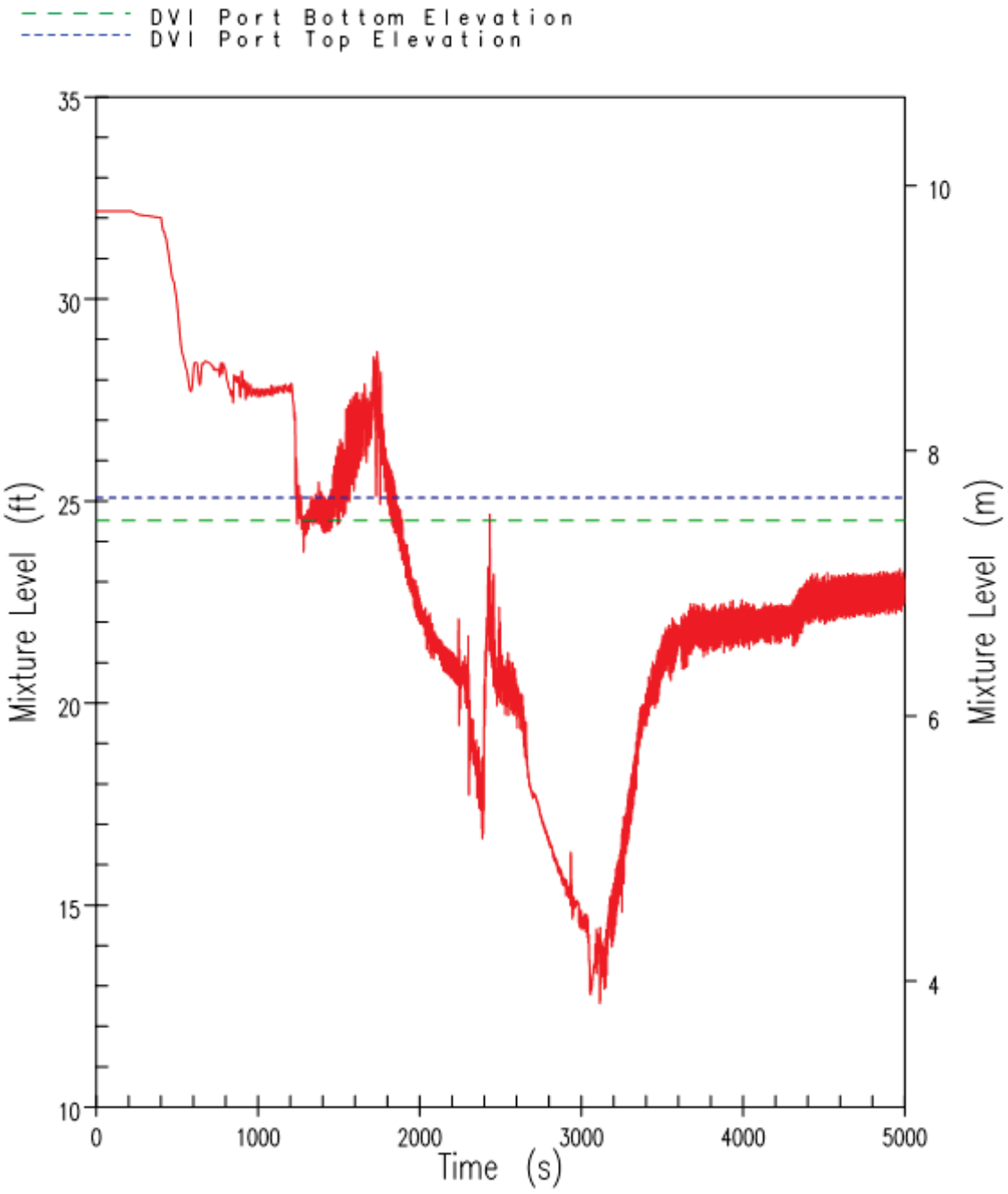


Figure 9.6.5-21. DBA 50.8 mm (2-Inch) Cold Leg Break – Downcomer Mixture Level

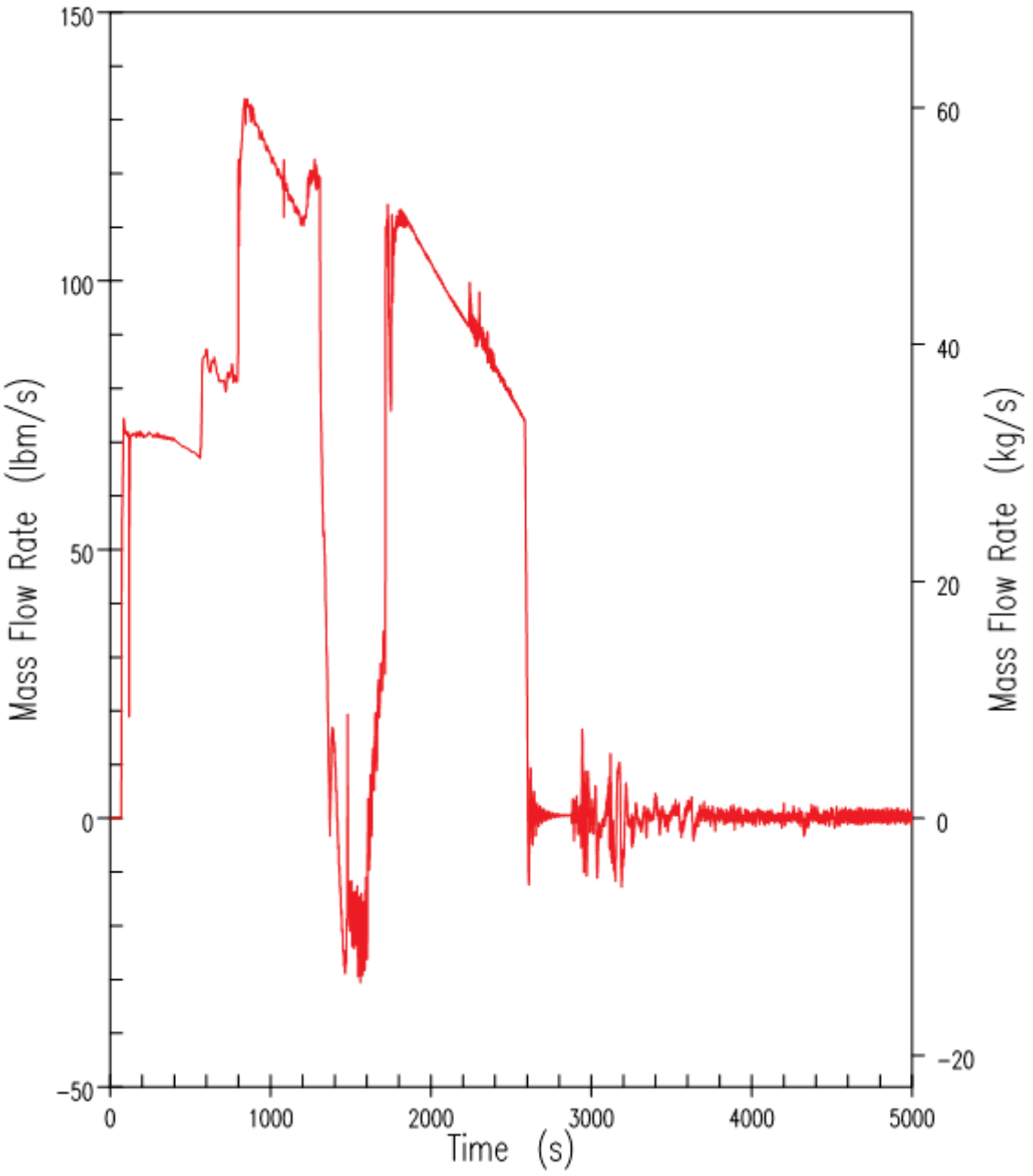


Figure 9.6.5-22. DBA 50.8 mm (2-Inch) Cold Leg Break – CMT-1 Injection Rate

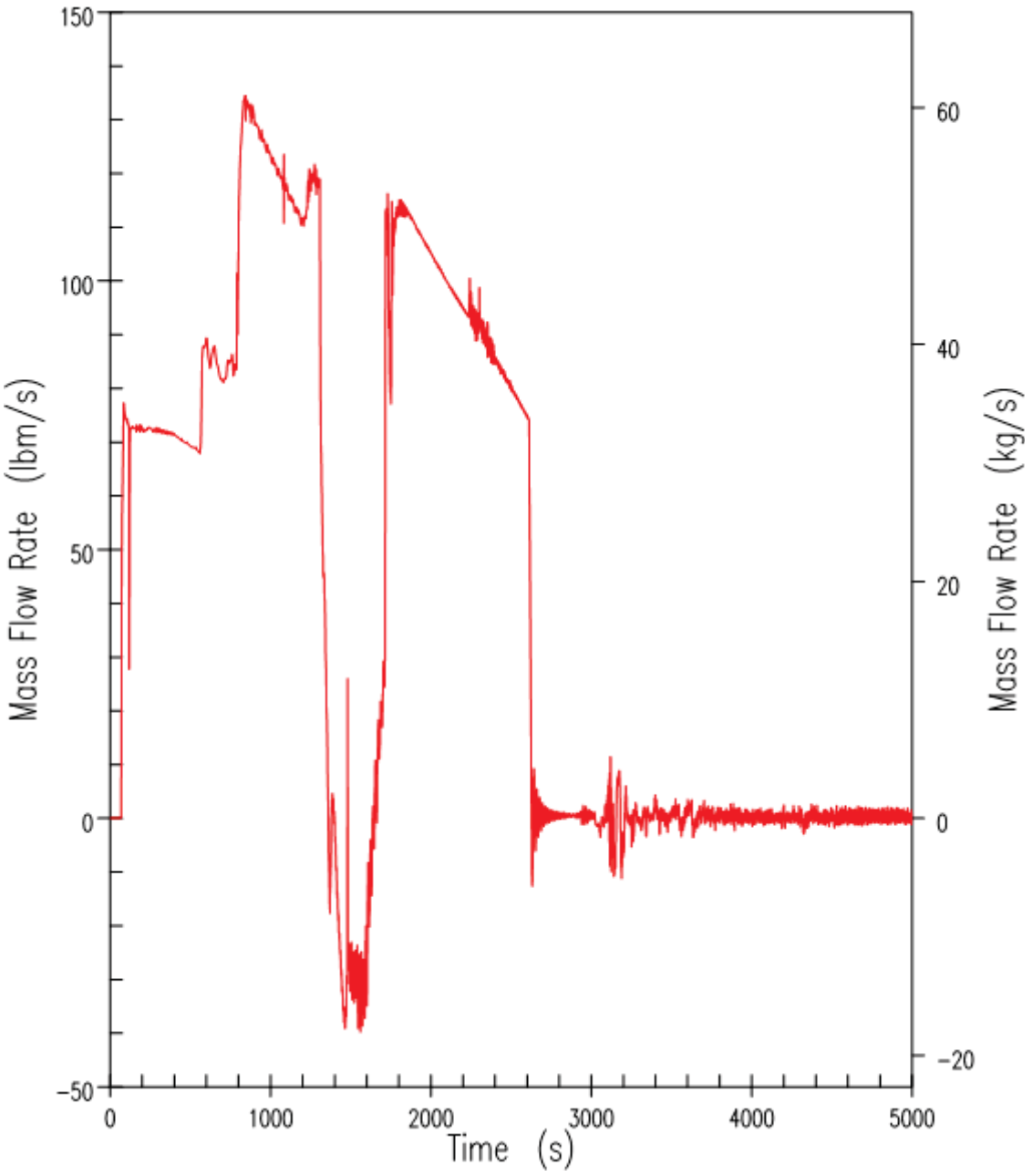


Figure 9.6.5-23. DBA 50.8 mm (2-Inch) Cold Leg Break – CMT-2 Injection Rate

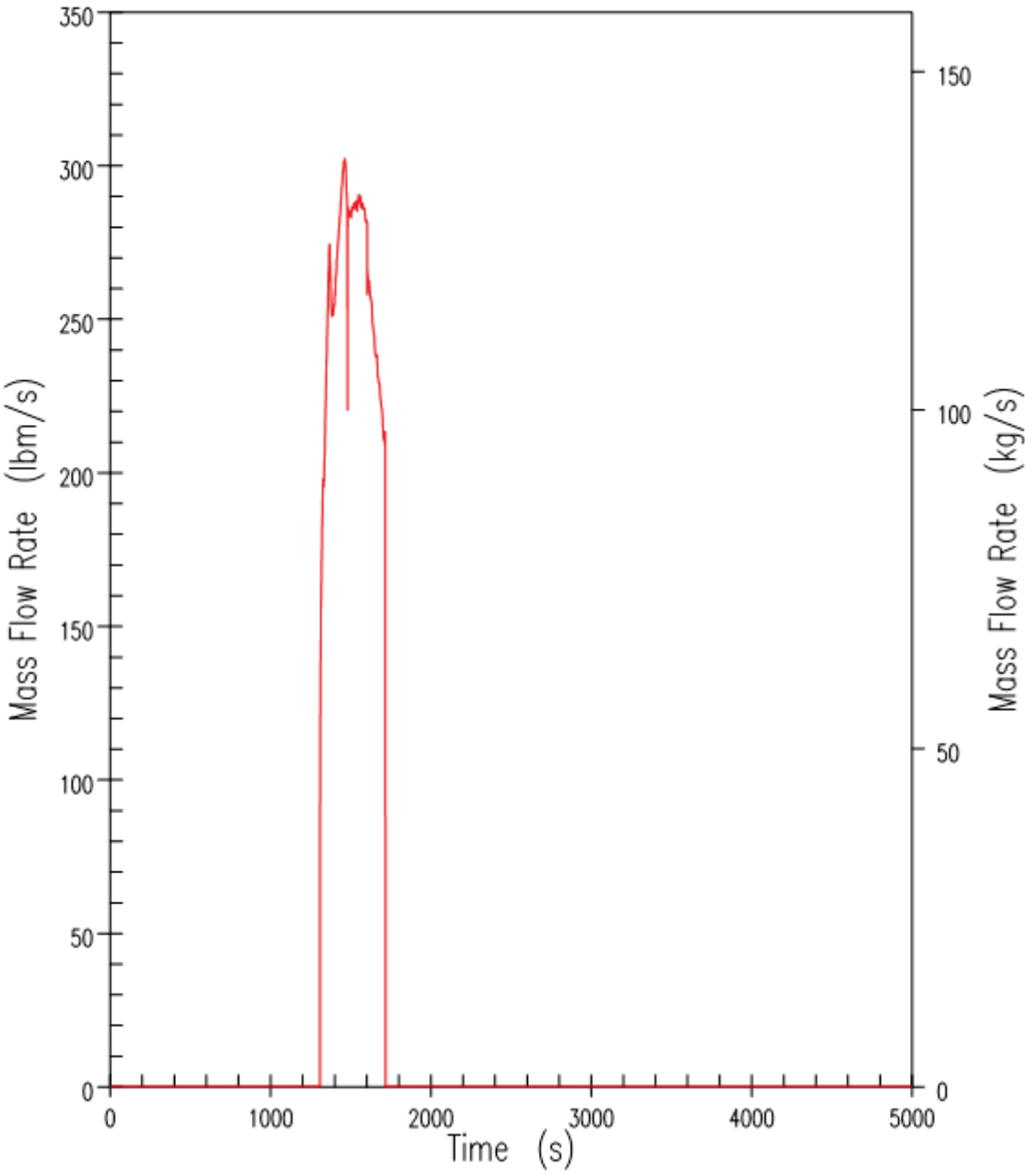


Figure 9.6.5-24. DBA 50.8 mm (2-Inch) Cold Leg Break – Accumulator-1 Injection Rate

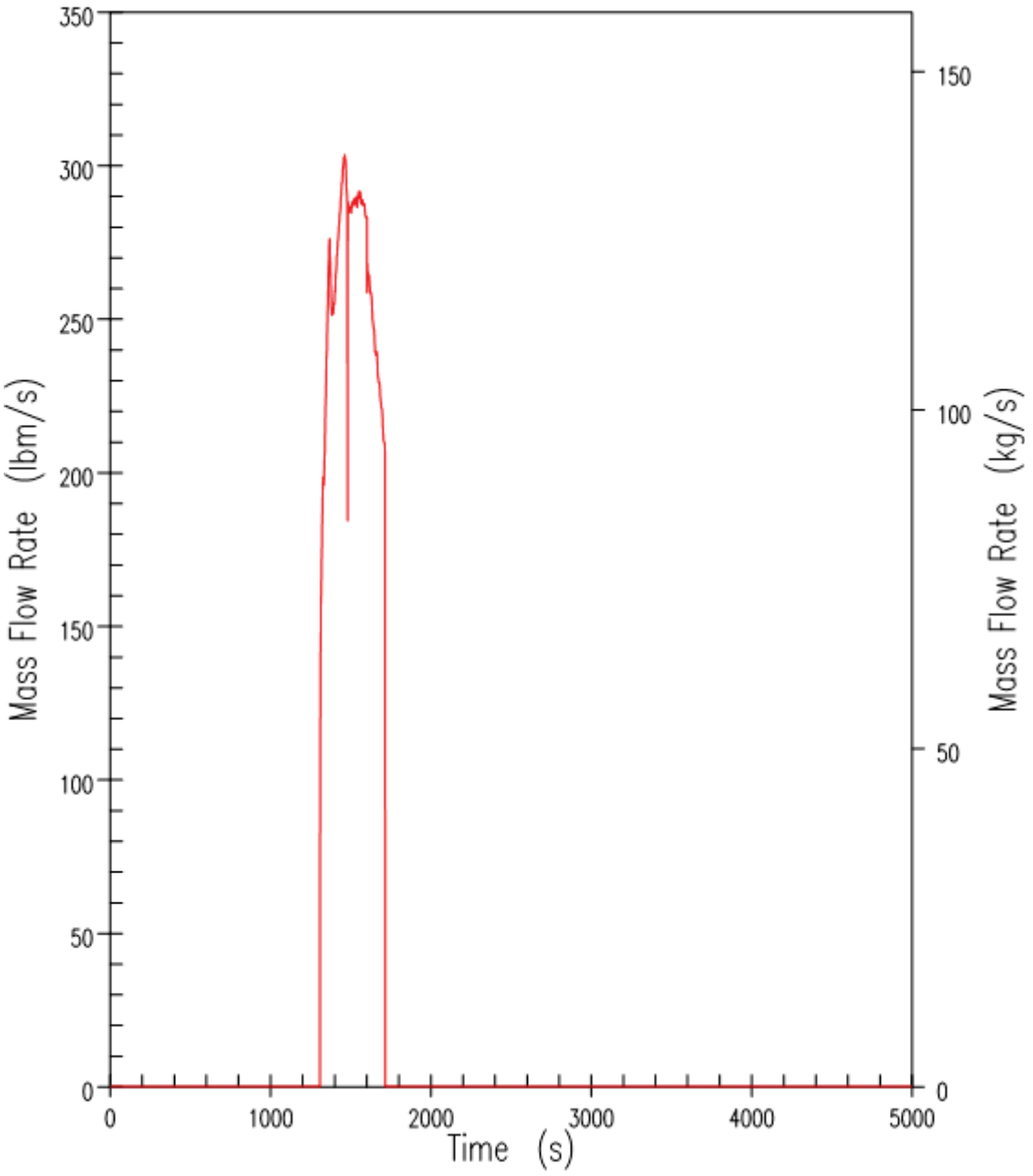


Figure 9.6.5-25. DBA 50.8 mm (2-Inch) Cold Leg Break – Accumulator-2 Injection Rate

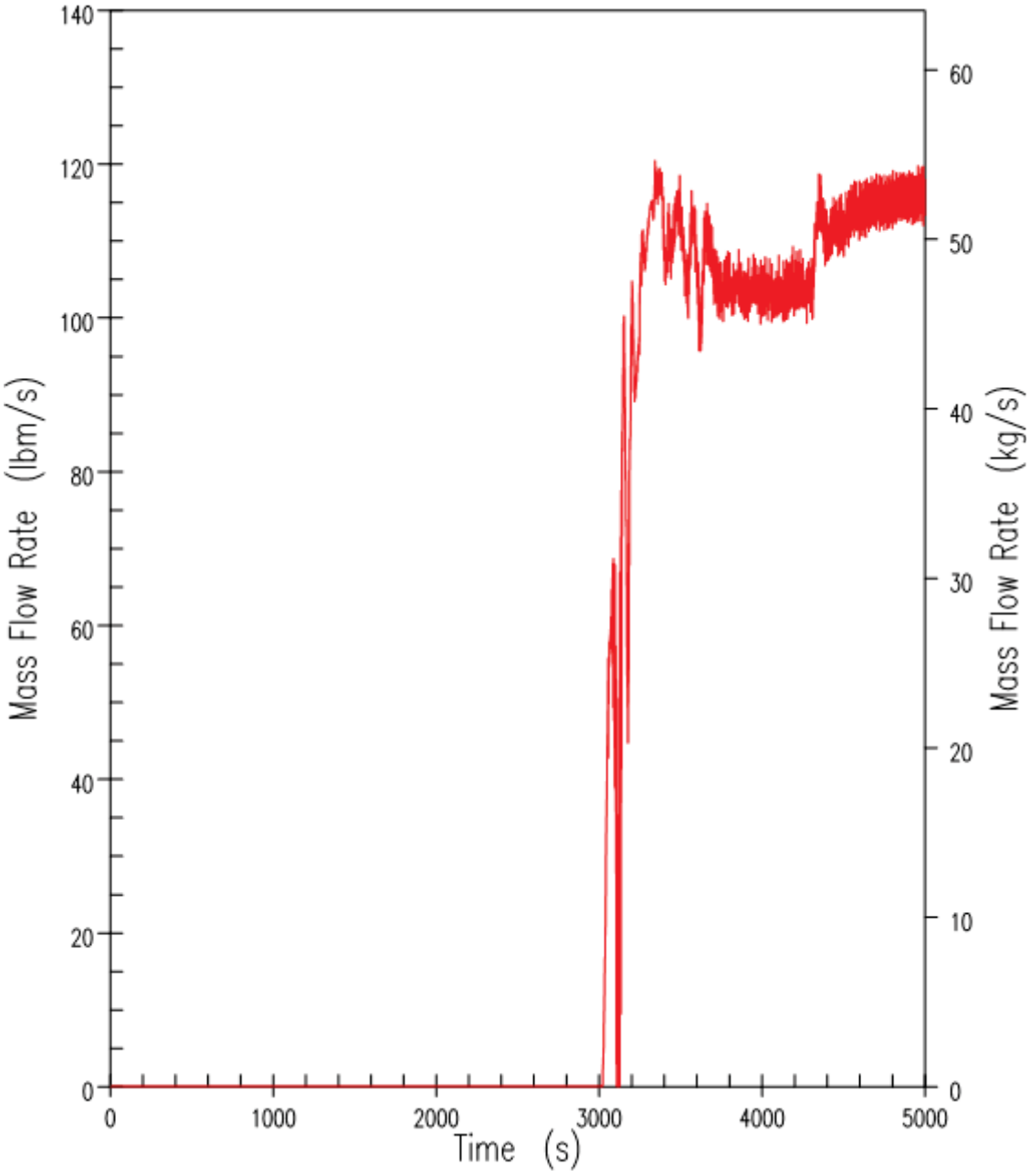


Figure 9.6.5-26. DBA 50.8 mm (2-Inch) Cold Leg Break – IRWST-1 Injection Rate

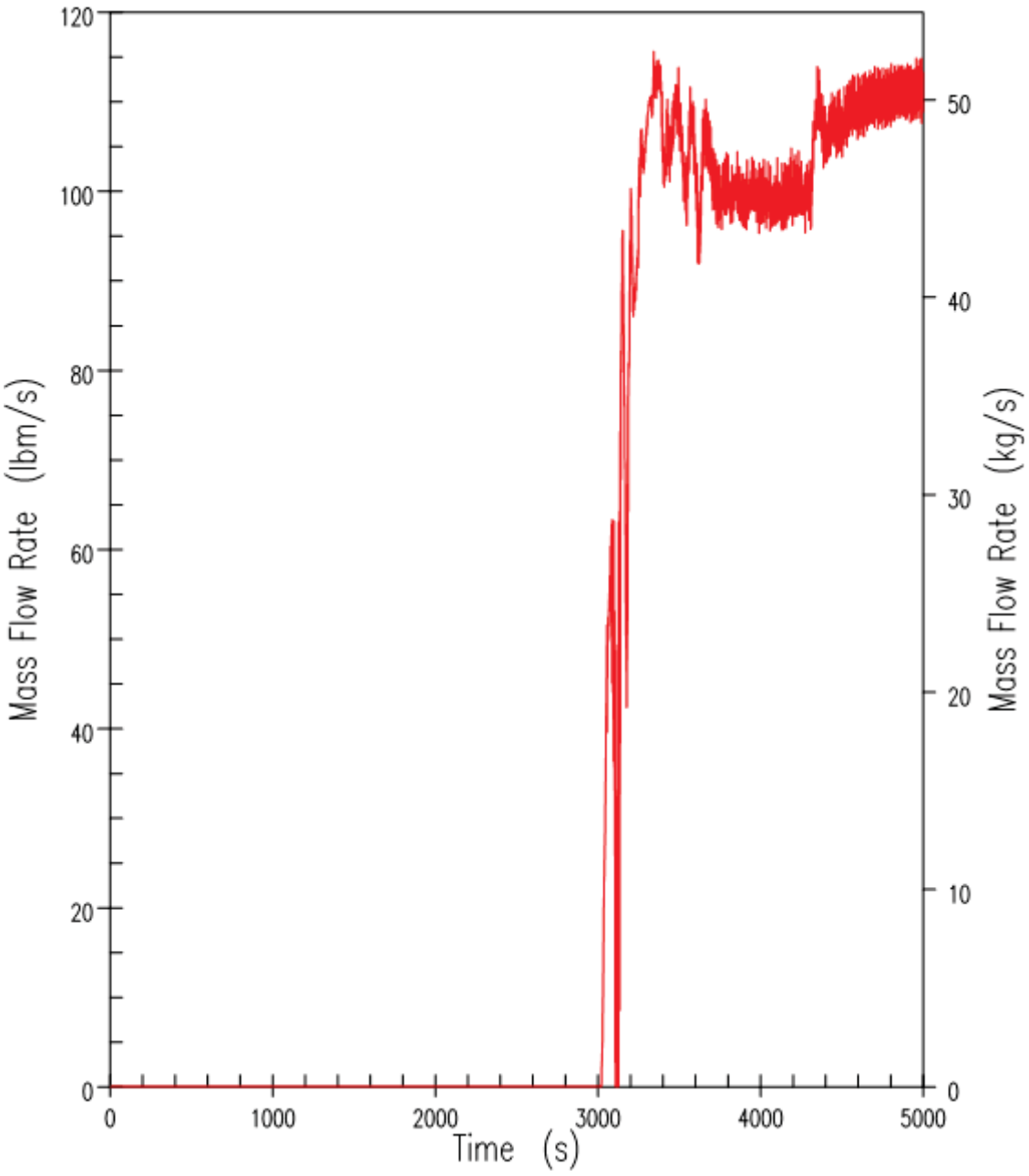


Figure 9.6.5-27. DBA 50.8 mm (2-Inch) Cold Leg Break – IRWST-2 Injection Rate

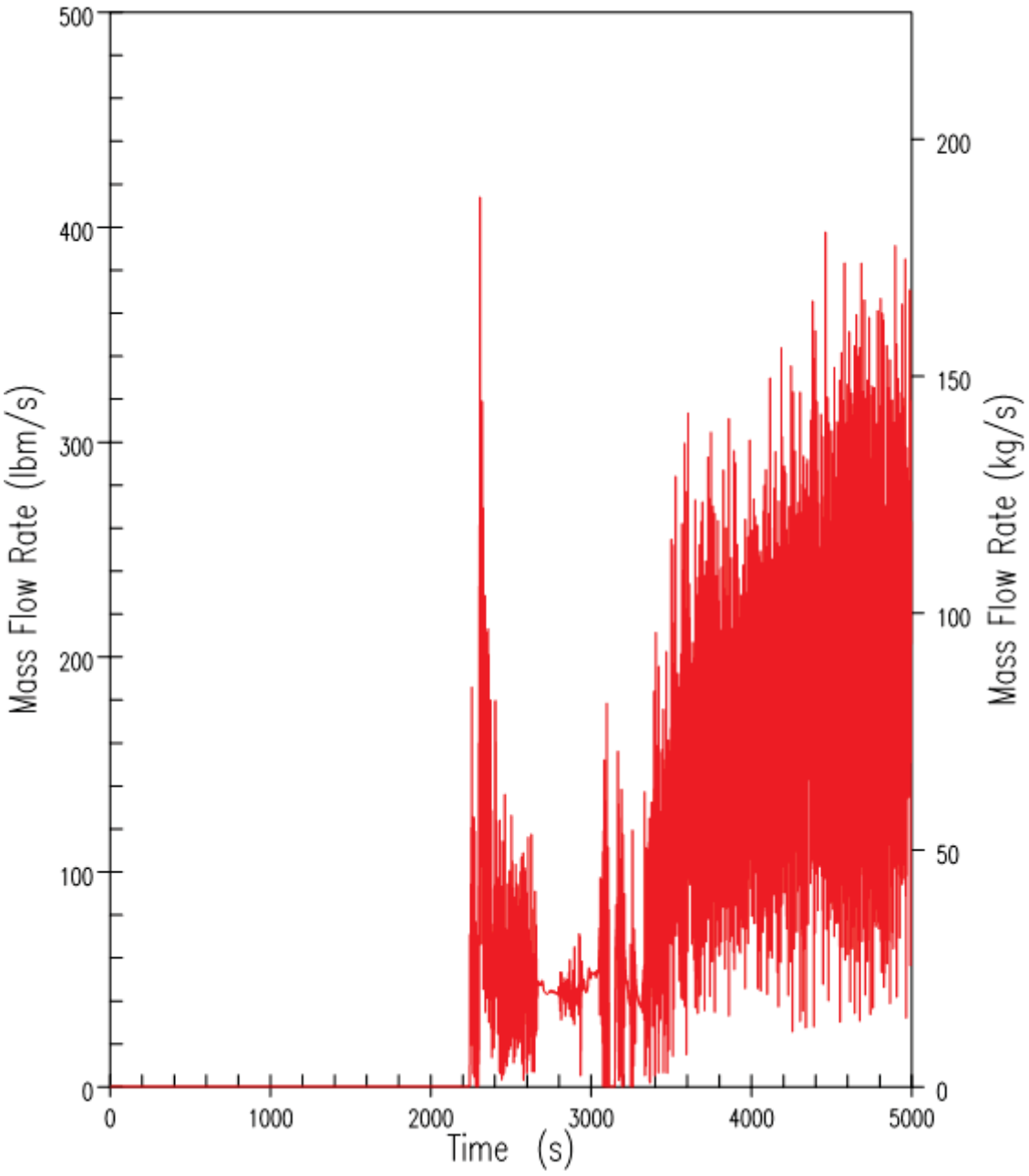


Figure 9.6.5-28(a). DBA 50.8 mm (2-Inch) Cold Leg Break – ADS-4 Liquid Discharge

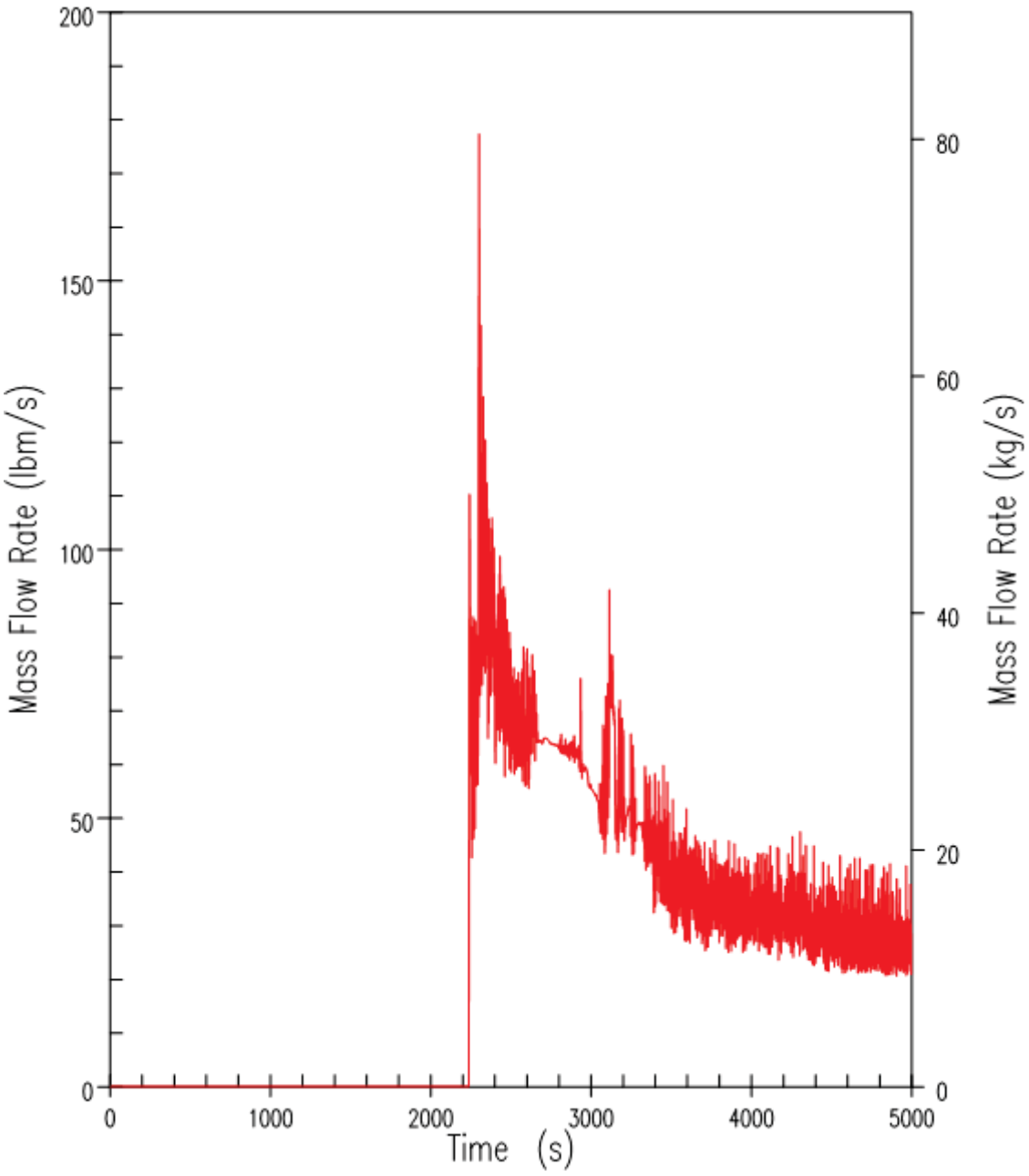


Figure 9.6.5-28(b). DBA 50.8 mm (2-Inch) Cold Leg Break – ADS-4 Vapour Discharge

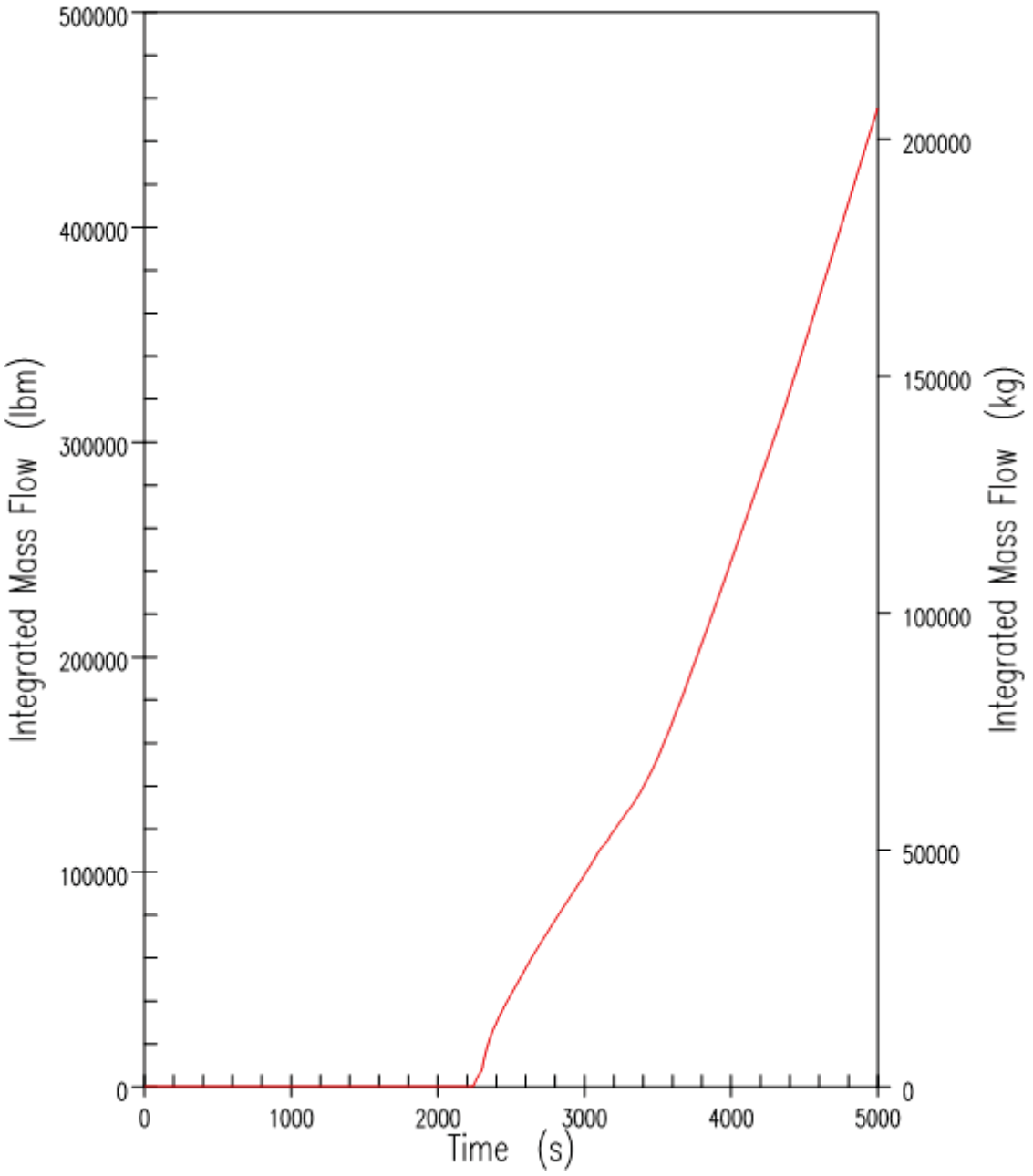


Figure 9.6.5-28(c). DBA 50.8 mm (2-Inch) Cold Leg Break – ADS-4 Integrated Discharge

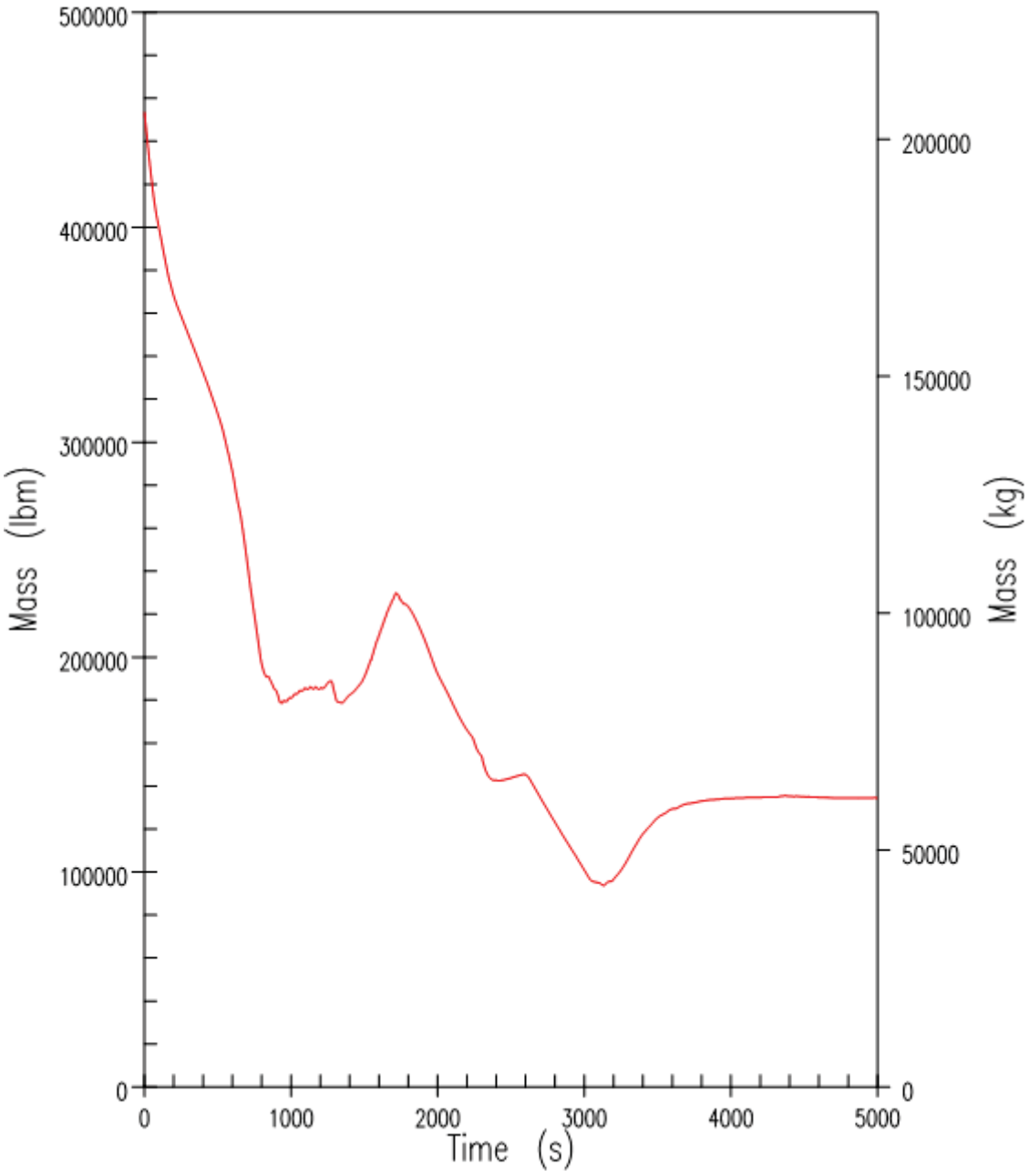


Figure 9.6.5-29(a). DBA 50.8 mm (2-Inch) Cold Leg Break – RCS System Inventory

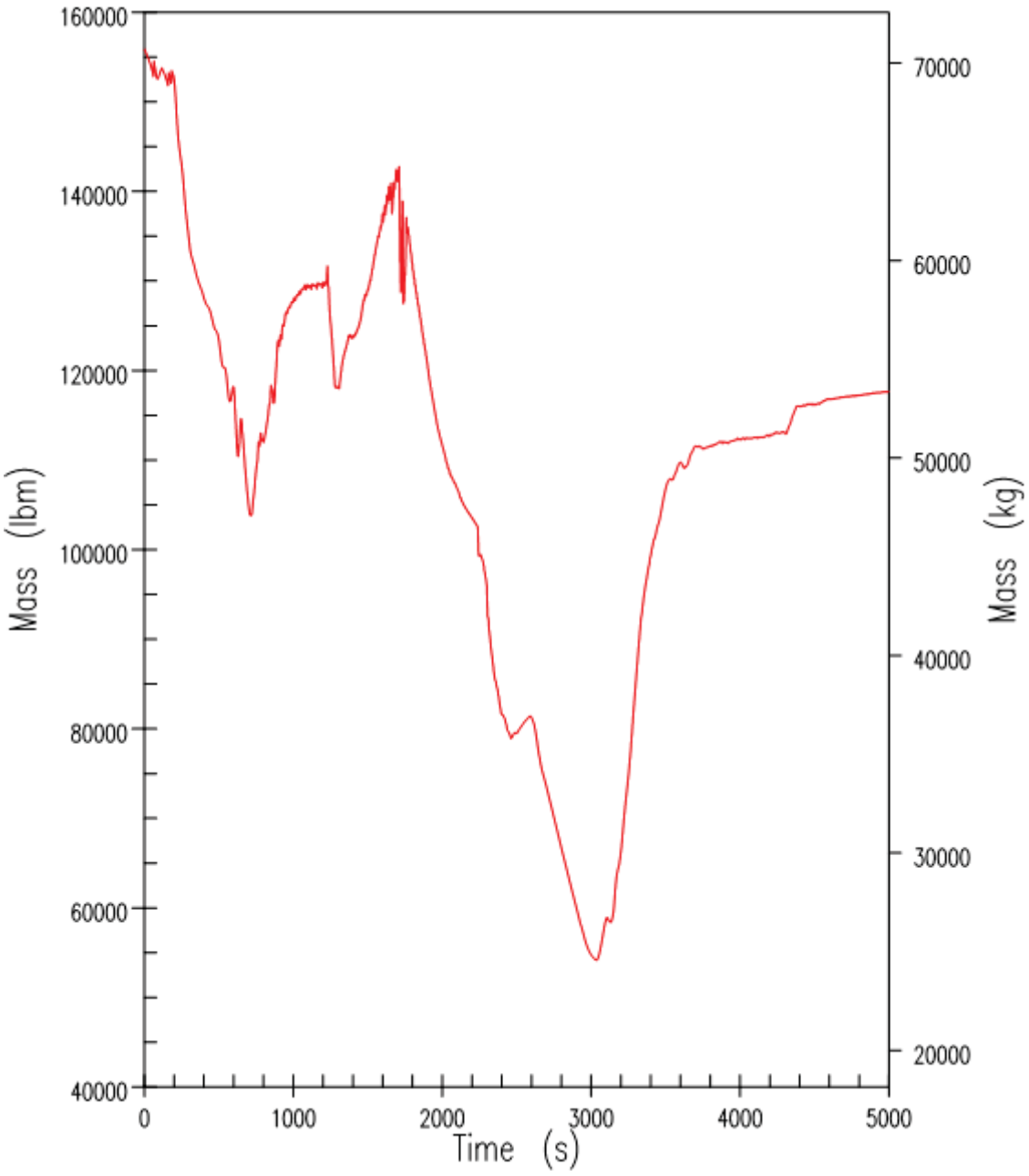


Figure 9.6.5-29(b). DBA 50.8 mm (2-Inch) Cold Leg Break – Reactor Vessel Mixture Inventory

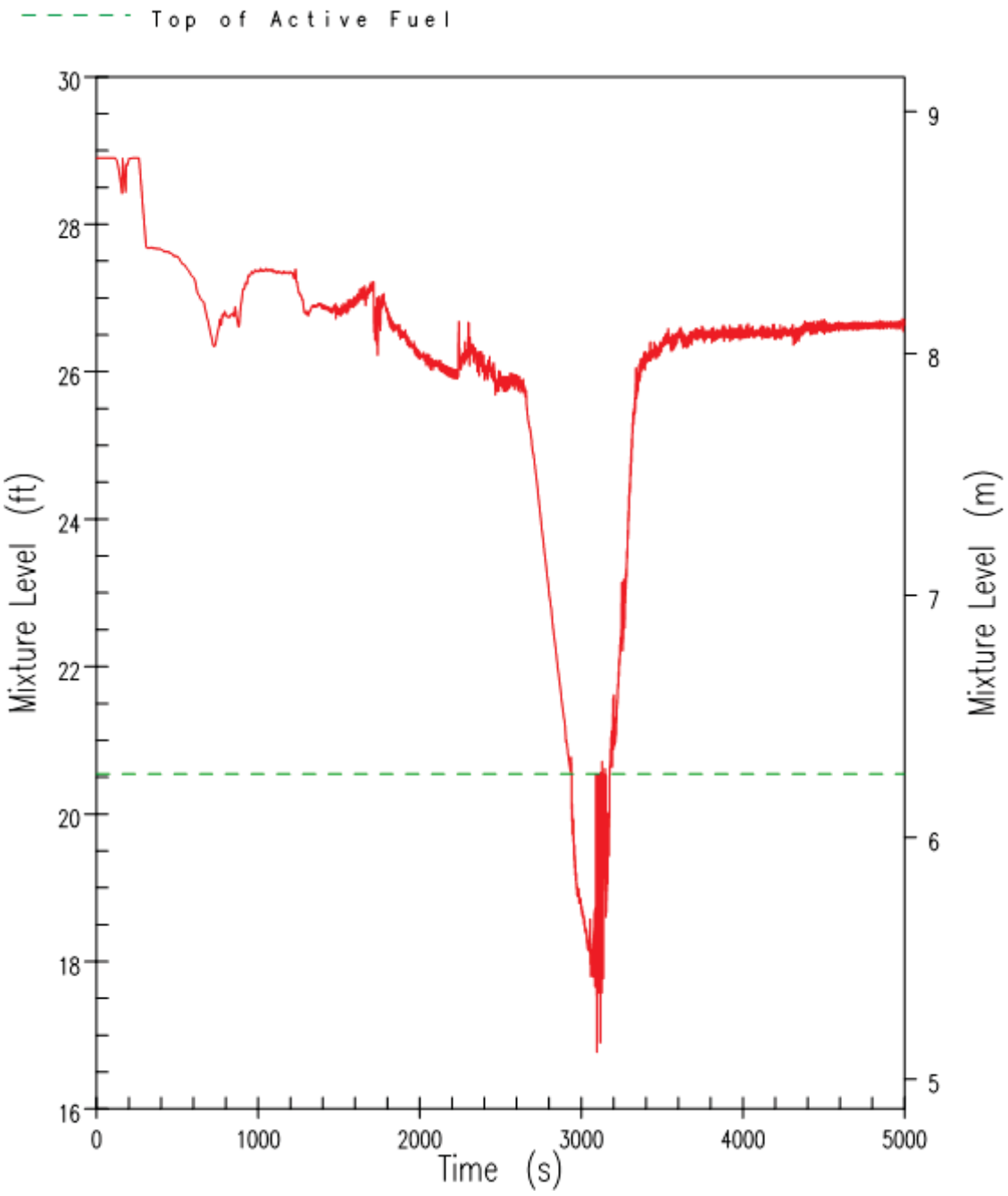


Figure 9.6.5-30(a). DBA 50.8 mm (2-Inch) Cold Leg Break – Core/Upper Plenum Mixture Level

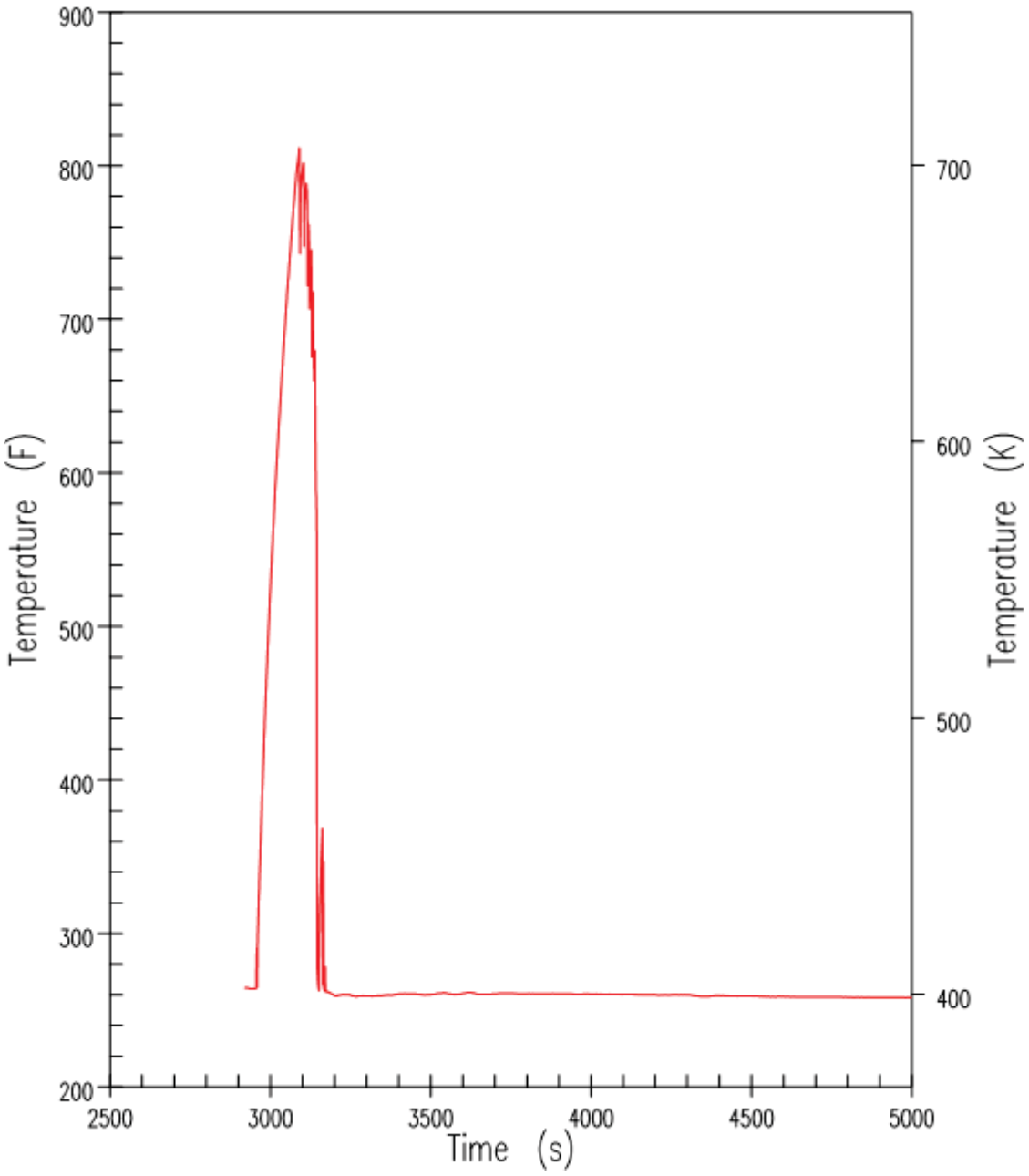


Figure 9.6.5-30(b). DBA 50.8 mm (2-Inch) Cold Leg Break – Peak Cladding Temperature

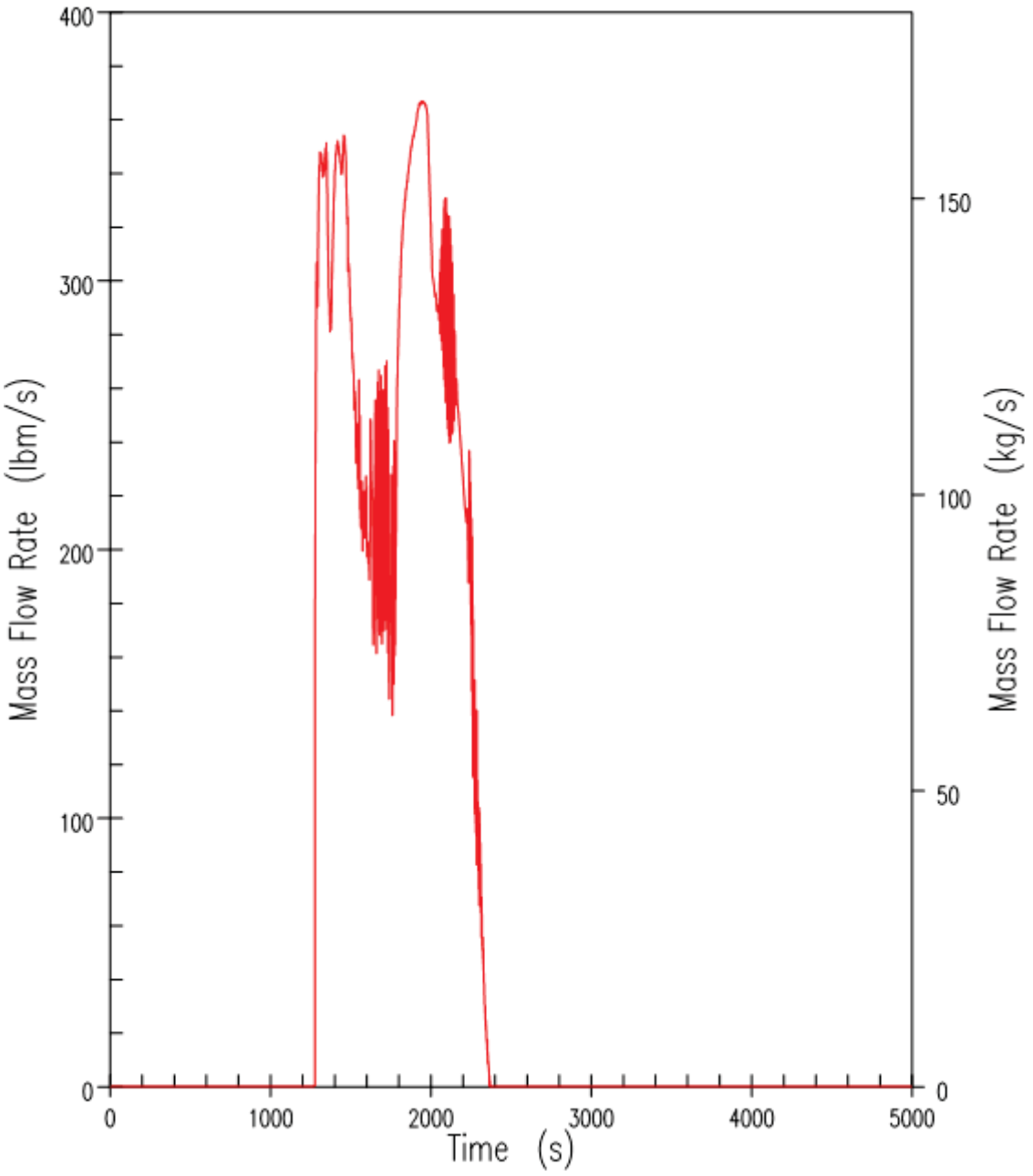


Figure 9.6.5-31(a). DBA 50.8 mm (2-Inch) Cold Leg Break – ADS 1-3 Liquid Discharge

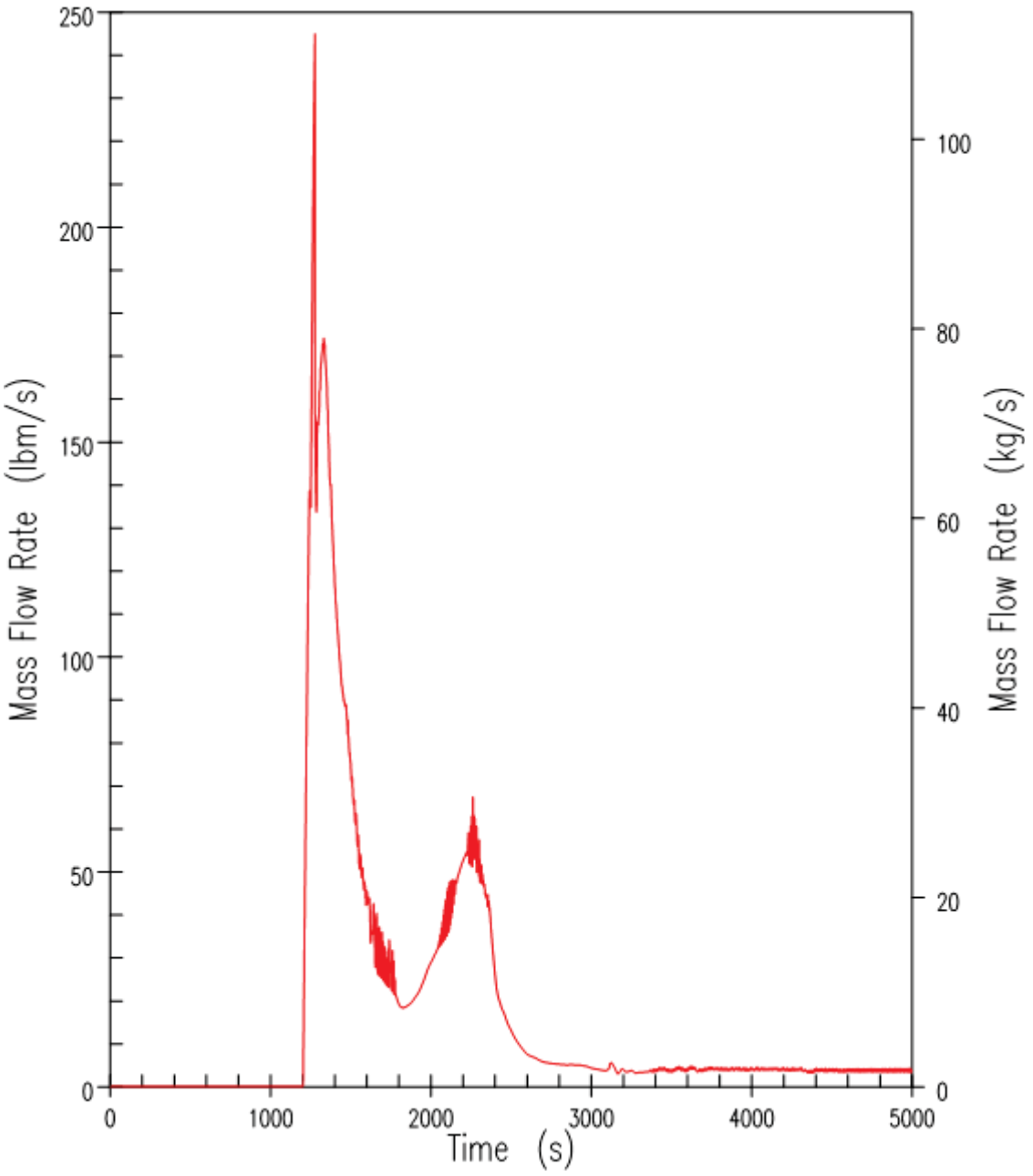


Figure 9.6.5-31(b). DBA 50.8 mm (2-Inch) Cold Leg Break – ADS 1-3 Vapour Discharge

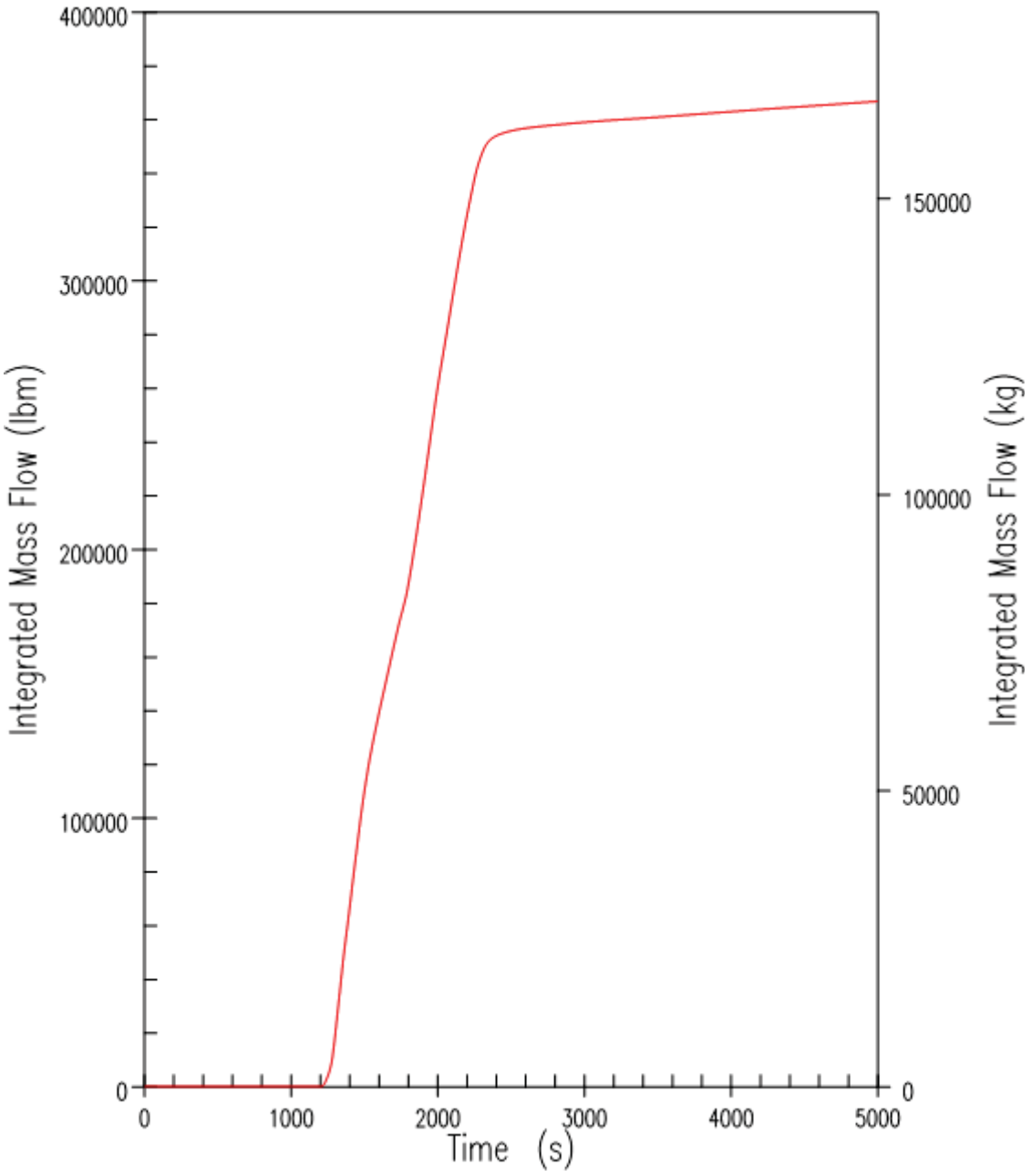


Figure 9.6.5-31(c). DBA 50.8 mm (2-Inch) Cold Leg Break – ADS 1-3 Integrated Discharge

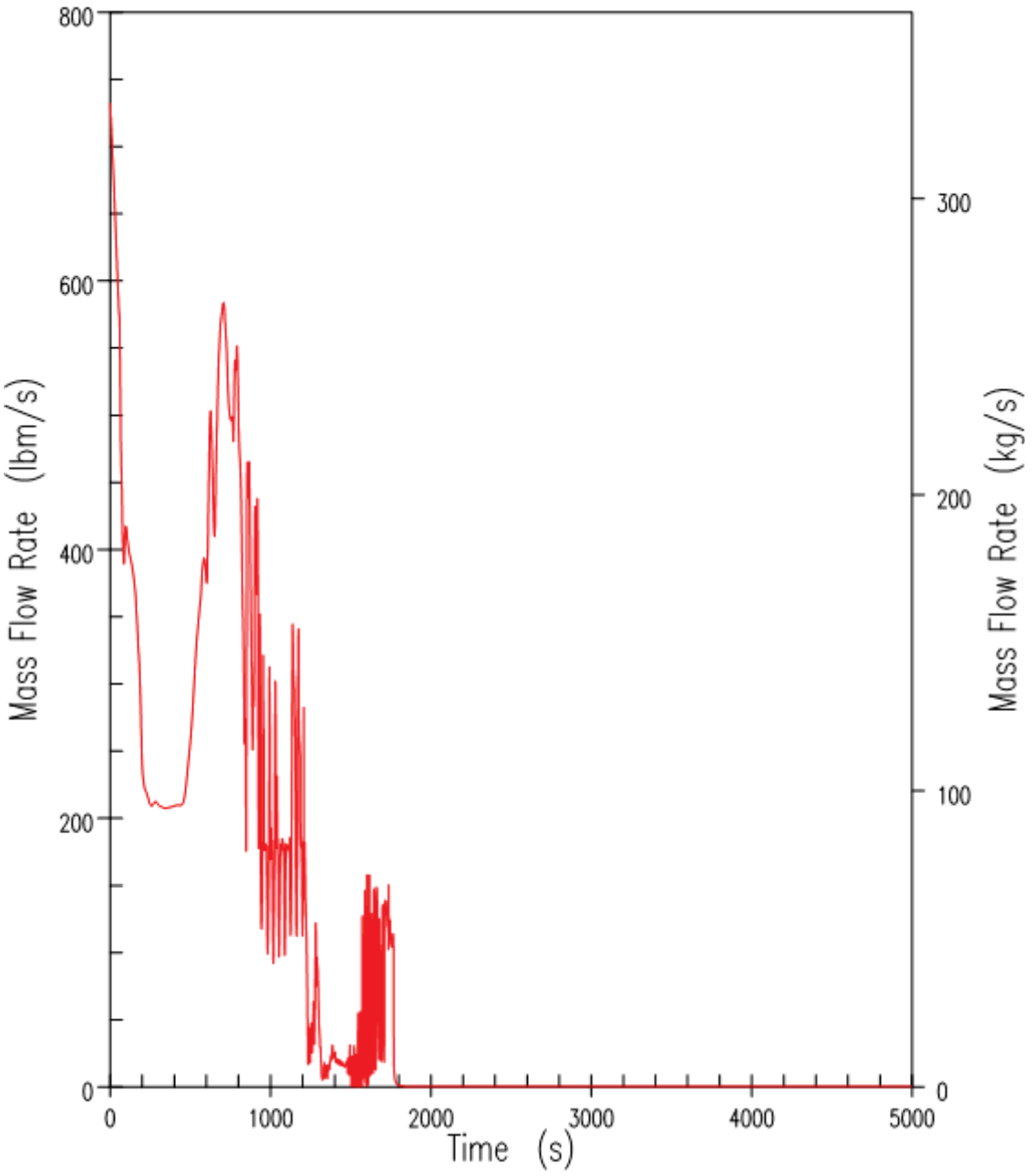


Figure 9.6.5-32. DBA 50.8 mm (2-Inch) Cold Leg Break – Liquid Break Discharge

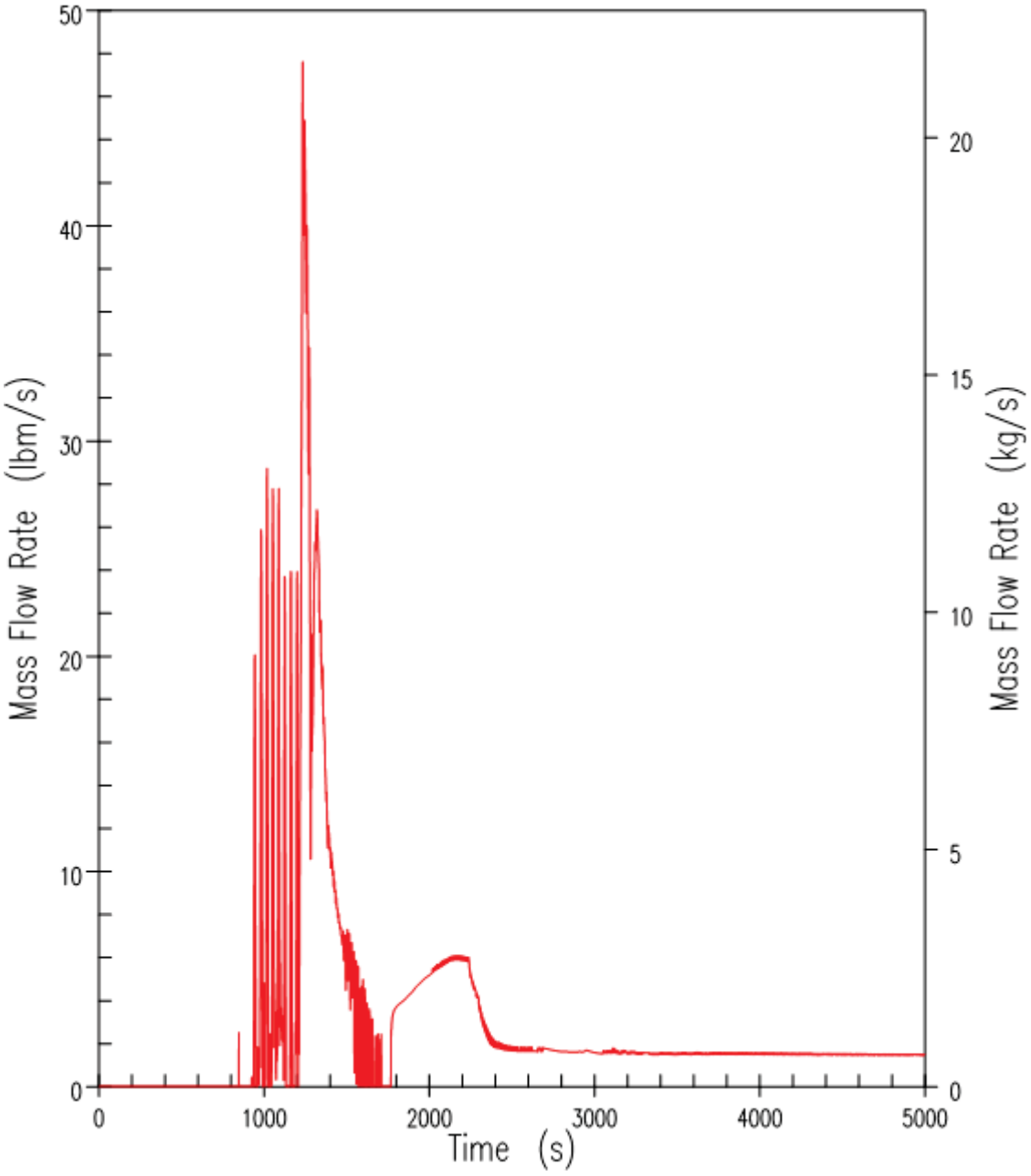


Figure 9.6.5-33. DBA 50.8 mm (2-Inch) Cold Leg Break – Vapour Break Discharge

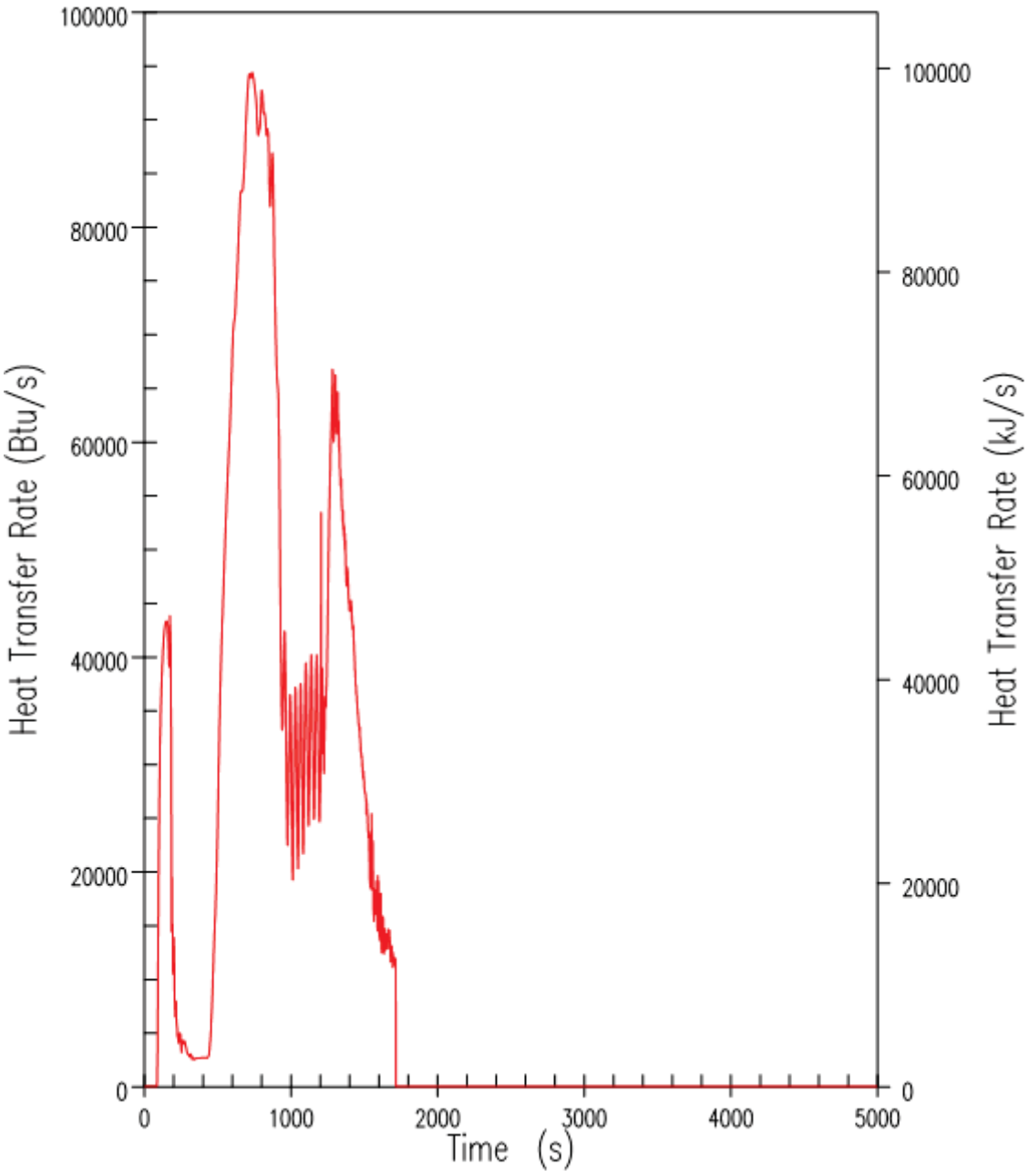


Figure 9.6.5-34. DBA 50.8 mm (2-Inch) Cold Leg Break – PRHR Heat Removal Rate

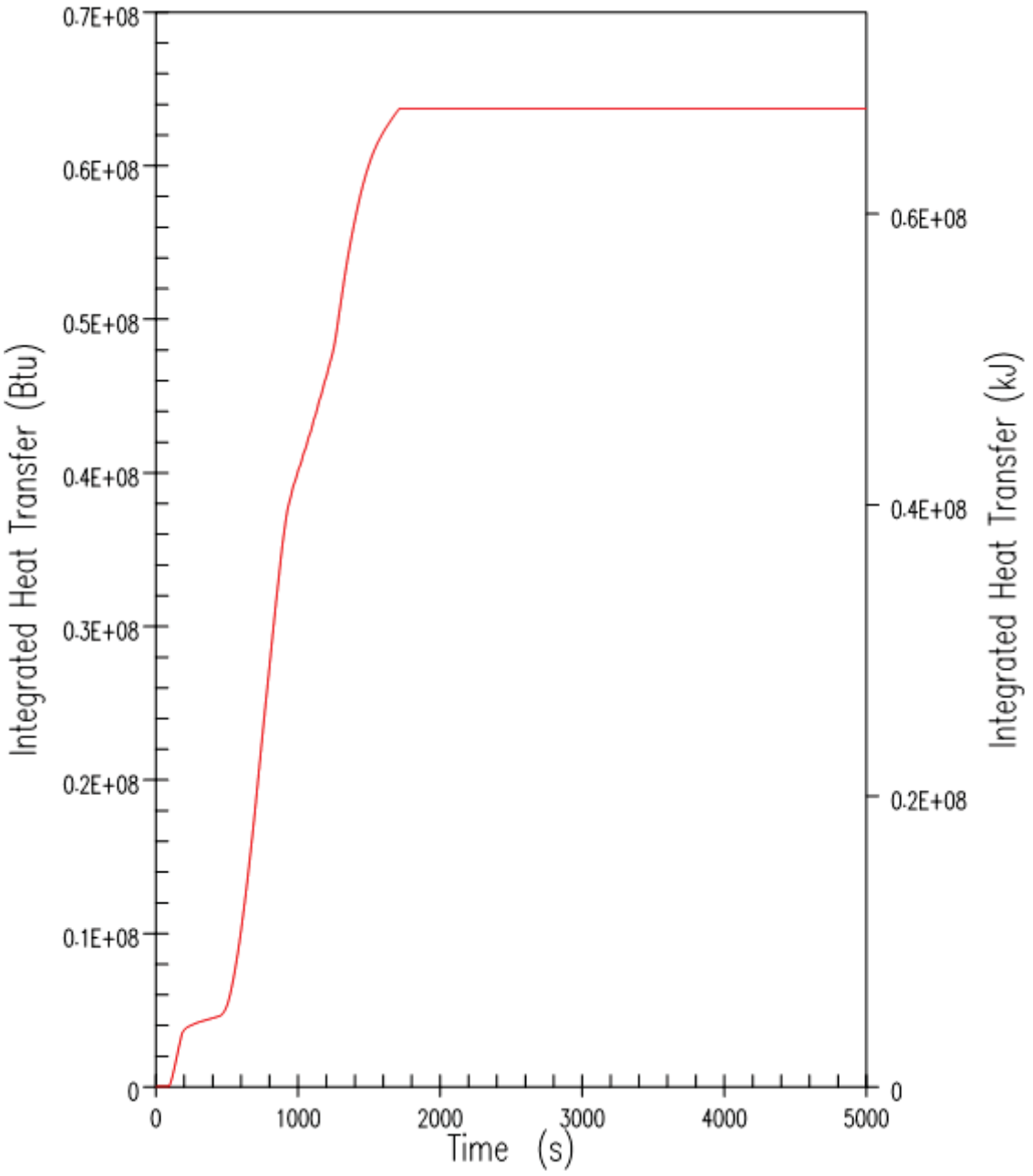


Figure 9.6.5-35. DBA 50.8 mm (2-Inch) Cold Leg Break – Integrated PRHR Heat Removal

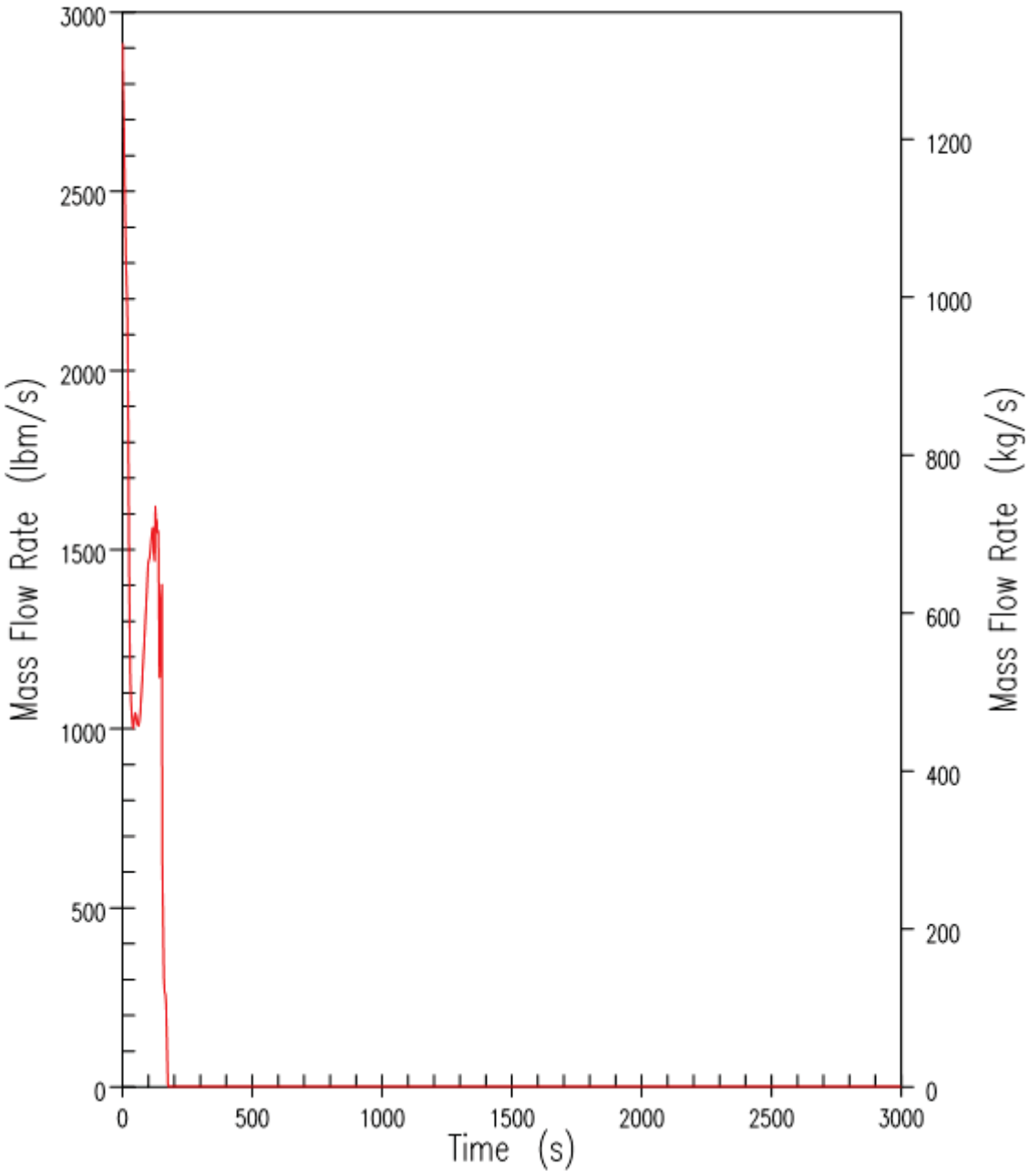


Figure 9.6.5-36. DBA DEDVI with 0.138 MPa abs (20 psia) Cont. – Vessel Side Liquid Break Discharge

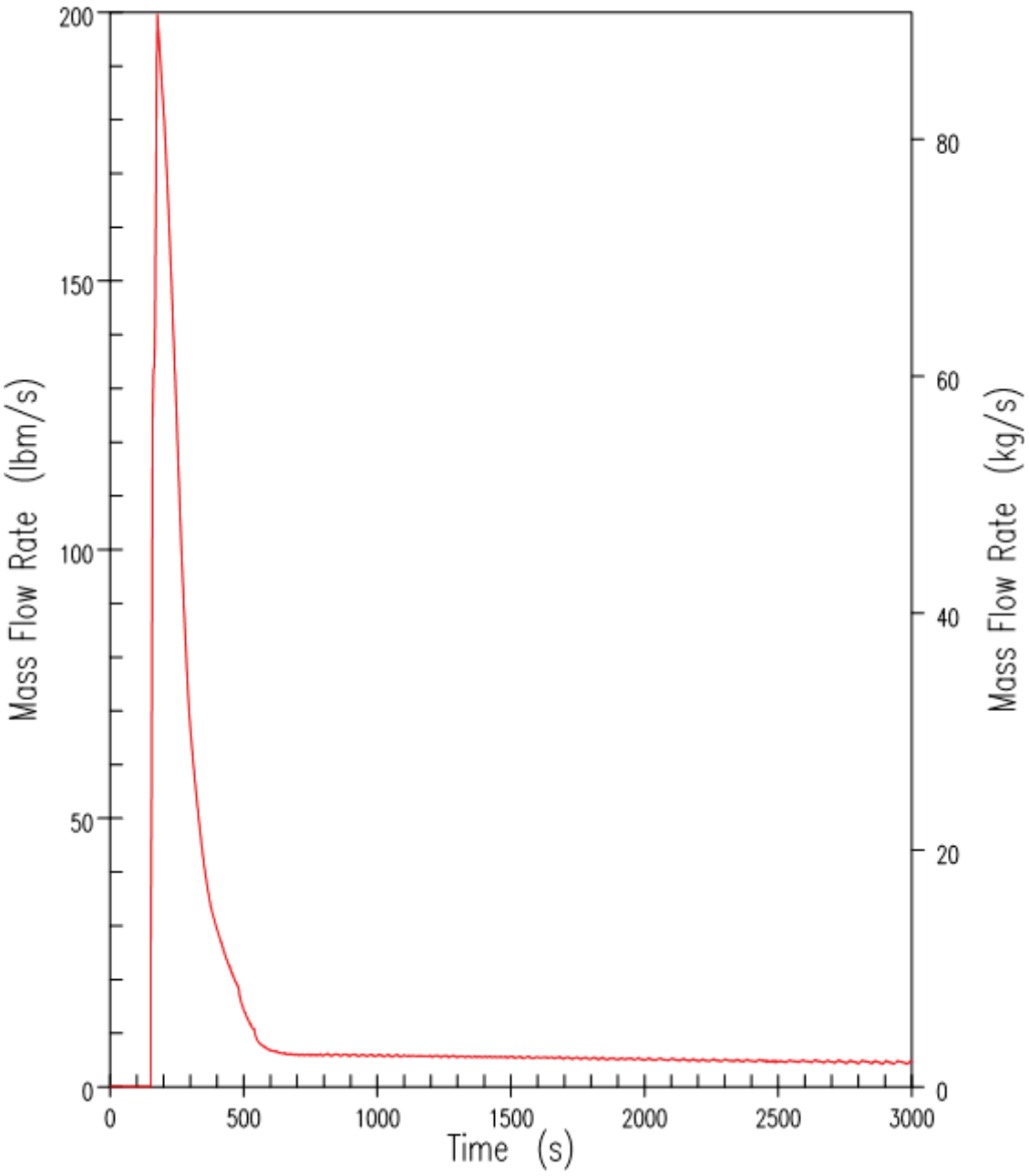


Figure 9.6.5-37. DBA DEDVI with 0.138 MPa abs (20 psia) Cont. – Vessel Side Vapour Break Discharge

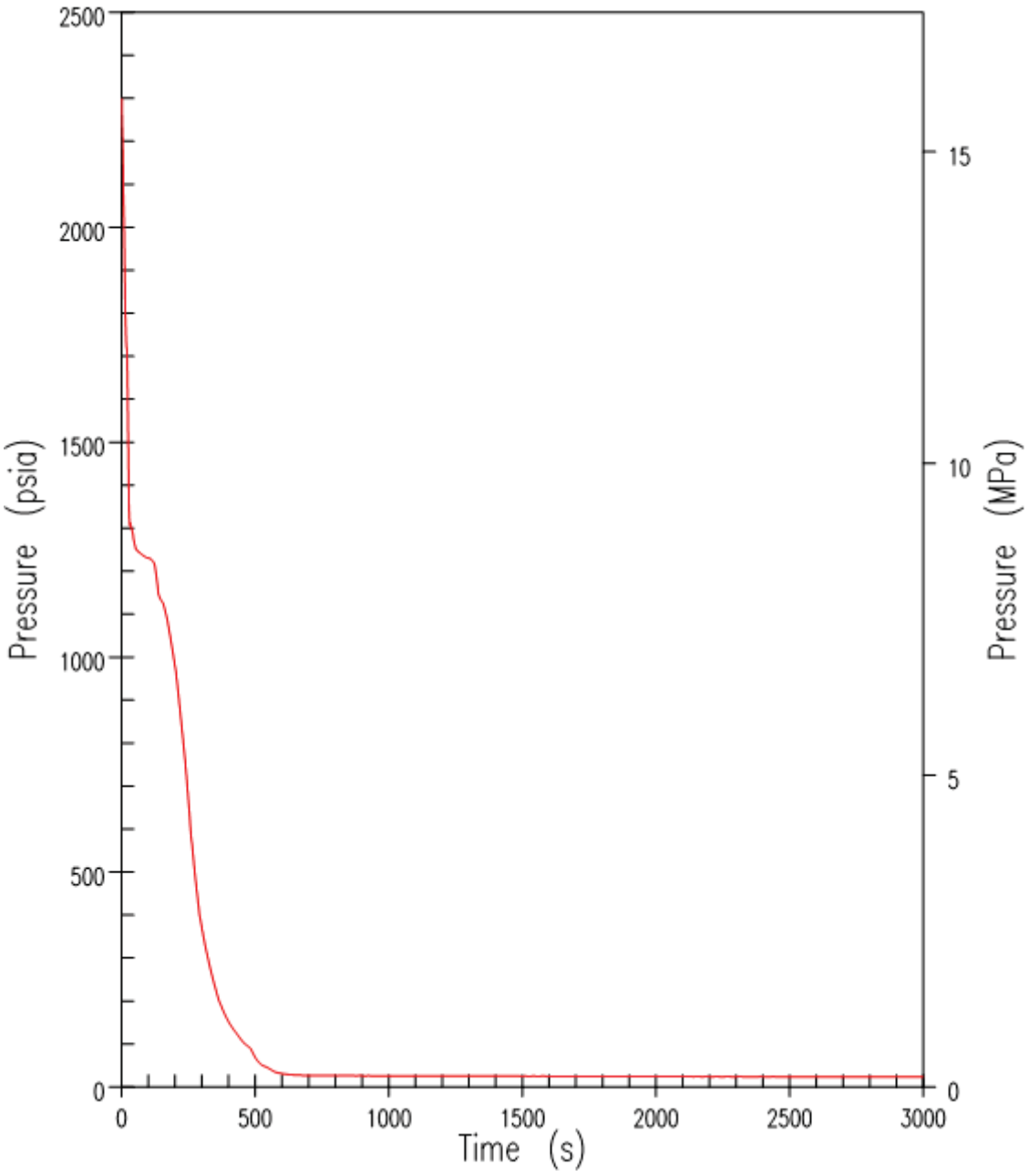


Figure 9.6.5-38(a). DBA DEDVI with 0.138 MPa abs (20 psia) Cont. – RCS Pressure

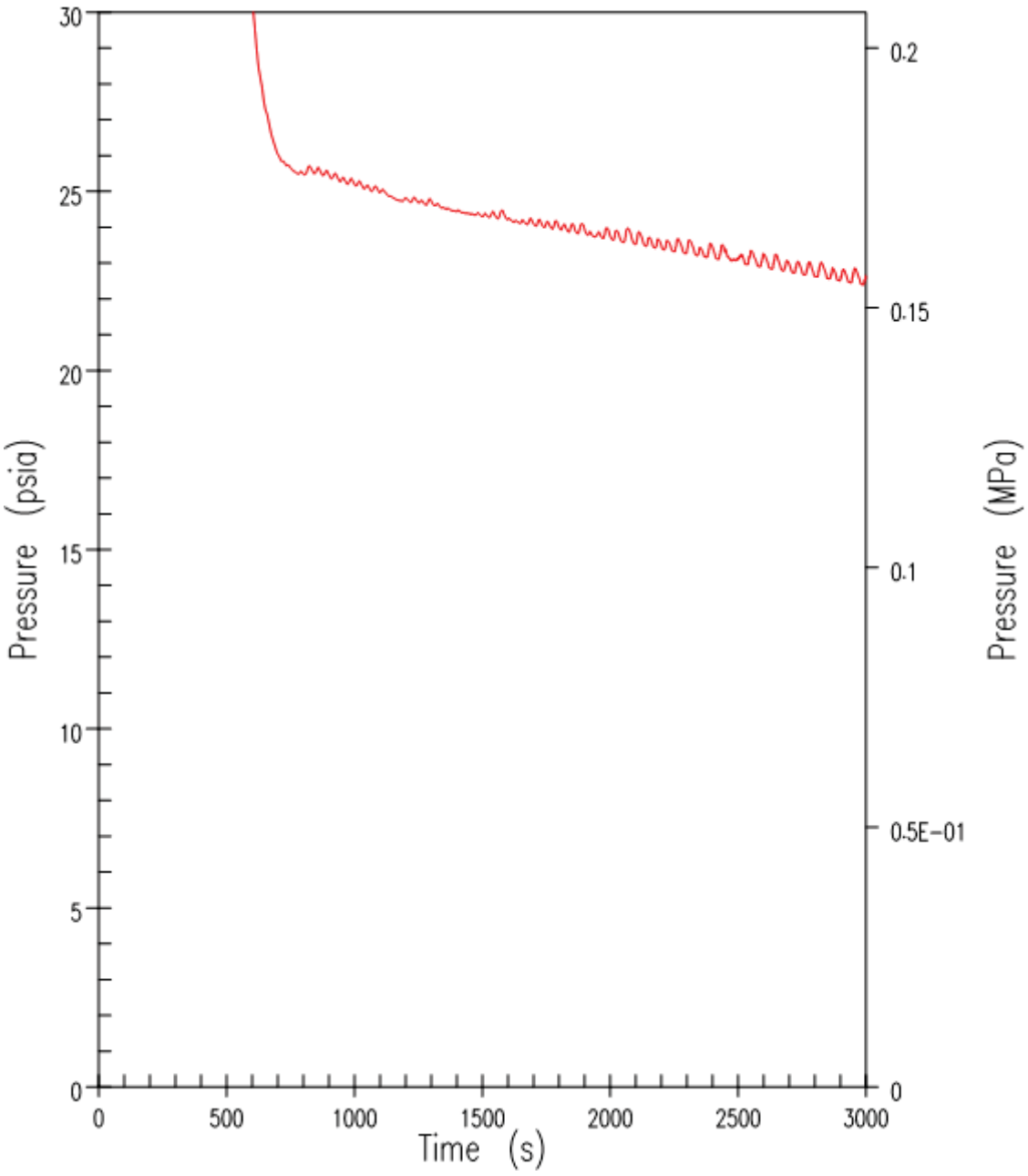


Figure 9.6.5-38(b). DBA DEDVI with 0.138 MPa abs (20 psia) Cont. – RCS Pressure (Zoomed)

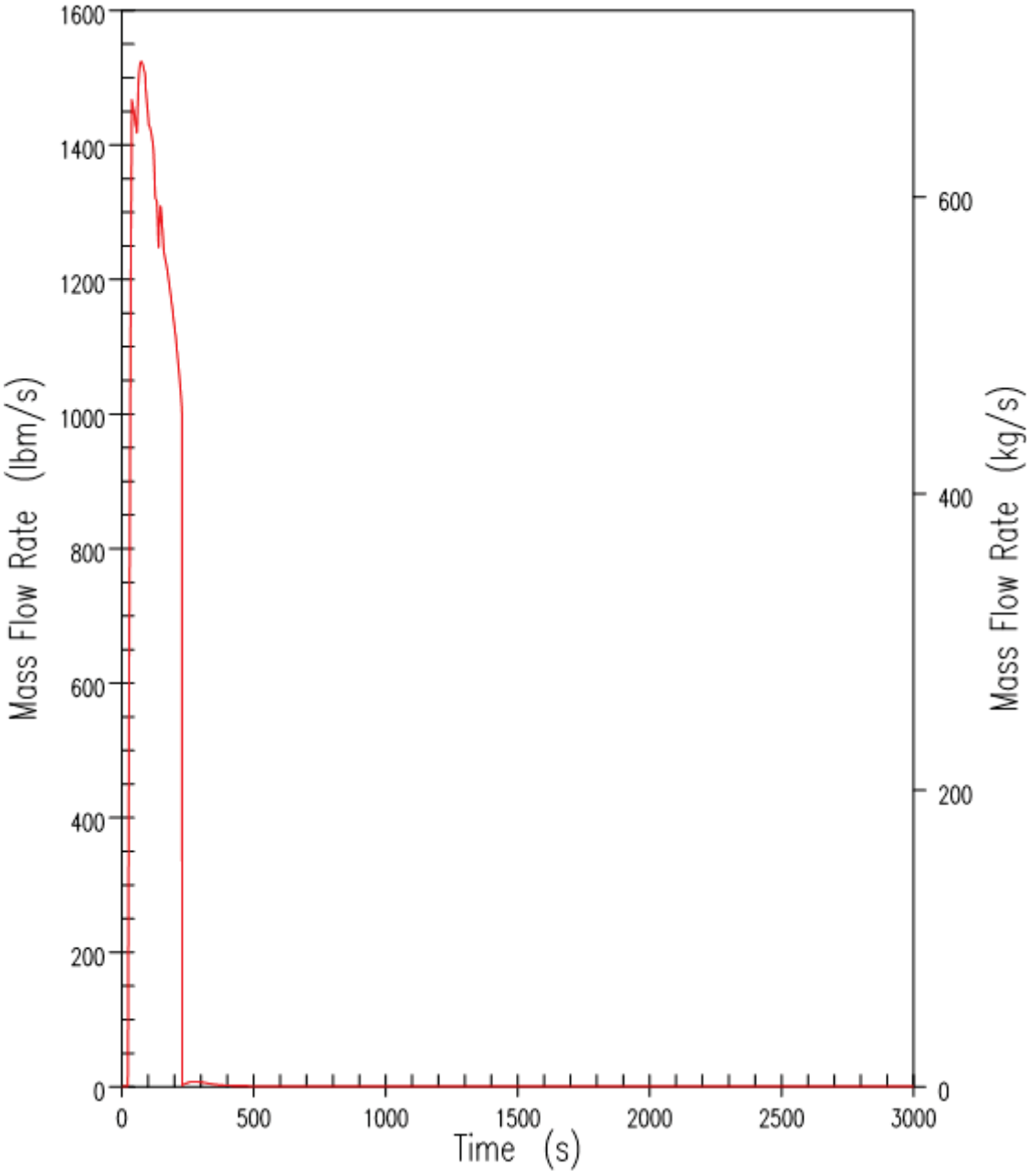


Figure 9.6.5-39. DBA DEDVI with 0.138 MPa abs (20 psia) Cont. – Broken CMT Injection Rate

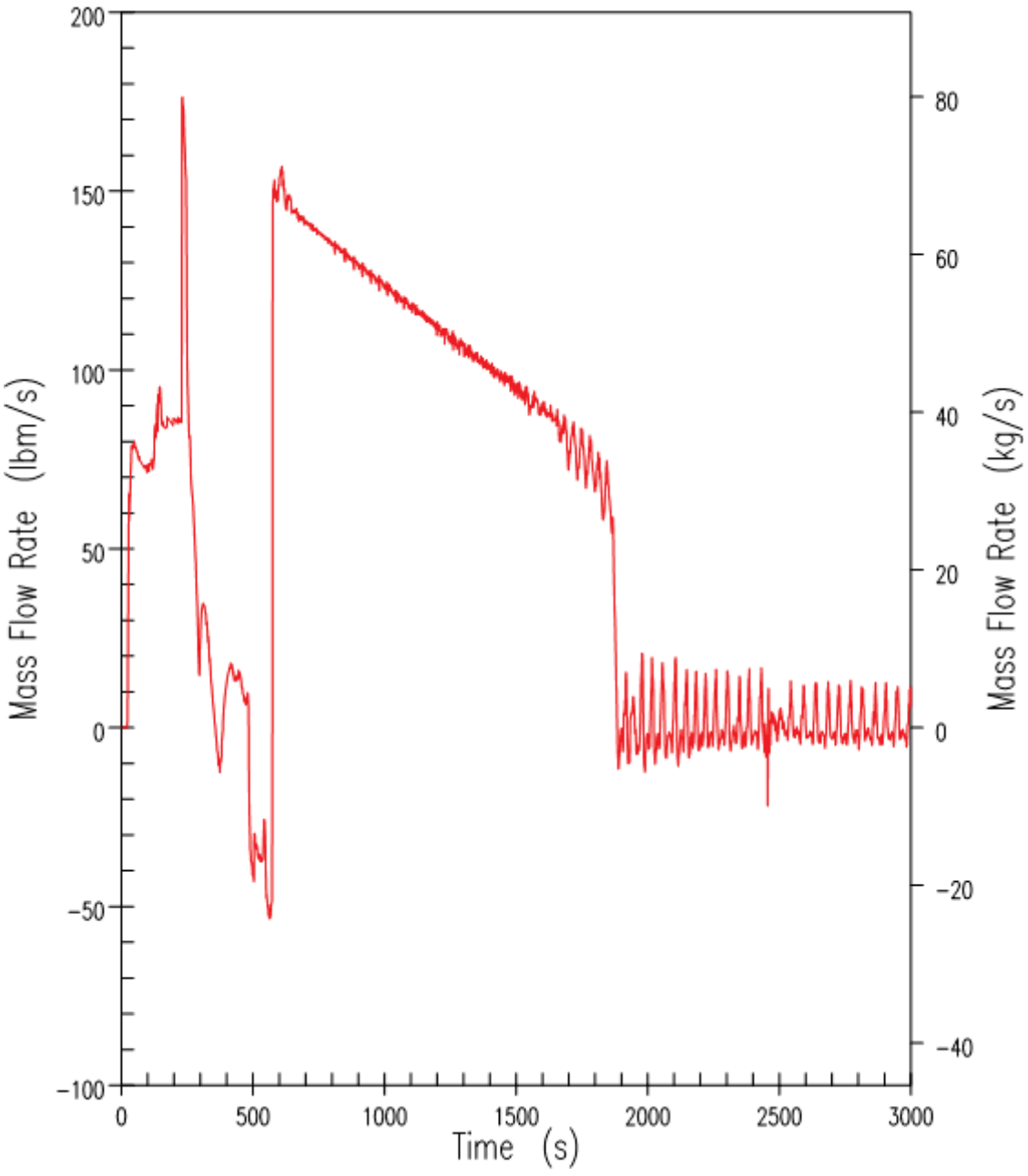


Figure 9.6.5-40. DBA DEDVI with 0.138 MPa abs (20 psia) Cont. – Intact CMT Injection Rate

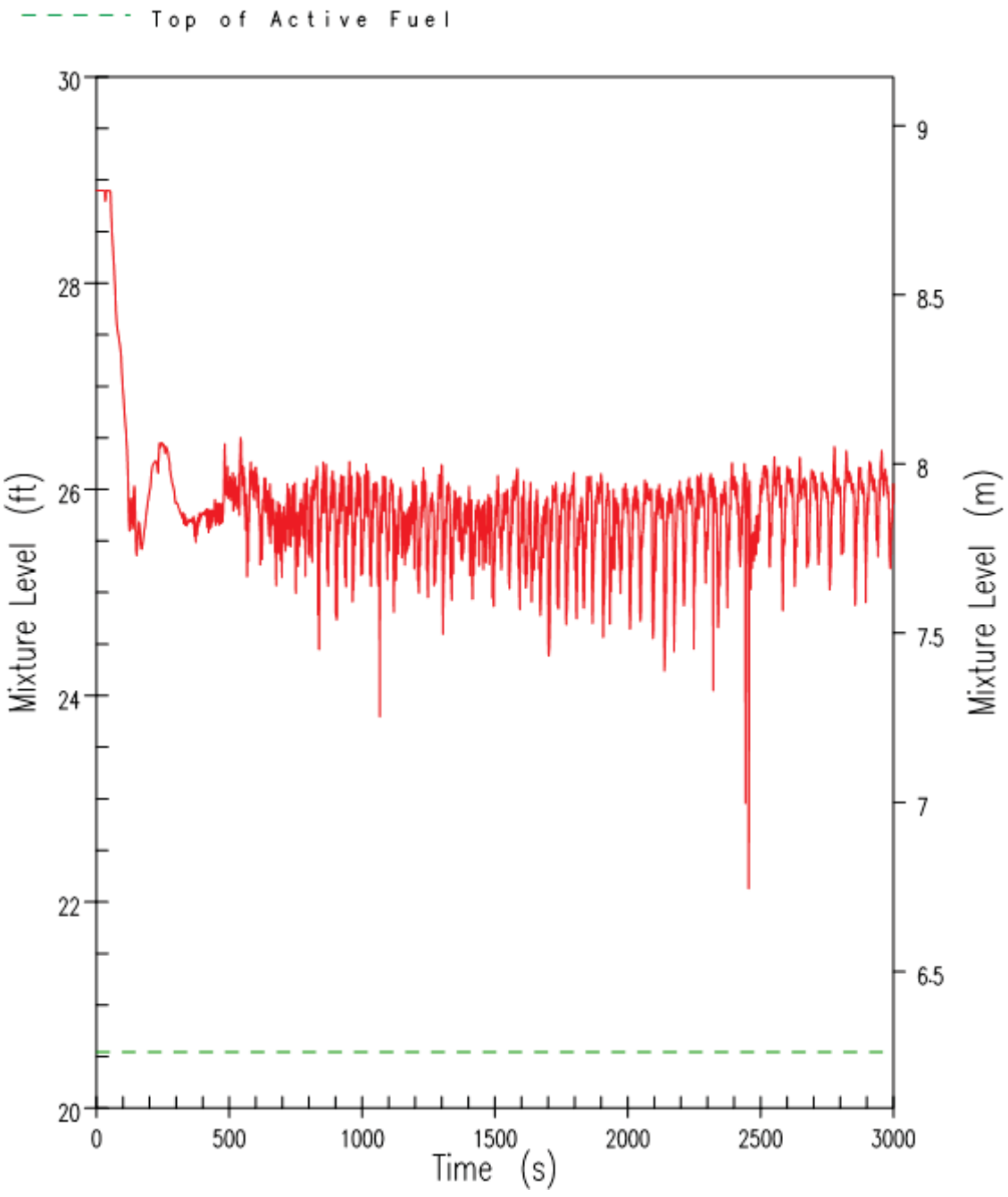


Figure 9.6.5-41. DBA DEDVI with 0.138 MPa abs (20 psia) Cont. – Core/Upper Plenum Mixture Level

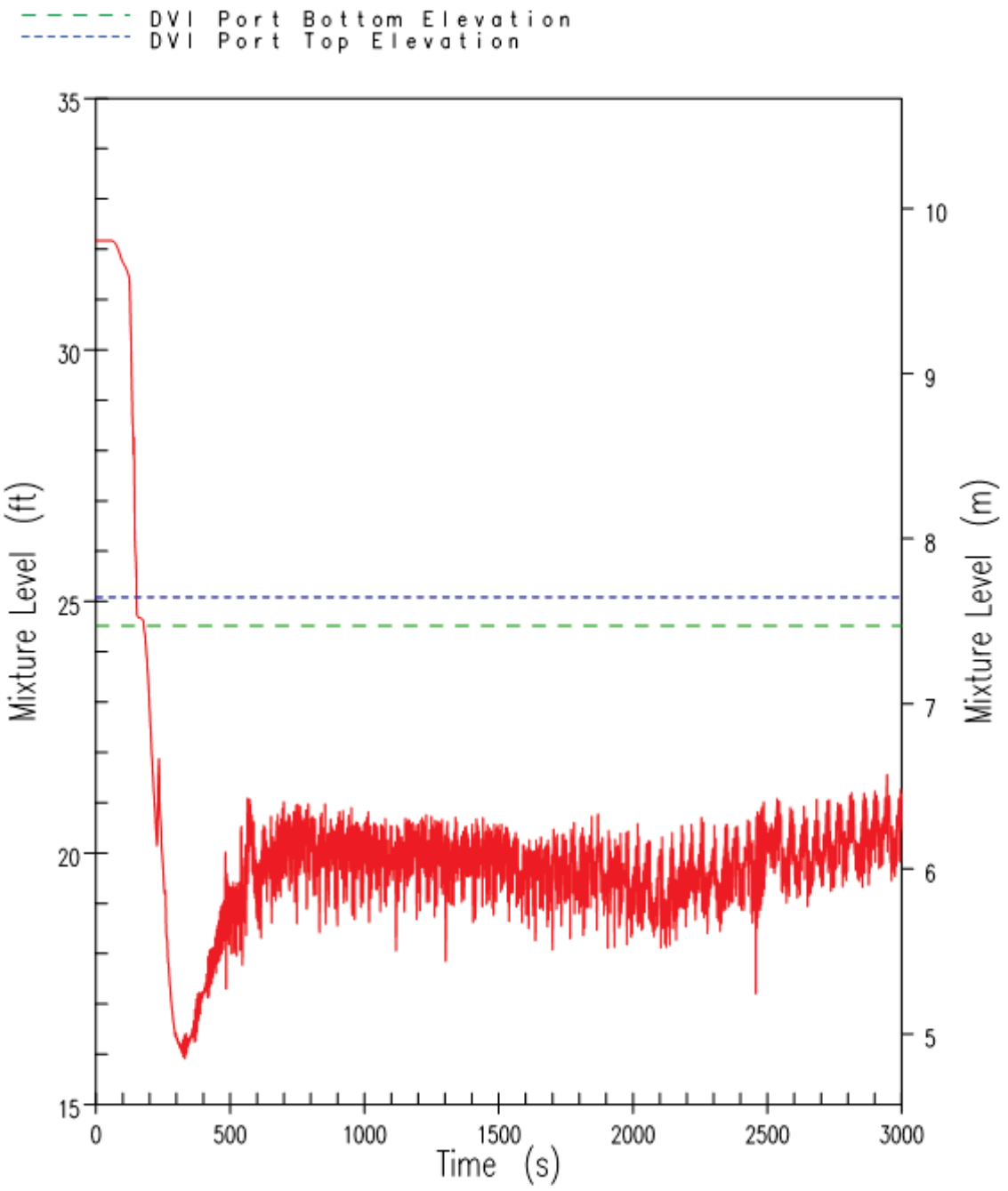


Figure 9.6.5-42. DBA DEDVI with 0.138 MPa abs (20 psia) Cont. – Downcomer Mixture Level

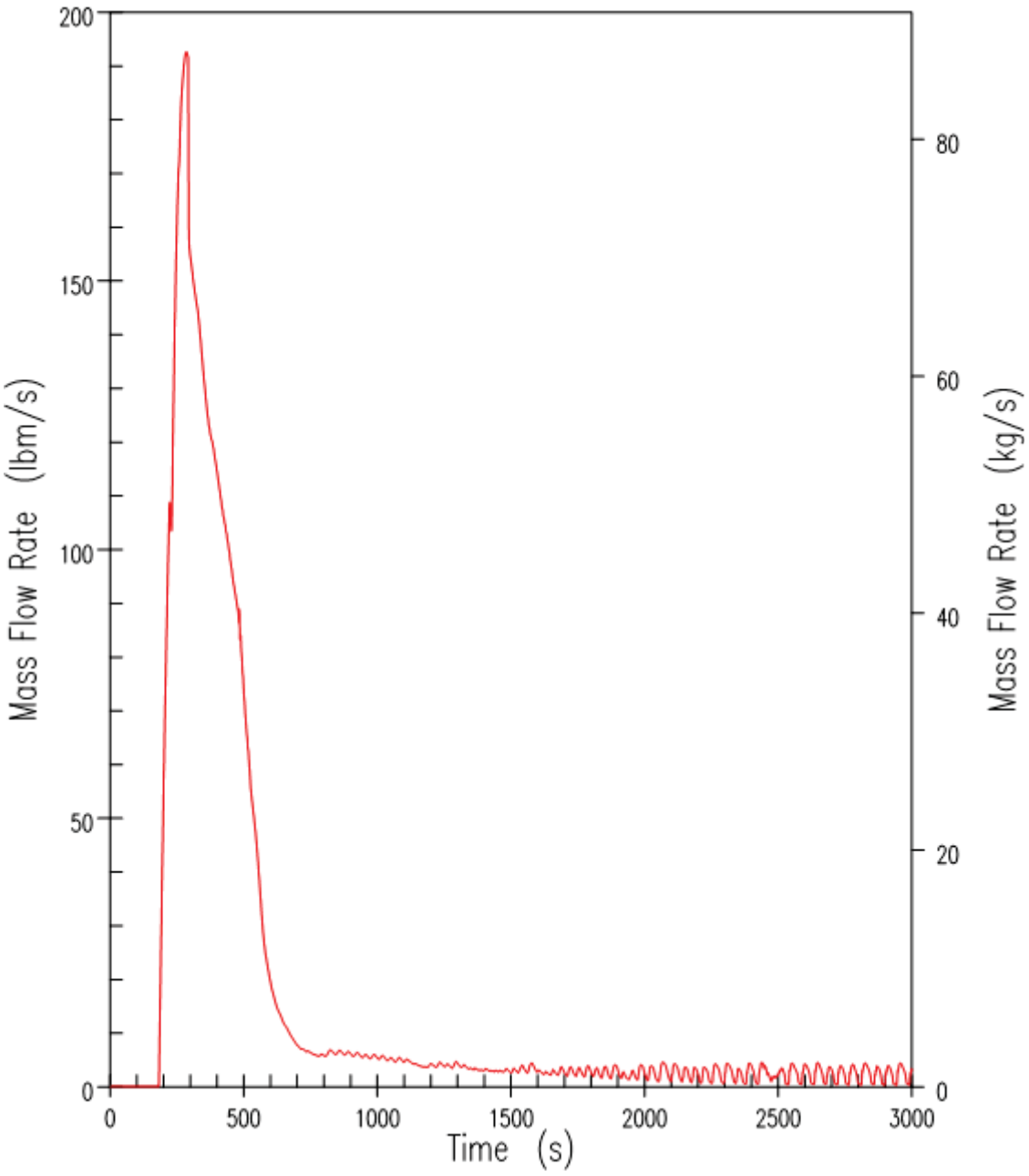


Figure 9.6.5-43(a). DBA DEDVI with 0.138 MPa abs (20 psia) Cont. – ADS 1-3 Vapour Discharge

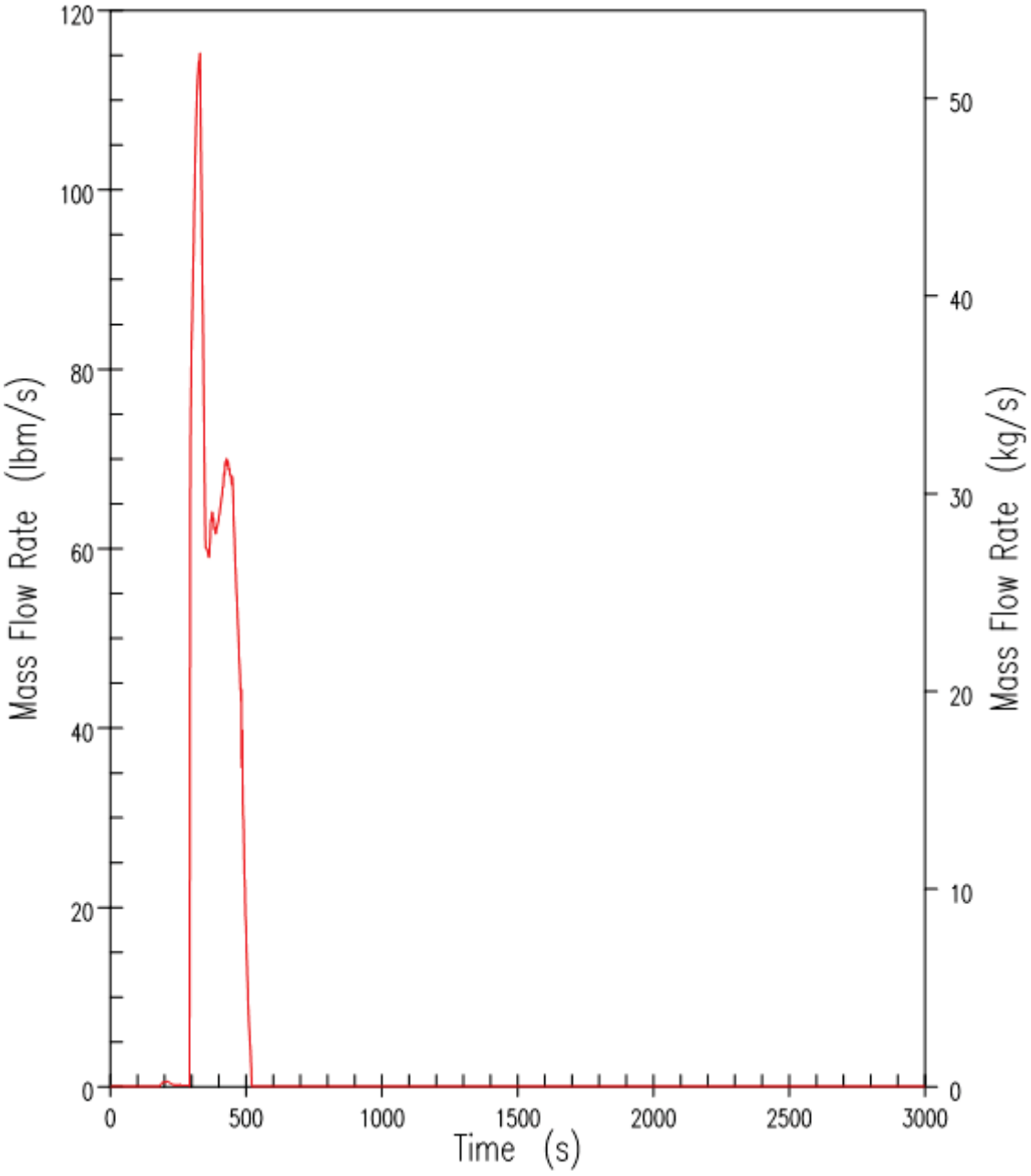


Figure 9.6.5-43(b). DBA DEDVI with 0.138 MPa abs (20 psia) Cont. – ADS 1-3 Liquid Discharge

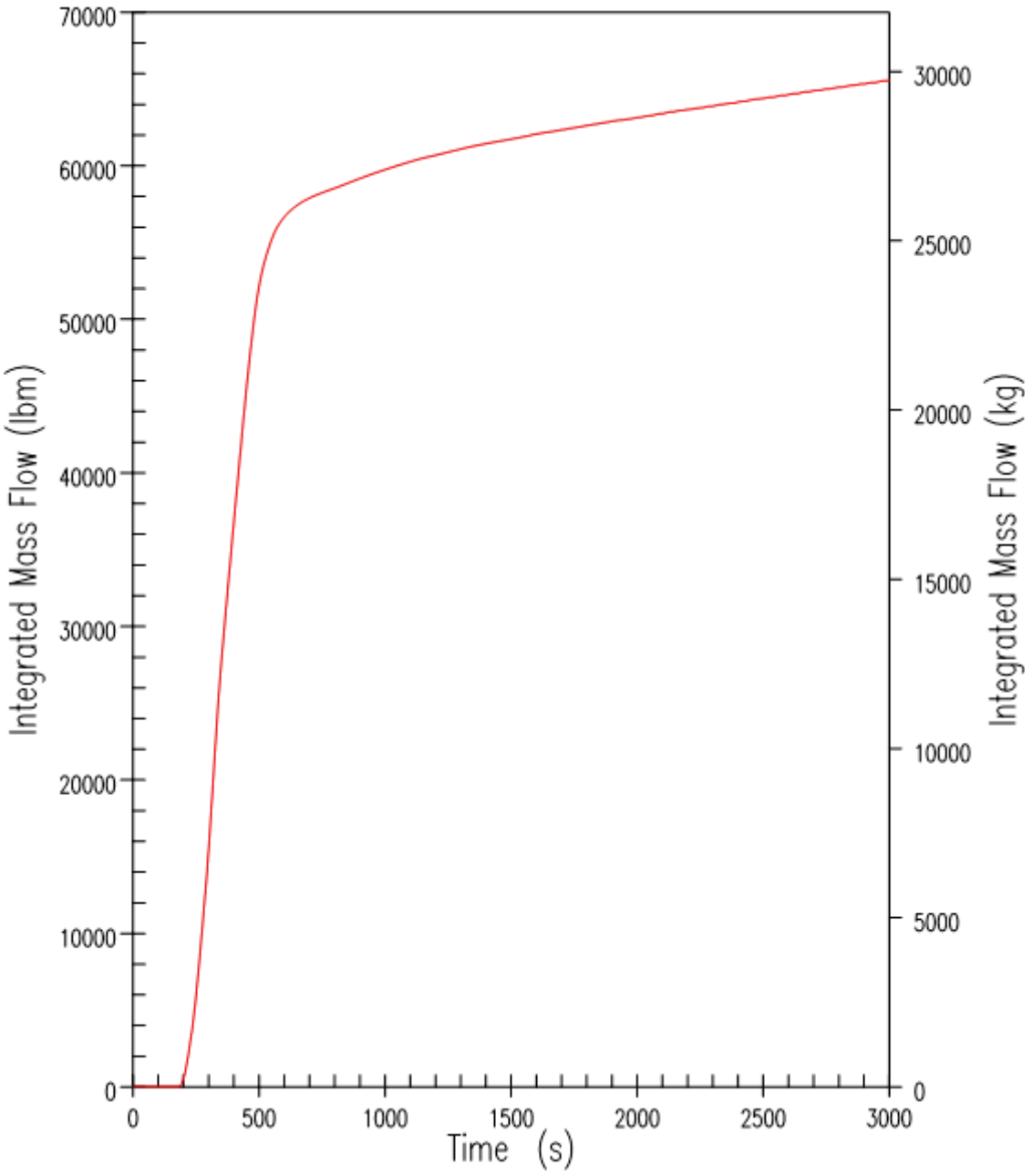


Figure 9.6.5-43(c). DBA DEDVI with 0.138 MPa abs (20 psia) Cont. – ADS 1-3 Integrated Discharge

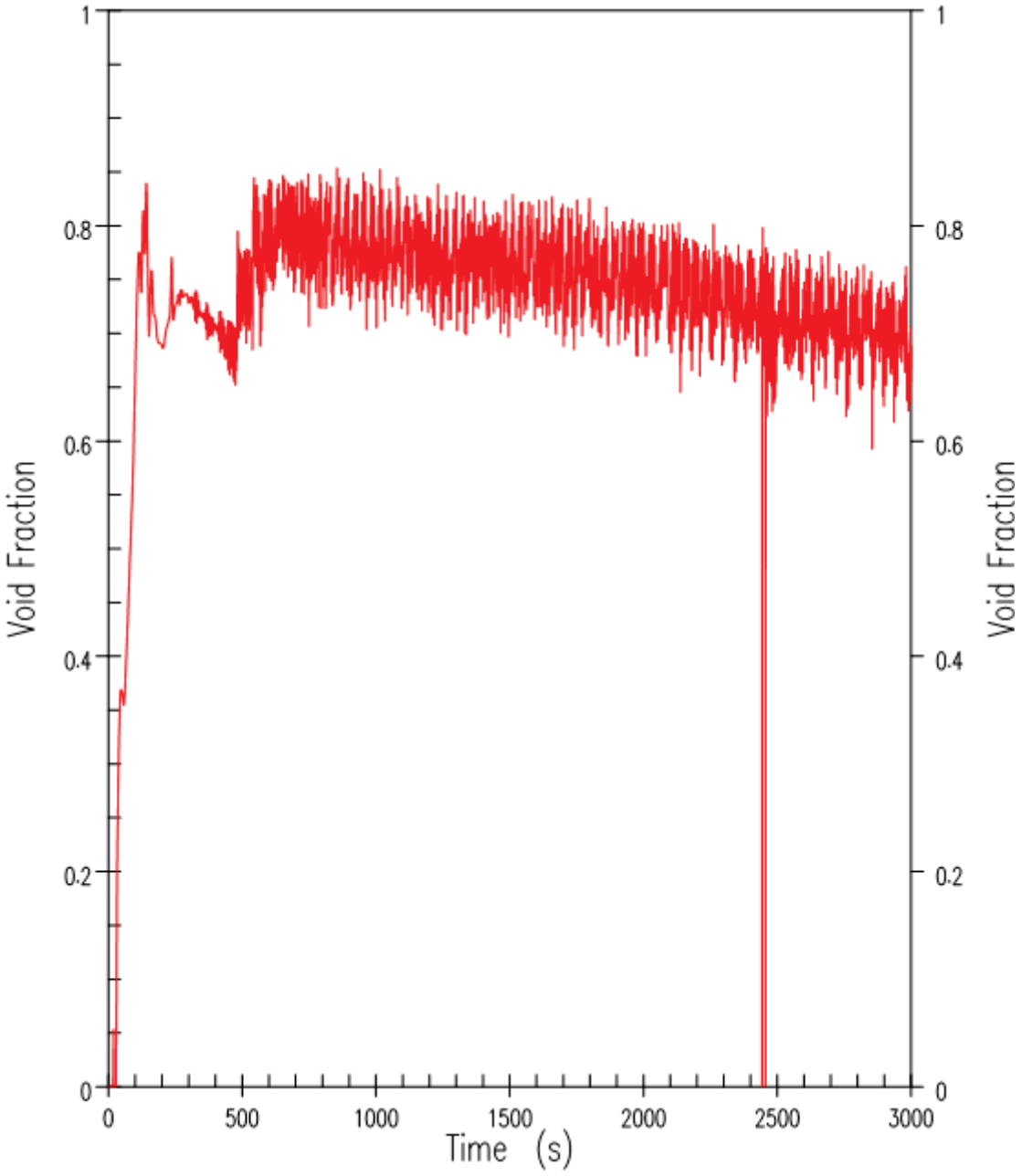


Figure 9.6.5-44. DBA DEDVI with 0.138 MPa abs (20 psia) Cont. – Core Exit Void Fraction

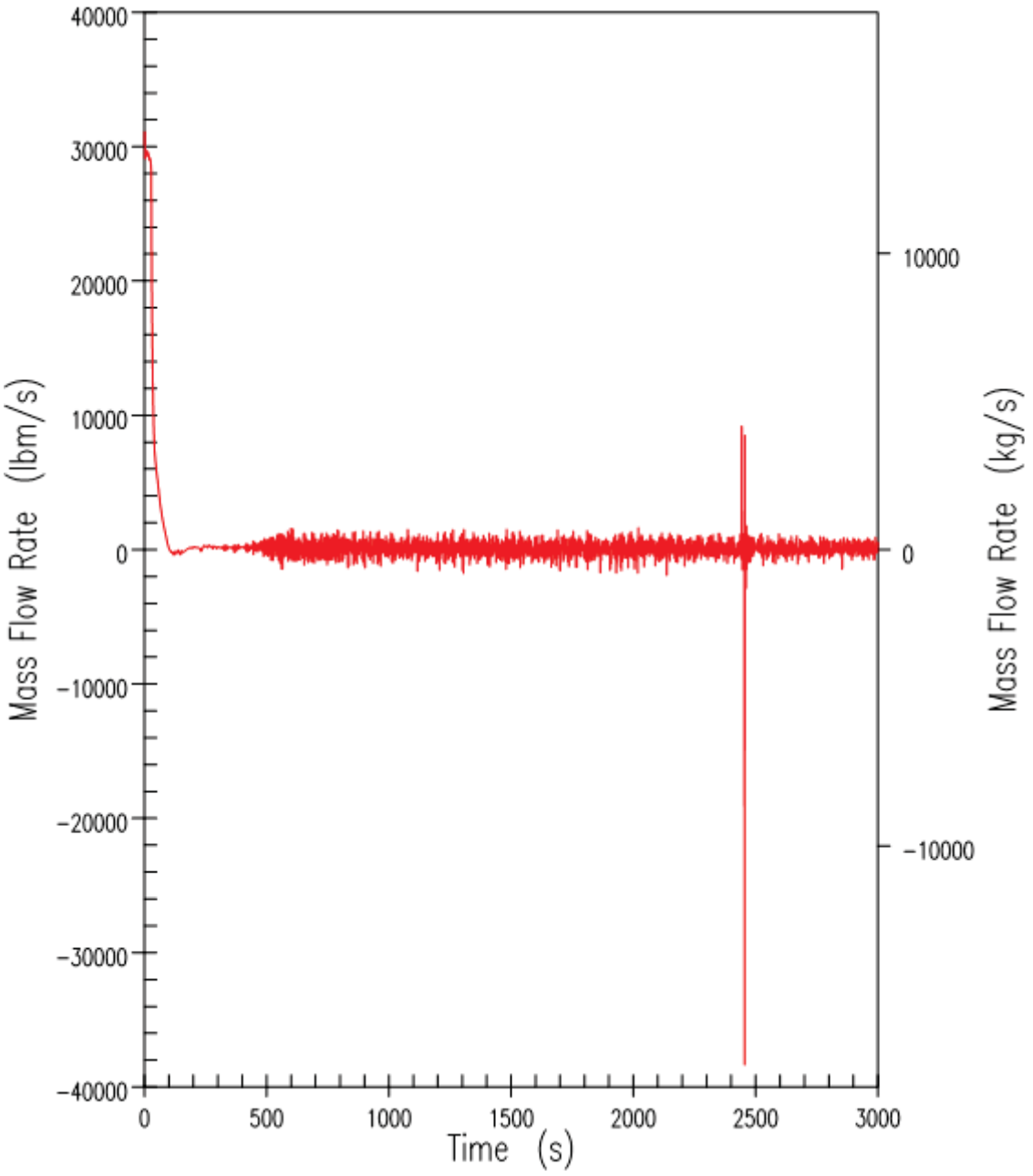


Figure 9.6.5-45. DBA DEDVI with 0.138 MPa abs (20 psia) Cont. – Core Exit Liquid Flow Rate

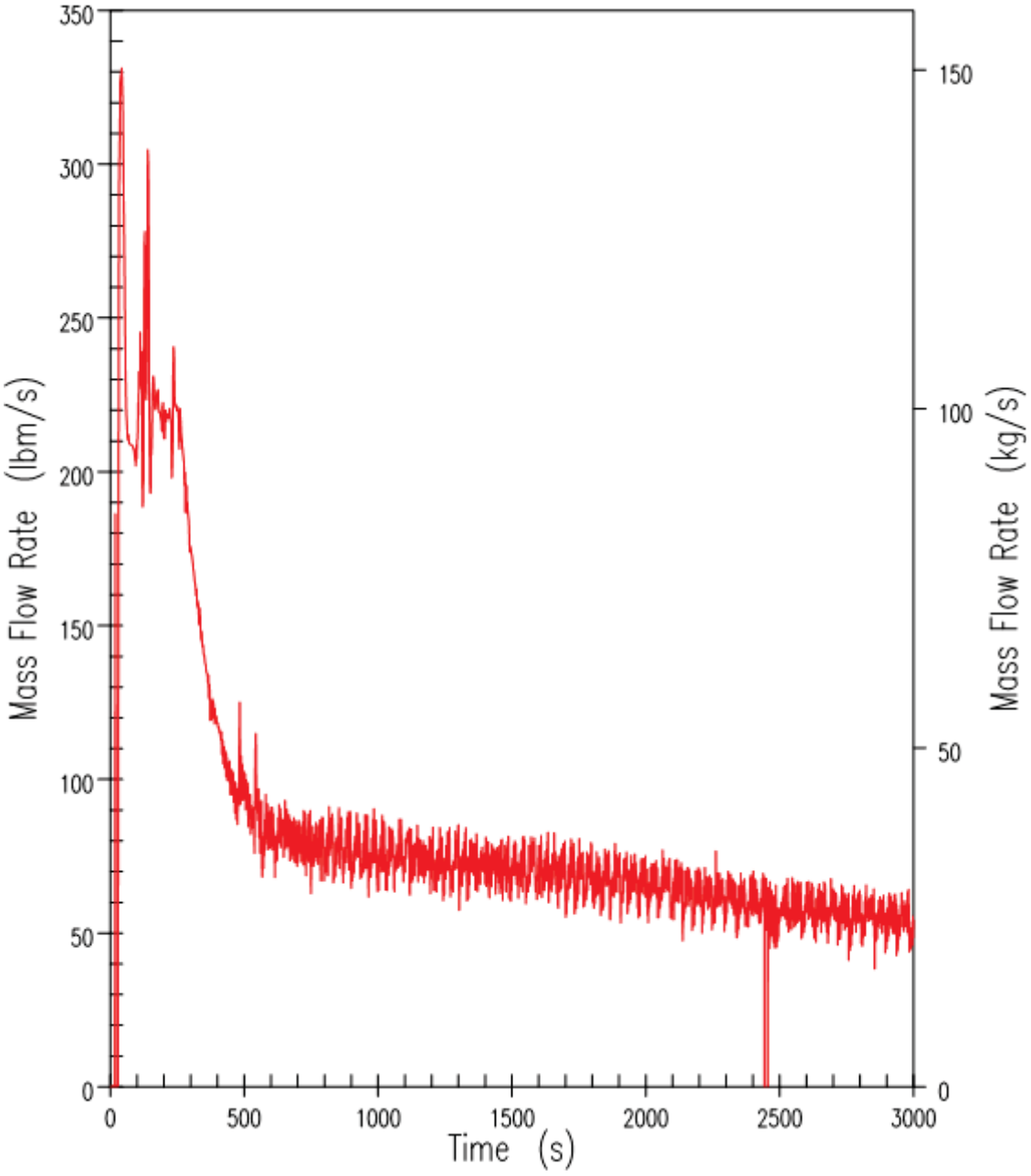


Figure 9.6.5-46. DBA DEDVI with 0.138 MPa abs (20 psia) Cont. – Core Exit Vapour Flow Rate

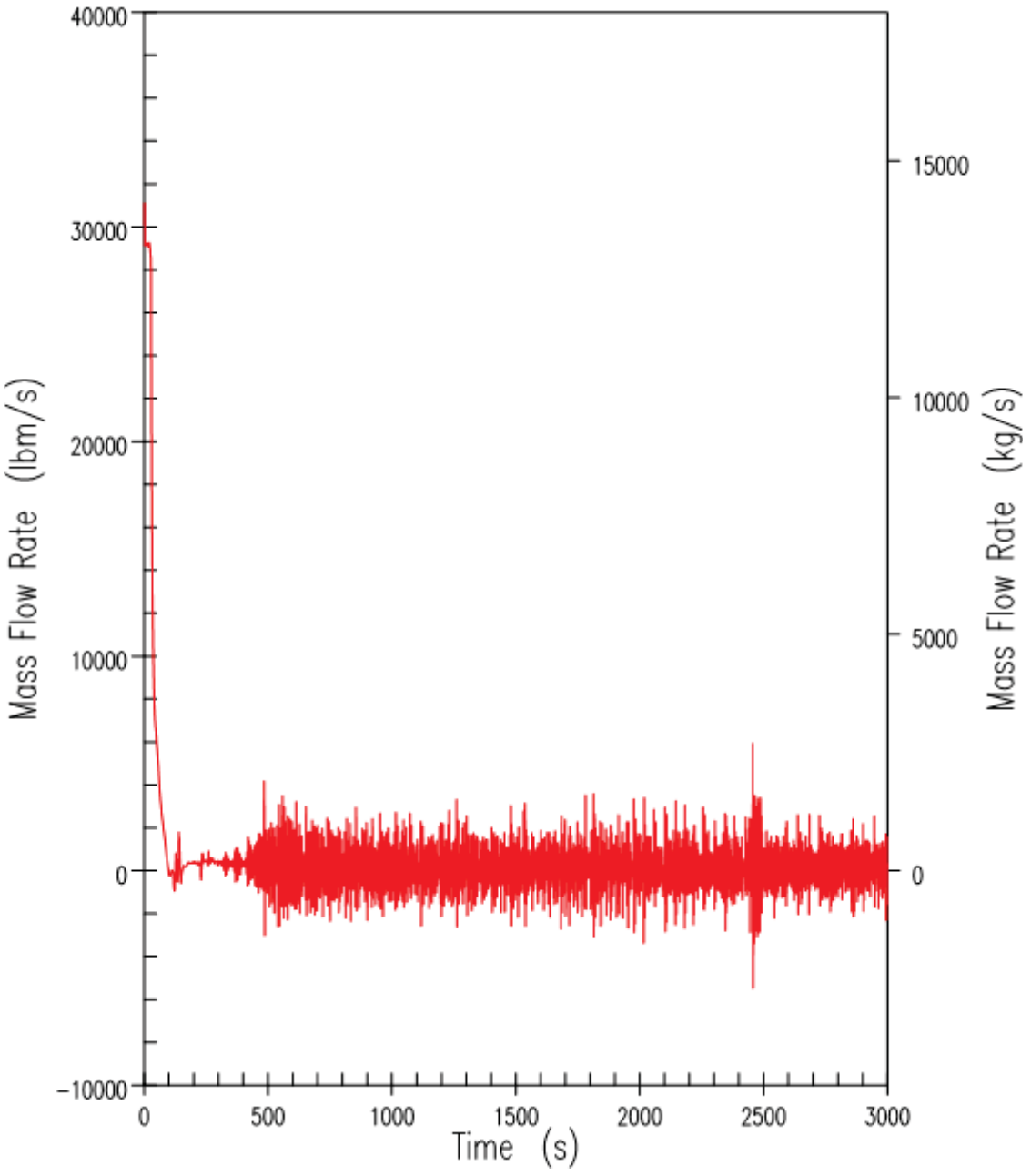


Figure 9.6.5-47. DBA DEDVI with 0.138 MPa abs (20 psia) Cont. – Lower Plenum to Core Flow Rate

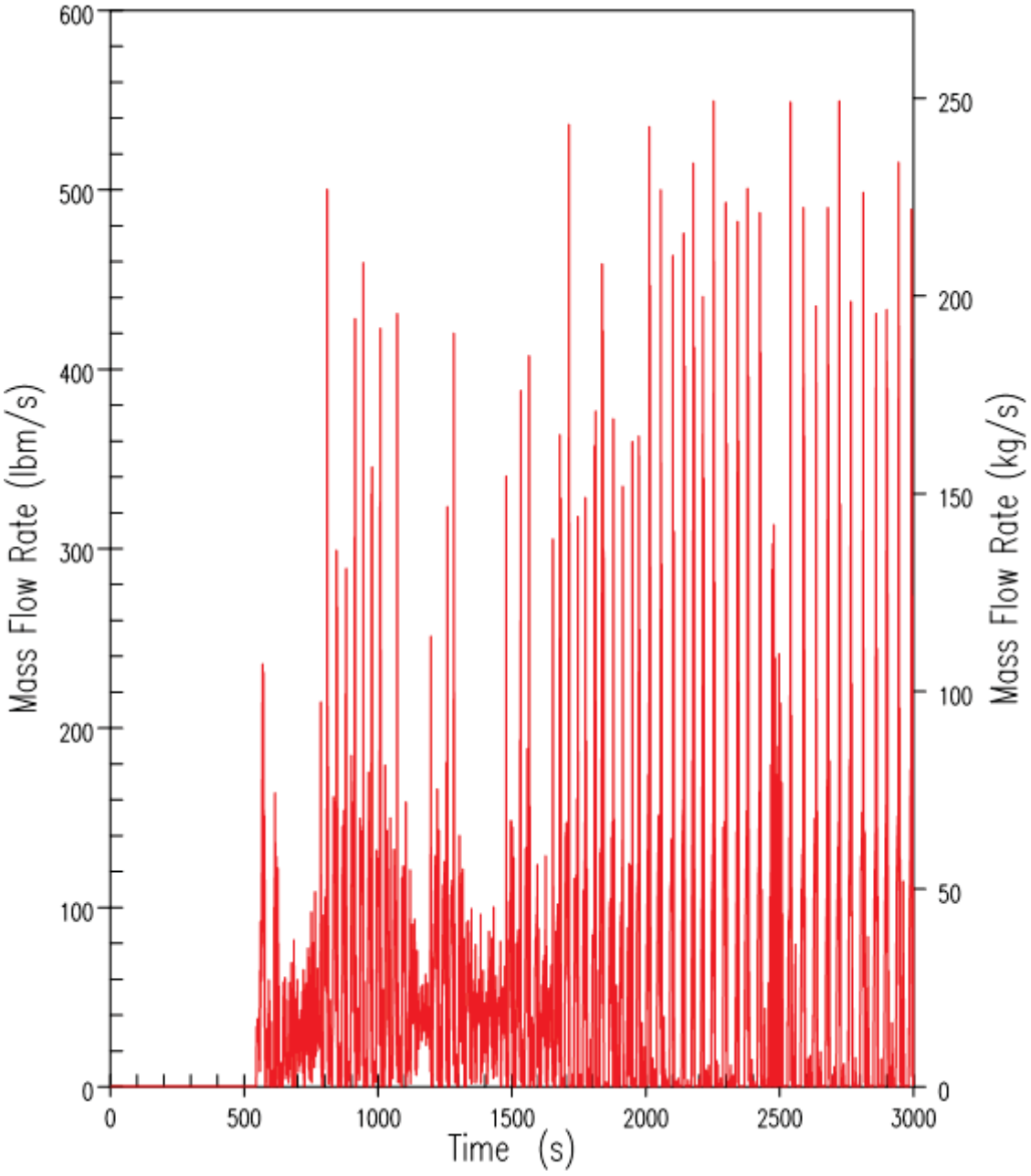


Figure 9.6.5-48(a). DBA DEDVI with 0.138 MPa abs (20 psia) Cont. – ADS-4 Liquid Discharge

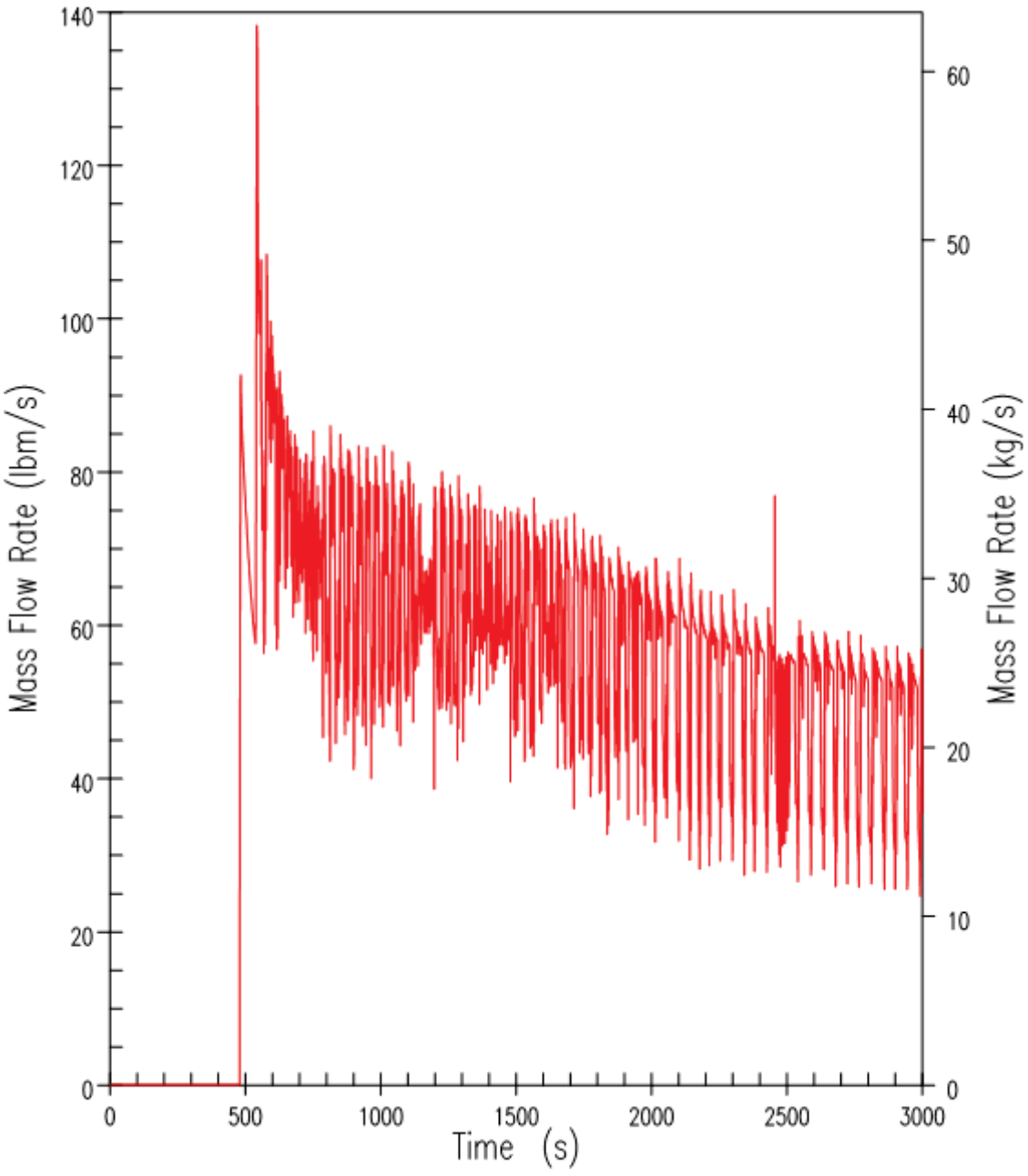


Figure 9.6.5-48(b). DBA DEDVI with 0.138 MPa abs (20 psia) Cont. – ADS-4 Vapour Discharge

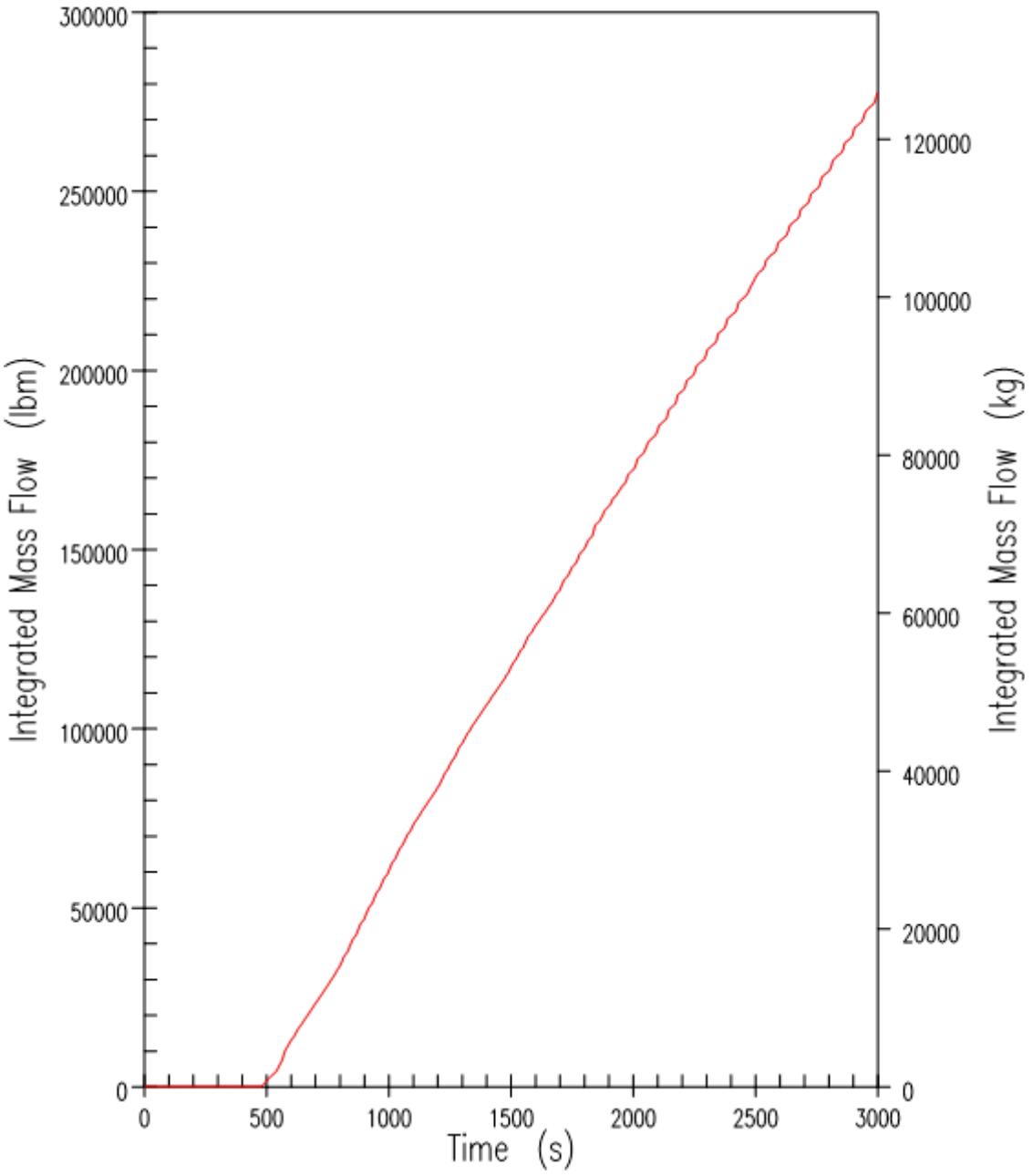


Figure 9.6.5-49. DBA DEDVI with 0.138 MPa abs (20 psia) Cont. – ADS-4 Integrated Discharge

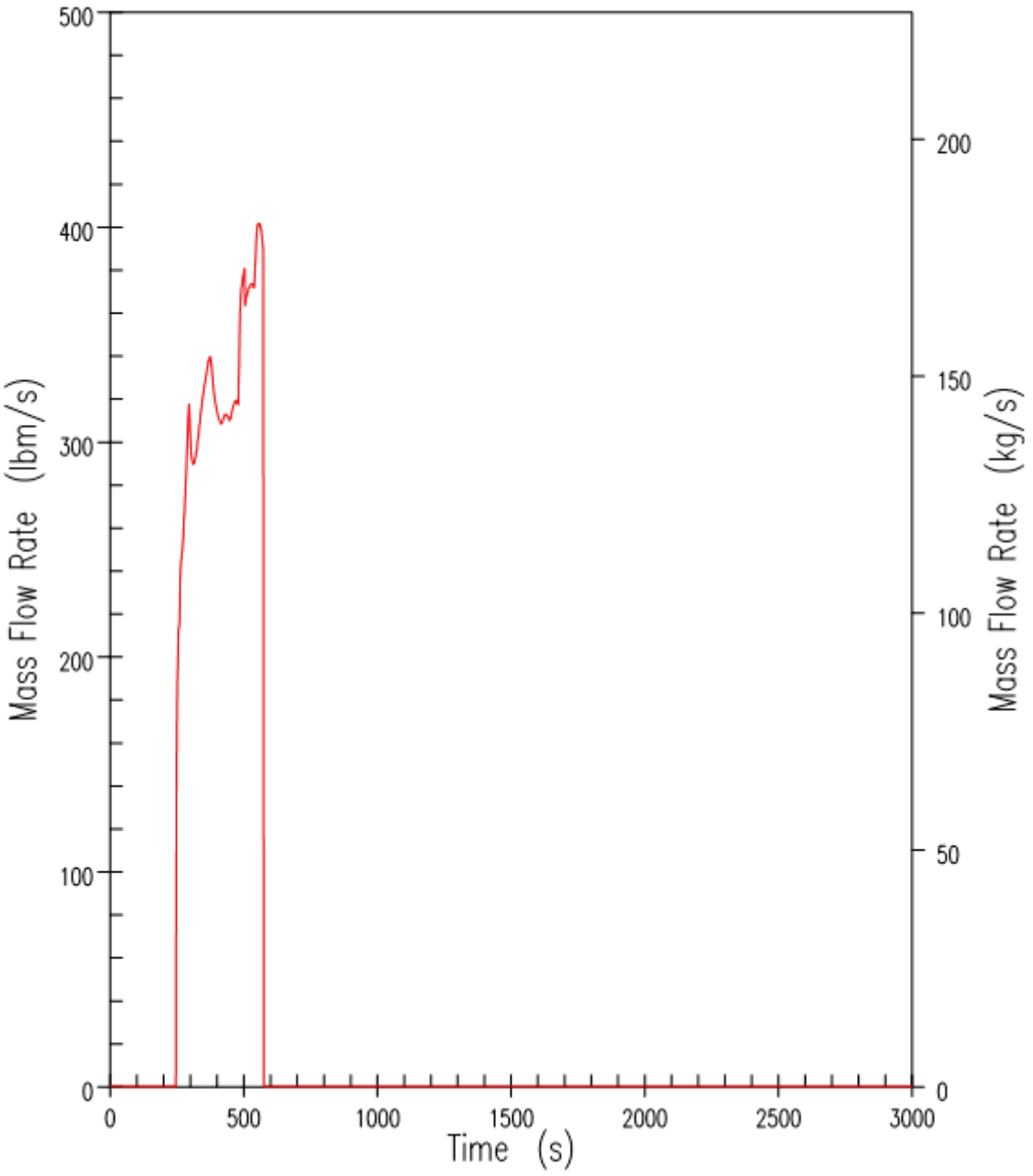


Figure 9.6.5-50. DBA DEDVI with 0.138 MPa abs (20 psia) Cont. – Intact Accumulator Flow Rate

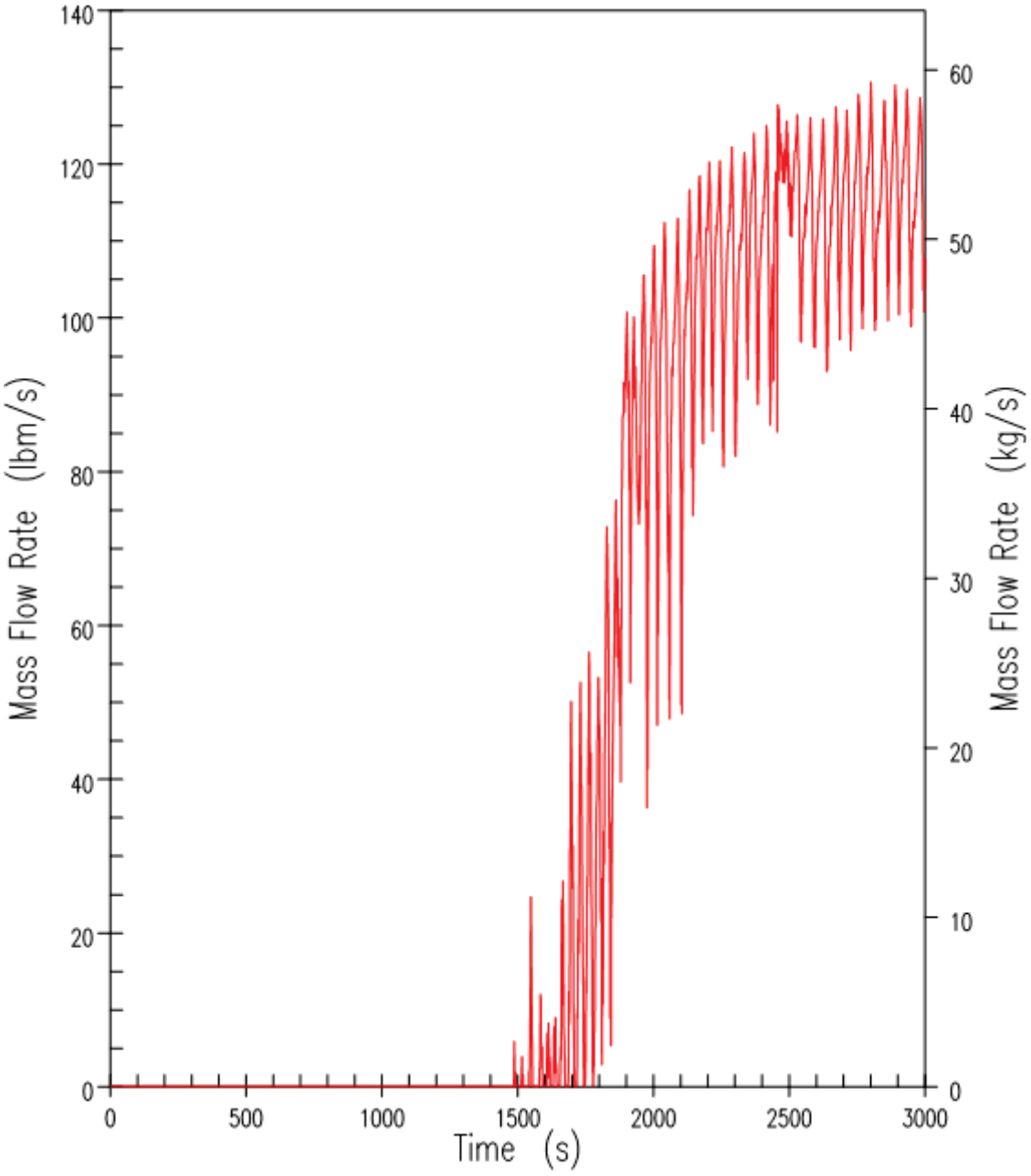


Figure 9.6.5-51. DBA DEDVI with 0.138 MPa abs (20 psia) Cont. – Intact IRWST Injection Rate

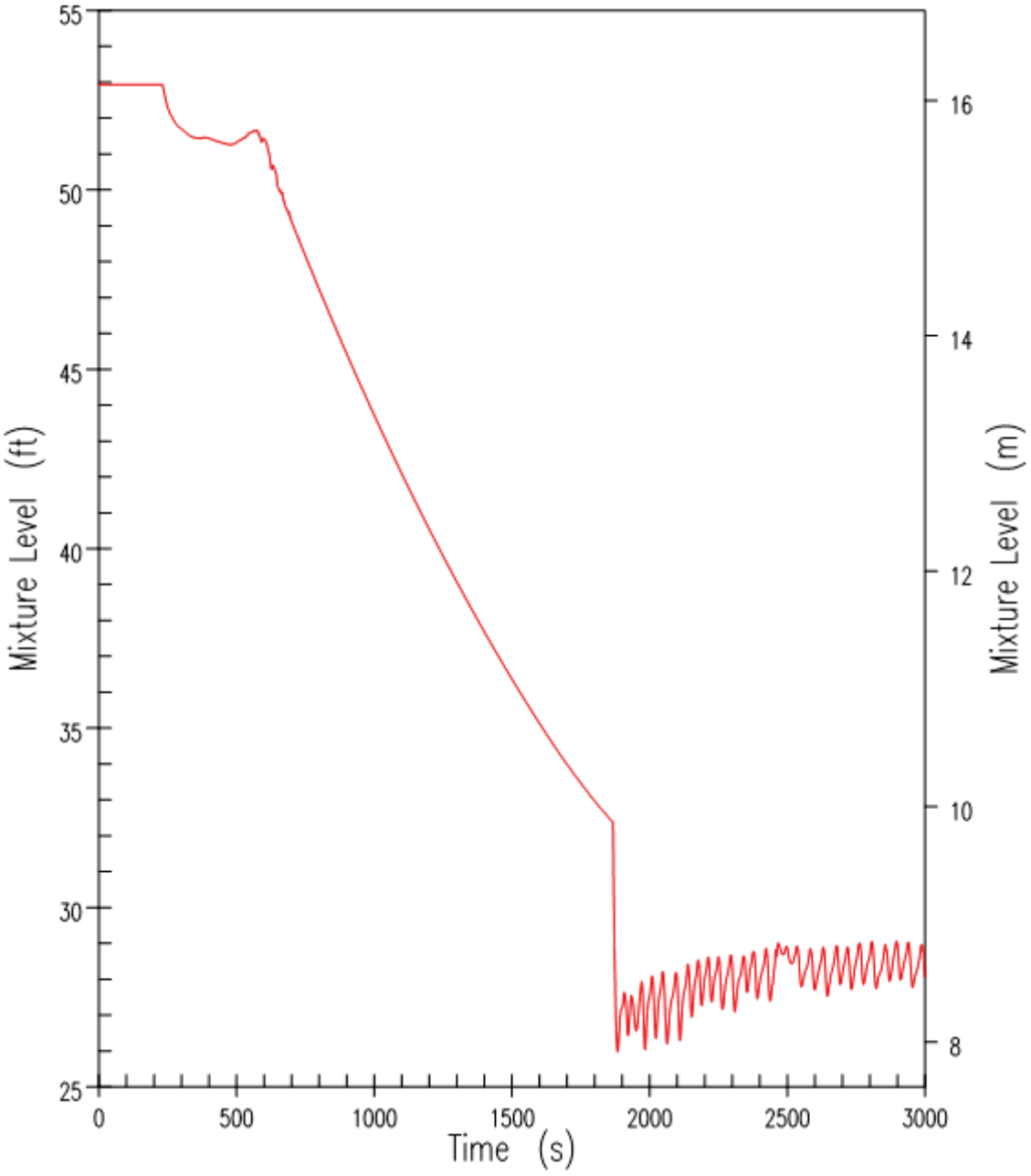


Figure 9.6.5-52. DBA DEDVI with 0.138 MPa abs (20 psia) Cont. – Intact CMT Mixture Level

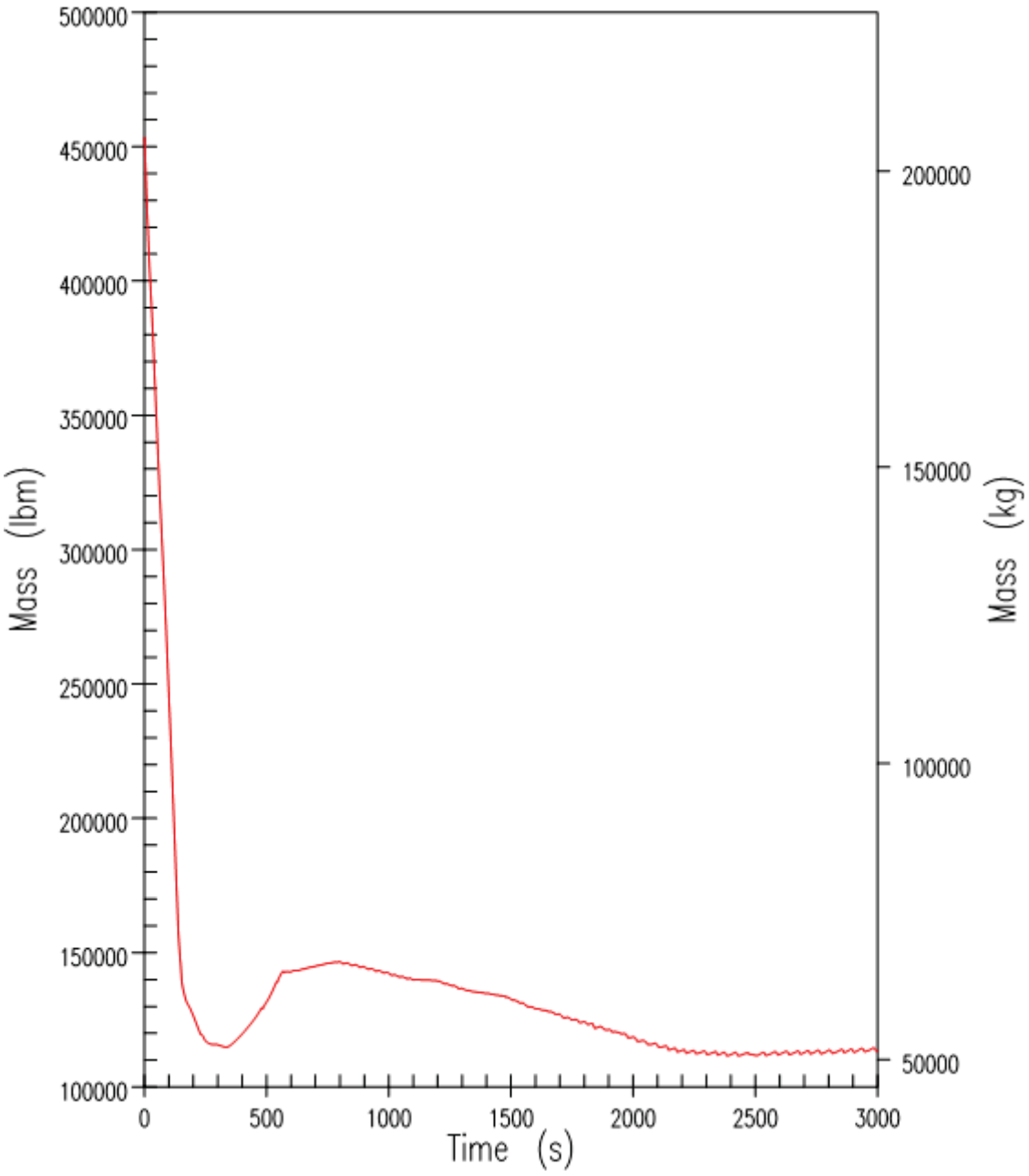


Figure 9.6.5-53(a). DBA DEDVI with 0.138 MPa abs (20 psia) Cont. – RCS System Inventory

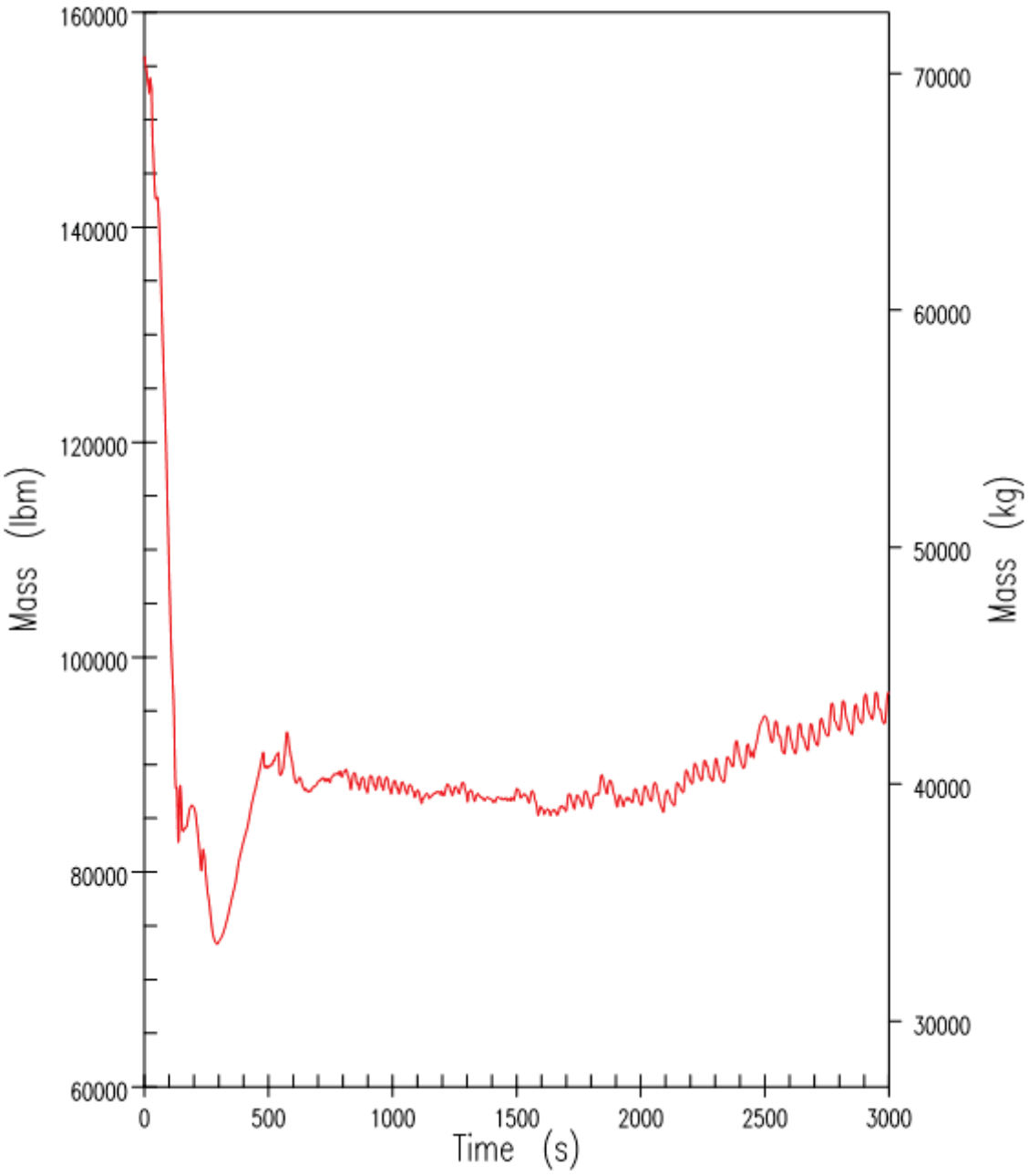


Figure 9.6.5-53(b). DBA DEDVI with 0.138 MPa abs (20 psia) Cont. – Reactor Vessel Mixture Inventory

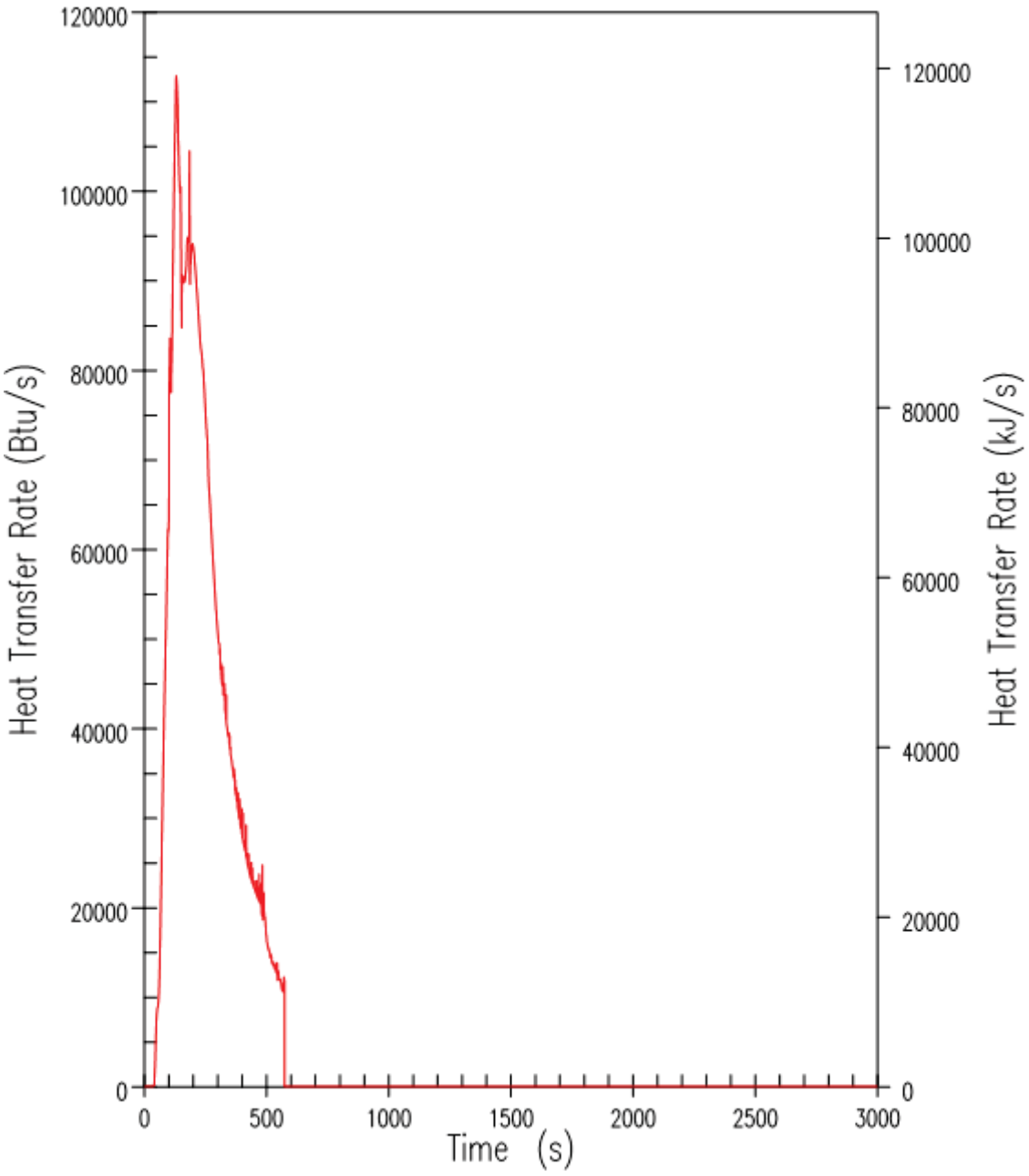


Figure 9.6.5-54. DBA DEDVI with 0.138 MPa abs (20 psia) Cont. – PRHR Heat Removal Rate

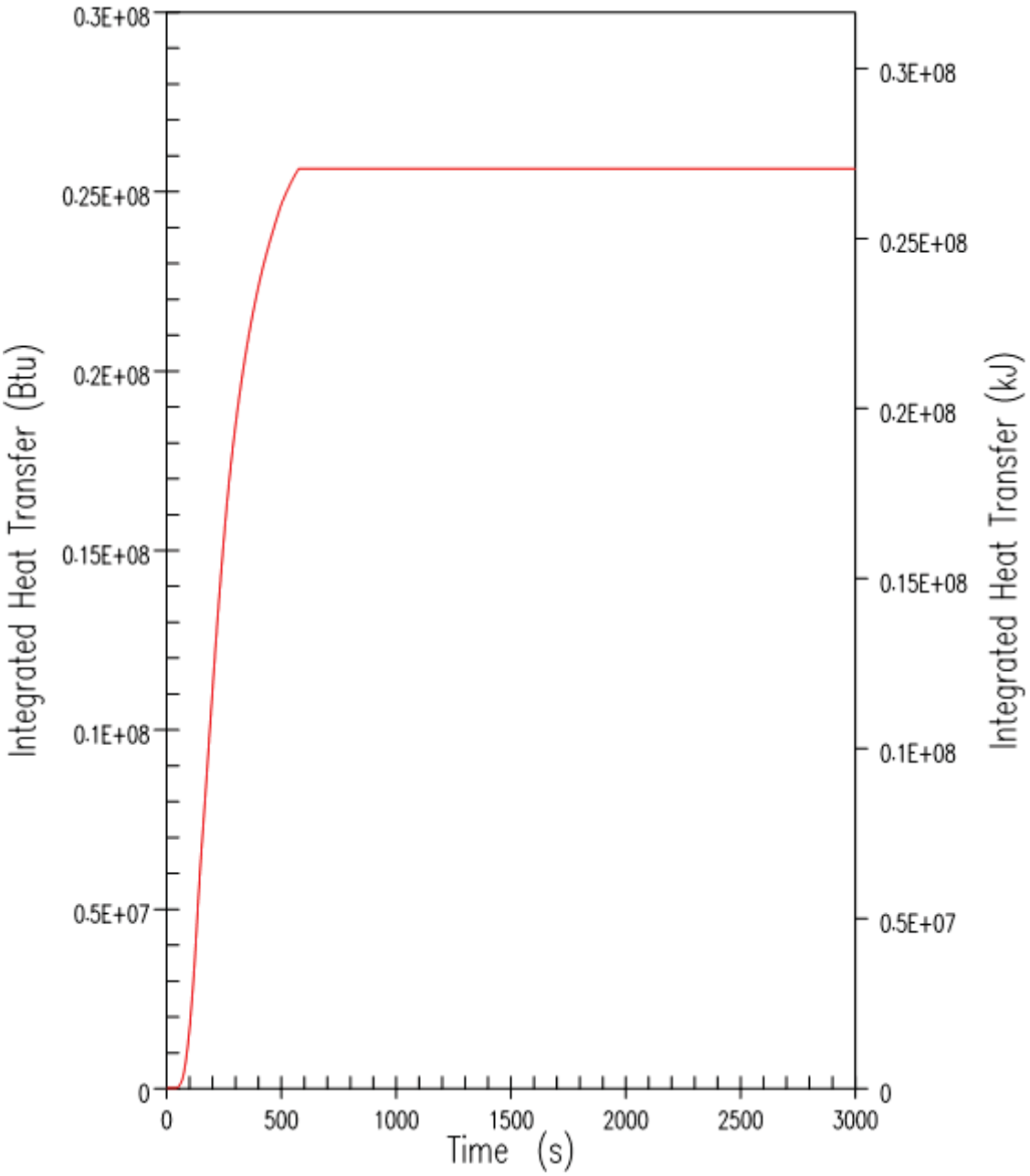


Figure 9.6.5-55. DBA DEDVI with 0.138 MPa abs (20 psia) Cont. – Integrated PRHR Heat Removal

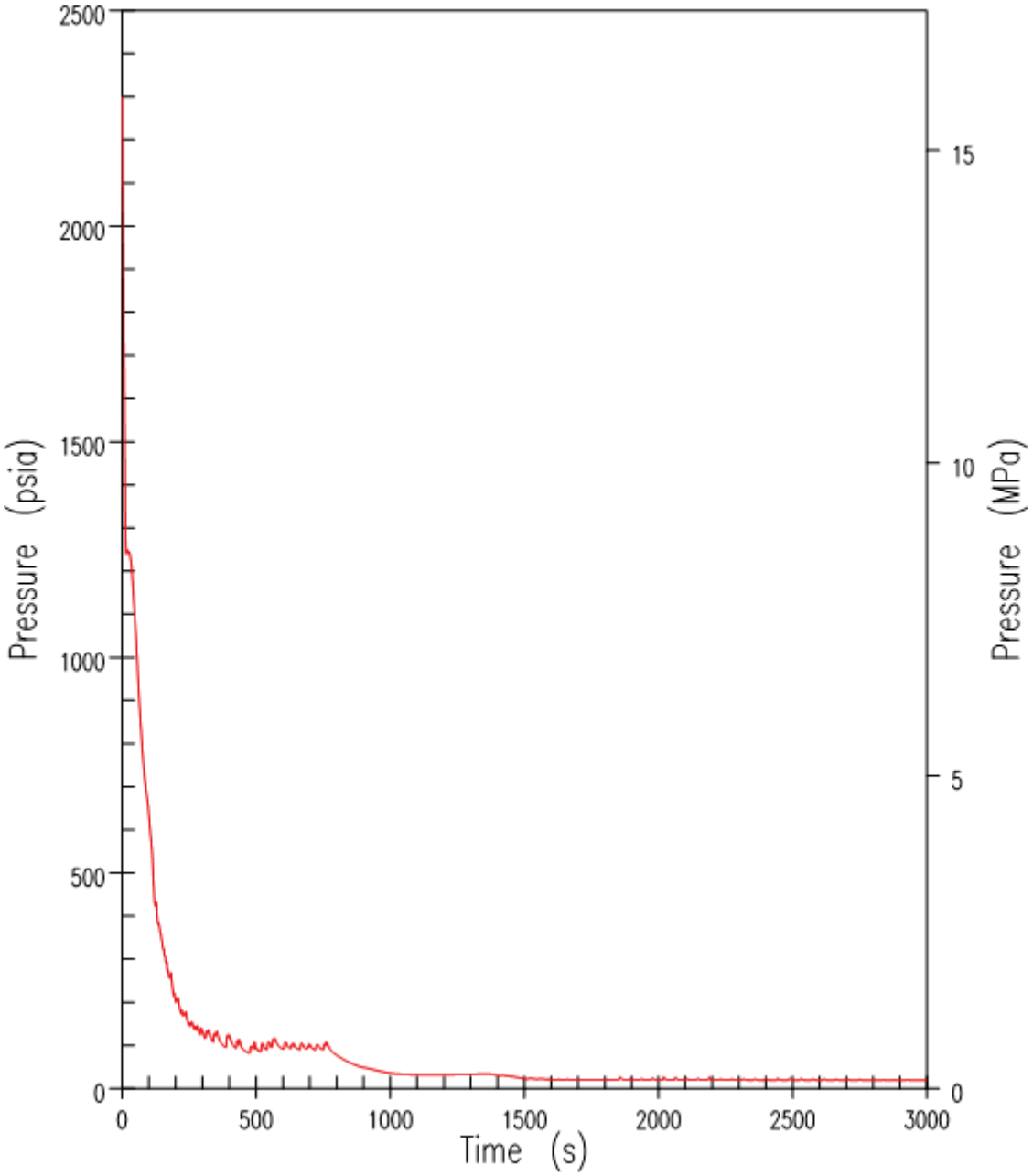


Figure 9.6.5-56(a). DBA 254 mm (10-Inch) Cold Leg Break – RCS Pressure

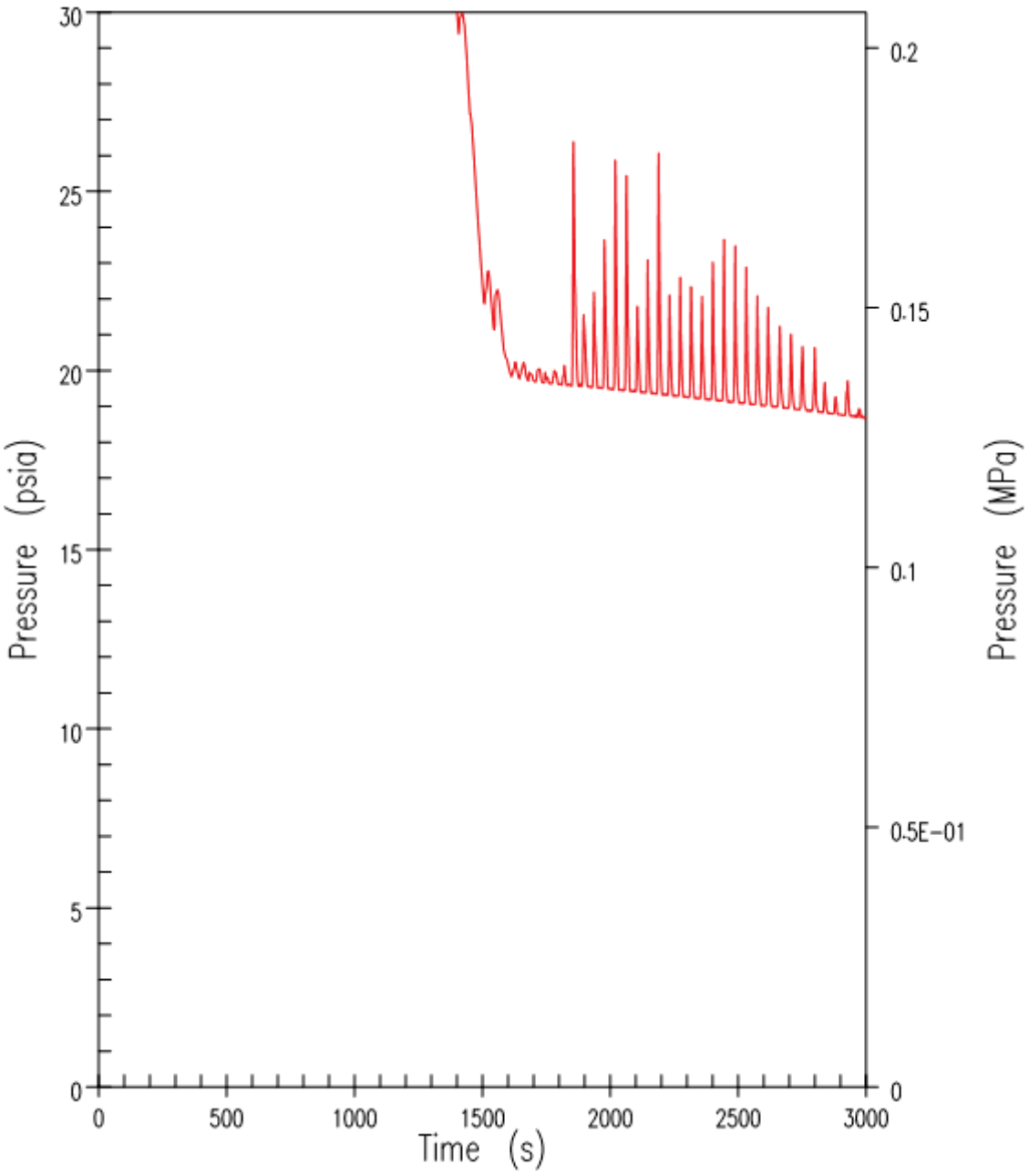


Figure 9.6.5-56(b). DBA 254 mm (10-Inch) Cold Leg Break – RCS Pressure (Zoomed)

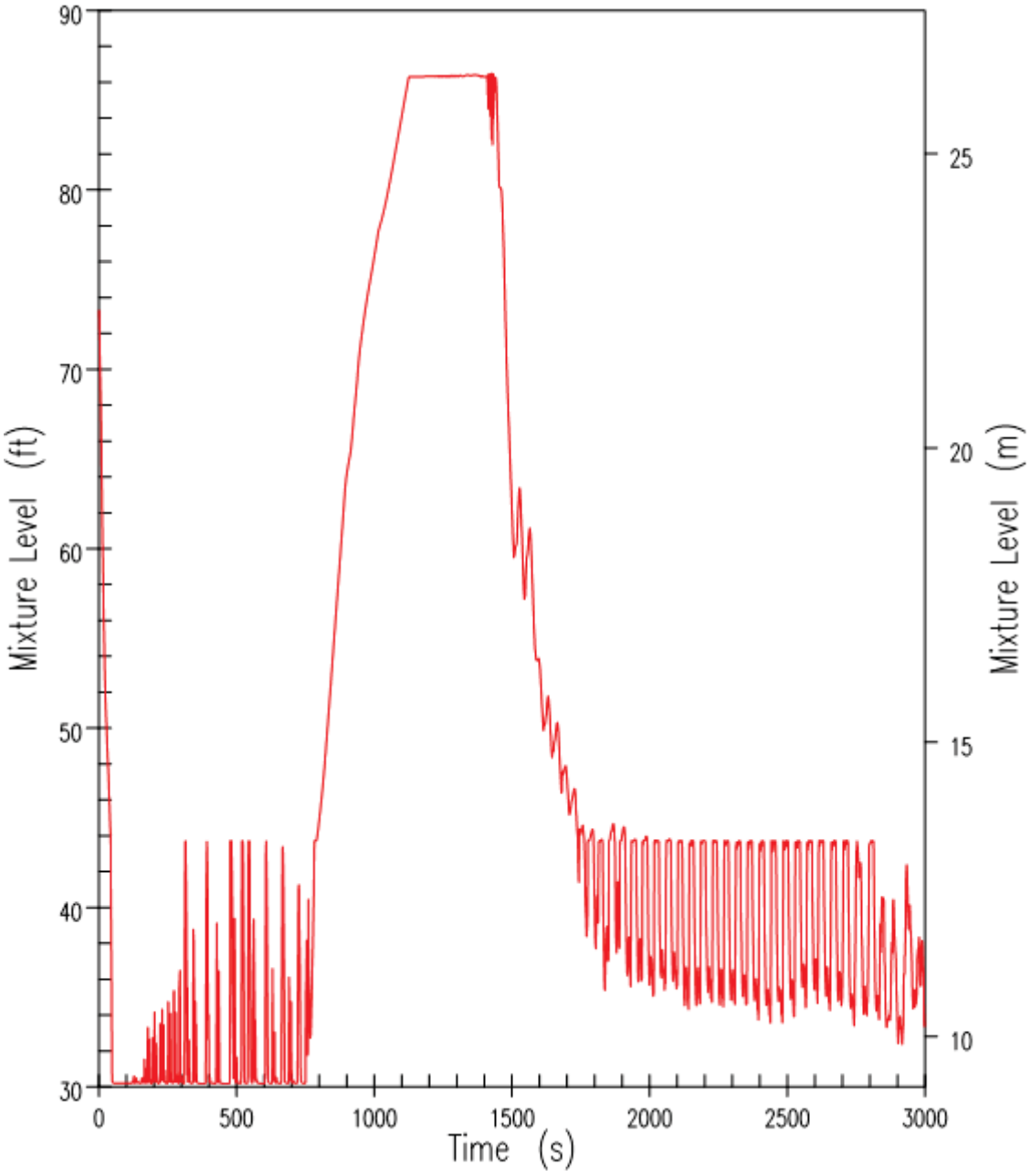


Figure 9.6.5-57. DBA 254 mm (10-Inch) Cold Leg Break – Pressuriser Mixture Level

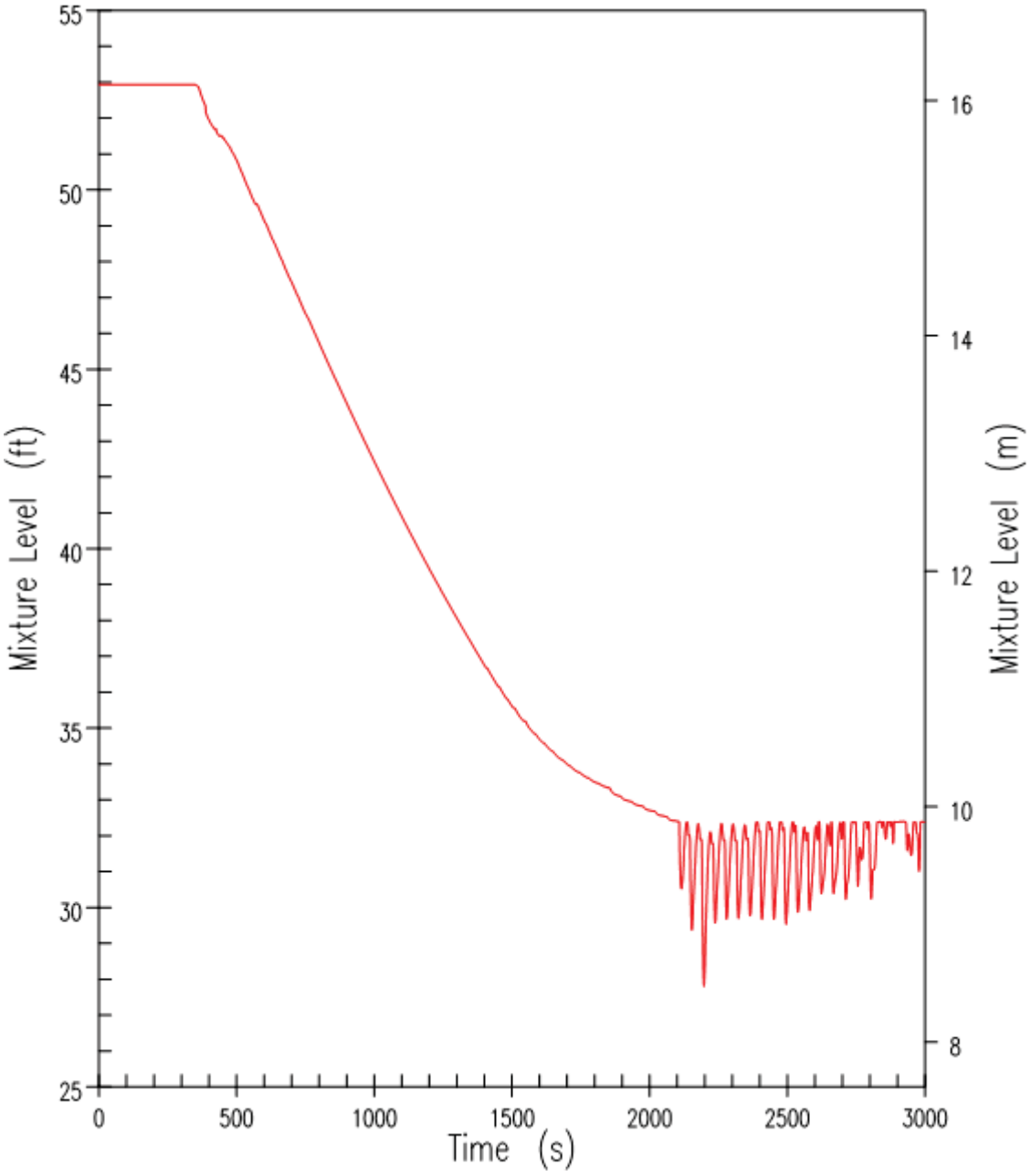


Figure 9.6.5-58. DBA 254 mm (10-Inch) Cold Leg Break – CMT-1 Mixture Level

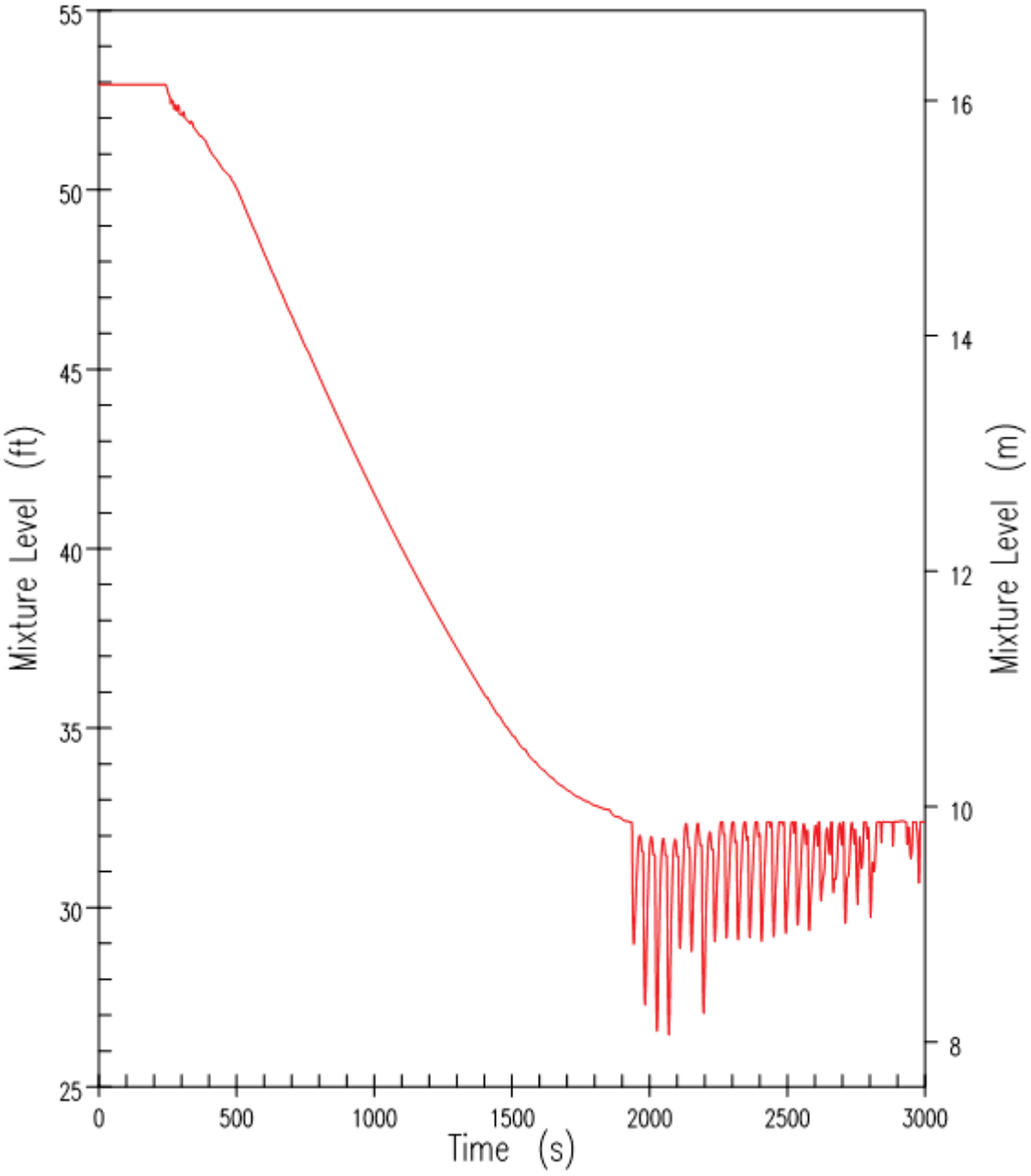


Figure 9.6.5-59. DBA 254 mm (10-Inch) Cold Leg Break – CMT-2 Mixture Level

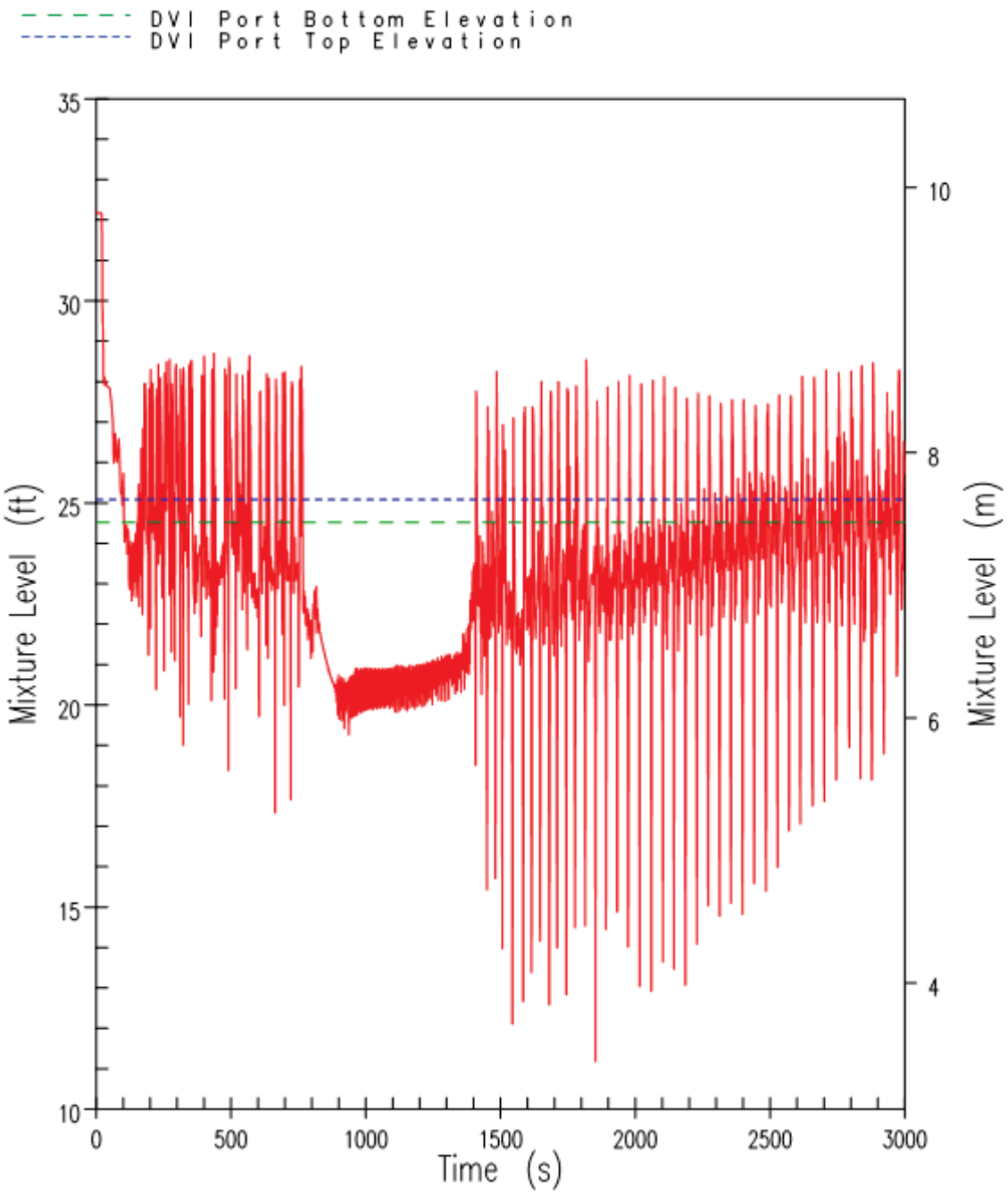


Figure 9.6.5-60. DBA 254 mm (10-Inch) Cold Leg Break – Downcomer Mixture Level

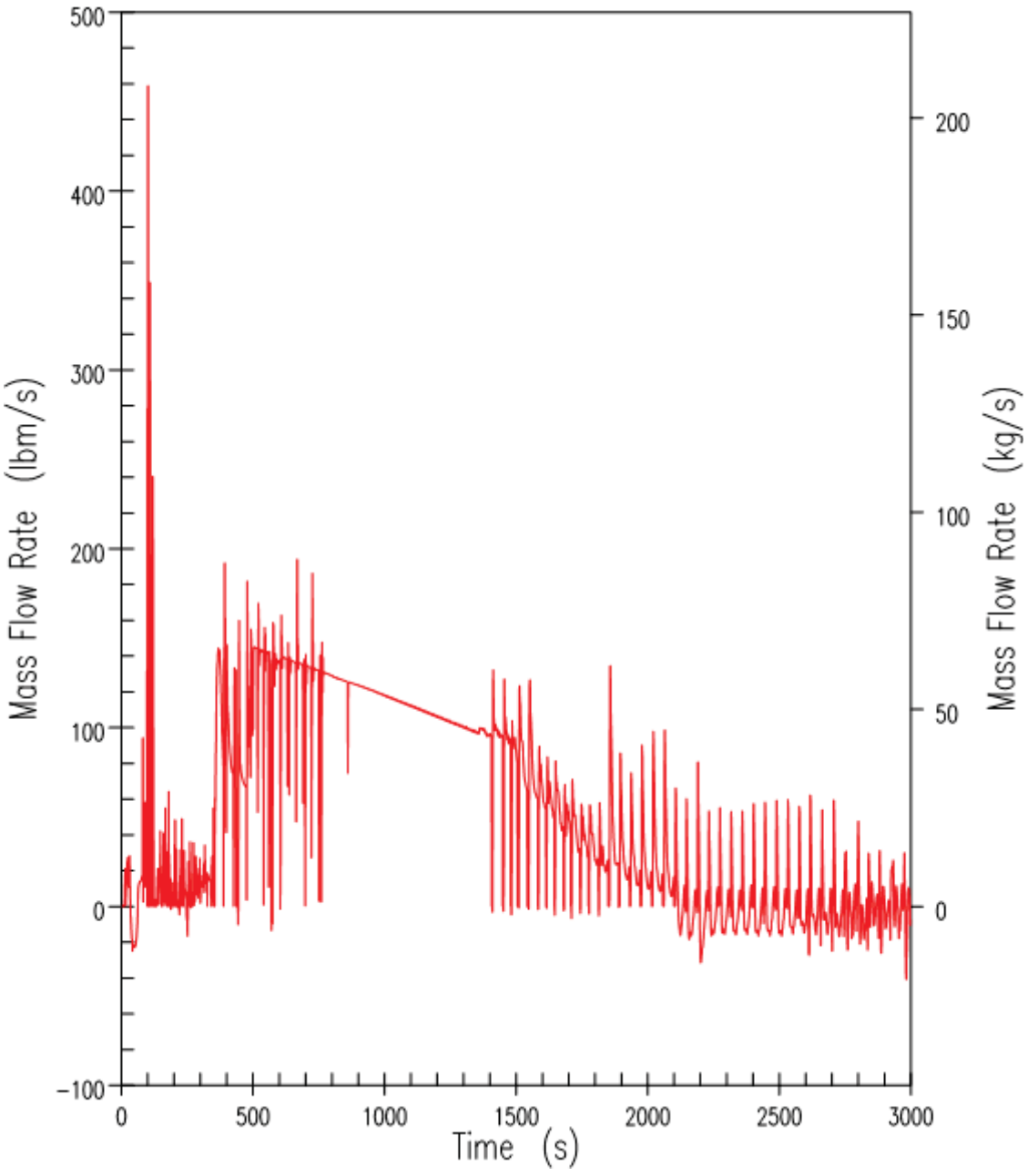


Figure 9.6.5-61. DBA 254 mm (10-Inch) Cold Leg Break – CMT-1 Injection Rate

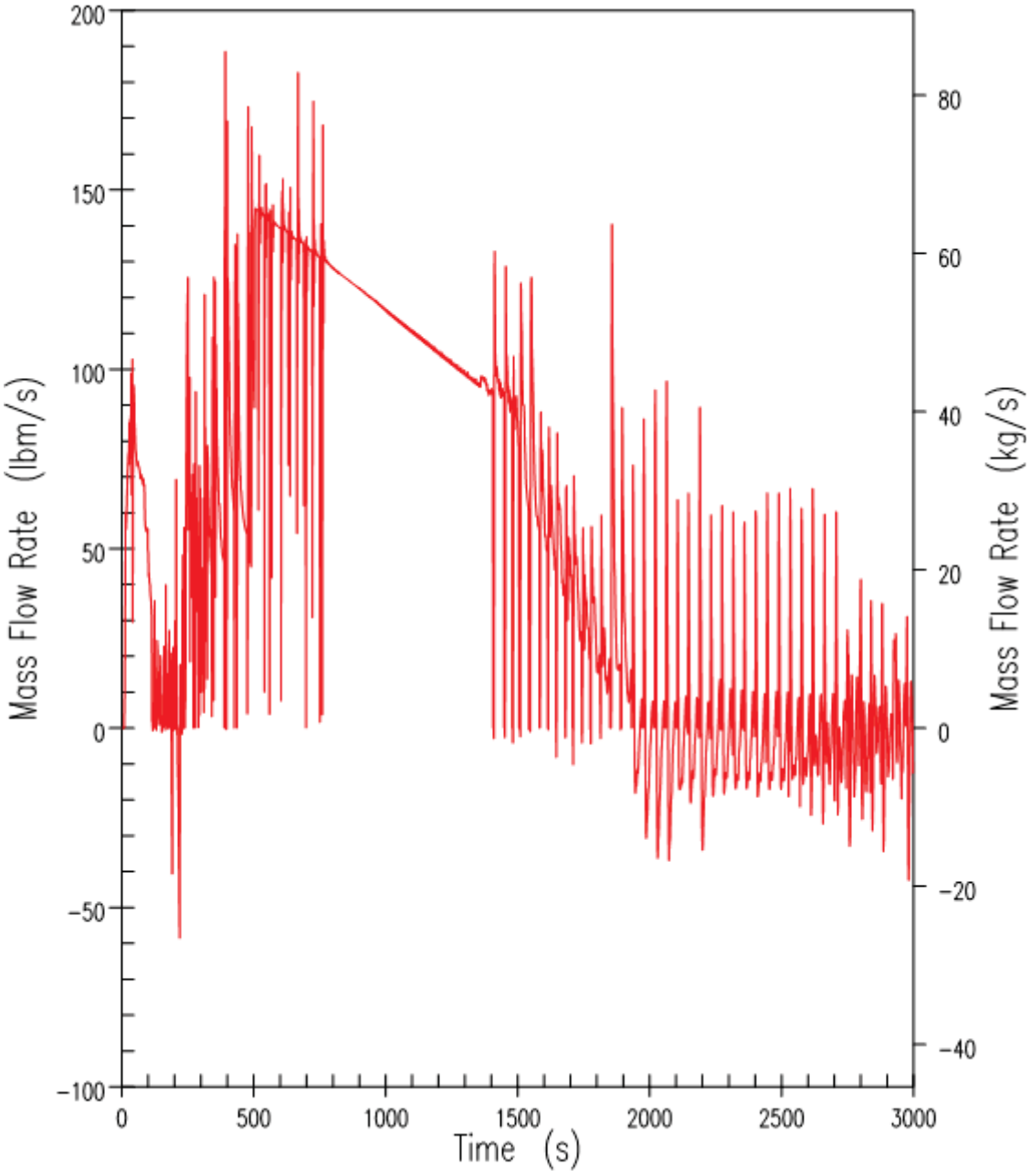


Figure 9.6.5-62. DBA 254 mm (10-Inch) Cold Leg Break – CMT-2 Injection Rate

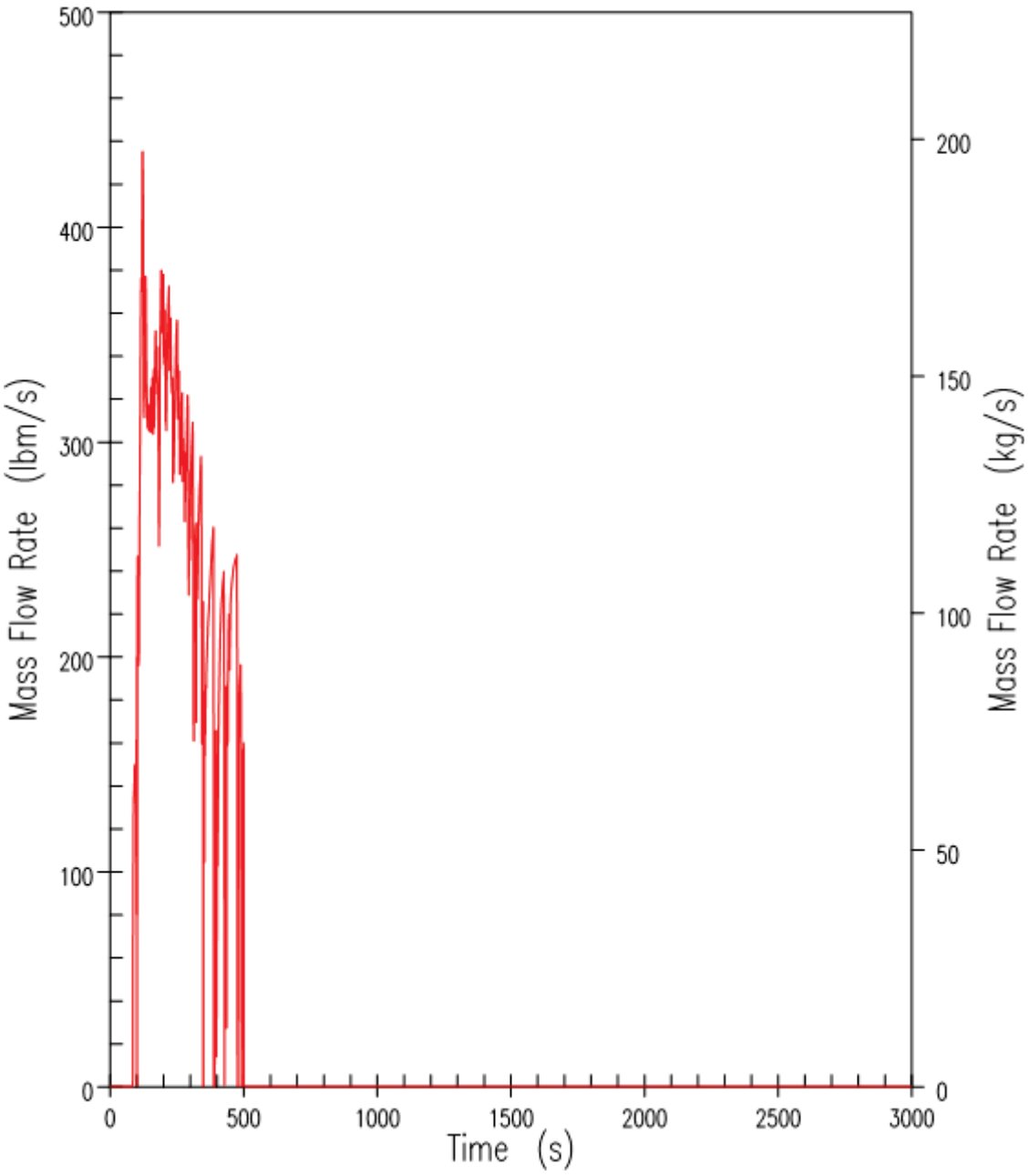


Figure 9.6.5-63. DBA 254 mm (10-Inch) Cold Leg Break – Accumulator-1 Injection Rate

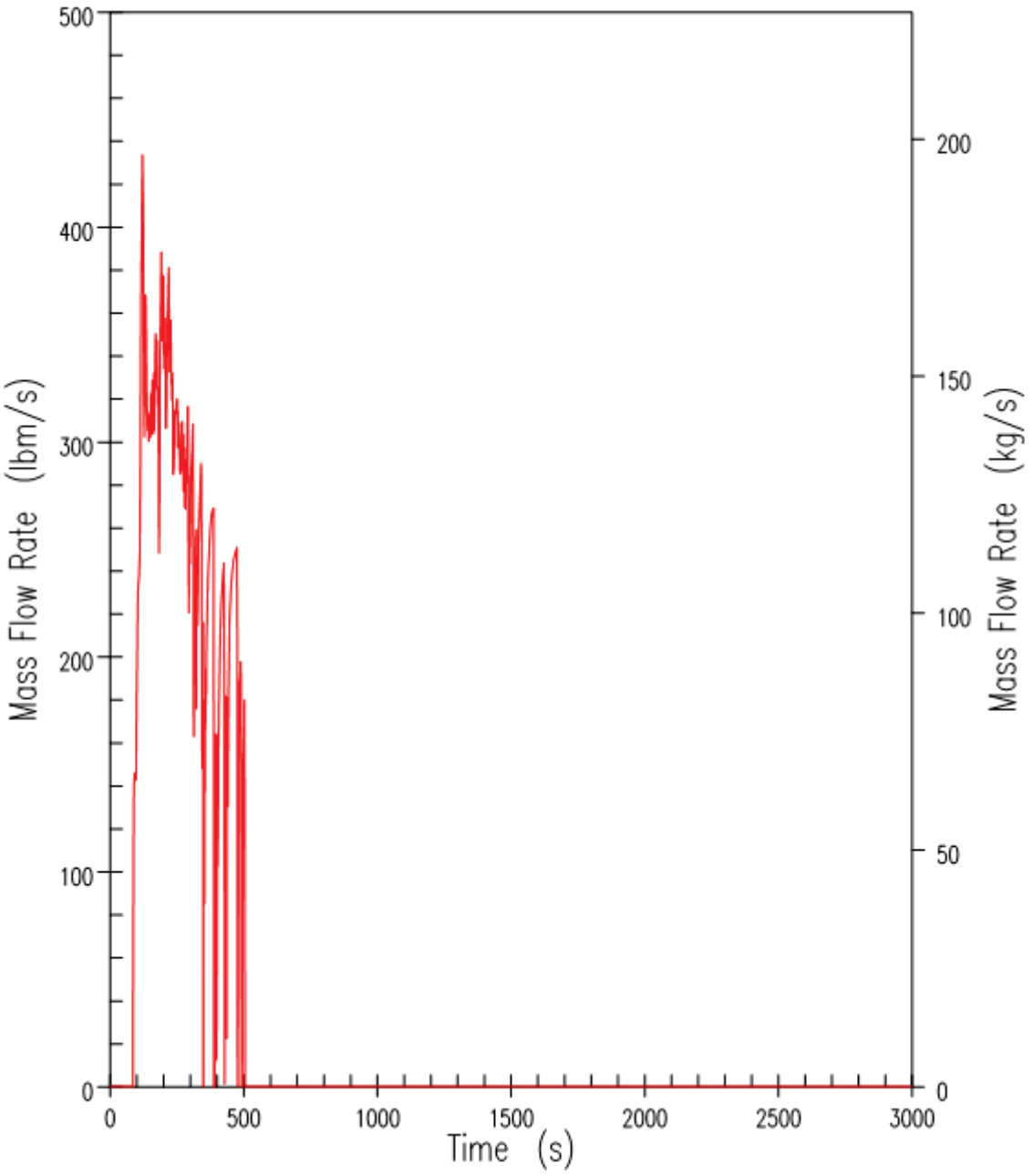


Figure 9.6.5-64. DBA 254 mm (10-Inch) Cold Leg Break – Accumulator-2 Injection Rate

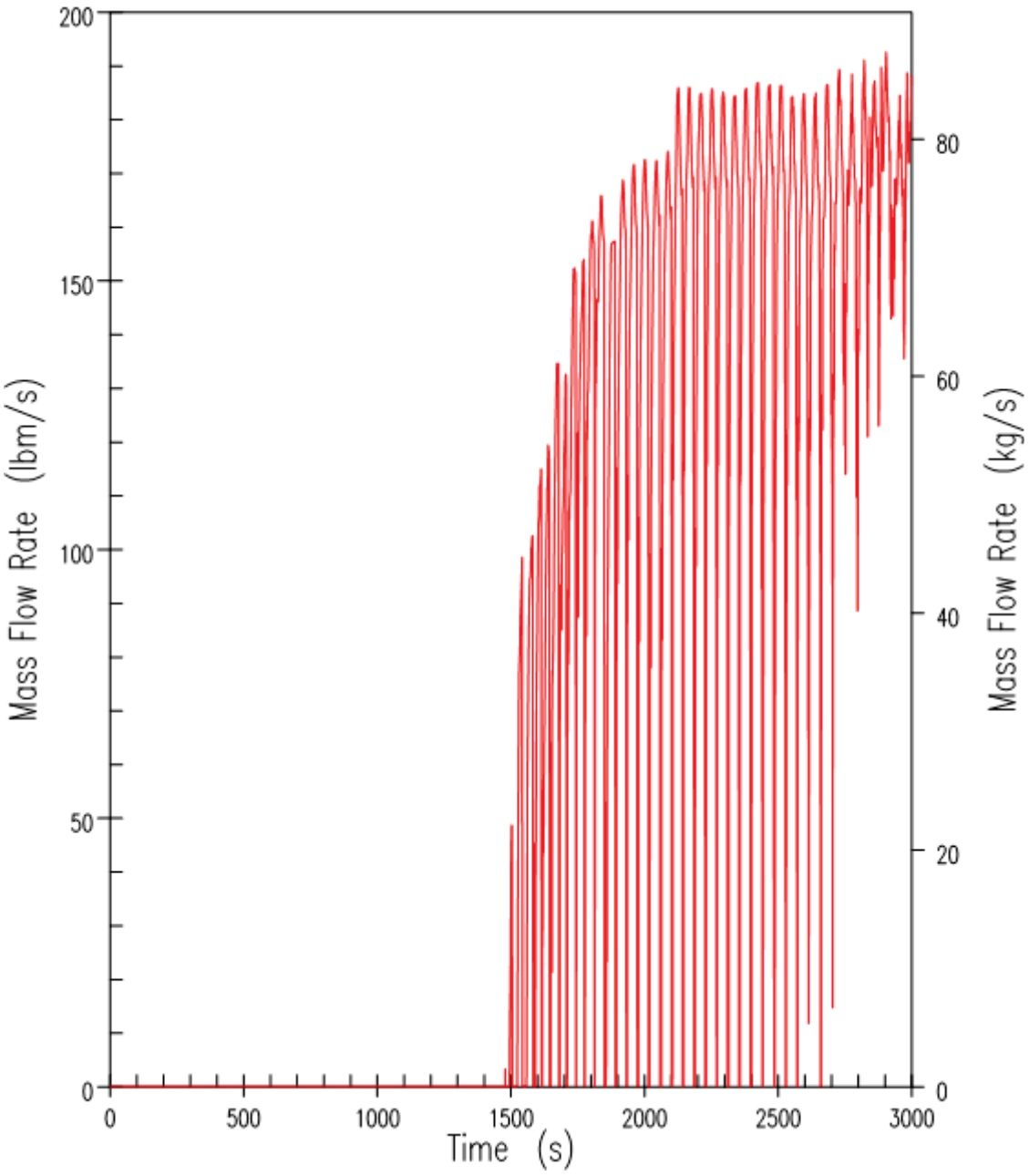


Figure 9.6.5-65. DBA 254 mm (10-Inch) Cold Leg Break – IRWST-1 Injection Rate

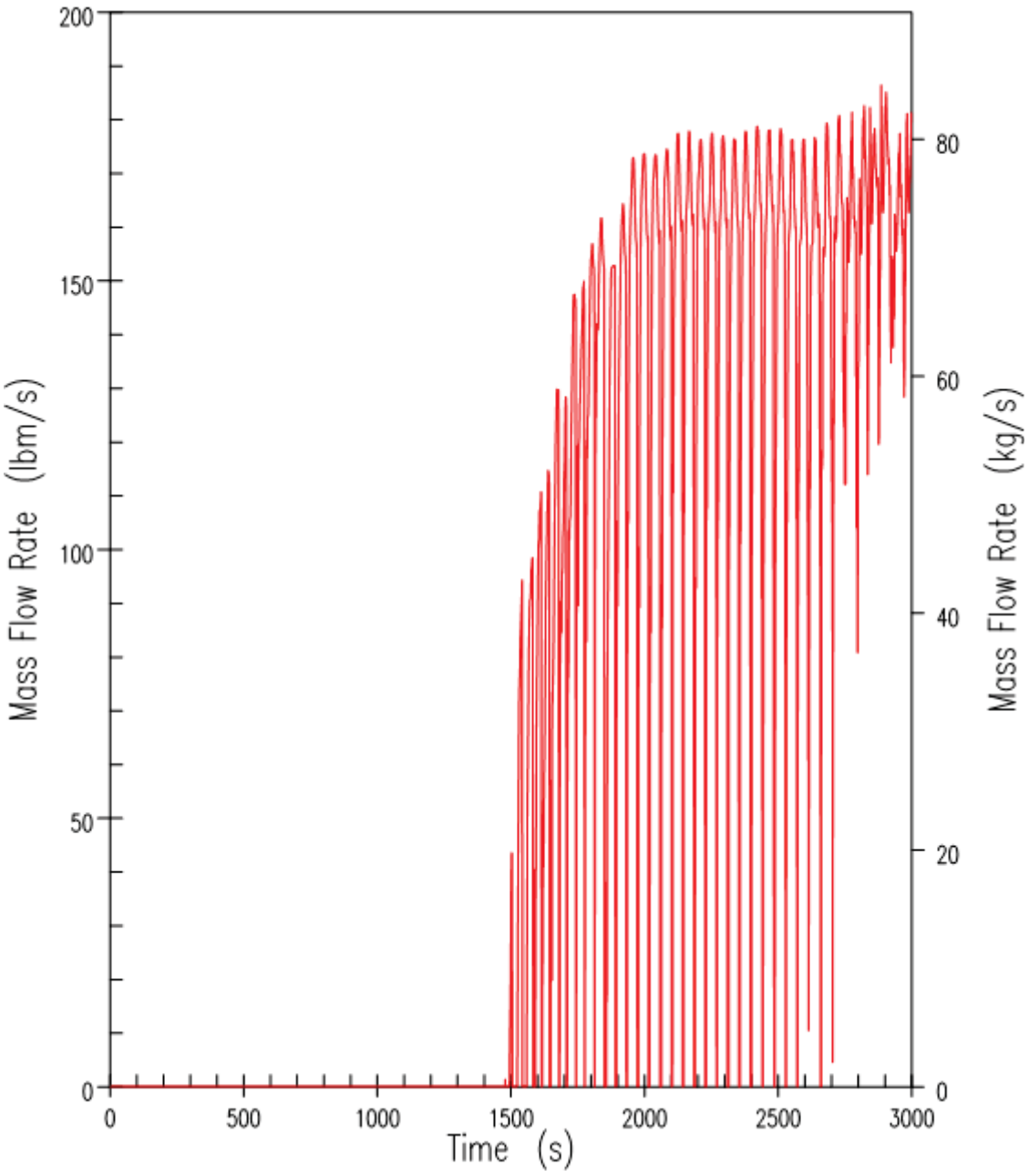


Figure 9.6.5-66. DBA 254 mm (10-Inch) Cold Leg Break – IRWST-2 Injection Rate

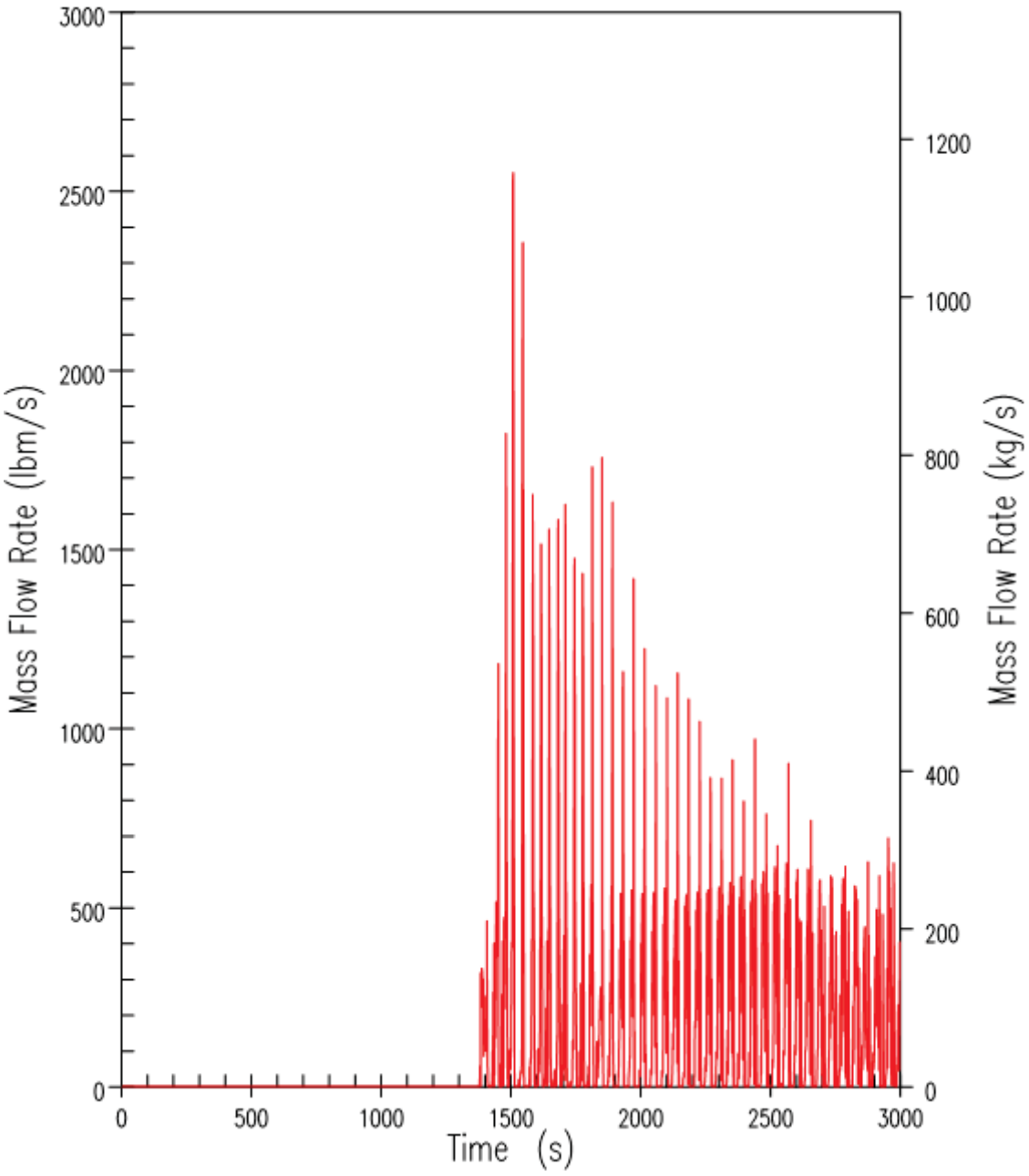


Figure 9.6.5-67(a). DBA 254 mm (10-Inch) Cold Leg Break – ADS-4 Liquid Discharge

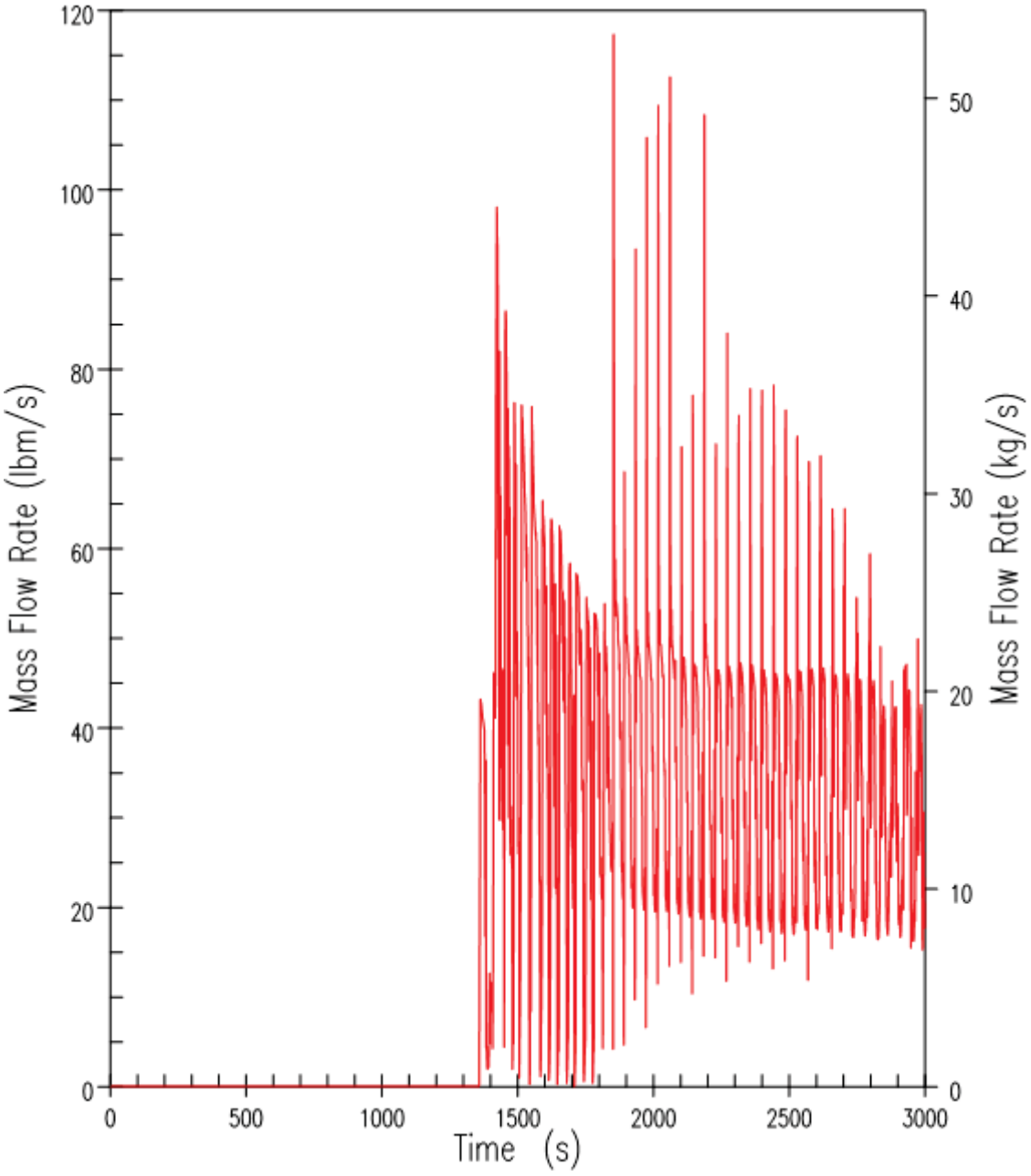


Figure 9.6.5-67(b). DBA 254 mm (10-Inch) Cold Leg Break – ADS-4 Vapour Discharge

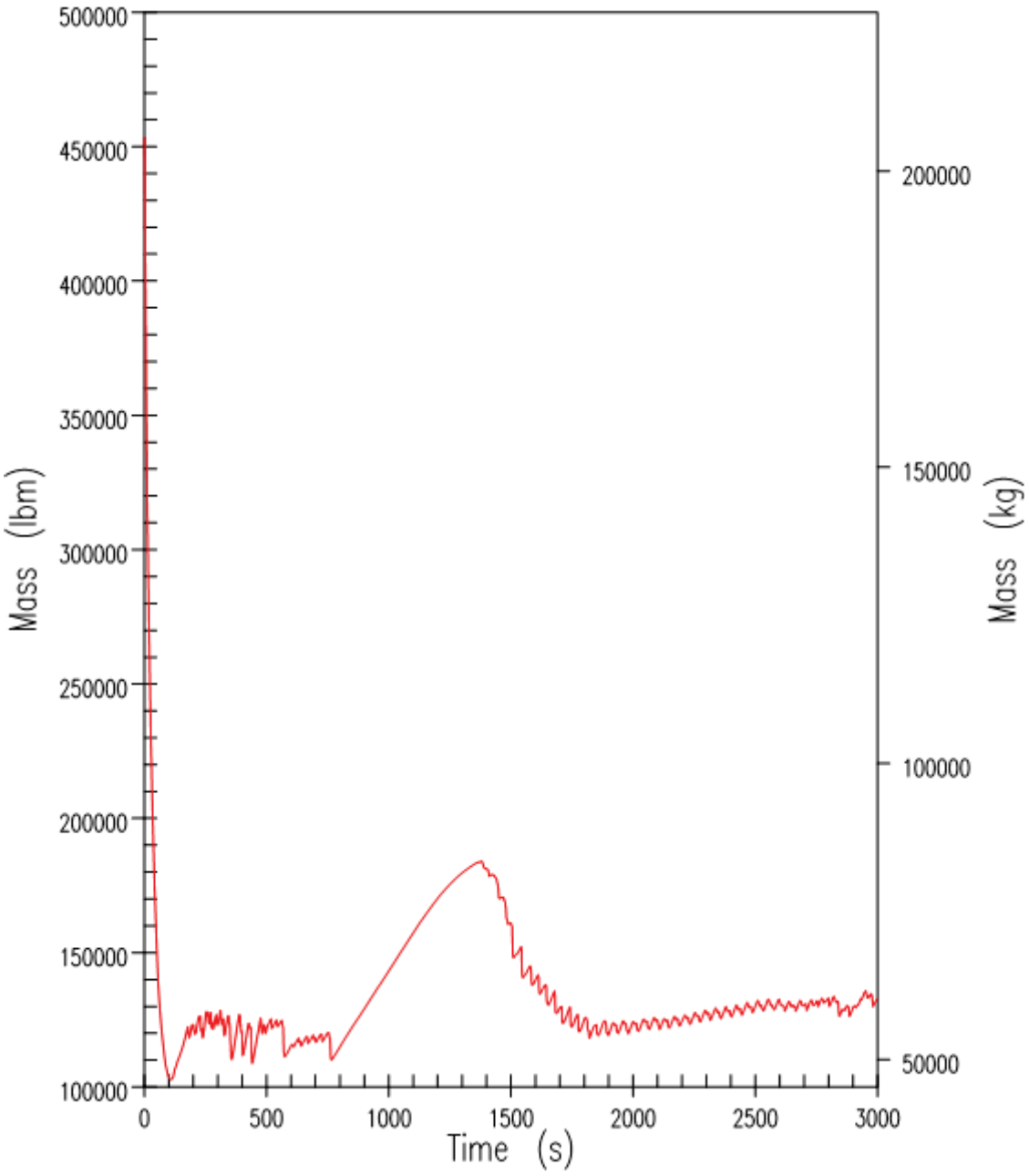


Figure 9.6.5-68(a). DBA 254 mm (10-Inch) Cold Leg Break – RCS System Inventory

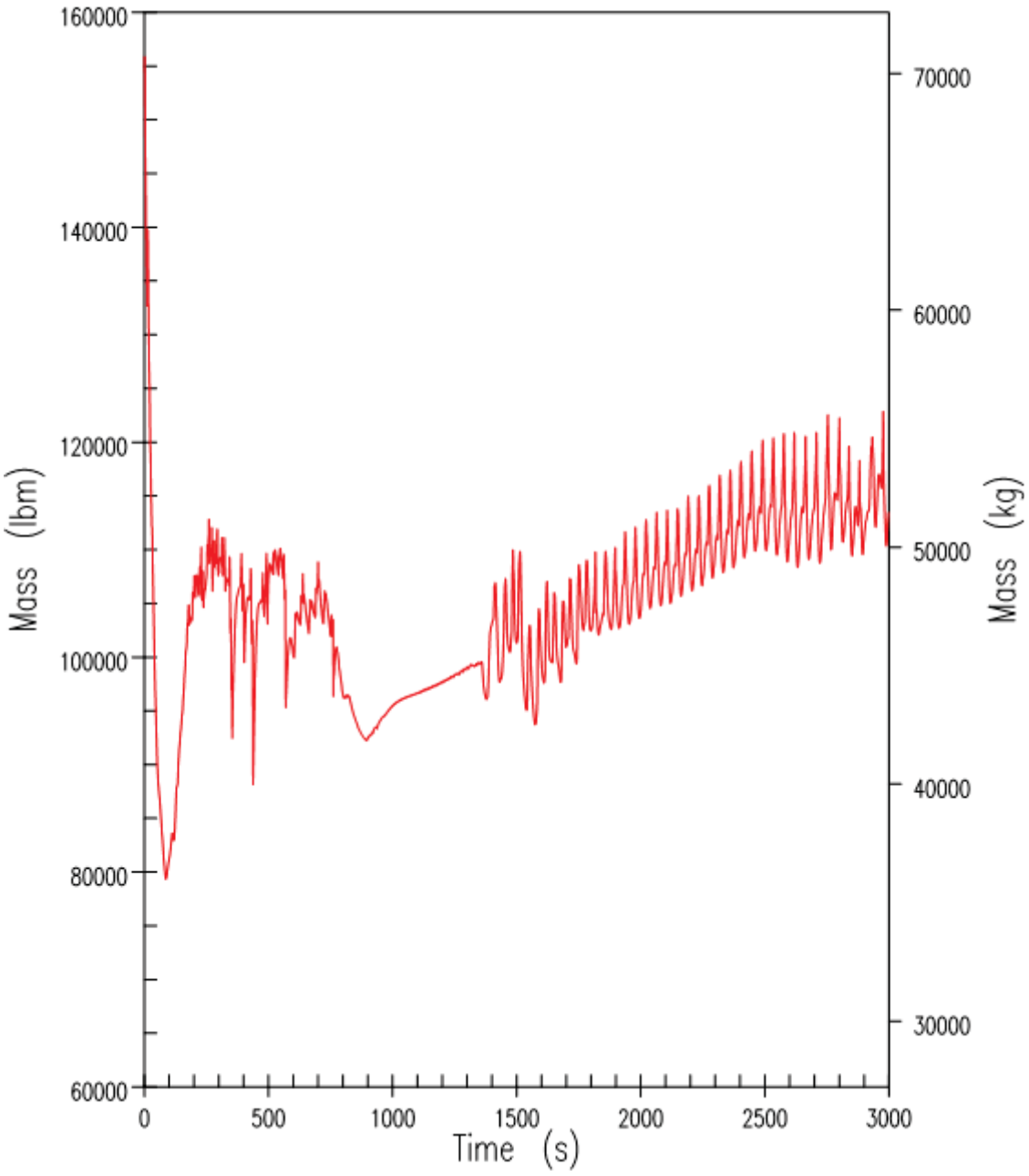


Figure 9.6.5-68(b). DBA 254 mm (10-Inch) Cold Leg Break – Reactor Vessel Mixture Inventory

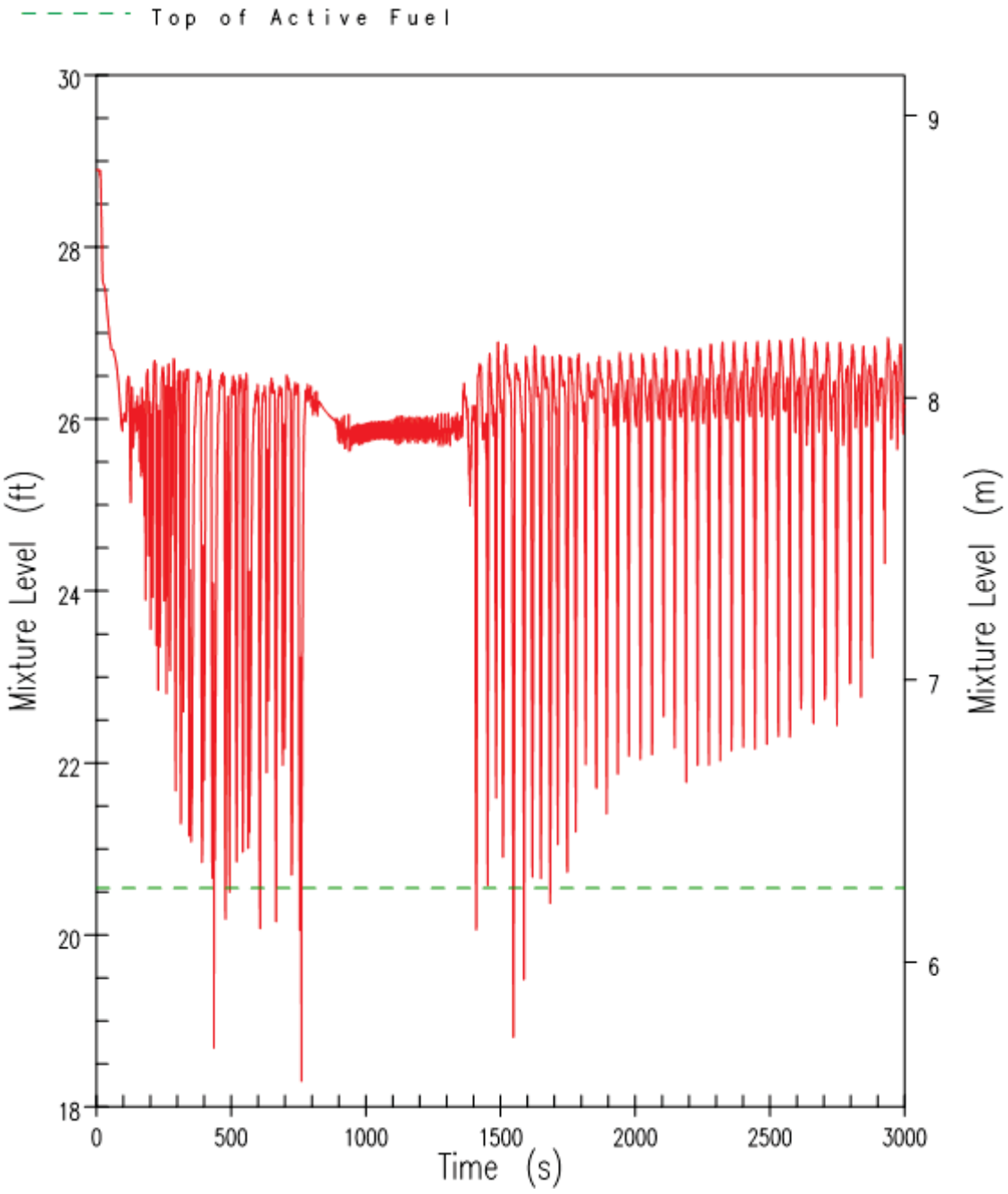


Figure 9.6.5-69. DBA 254 mm (10-Inch) Cold Leg Break – Core/Upper Plenum Mixture Level

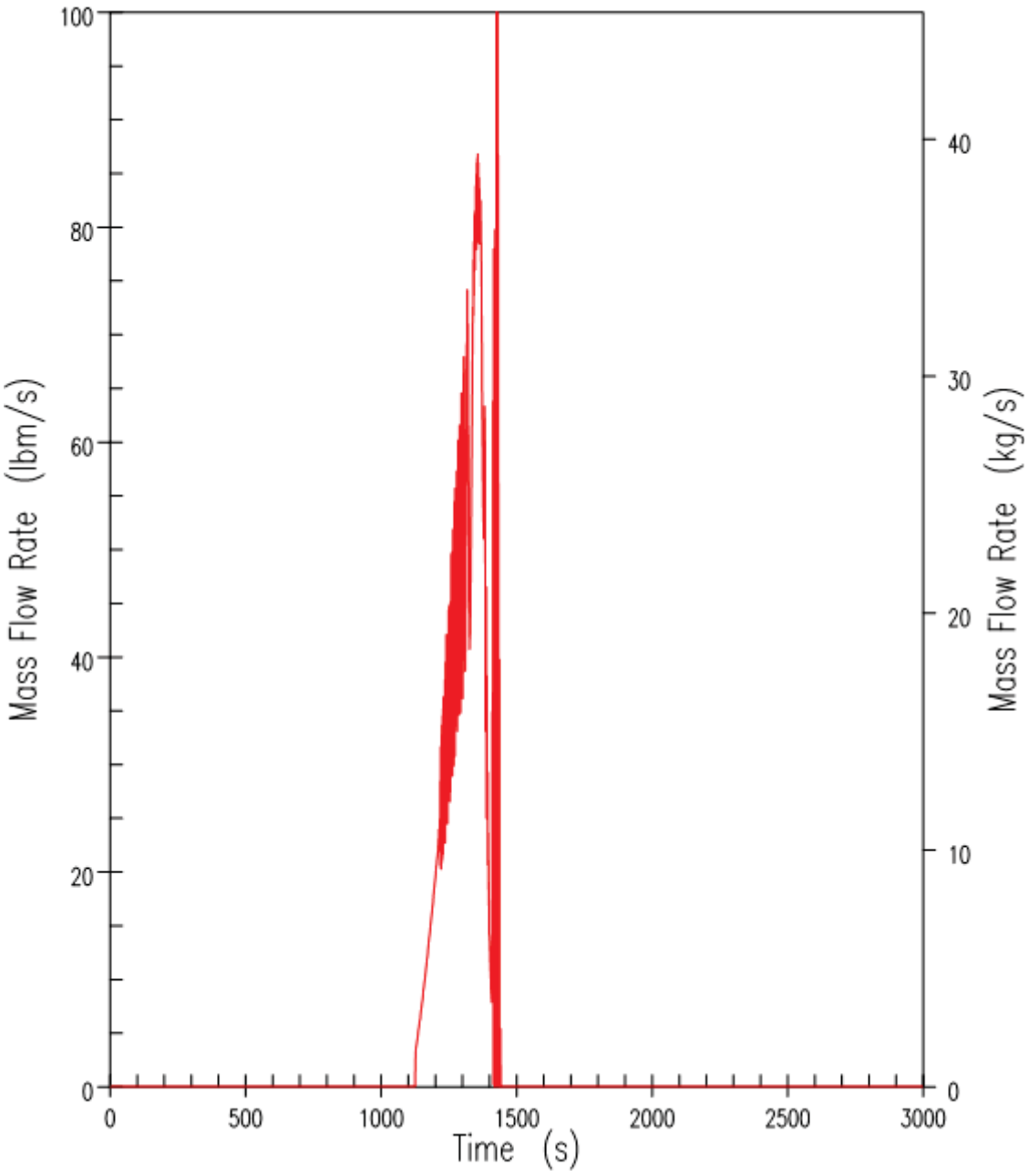


Figure 9.6.5-70(a). DBA 254 mm (10-Inch) Cold Leg Break – ADS 1-3 Liquid Discharge

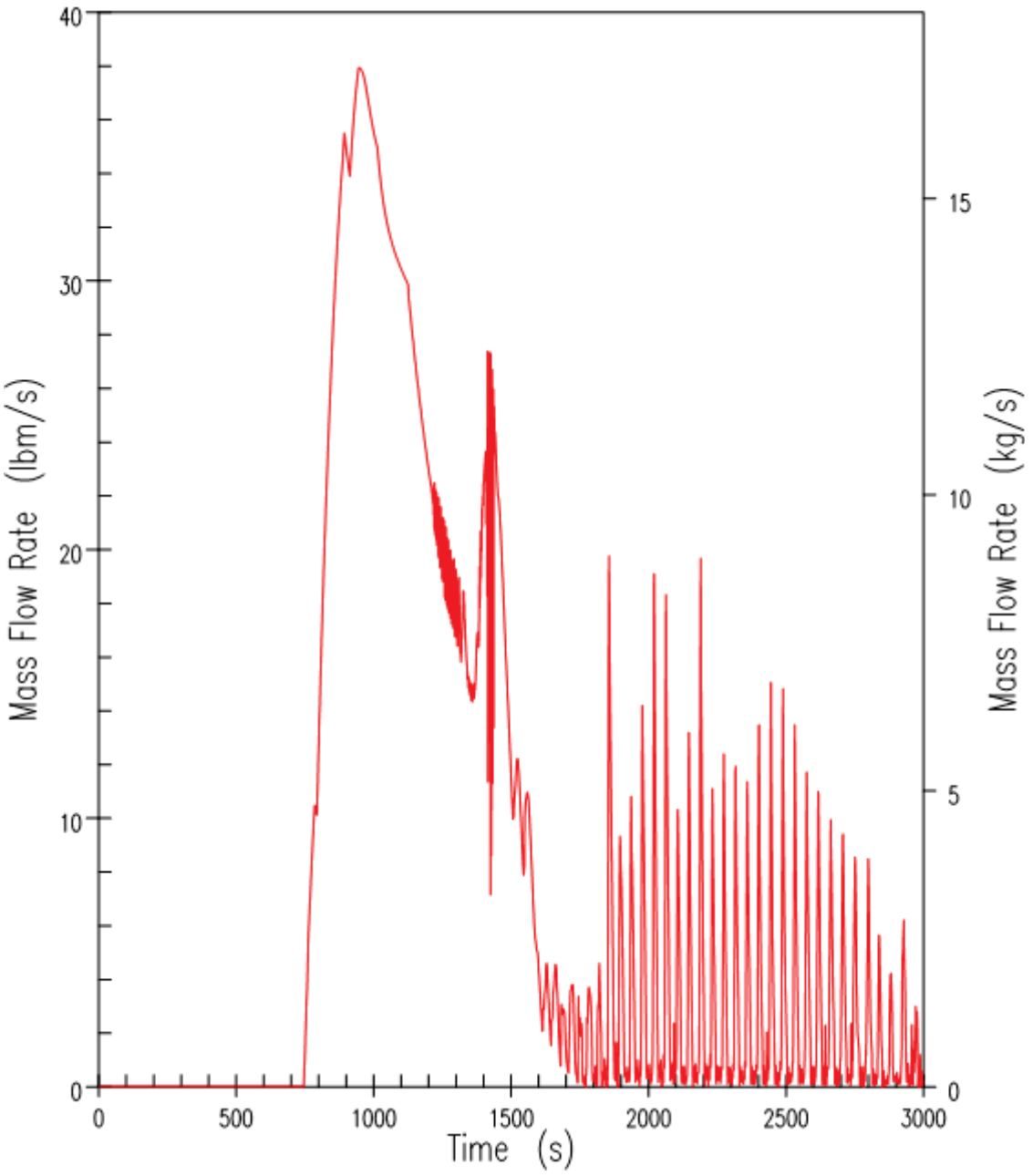


Figure 9.6.5-70(b). DBA 254 mm (10-Inch) Cold Leg Break – ADS 1-3 Vapour Discharge

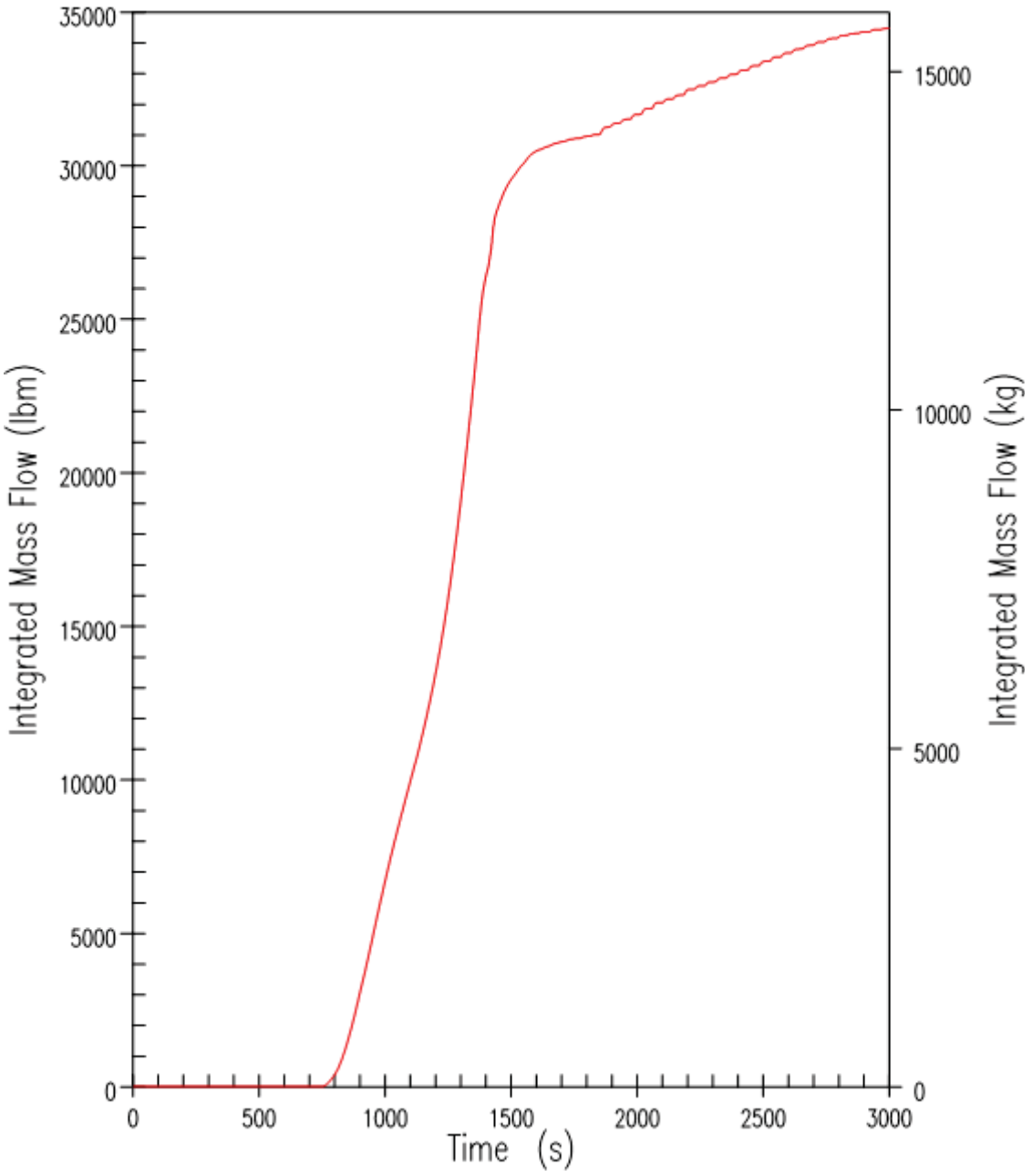


Figure 9.6.5-70(c). DBA 254 mm (10-Inch) Cold Leg Break – ADS 1-3 Integrated Discharge

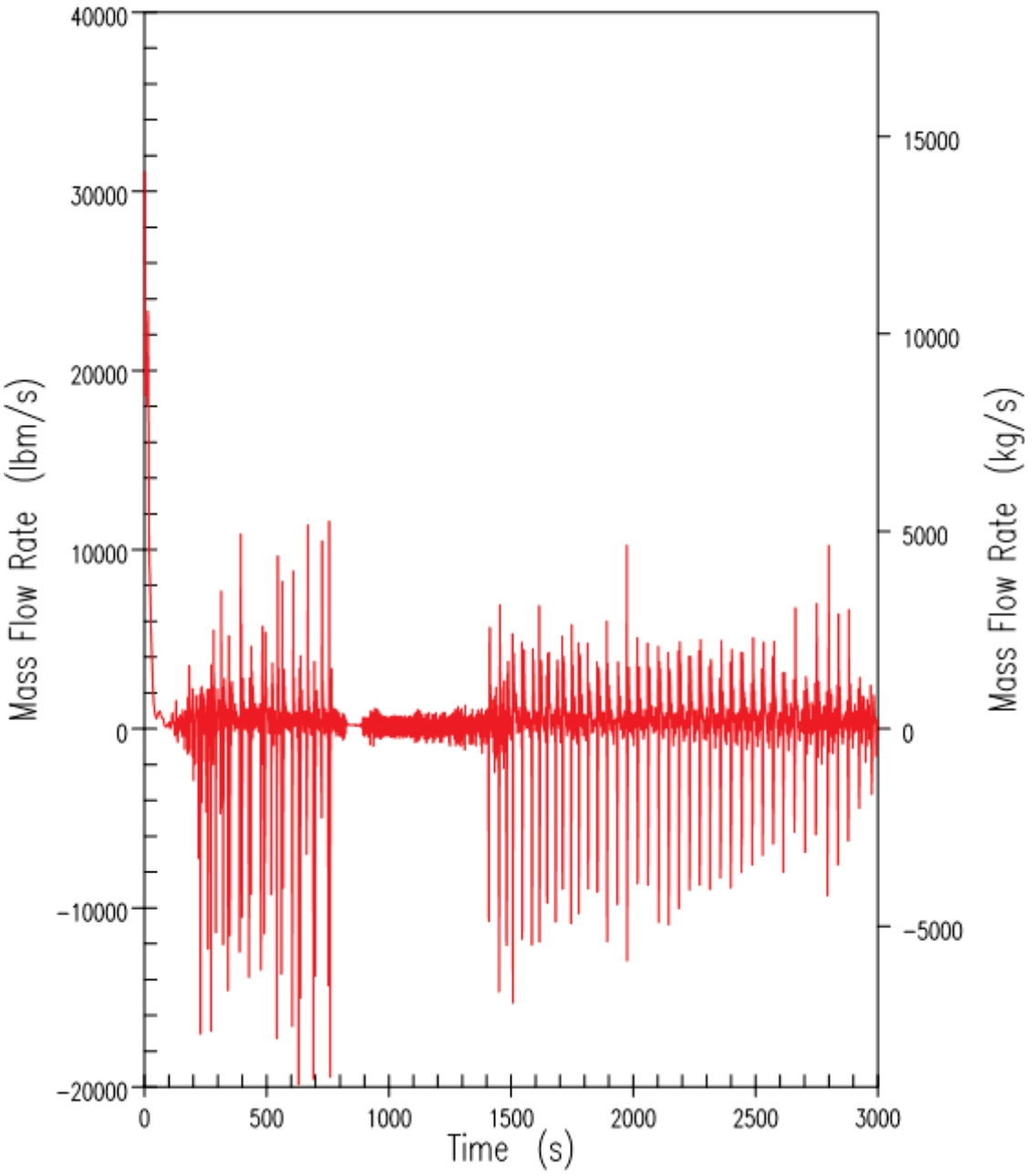


Figure 9.6.5-71. DBA 254 mm (10-Inch) Cold Leg Break – Core Exit Liquid Flow

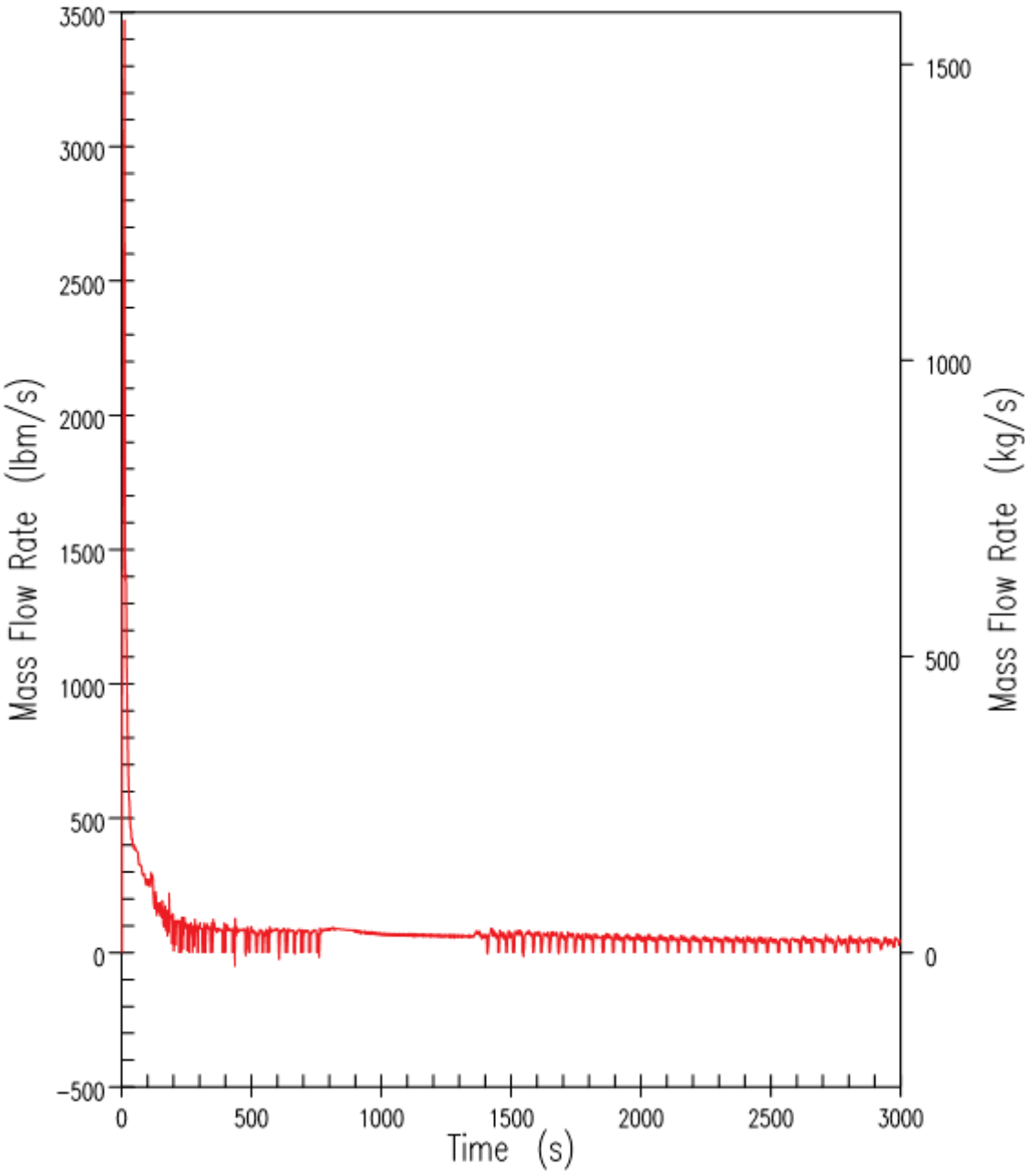


Figure 9.6.5-72. DBA 254 mm (10-Inch) Cold Leg Break – Core Exit Vapour Flow

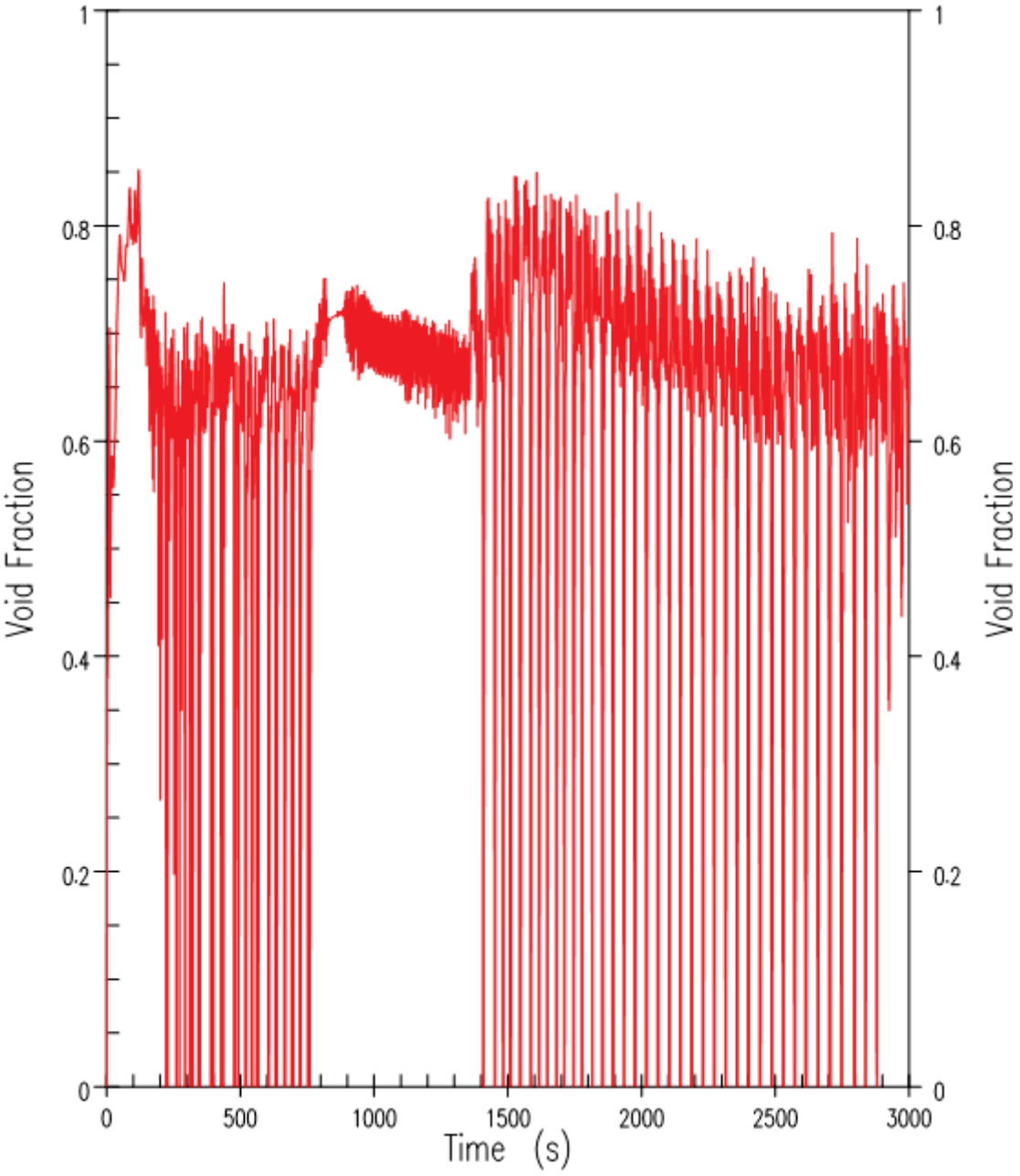


Figure 9.6.5-73. DBA 254 mm (10-Inch) Cold Leg Break – Core Exit Void Fraction

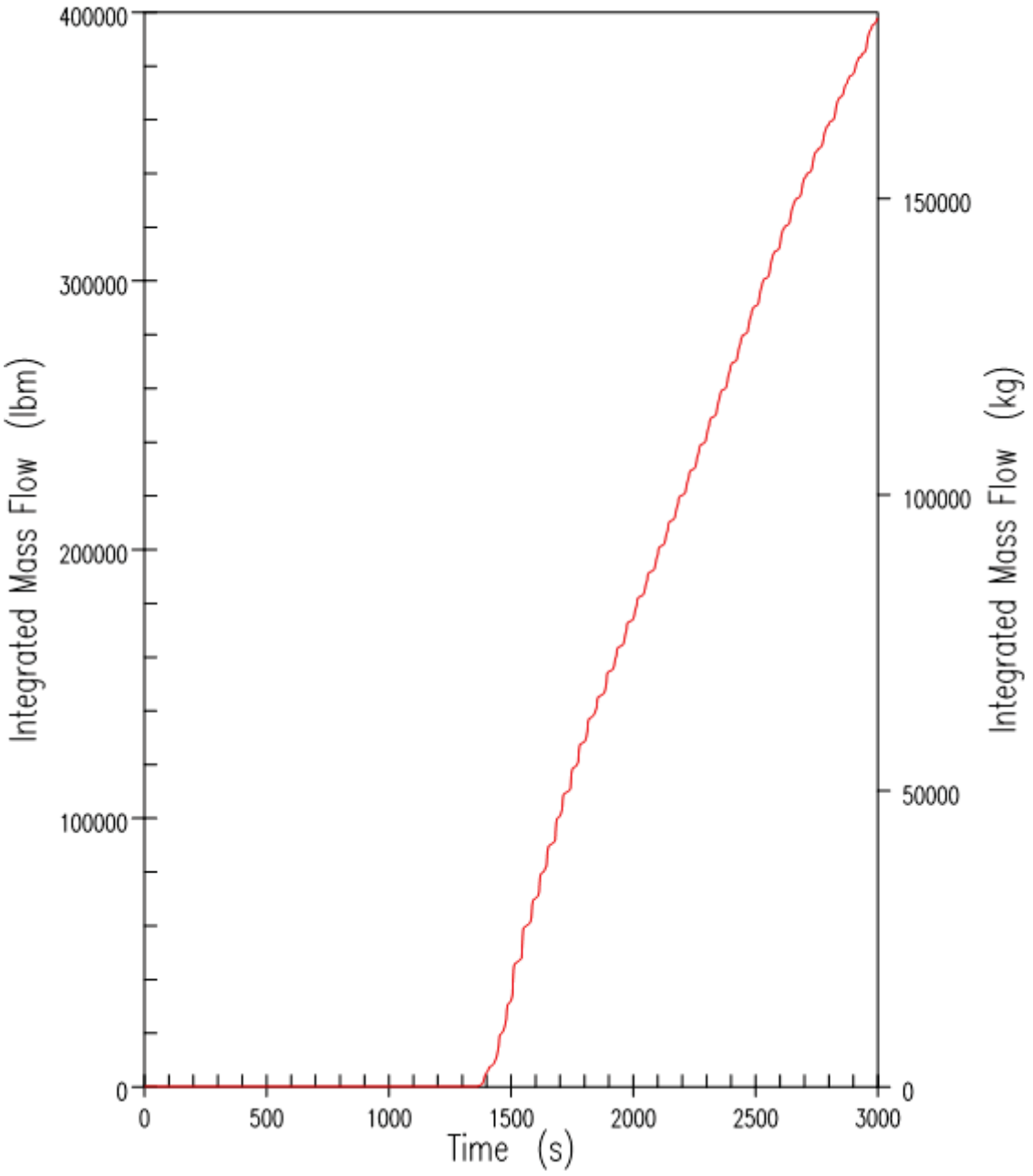


Figure 9.6.5-74. DBA 254 mm (10-Inch) Cold Leg Break – ADS-4 Integrated Discharge

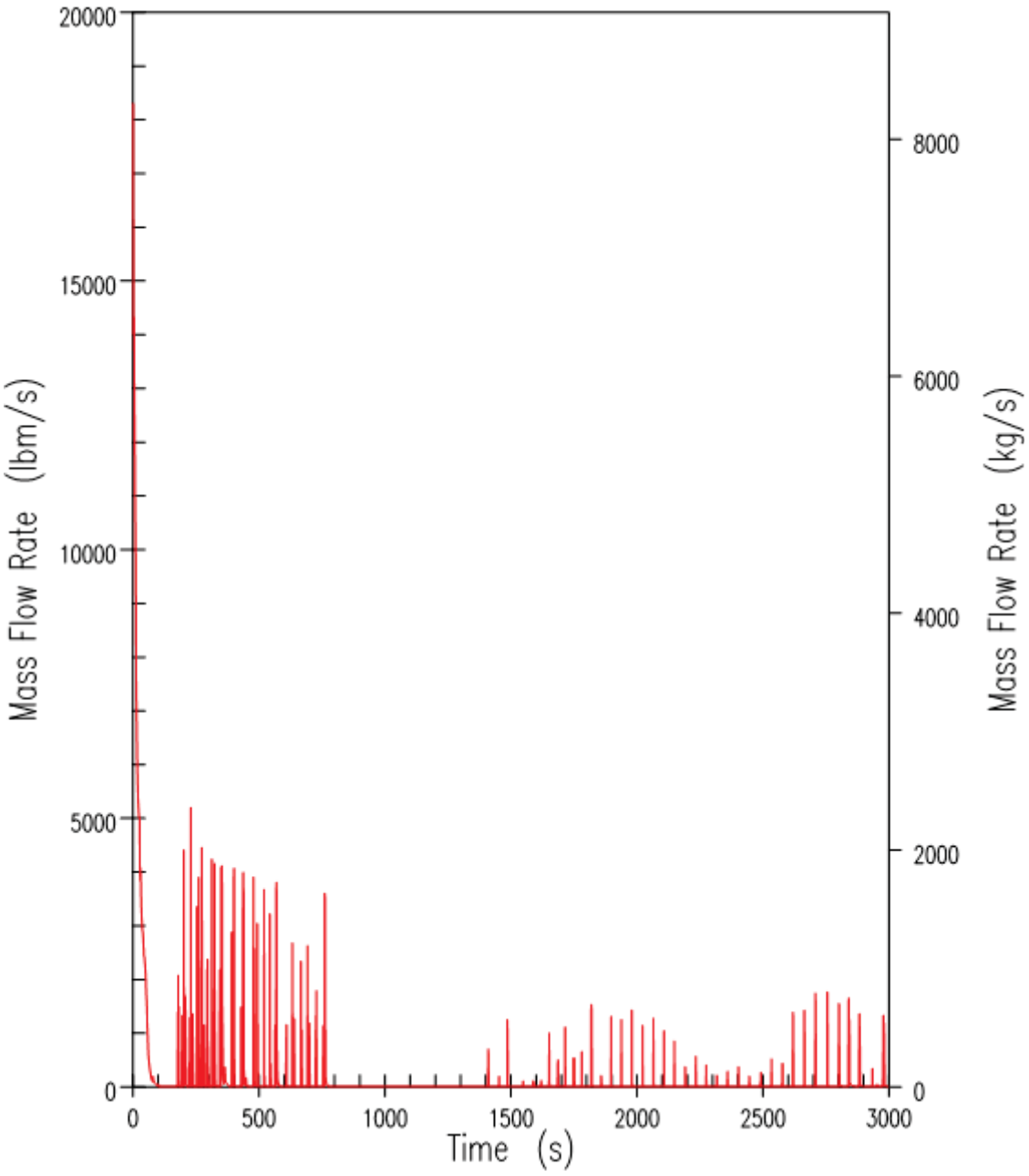


Figure 9.6.5-75. DBA 254 mm (10-Inch) Cold Leg Break – Liquid Break Discharge

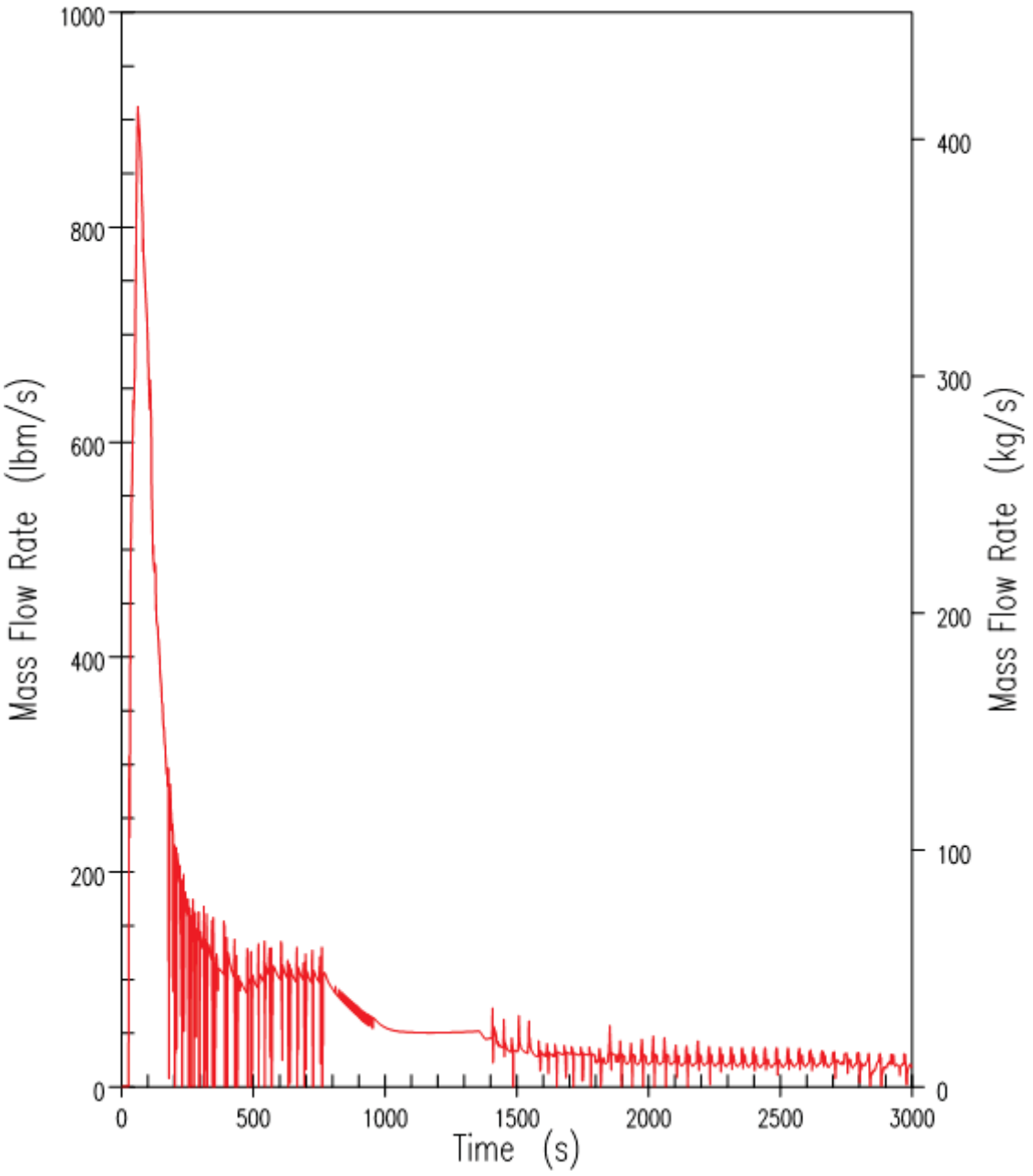


Figure 9.6.5-76. DBA 254 mm (10-Inch) Cold Leg Break – Vapour Break Discharge

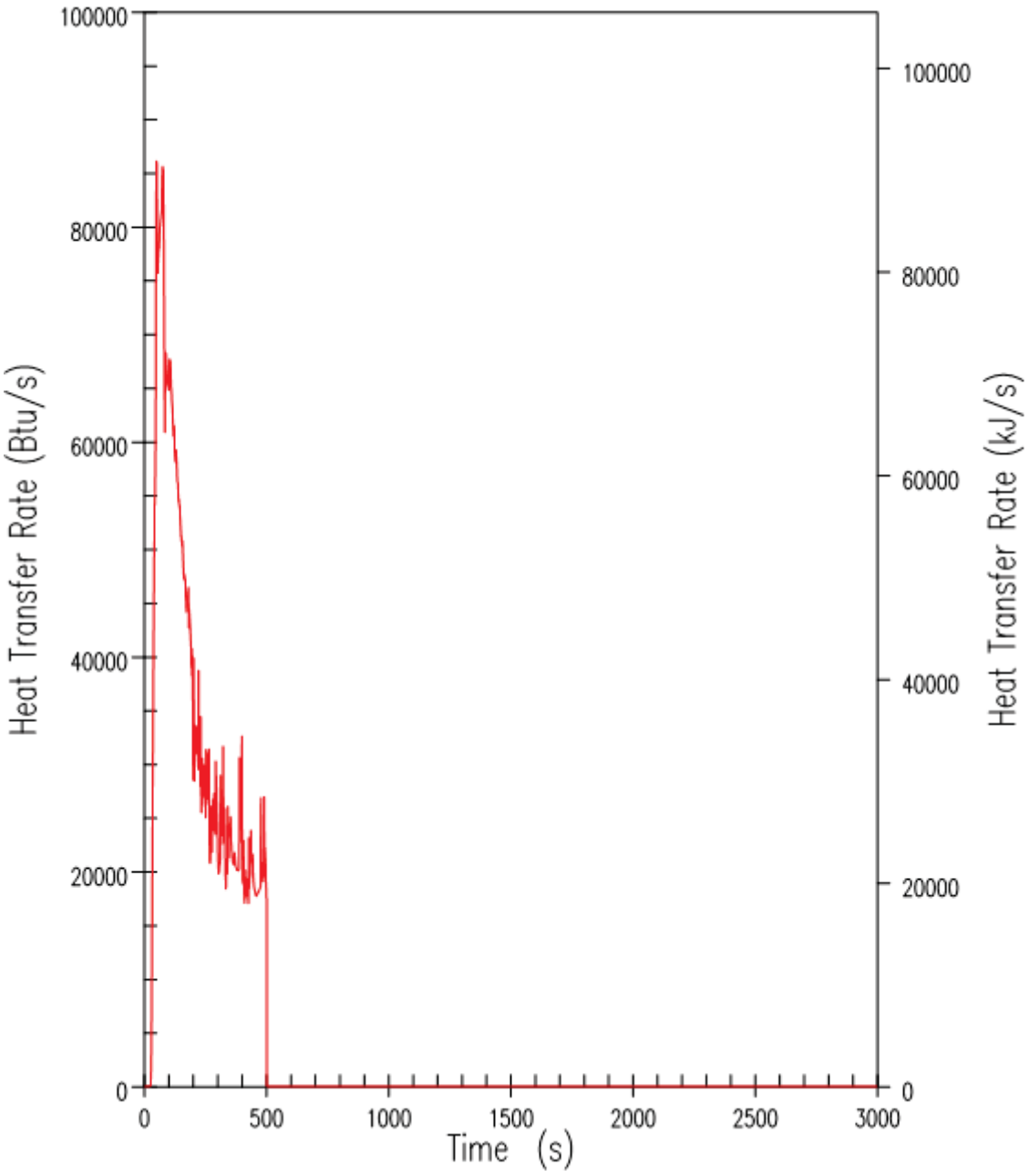


Figure 9.6.5-77. DBA 254 mm (10-Inch) Cold Leg Break – PRHR Heat Removal Rate

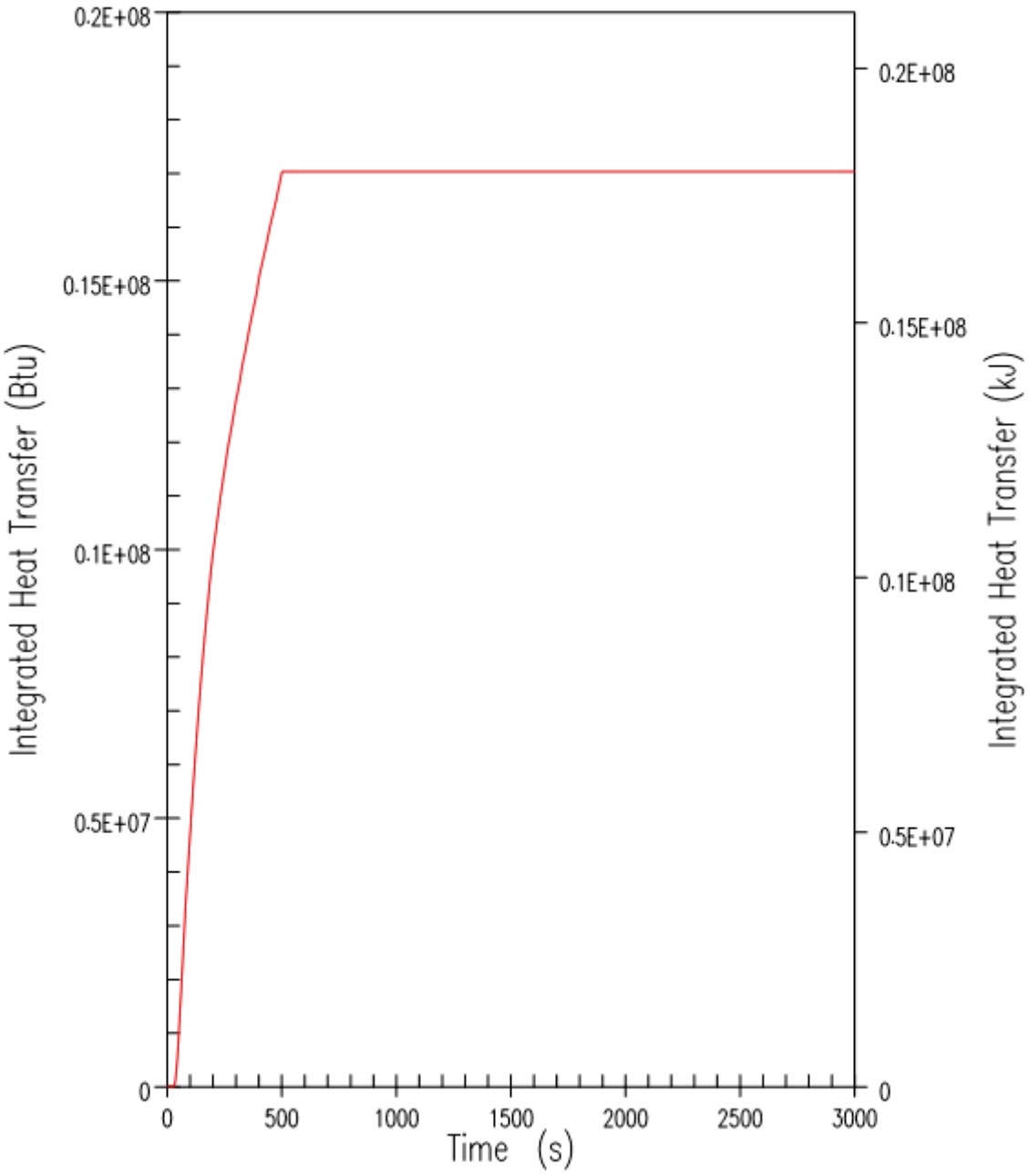


Figure 9.6.5-78. DBA 254 mm (10-Inch) Cold Leg Break – Integrated PRHR Heat Removal

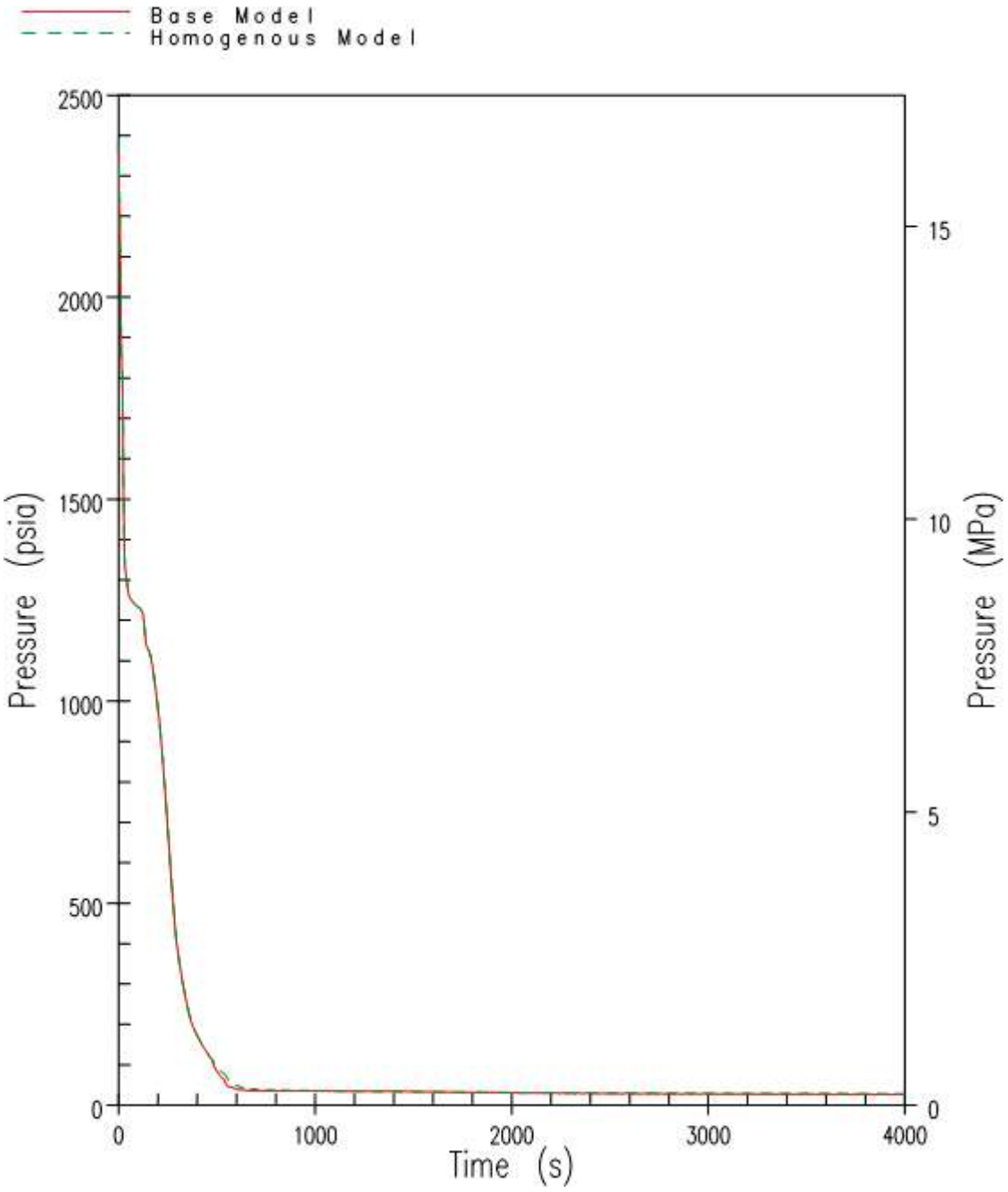


Figure 9.6.5-79(a). DBA DEDVI Entrainment – Downcomer Pressure Comparison

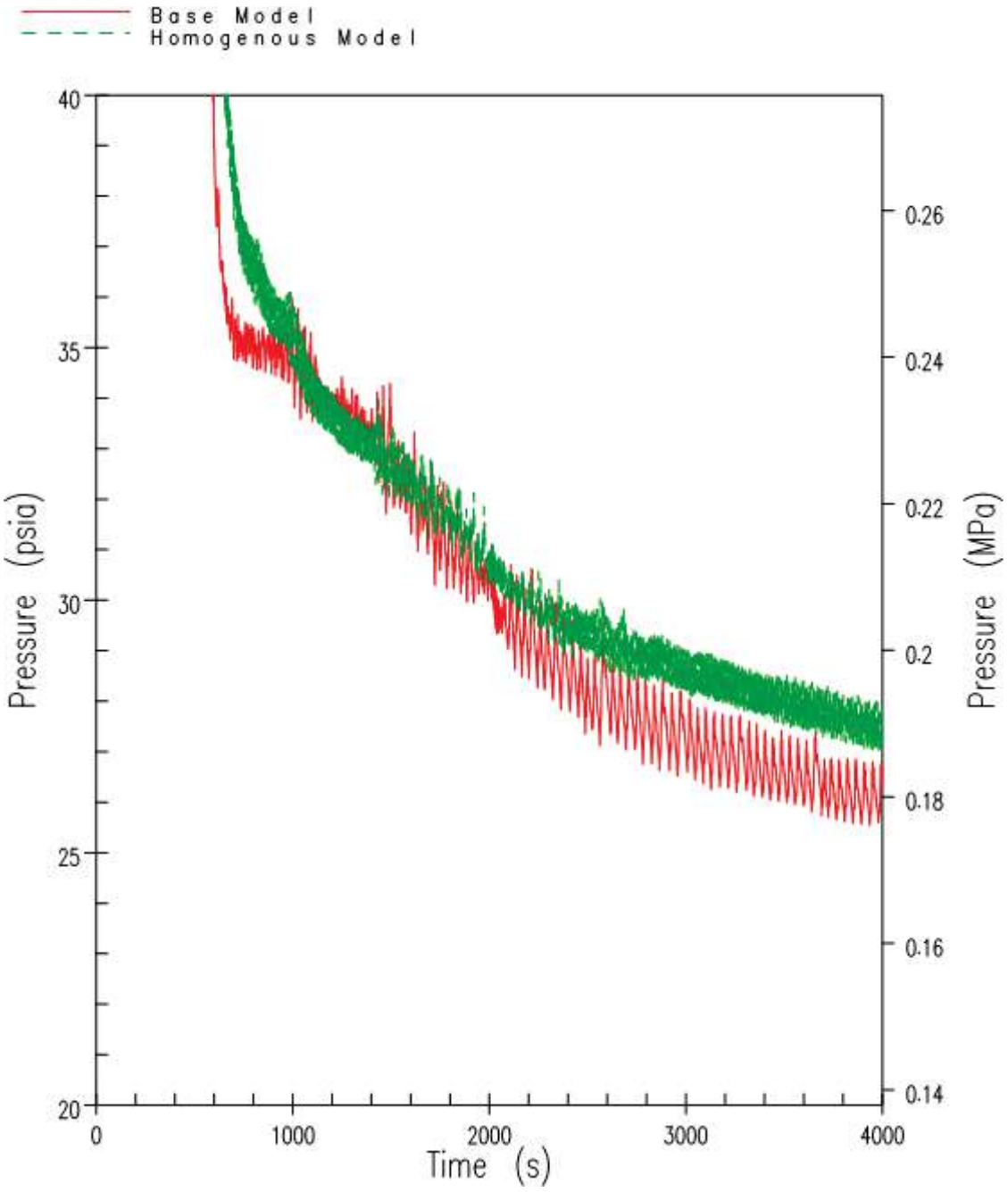


Figure 9.6.5-79(b). DBA DEDVI Entrainment – Downcomer Pressure Comparison (Zoomed)

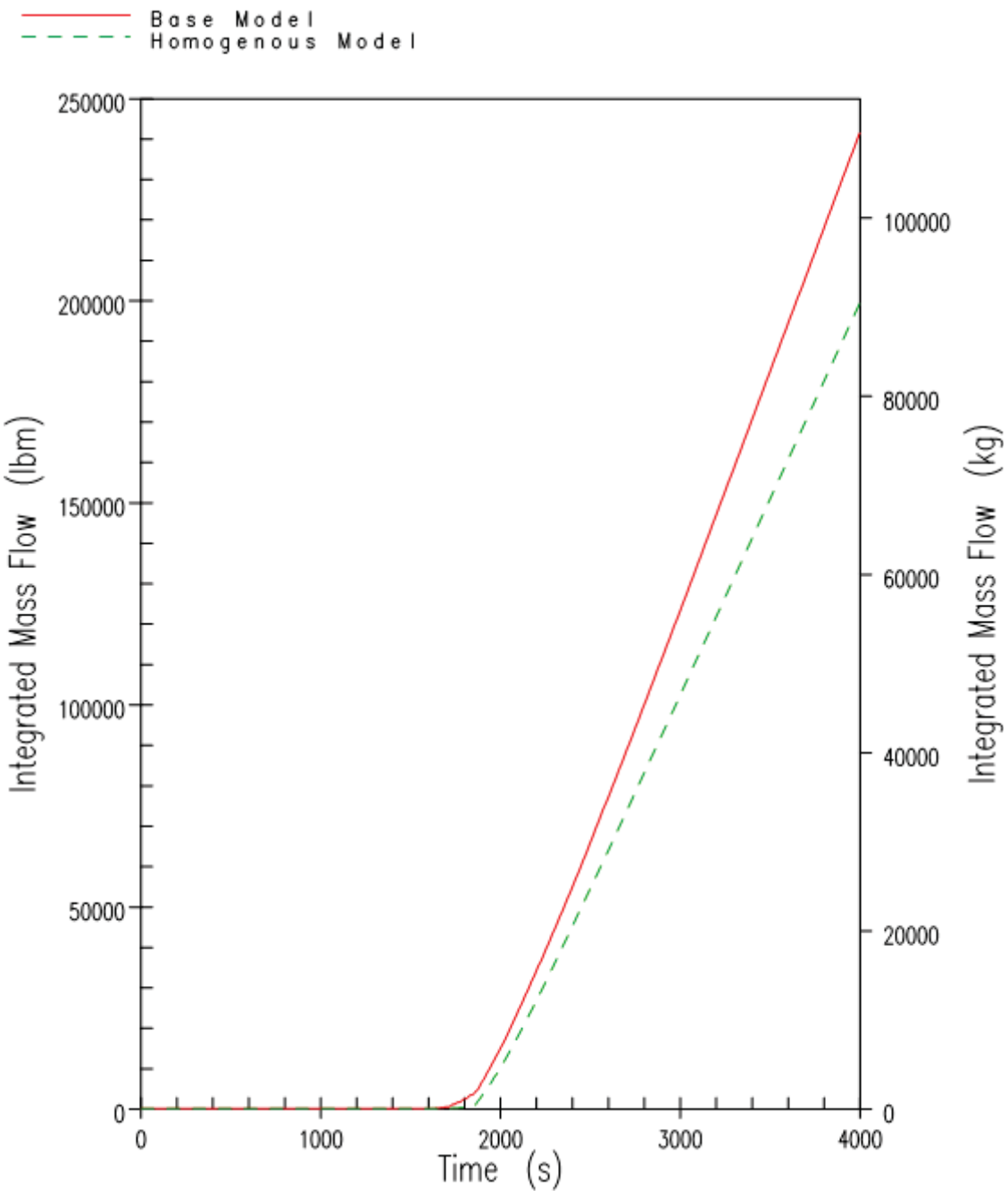


Figure 9.6.5-80. DBA DEDVI Entrainment – Intact IRWST Injection Flow

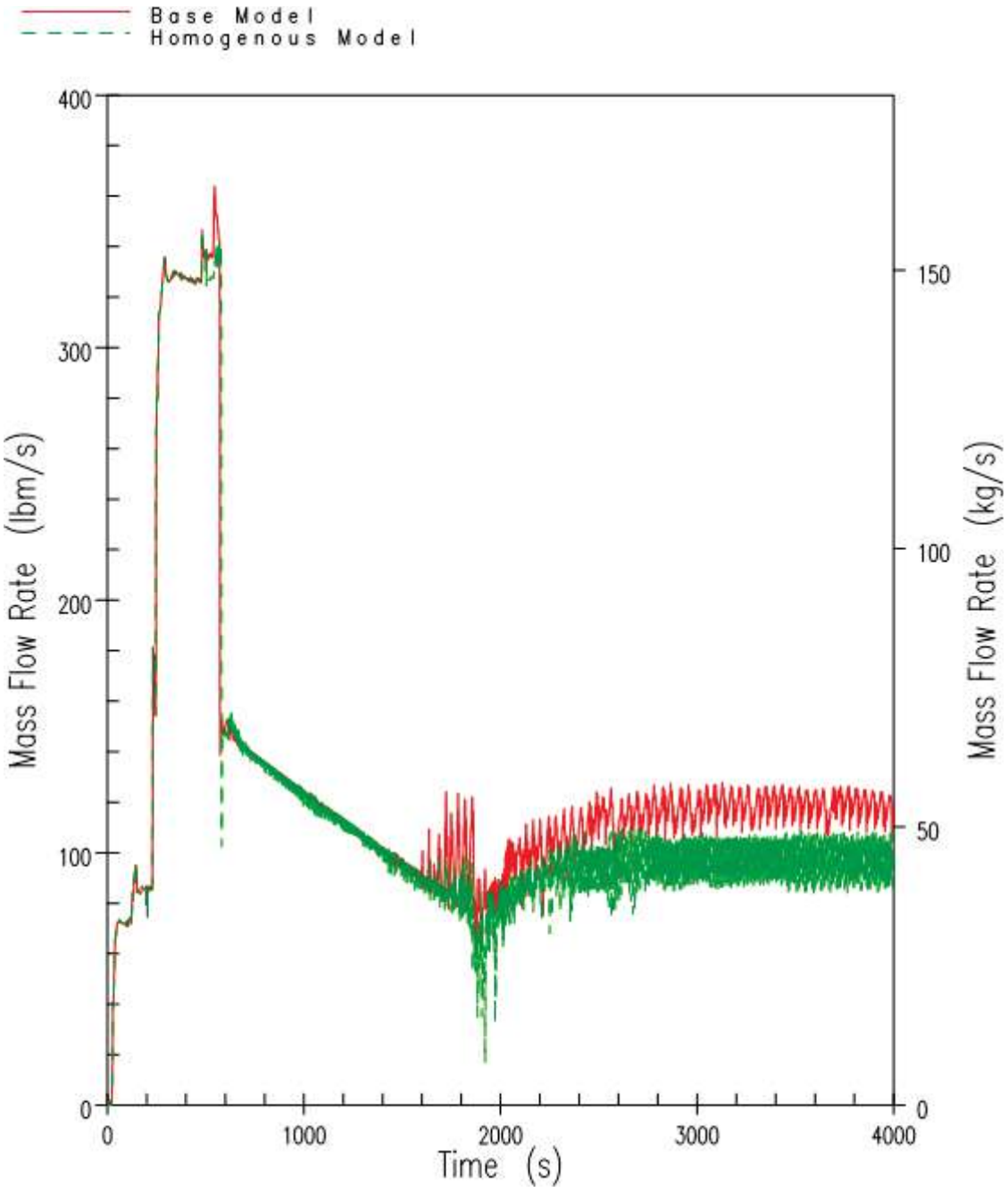


Figure 9.6.5-81. DBA DEDVI Entrainment – Intact DVI Line Injection Flow

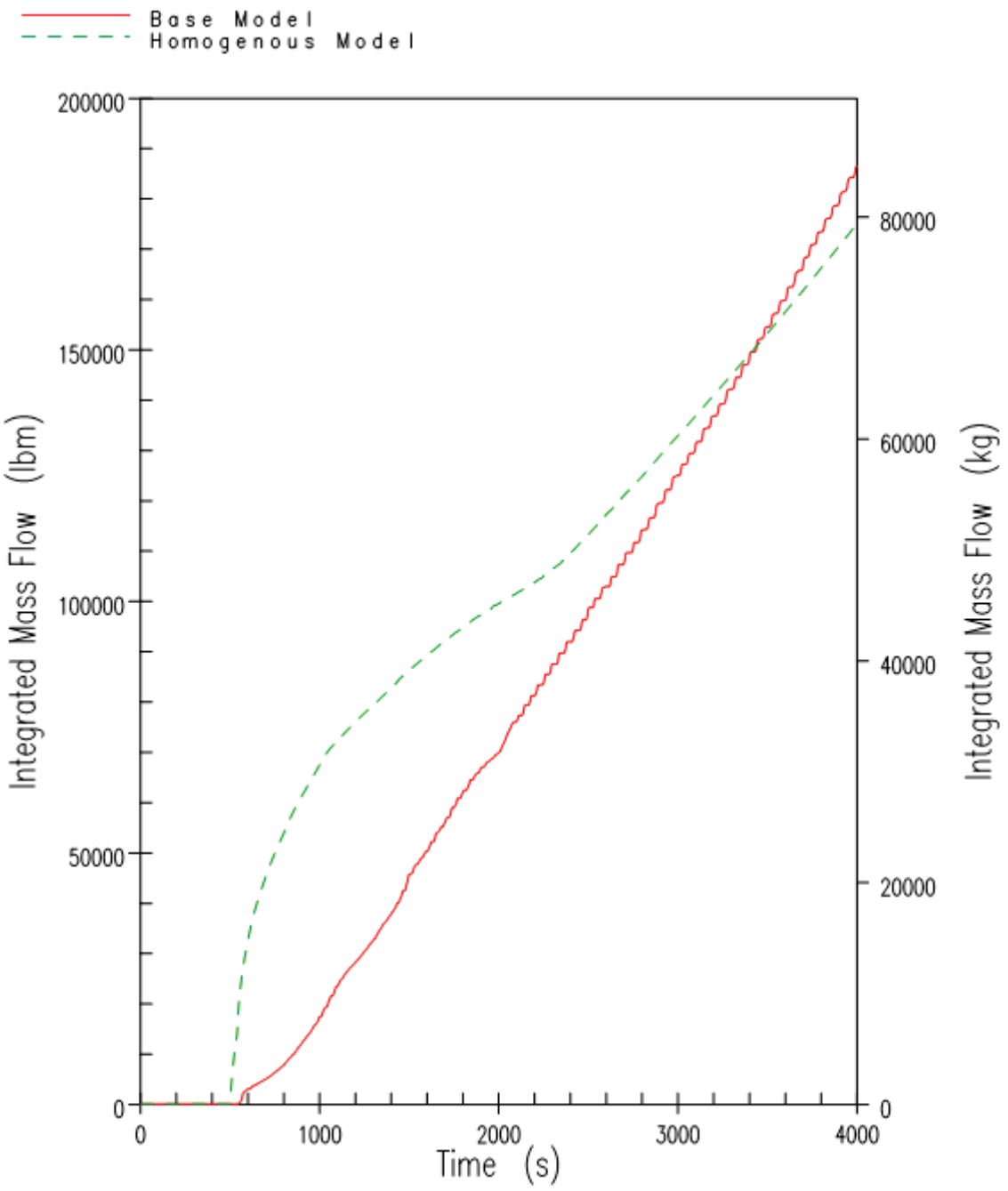


Figure 9.6.5-82. DBA DEDVI Entrainment – ADS-4 Integrated Liquid Discharge Comparison

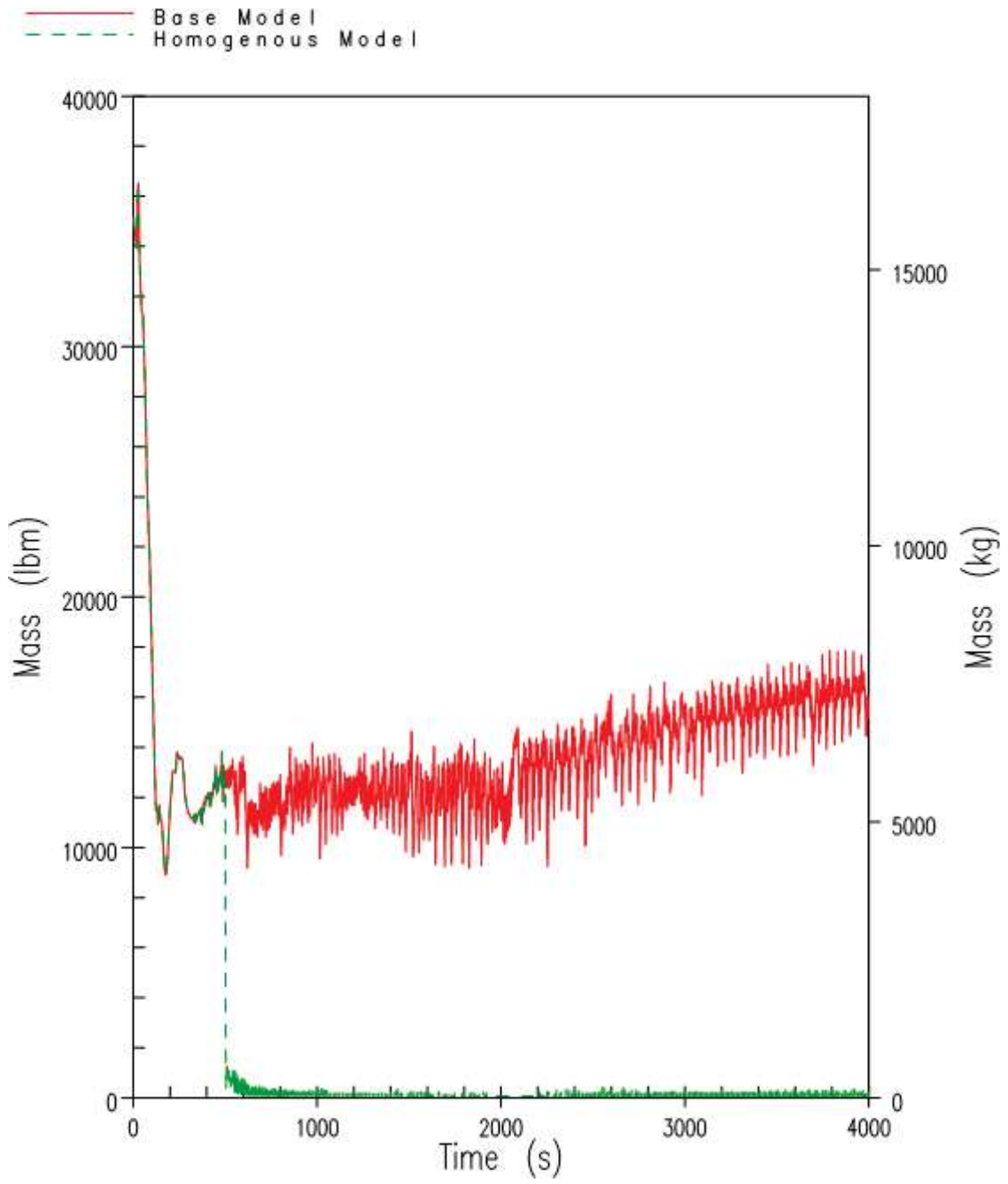


Figure 9.6.5-83. DBA DEDVI Entrainment – Upper Plenum Mixture Mass Comparison

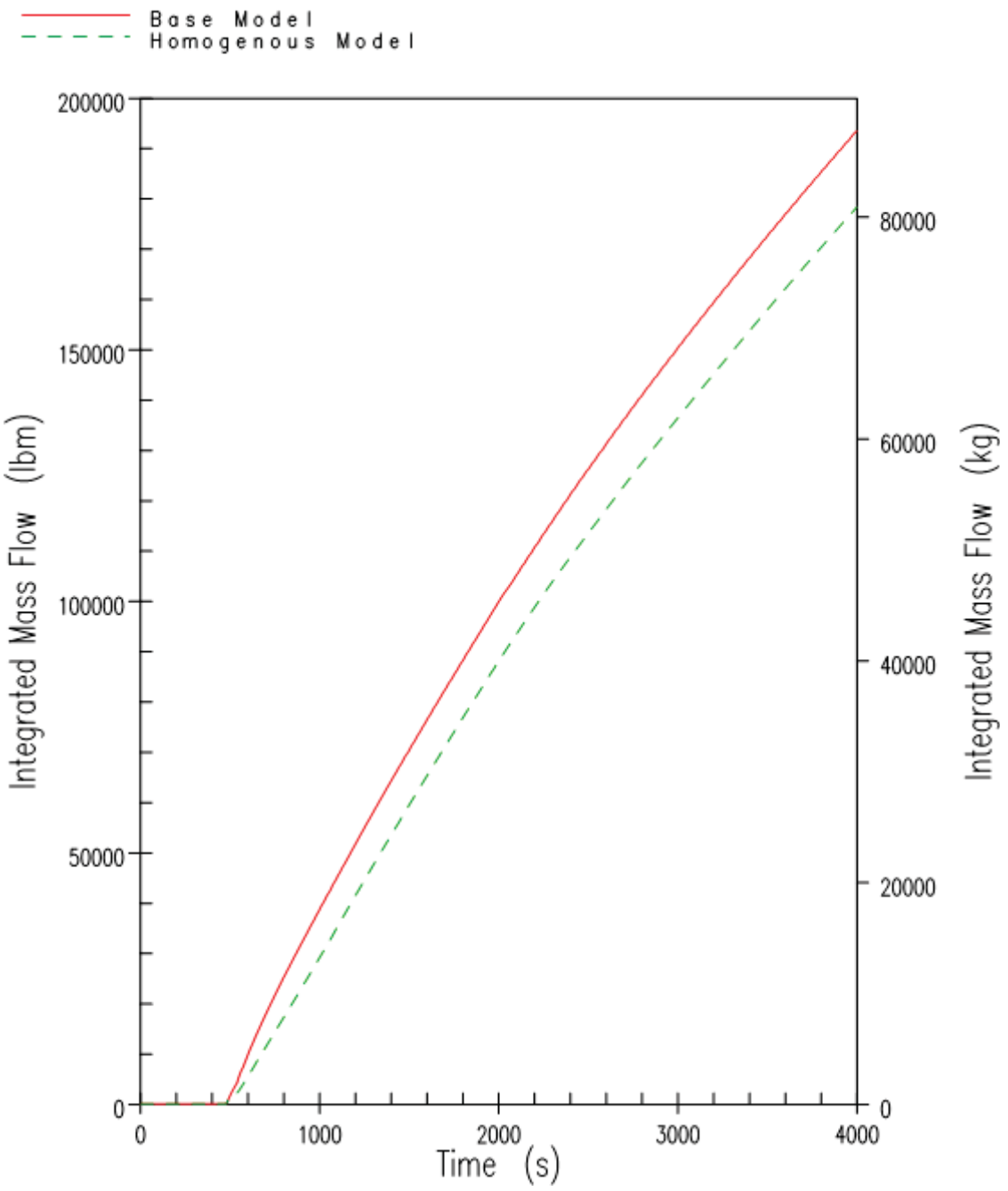


Figure 9.6.5-84. DBA DEDVI Entrainment – ADS-4 Integrated Vapour Discharge Comparison

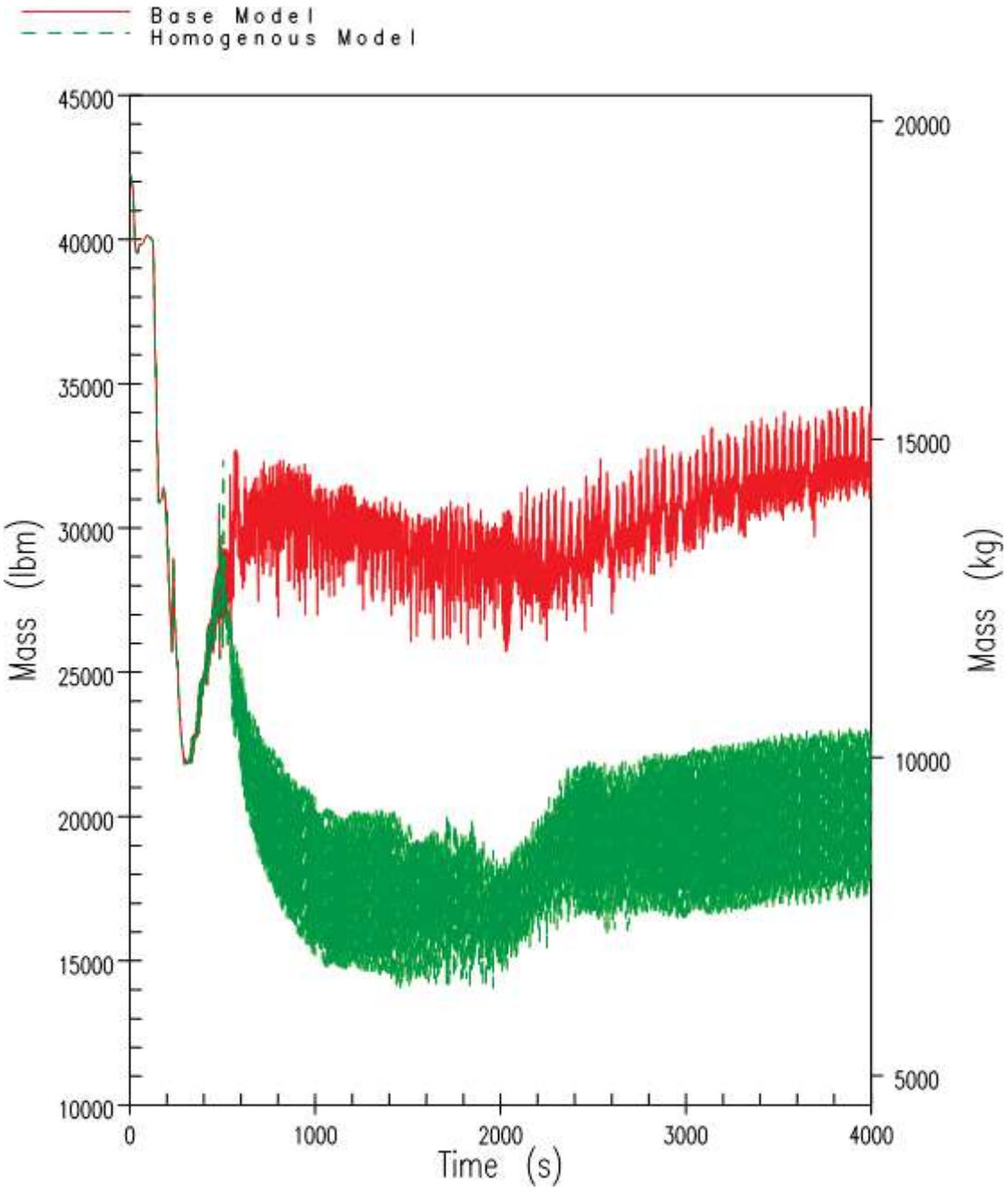


Figure 9.6.5-85. DBA DEDVI Entrainment – Downcomer Region Mass Comparison

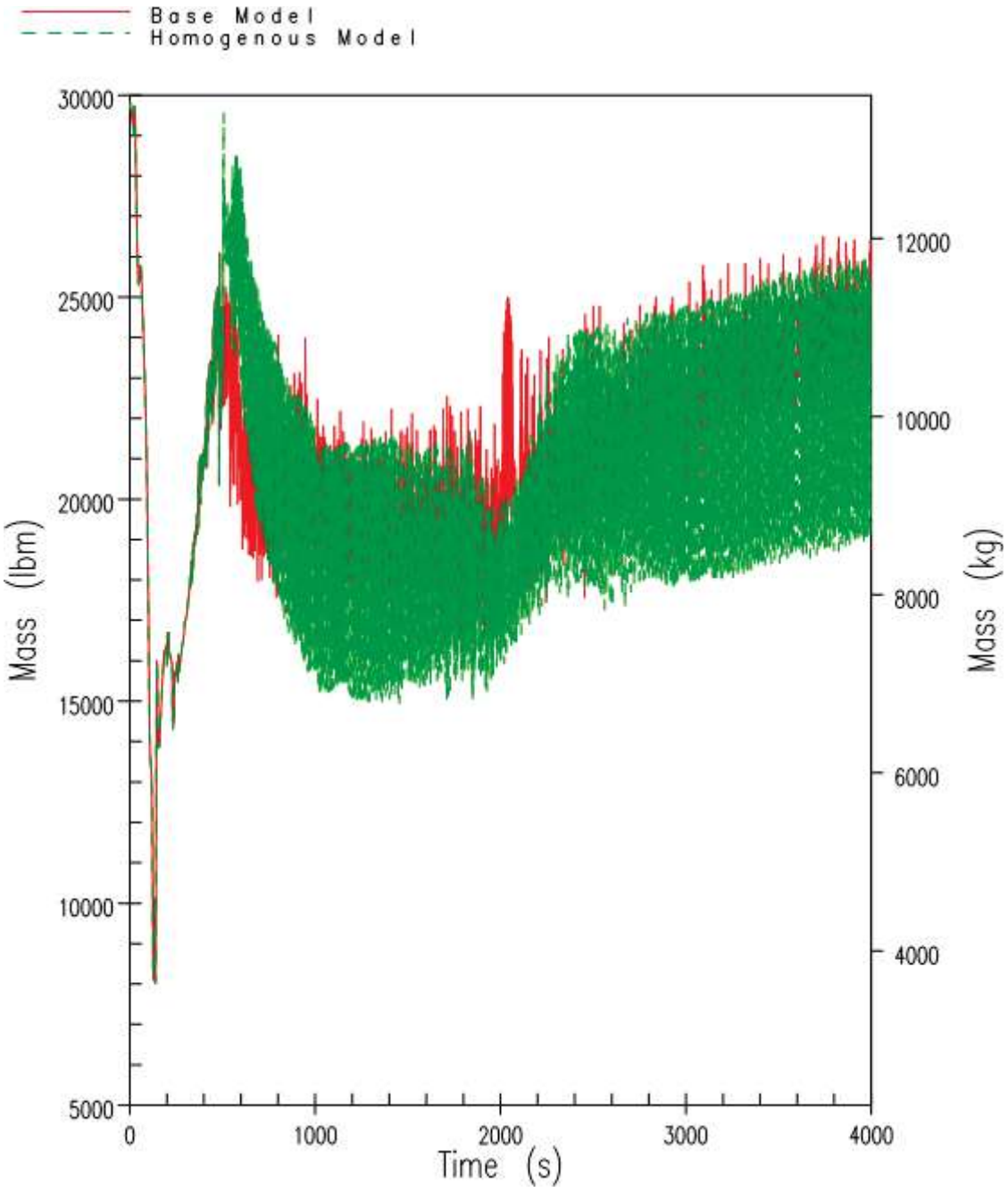


Figure 9.6.5-86(a). DBA DEDVI Entrainment – Core Region Mass Comparison

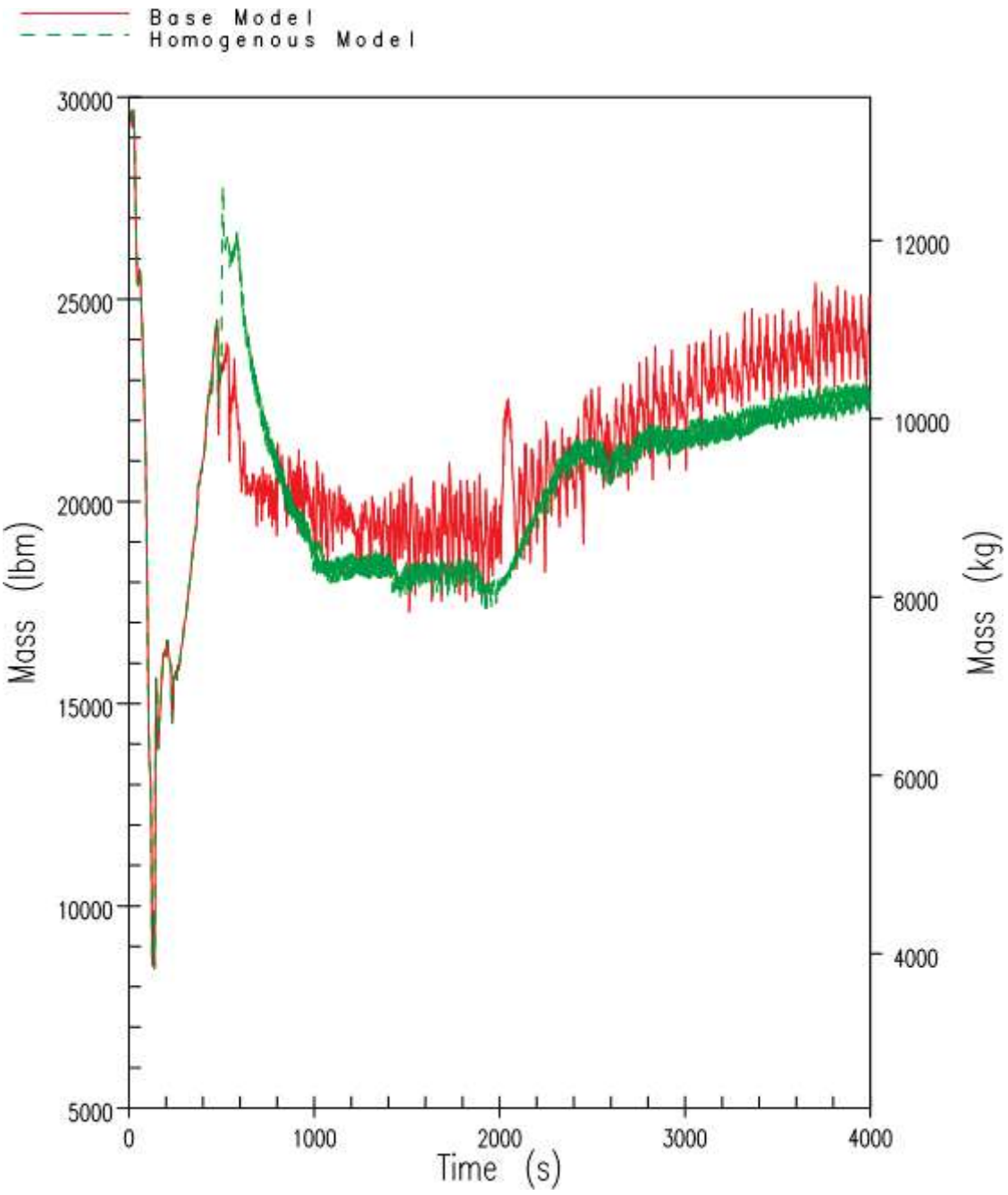


Figure 9.6.5-86(b). DBA DEDVI Entrainment – Core Region Mass Comparison (Smoothed)

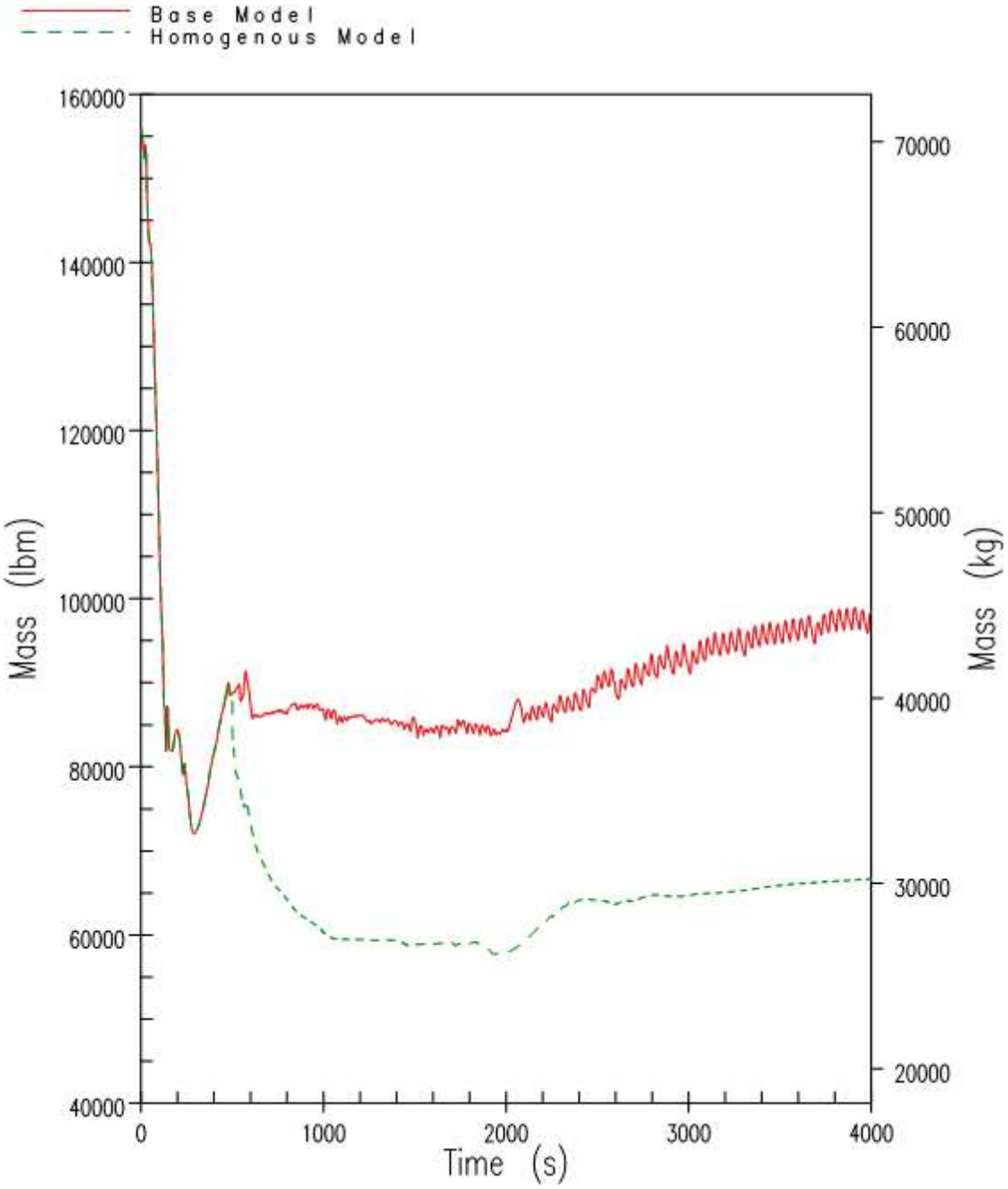


Figure 9.6.5-87. DBA DEDVI Entrainment – Vessel Mixture Mass Comparison

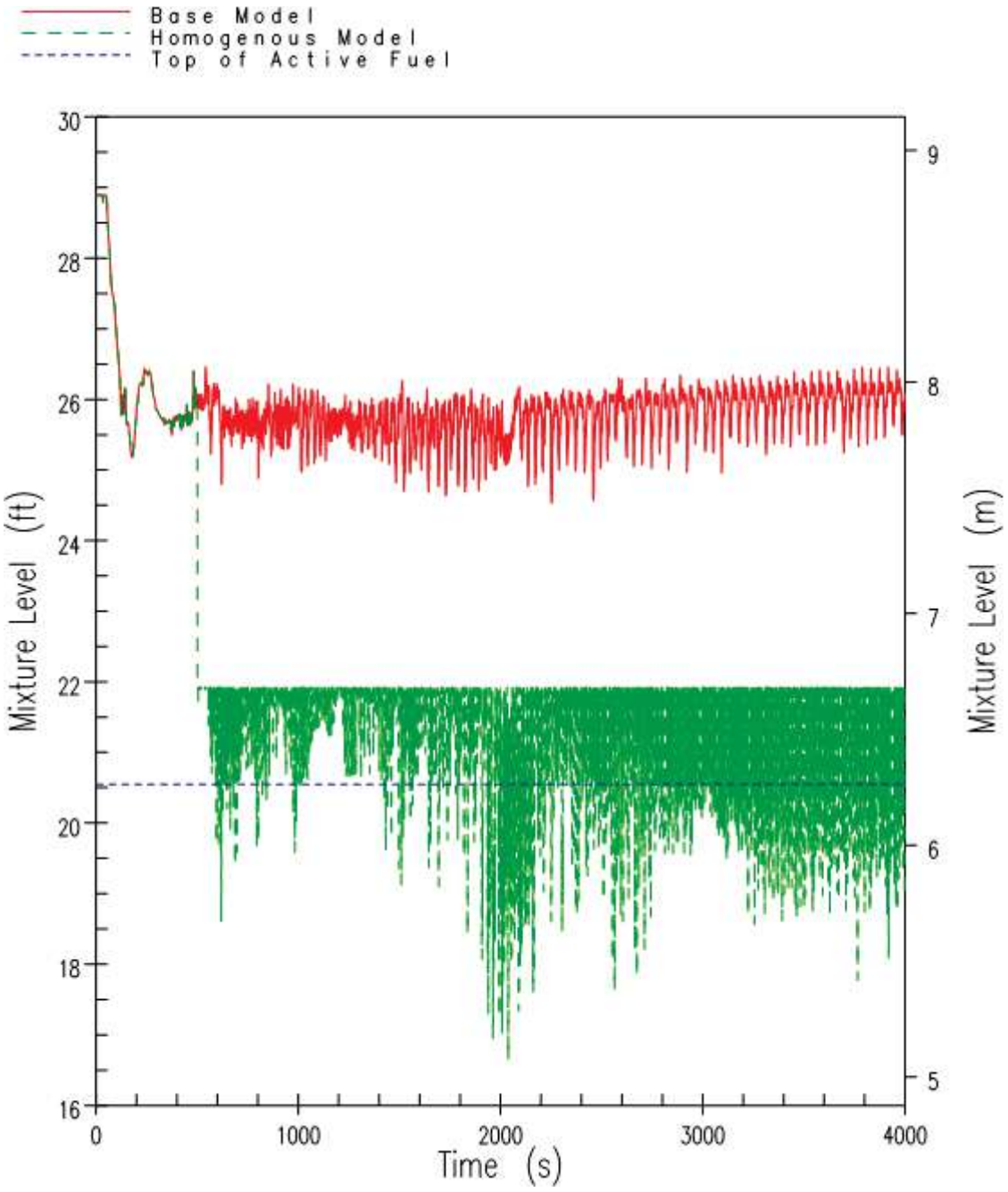


Figure 9.6.5-88. DBA DEDVI Entrainment – Core/Upper Plenum Mixture Level Comparison

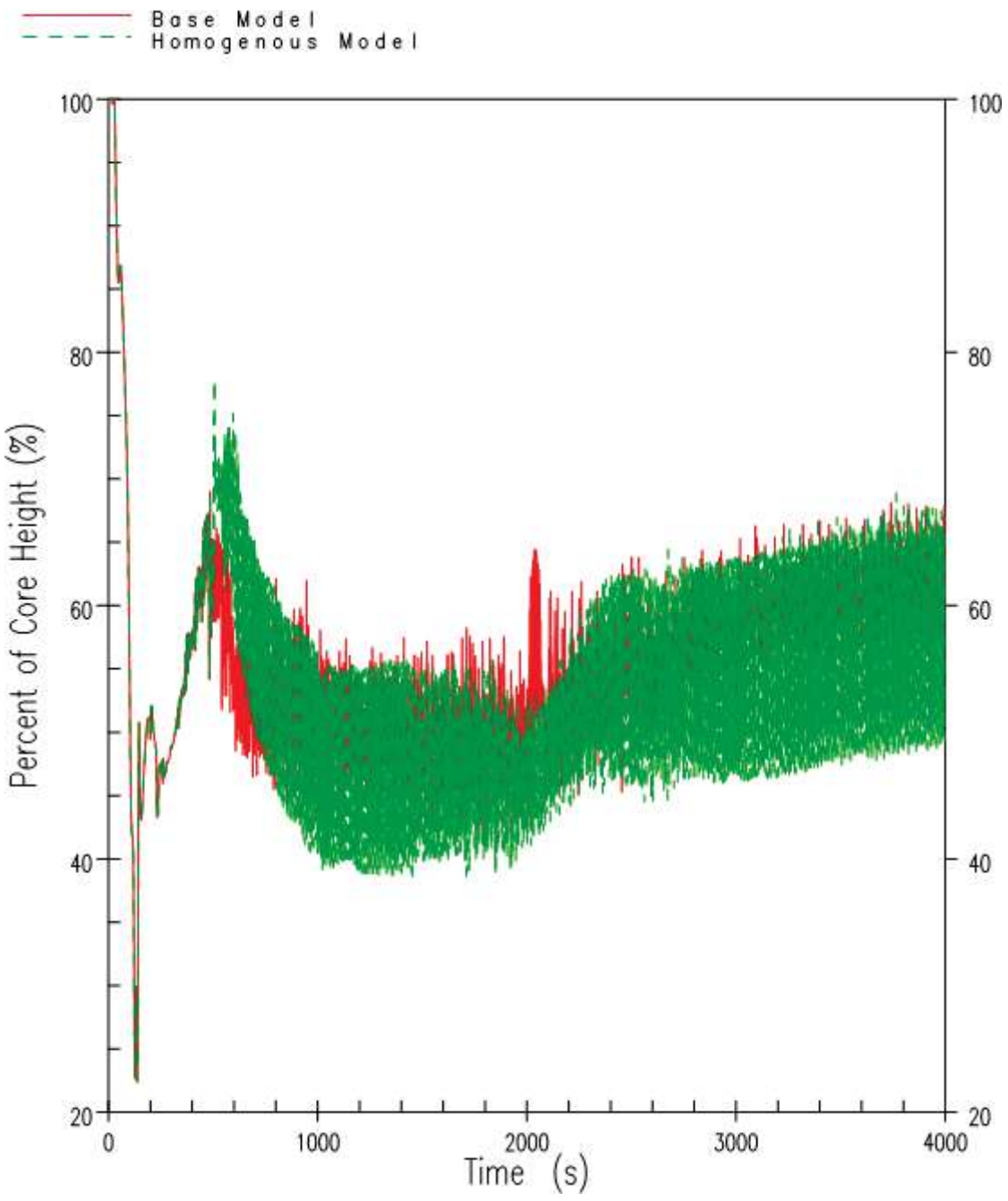


Figure 9.6.5-89(a). DBA DEDVI Entrainment – Core Collapsed Liquid Level Comparison

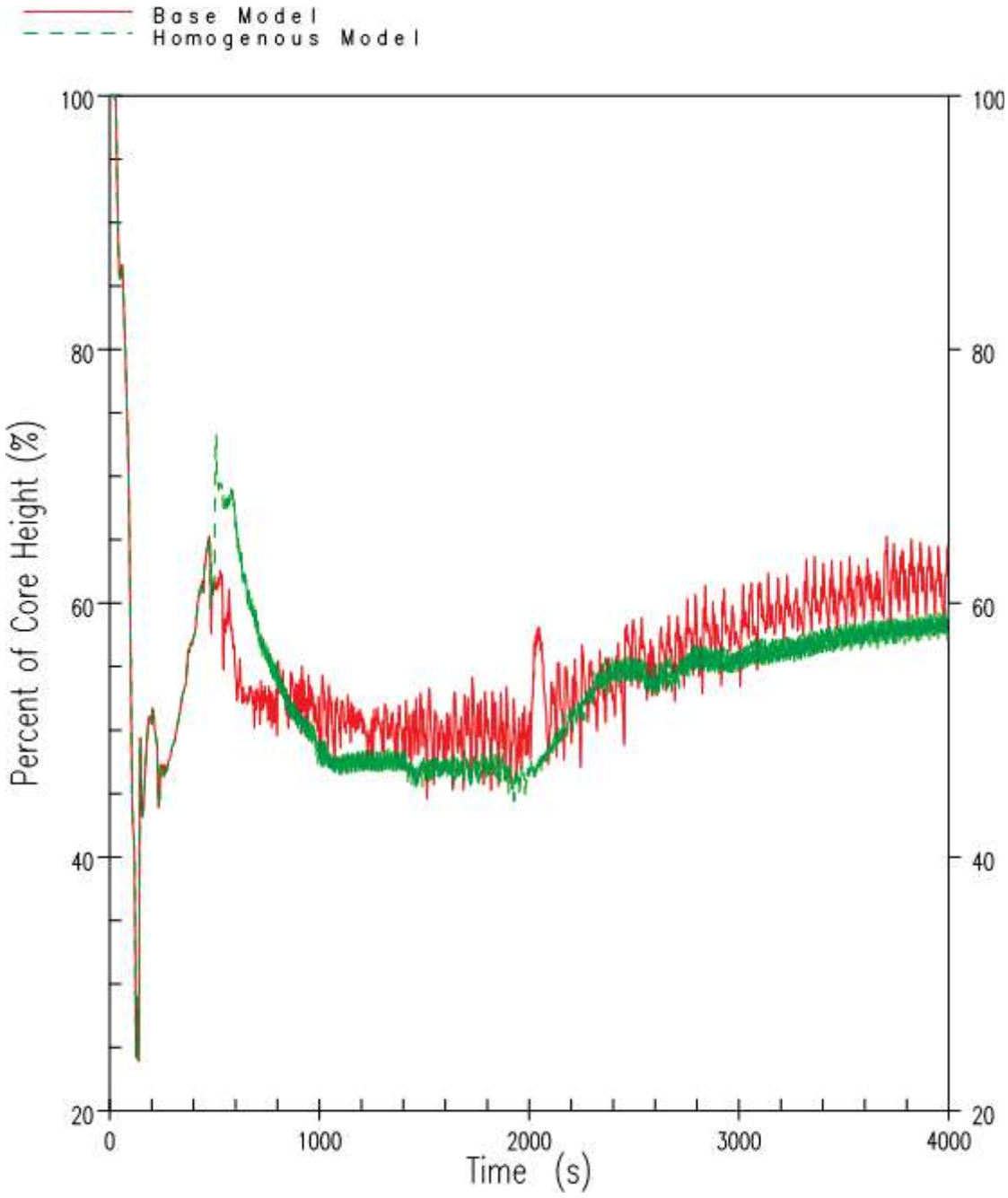


Figure 9.6.5-89(b). DBA DEDVI Entrainment – Core Collapsed Liquid Level Comparison (Smoothed)

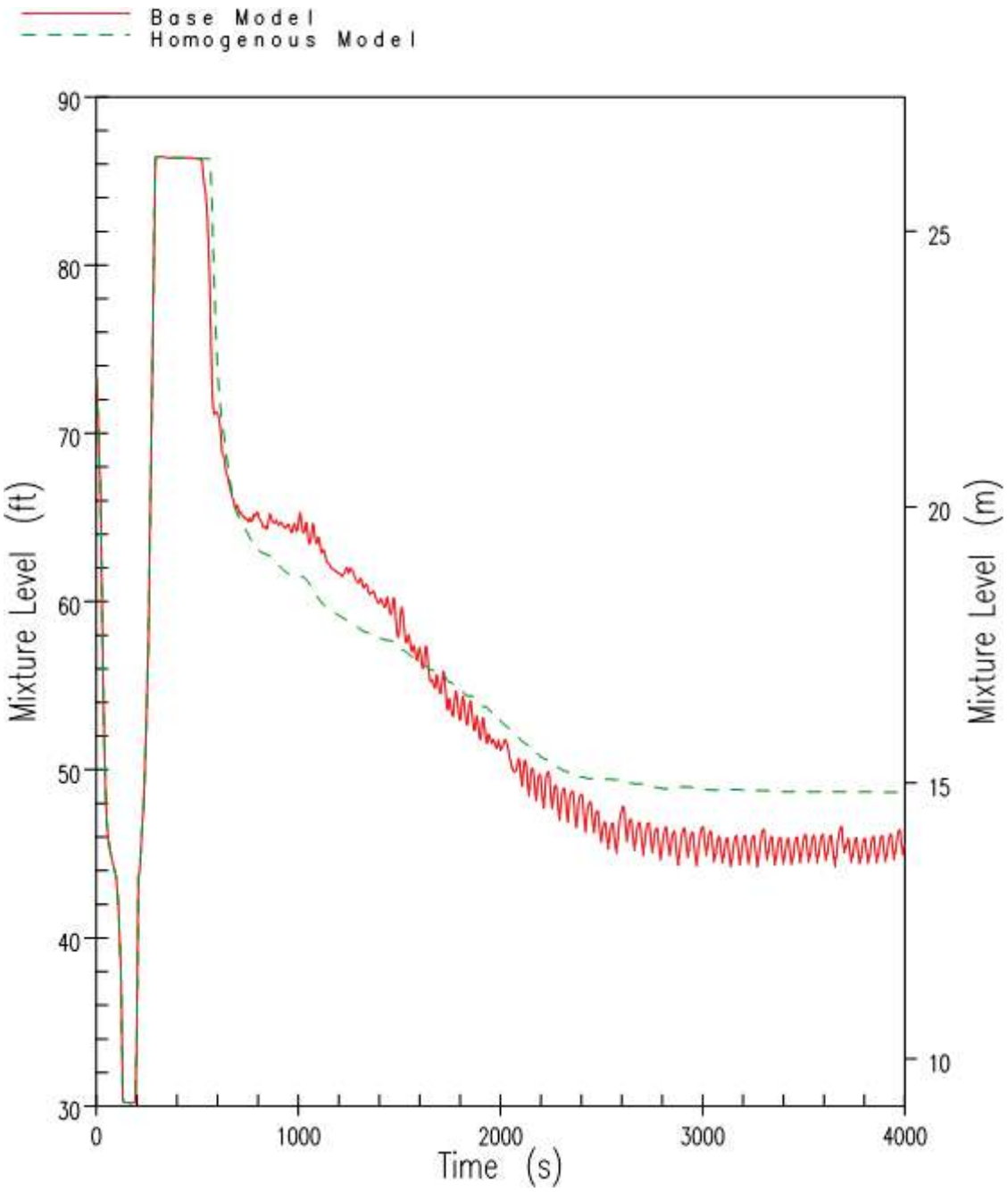


Figure 9.6.5-90. DBA DEDVI Entrainment – Pressuriser Mixture Level Comparison

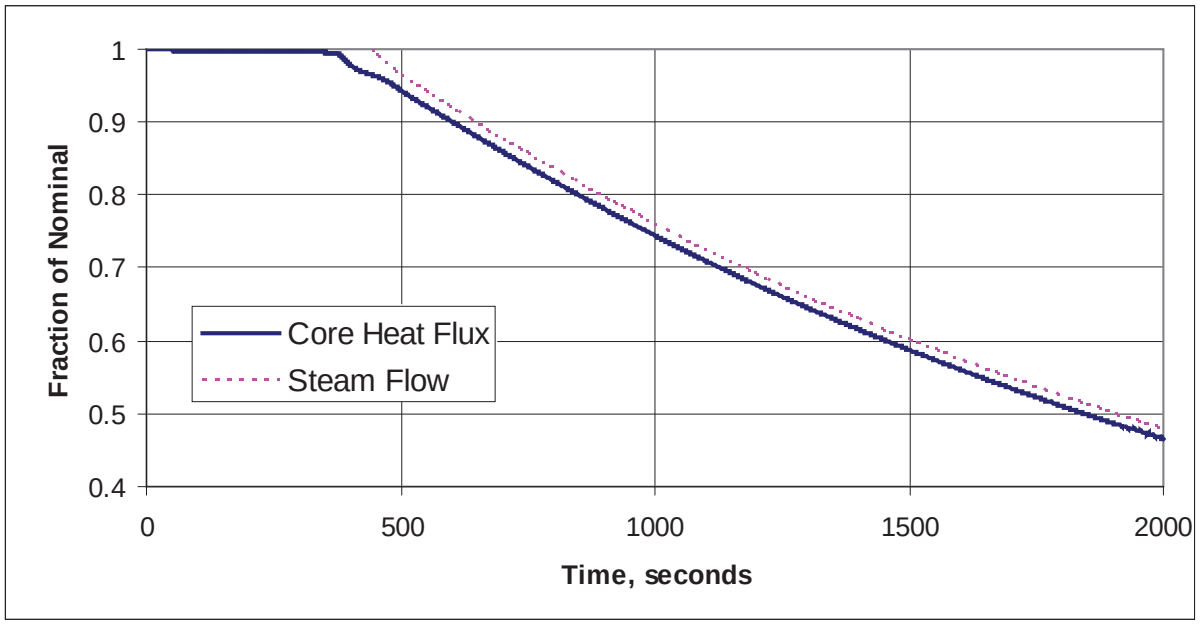


Figure 9.6.5-91. ATWT RCS Depressurisation, Core and Steam Power

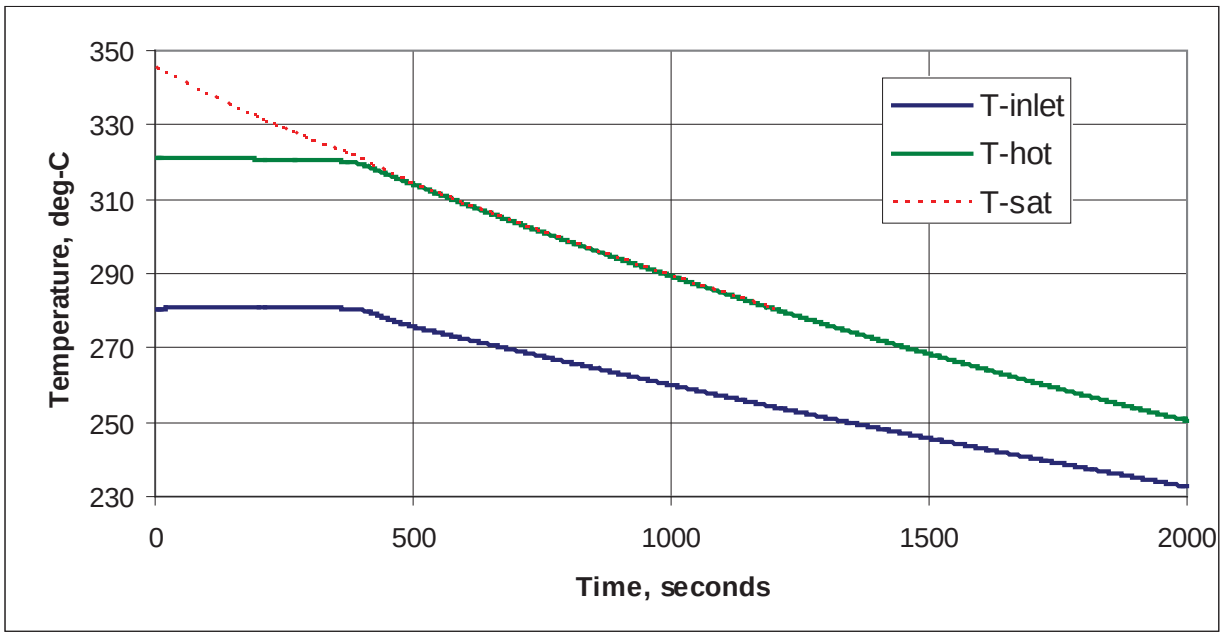


Figure 9.6.5-92. ATWT RCS Depressurisation, Hot-Leg and Cold-Leg Temperature

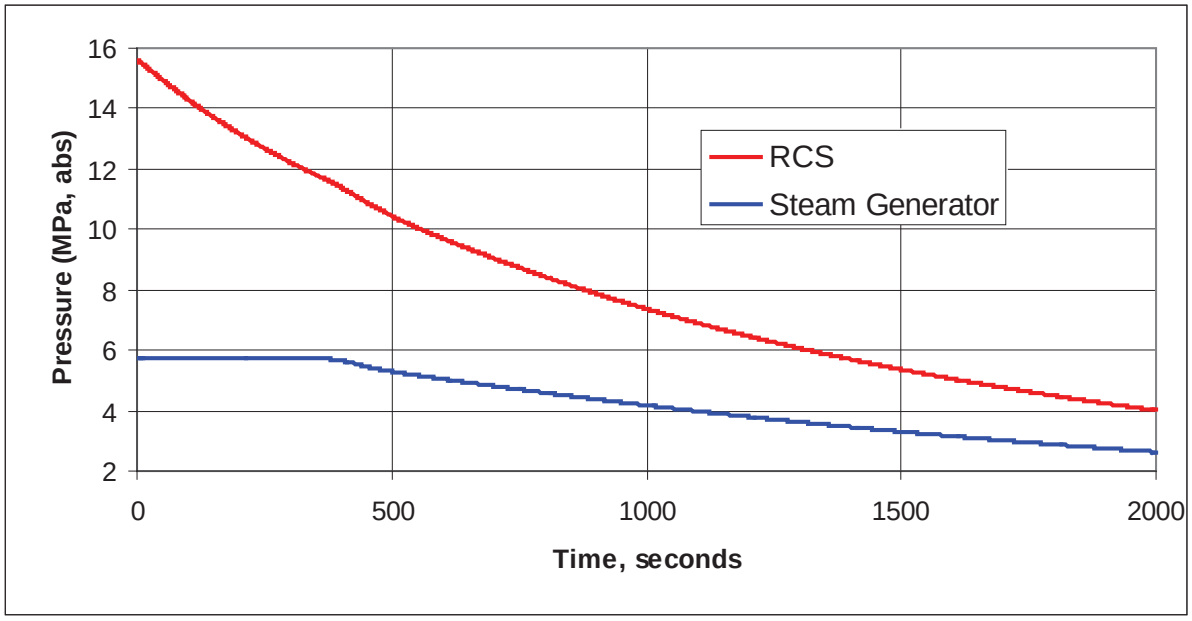


Figure 9.6.5-93. ATWT RCS Depressurisation, Primary and Secondary Pressure

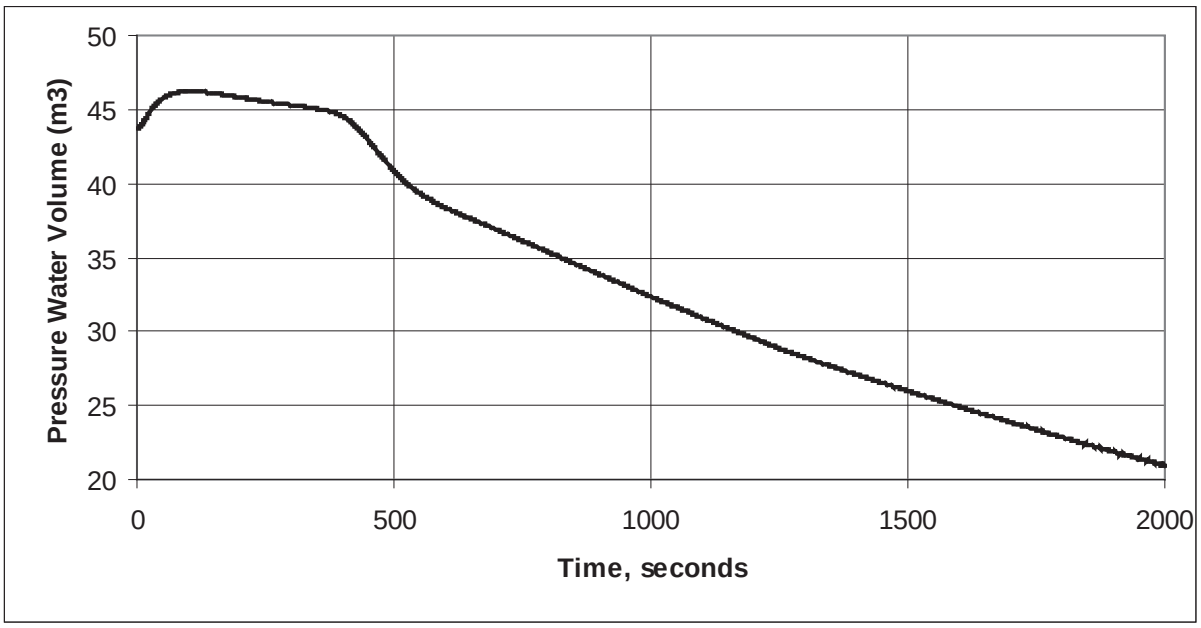


Figure 9.6.5-94. ATWT RCS Depressurisation, Pressuriser Water Volume

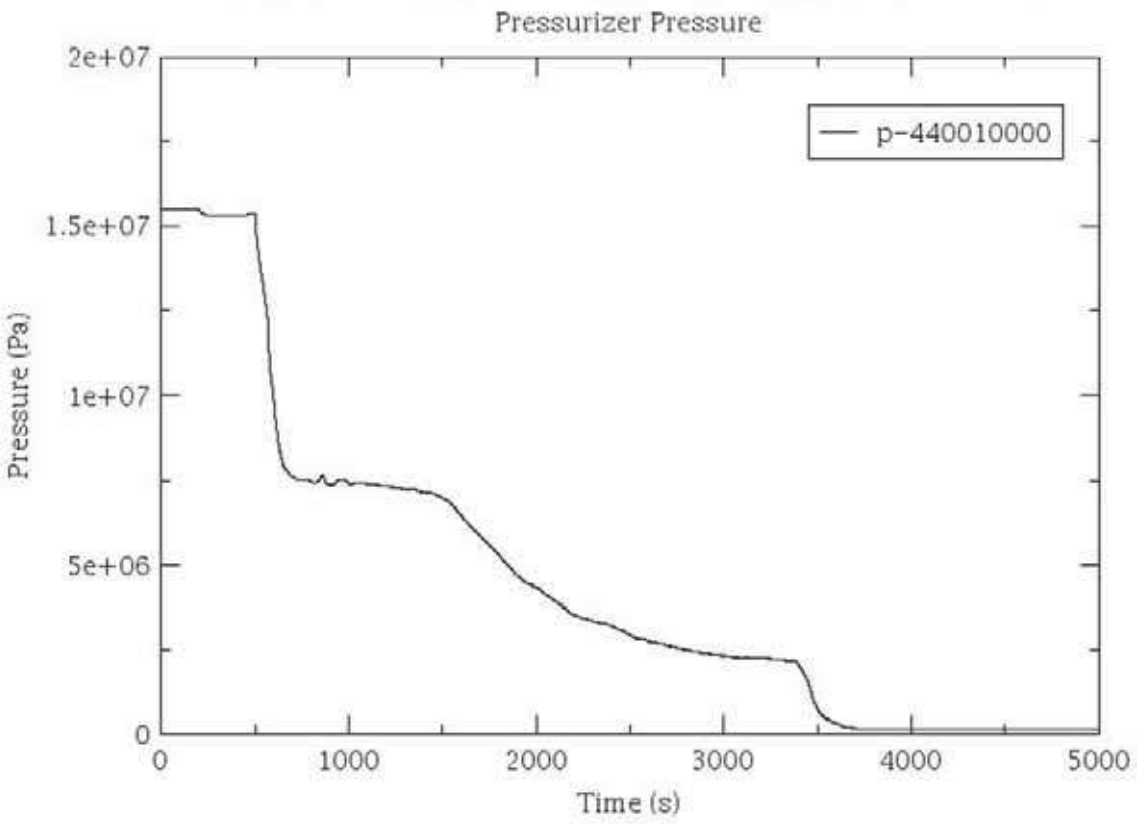


Figure 9.6.5-95. Diverse Core Cooling, Small LOCA Case 1, Pressuriser Pressure

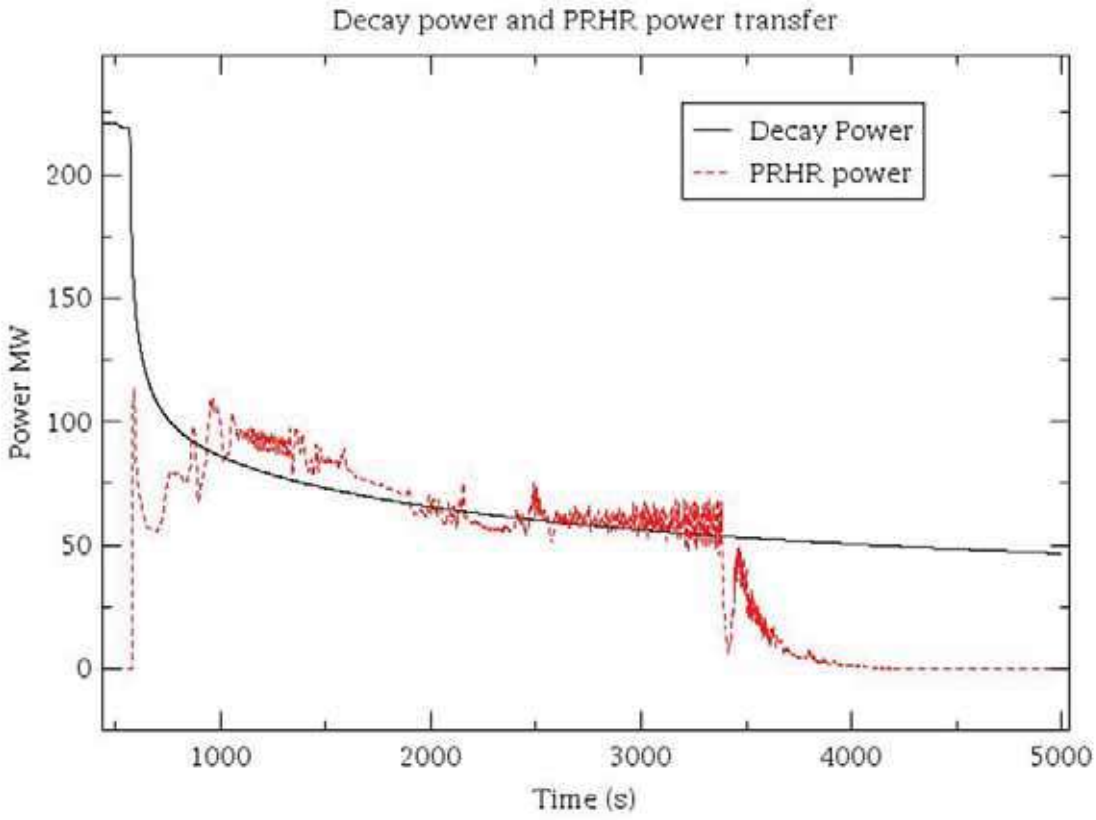


Figure 9.6.5-96. Diverse Core Cooling, Small LOCA Case 1, PRHR Heat Removal vs Decay Heat

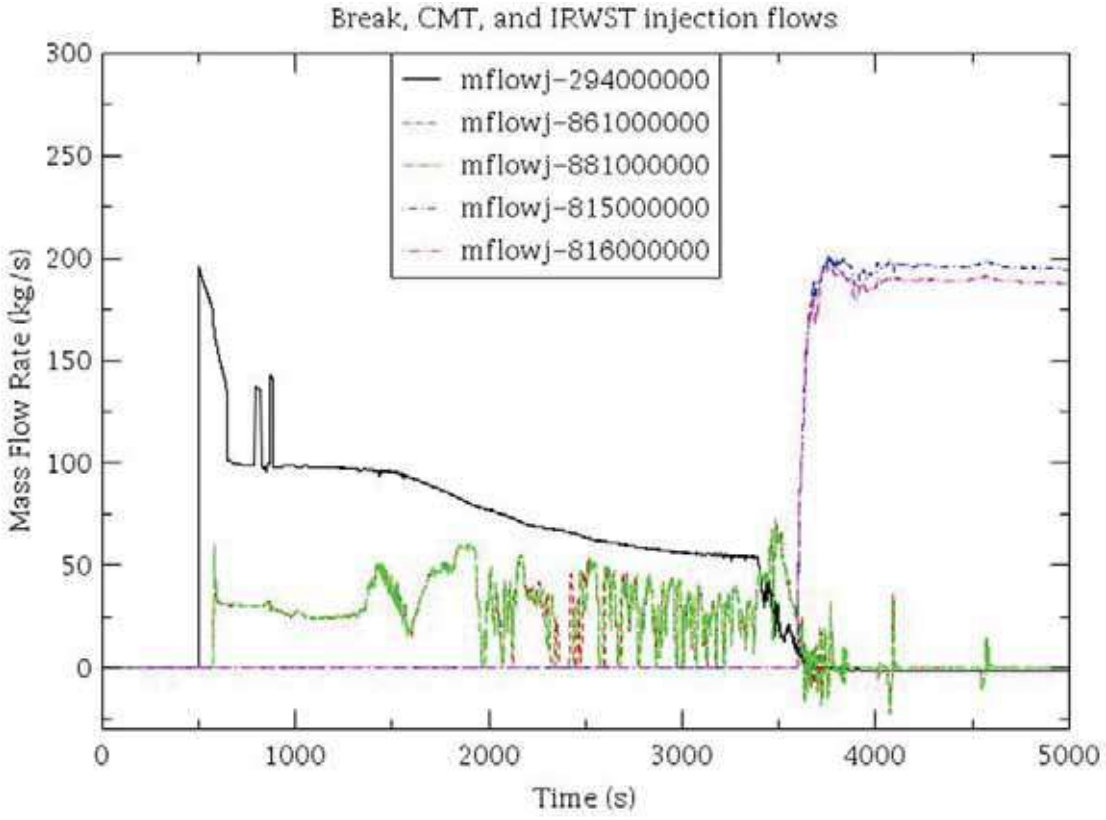


Figure 9.6.5-97. Diverse Core Cooling, Small LOCA Case 1, Break, CMT and IRWST Flows

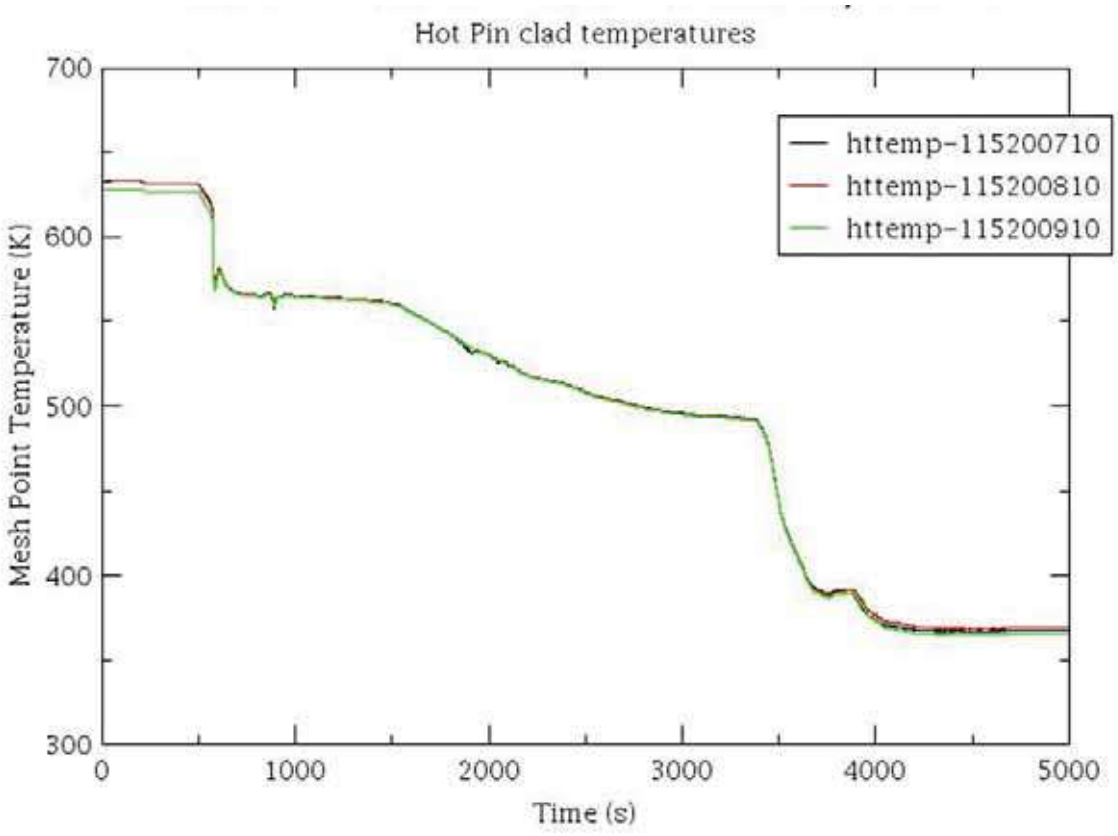


Figure 9.6.5-98. Diverse Core Cooling, Small LOCA Case 1, Peak Clad Temperature

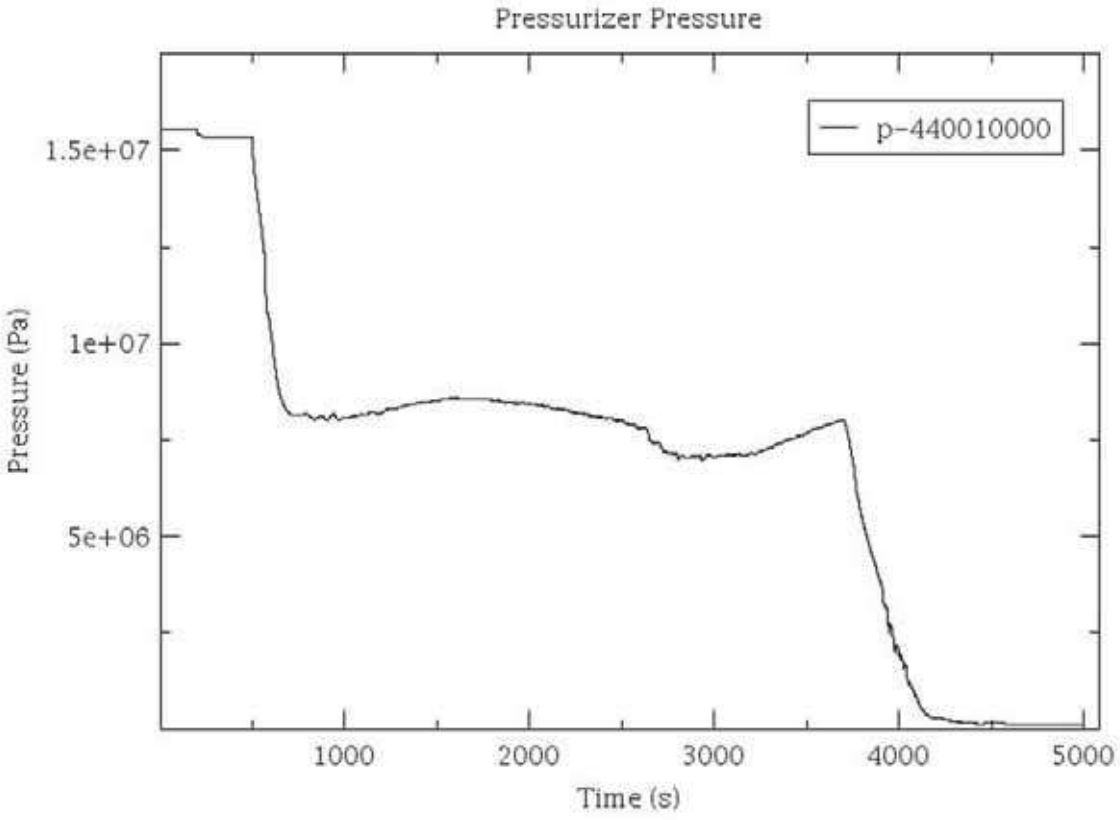


Figure 9.6.5-99. Diverse Core Cooling, Small LOCA Case 2, Pressuriser Pressure

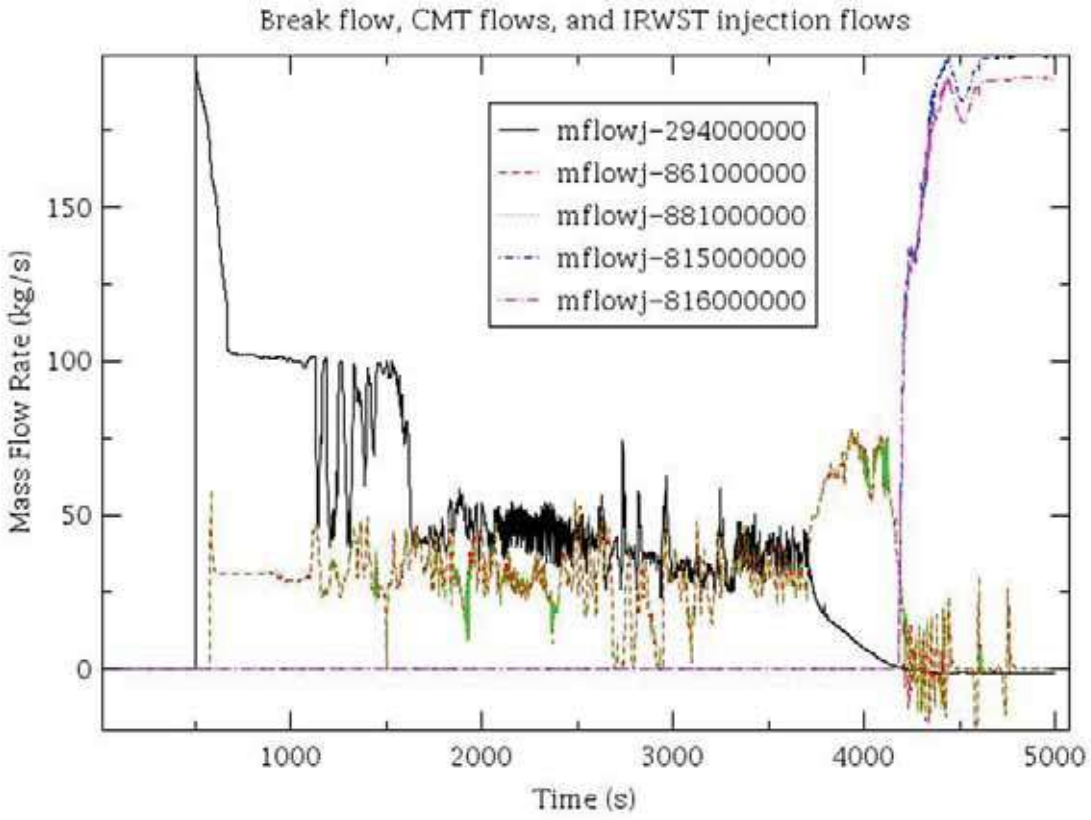


Figure 9.6.5-100. Diverse Core Cooling, Small LOCA Case 2, Break, CMT, IRWST Flows

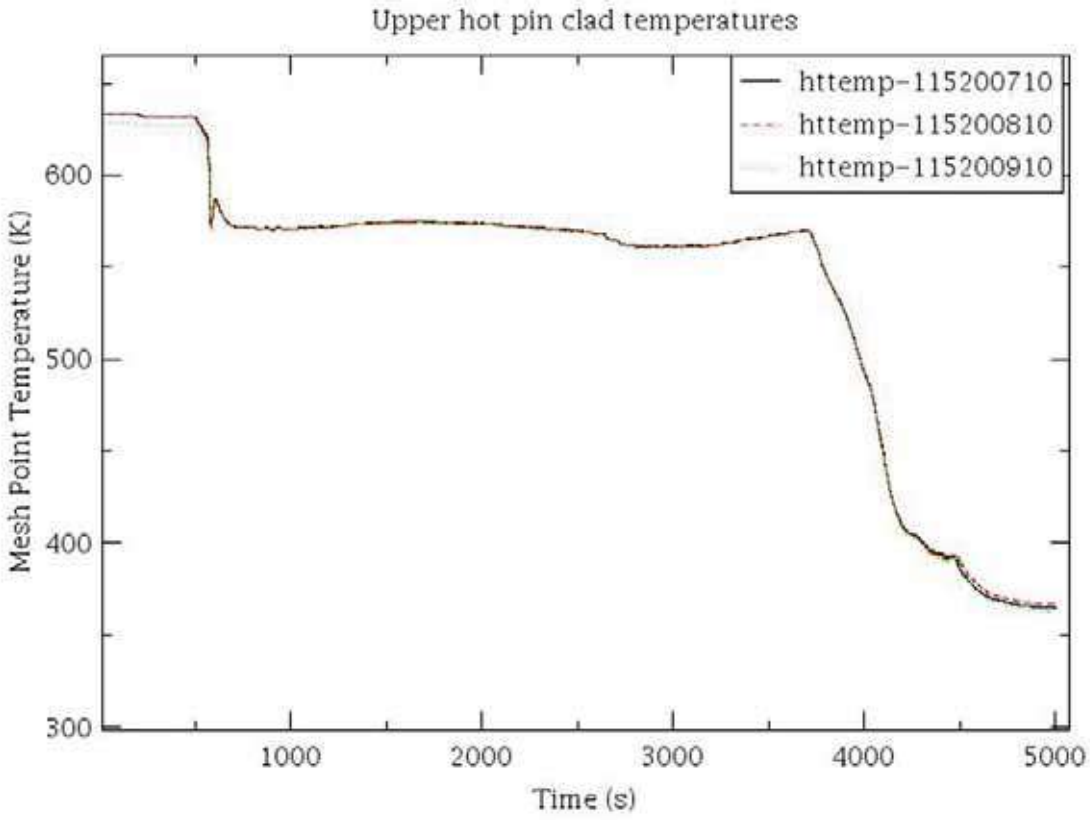


Figure 9.6.5-101. Diverse Core Cooling, Small LOCA Case 2, Peak Clad Temperature

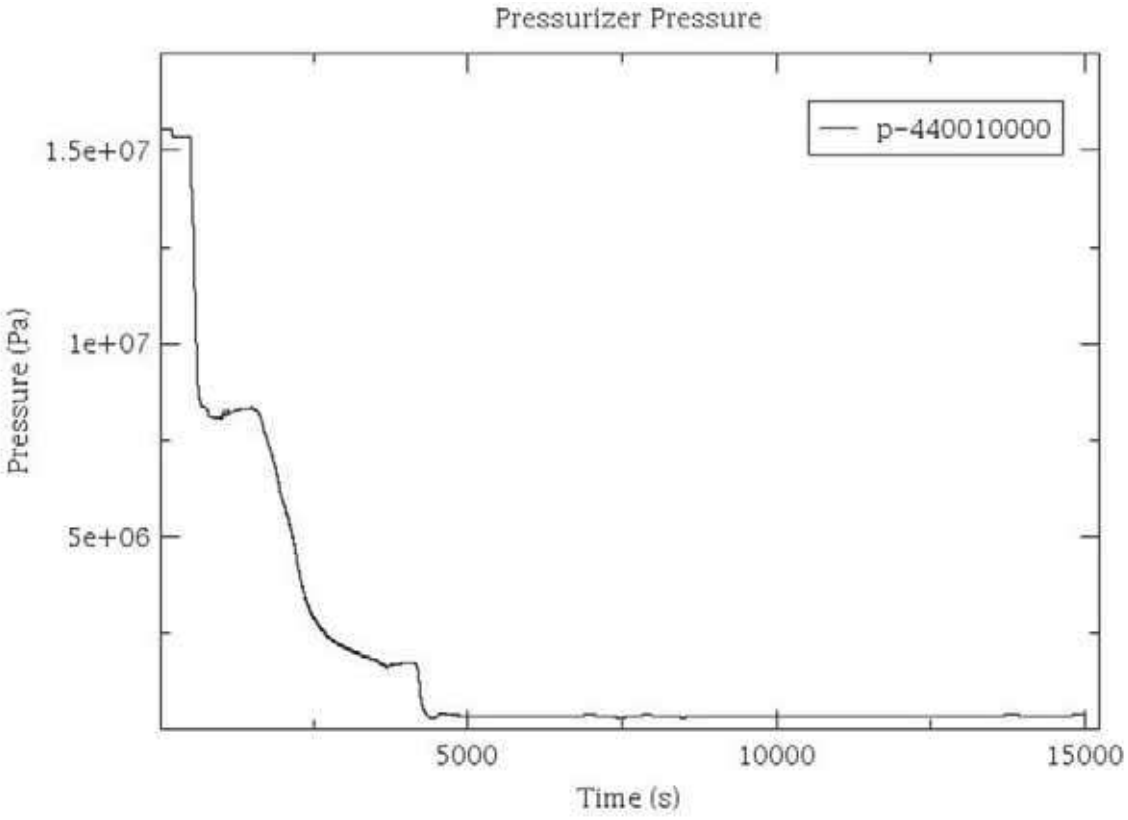


Figure 9.6.5-102. Diverse Core Cooling, Small LOCA Case 3, Pressuriser Pressure

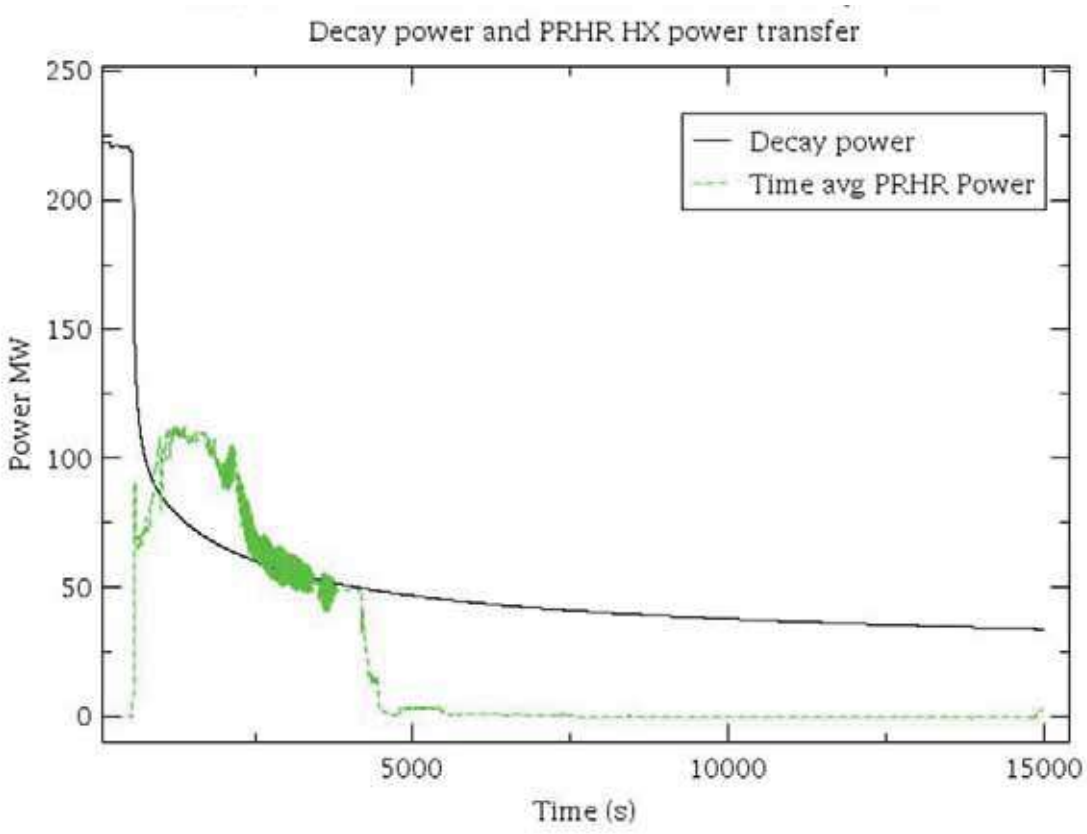


Figure 9.6.5-103. Diverse Core Cooling, Small LOCA Case 3, PRHR Heat Removal and Decay Heat

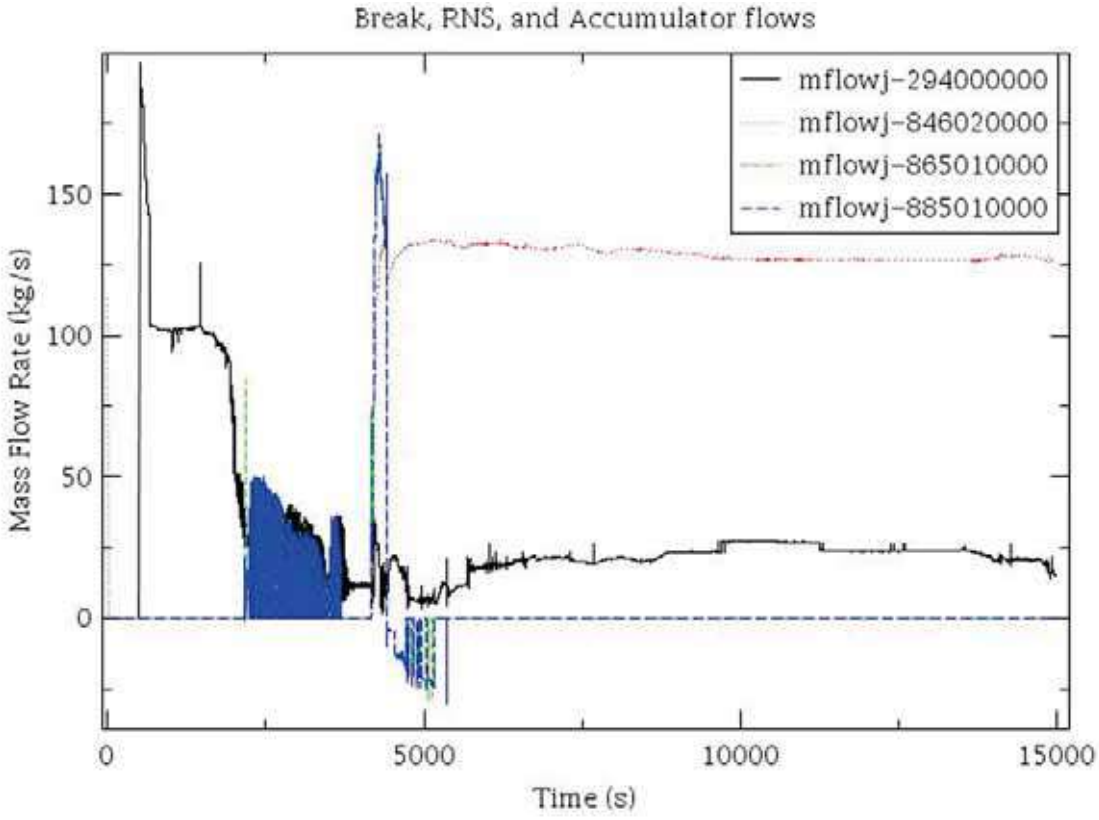


Figure 9.6.5-104. Diverse Core Cooling, Small LOCA Case 3, Break, RNS, Accumulator Flows

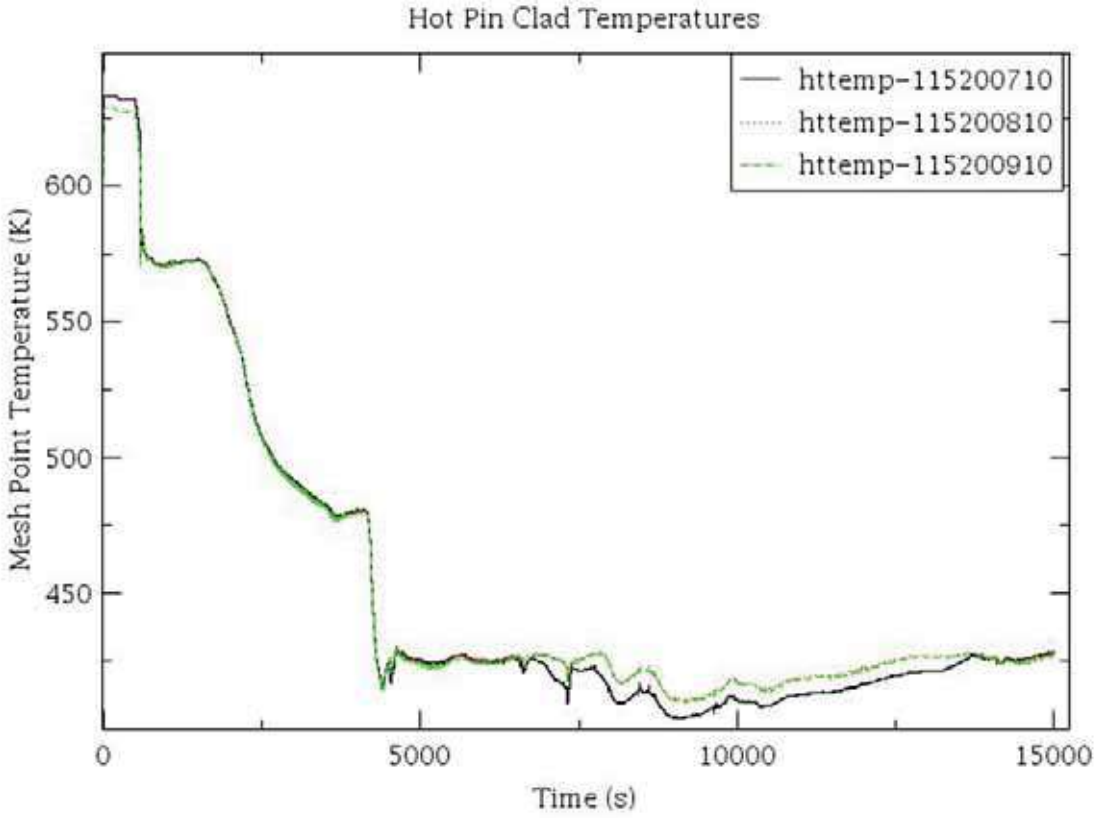


Figure 9.6.5-105. Diverse Core Cooling, Small LOCA Case 3, peak Clad Temperature

9.6.6 Post-LOCA Long-Term Cooling

9.6.6.1 Long-Term Cooling Analysis Methodology

The AP1000 plant Class 1 systems are designed to provide adequate cooling of the reactor indefinitely. Initially, this is achieved by discharging water from the IRWST into the vessel. When the low-3 level setpoint is reached in the IRWST, the containment recirculation subsystem isolation valves open and water from the containment RCS compartment can flow into the vessel through the PXS piping. The water in containment rises in temperature toward the saturation temperature. Long-term heat removal from the reactor and containment is by heat transfer through the containment shell to atmosphere.

The purpose of the post-LOCA long-term cooling analysis is to demonstrate that the passive systems provide adequate emergency core cooling system performance during the IRWST injection/containment recirculation time scale. The long-term cooling analysis is performed using the WCOBRA/TRAC computer code to verify that the passive injection system is providing sufficient flow to the reactor vessel to cool the core and to preclude boron precipitation.

The AP1000 plant long-term cooling analysis is supported by the series of tests at the Oregon State University AP600 APEX Test Facility. This test facility is designed to represent the AP600 reactor Class 1 and Class 2 systems at quarter-scale during long-term cooling. The data obtained during testing at this facility has been shown to apply to the AP1000 design (Reference 9.6.6-3). These tests were modelled using WCOBRA/TRAC with an equivalent noding scheme to that used for the AP600 design (Reference 9.6.6-1) in order to validate the code for long-term cooling analysis.

Reference 9.6.6-2 provides details of the AP1000 plant WCOBRA/TRAC modelling. The coarse reactor vessel modelling used for the AP600 design has been replaced with a detailed noding like that applied in the large-break LOCA analyses described in Section 9.6.5. The reactor vessel noding used in the AP1000 plant long-term cooling analyses in core and upper plenum regions is equivalent to that used in full-scale test simulations (see Reference 9.6.6-2).

A DEDVI line break is analysed because it is the most limiting long-term cooling case in the relationship between decay power and available liquid driving head. Because the IRWST spills directly onto the containment floor in a DEDVI break, this event has the highest core decay power when the transfer to sump injection is initiated. In postulated DEDVI break cases, the compartment water level exceeds the elevation at which the DVI line enters the reactor vessel, so water can flow from the containment into the reactor vessel through the broken DVI line; this in-flow of water through the broken DVI line assists in the heat removal from the core. The steam produced by boiling in the core vents to the containment through the ADS valves and condenses on the inner surface of the steel containment vessel. The condensate is collected and drains to the IRWST to become available for injection into the reactor coolant system. The WCOBRA/TRAC analysis presented analyses the DEDVI small-break LOCA event from a time (3000 seconds) at which IRWST injection is fully established to beyond the time of containment recirculation. During this time, the head of water to drive the flow into the vessel for IRWST injection decreases from the initial level to its lowest value at the containment recirculation switchover time. PXS Room B is the location of the break in the DVI line. At this break location, liquid level in containment at the time of recirculation is a minimum.

A continuous analysis of the post-LOCA long term cooling is provided from the time of stable IRWST injection through the time of sump recirculation for the DEDVI break. Maximum design resistances are applied in WCOBRA/TRAC for both the ADS Stage 4 flow paths and the IRWST injection and containment recirculation flow paths.

The break modelled is a double-ended guillotine rupture of one of the direct vessel injection lines. The long-term cooling phase begins after the simultaneous opening of the isolation valves in the IRWST DVI lines and the opening of ADS Stage 4 squib valves, when flow injection from the IRWST has been fully established. Initial conditions are consistent with the NOTRUMP DEDVI case at 0.14 MPa (20 psia) containment pressure reported in Section 9.6.5.

Appendix 9C provides the means for safe shutdown for all design basis faults.

9.6.6.2 DEDVI Line Break with ADS Stage 4 Single Failure, Passive Core Cooling System Only Case; Continuous Case

This section presents the results of a DEDVI line break analysis during IRWST injection phase continuing into sump recirculation. Initial conditions at the start of the case are prescribed based on the NOTRUMP DEDVI break results to allow a calculation to begin shortly after IRWST injection begins in the small break long-term cooling transient. The WCOBRA/TRAC calculation is then allowed to proceed until a quasi-steady-state is achieved. At this time, the predicted results are independent of the assumed initial conditions. This calculation uses boundary conditions taken from a WGOTHIC analysis of this event. During the calculation, which is carried out for 10,000 seconds until a quasi-steady-state sump recirculation condition has been established, the IRWST water level is decreased continuously until the sump recirculation setpoint is reached.

In the analysis, one of the two ADS Stage 4 valves in the PRHR loop is assumed to have failed. The initial reactor coolant system liquid inventory and temperatures are determined from the NOTRUMP calculation. The core makeup tanks do not contribute to the DVI injection during this phase of the transient. Steam generator secondary side conditions are taken from the NOTRUMP calculation (at the beginning of long-term cooling). The reactor coolant pumps are tripped and not rotating.

The temperatures of the liquid in the containment sump and the containment pressure are based on WGOTHIC calculations of the conservative minimum pressure during this long-term cooling transient, including operation of the containment fan coolers. Small changes in the RCS compartment level do not have a major effect on the predicted core collapsed liquid level or on the predicted flow rate through the core. The minimum compartment floodup level for this break scenario is 102.4 meters (107.8 feet) or greater.

In this transient, the IRWST provides a hydraulic head sufficient to drive water into the downcomer through the intact DVI nozzle. Also, water flows into the downcomer from the broken DVI line once the liquid level in the compartment with the broken line is adequate to support flow. The water flows down the downcomer and up through the core, into the upper plenum. Steam produced in the core and liquid flow out of the reactor coolant system via the ADS Stage 4 valves. There is little flow out of ADS Stages 1, 2, and 3 even when the IRWST liquid level falls below the sparger elevation, so they are not modelled in this calculation. The venting provided by the ADS-4 paths enables the liquid flow through the core to maintain core cooling.

Approximately 500 seconds of WCOBRA/TRAC calculation are required to establish the quasi-steady-state condition associated with IRWST injection at the start of long-term cooling and so are ignored in the following discussion. The hot leg levels are such that during the IRWST injection phase the quality of the ADS Stage 4 mass flows varies as water is carried out of the hot legs. This periodically increases the pressure drop across the ADS Stage 4 valves and the upper plenum pressure. The higher pressure in the upper plenum reduces the injection flow. This cycle of pressure variations due to changing void fractions in the flow through ADS Stage 4 is consistent with test observations and is expected to recur often during long-term cooling.

The head of water in the IRWST causes a flow of subcooled water into the downcomer at an approximate rate of 81.6 kg/s (180 lbm/s) through the intact DVI nozzle at the start of long-term cooling. The downcomer level at the end of the code initiation (the start of long-term cooling) is about 5.49 meters (18.0 feet) (Figure 9.6.6-1). Note that the time scale of this and other figures in Section 9.6.6.2 is offset by 2500 seconds; that is, a time of 500 seconds on the Figure 9.6.6-1 axis equals 3000 seconds transient time for the DEDVI break. All of the injection water flows down the downcomer and up through the core. The accumulators have been fully discharged before the start of the time window and do not contribute to the DVI flow.

Boiling in the core produces steam and a two-phase mixture, which flows into the upper plenum. The core is 4.27 meters (14 feet) high, and the core average collapsed liquid level (Figure 9.6.6-2) is shown from the start of long-term cooling. The boiling process causes a variable rate of steam production and resulting pressure changes, which in turn causes oscillations in the liquid flow rate at the bottom of the core and also variations in the core collapsed level and the flow rates of liquid and vapour out of the top of the core. In the WCOBRA/TRAC noding, the core is divided both axially and radially as described in Reference 9.6.6-2. The void fractions in the top two cells of the hot assembly are shown as Figures 9.6.6-3 and -4. The average void fraction of these upper core cells is approximately 0.8 during long-term cooling, during IRWST injection, and into the containment recirculation period. There is a continuous flow of two-phase fluid into the hot legs, and mainly vapour flow toward the ADS Stage 4 valve occurs at the top of the pipe. The collapsed liquid level in the hot leg averages around 0.46 meters (1.5 feet) (Figure 9.6.6-5). The hot legs on average are more than 50-percent full. Vapour and liquid flows at the top of the core are shown in Figures 9.6.6-6 and 9.6.6-7; the upper plenum collapsed liquid level in Figure 9.6.6-8. Figures 9.6.6-9 and 9.6.6-10 are ADS stage 4 mass flowrates.

The pressure in the upper plenum is shown in Figure 9.6.6-11. The upper plenum pressure fluctuation that occurs is due to the ADS Stage 4 water discharge. The PCT of the hot rod follows saturation temperature (Figure 9.6.6-12), which demonstrates that no uncovery and no cladding temperature excursion occurs. A small pressure drop is calculated across the reactor vessel, and injection rates through the DVI lines into the vessel are presented in Figures 9.6.6-13 and -14. Figure 9.6.6-14 shows the broken DVI line flow during the start of the long-term cooling period increases to about 34.0 kg/s (75 lbm/s) after the compartment water level has increased above the nozzle elevation to permit liquid injection into the reactor vessel. In contrast, the intact DVI line flow falls from 81.6 kg/s (180 lbm/s) with a full IRWST to about 34.9 kg/s (77 lbm/s) flow from the containment at the end of the calculation. The recirculation core liquid throughput is more than adequate to preclude any boron buildup on the fuel.

9.6.6.3 DEDVI Break and Wall-to-Wall Floodup; Containment Recirculation

This section presents a DEDVI line break analysis with wall-to-wall flooding due to leakage between compartments, using the window mode methodology. All containment free volume beneath the level of the liquid is assumed filled in this calculation to generate the minimum water level condition during containment recirculation. The time identified for this calculation is 14 days into the event, and the core power is calculated accordingly. The initial conditions at the start of the window are consistent with the analysis described in Section 9.6.6.2. Containment recirculation is simulated during the time window. The calculation is carried out over a time period long enough to establish a quasi-steady-state solution; after 500 seconds of problem time, the flow dynamics are quasi-steady-state and the predicted results are independent of the assumed initial conditions. The liquid level is simulated constant at 8.60 meters (28.2 feet) above the bottom inside surface of the reactor vessel (refer to Figure 9.0-2 for AP1000 reference plant elevations) during the time window, and the liquid temperatures in the containment sump and the PXS “B” room are both modelled at 100°C (212°F). The containment pressure is conservatively

assumed to be 0.101 MPa (14.7 psia). The single failure of an ADS Stage 4 flow path is assumed as in the Section 9.6.6.2 case.

Focusing on the post 400-second time interval of this case, the containment liquid provides a hydraulic head sufficient to drive water into the downcomer through the DVI nozzles. The water introduced into the downcomer flows down the downcomer and up through the core, into the upper plenum. Steam produced in the core entrains liquid and flows out of the reactor coolant system via the ADS Stage 4 valves. The DVI flow and the venting provided by the ADS paths provide a liquid flow through the core that enables the core to remain cool.

The downcomer collapsed liquid level (Figure 9.6.6-15) varies between 7.32 and 7.62 meters (24 and 25 feet) during the analysis. Pressure spikes produced by boiling in the core can cause the mass flow of the DVI flow rates shown in Figures 9.6.6-27 and -28 into the vessel to fluctuate upward and downward.

Boiling in the core produces steam and a two-phase mixture, which flows out of the core into the upper plenum. The core is 4.27 meters (14 feet) high, and the core collapsed liquid level (Figure 9.6.6-16) maintains a mean level close to the top of the core. The boiling process causes pressure variations, which in turn, cause variations in the core collapsed level and the flow rates of liquid and vapour out of the top of the core. In the WCOBRA/TRAC analysis, the core is nodalised as described in Reference 9.6.6-2. The void fraction in the top cell is shown in Figure 9.6.6-17 for the core hot assembly, and Figure 9.6.6-18 shows the void fraction that exists one cell further down in the hot assembly. The PCT does not rise appreciably above the saturation temperature (Figure 9.6.6.3-26). The flow through the core and out of the reactor coolant system is more than sufficient to provide adequate flushing to preclude concentration of the boric acid solution. Liquid collects above the upper core plate in the upper plenum, where the average collapsed liquid level is approximately 0.94 meters (3.1 feet) (Figure 9.6.6-22). There is no significant flow through the cold legs into either the broken or the intact loops, and there is no significant quantity of liquid residing in any of the cold legs.

The pressure in the upper plenum is shown in Figure 9.6.6-25. The upper plenum pressurisation, which occurs periodically, is due to the ADS Stage 4 water discharge. The collapsed liquid level in the hot leg of the pressuriser loop increases to greater than .046 meters (1.5 feet) by the end of the transient, as shown in Figure 9.6.6-19. Injection rates through the DVI lines into the vessel are presented in Figures 9.6.6-27 and -28.

9.6.6.4 Post Accident Core Boron Concentration

An evaluation has been performed of the potential for the boron concentration to build up in the core following a cold leg LOCA. The evaluation methodology, simplified calculations, and their results are discussed in Reference 9.6.6-2. This evaluation considers both short-term operations, before ADS is actuated, and long-term operations, after ADS is actuated. These evaluations and their results are discussed in the follow paragraphs.

Short-term – Prior to ADS actuation, it is not likely for boron to build up significantly in the core. Normally, water circulation mixes boron in the RCS and prevents buildup in the core. In order for boron to start to build up in the core region, water circulation through the steam generators and PRHR HX has to stop. In addition, significant injection of borated water is needed from the CMTs and the CVS. For this situation to happen, the hot legs need to void sufficiently to allow the steam generator tubes to drain. Once the steam generator tubes void, the cold legs will also void since they are located higher than the hot legs. When the top of the cold legs void, the CMTs will begin to drain. When the CMTs drain to the ADS stage 1 setpoint, ADS is actuated.

Short-term Results – As shown in Section 9.6.5.3.4.2, a 2-inch LOCA requires less than 16 minutes from the time that the hot legs void significantly until ADS is actuated. For larger LOCAs, this time difference is shorter, as seen for the 10-inch (254 mm) cold leg LOCA (Section 9.6.5.3.6.2). The core boron concentration will not build up significantly in this short time. If the break is smaller than 2 inches (50.8 mm), voiding of the hot legs will occur at a later time. With maximum operation of CVS makeup, it takes more than 3 hours for the core boron concentration to build up significantly. In addition, the volume of the boric acid tank limits the maximum buildup of boron in the core.

Following a small LOCA where ADS is not actuated, the operators are guided to sample the RCS boron concentration and to initiate a post-LOCA cooldown and depressurisation. The cooldown and depressurisation of the RCS reduces the leak rate and facilitates recovery of the pressuriser level. Recovery of the pressuriser level allows for re-establishment of water flow through the RCS loops, which mixes the boron. The operators are guided to take an RCS boron sample within 3 hours of the accident and several more during the plant cooldown. The purpose of the boron samples is to assess that there is adequate shutdown margin and that the RCS boron concentration has not built up to excessive levels. The maximum calculated core boron concentration 3 hours after a LOCA without ADS actuation is less than 16,000 ppm. Operator action within 3 hours maintains the maximum core boron concentration well below the boron solubility limit for the core inlet temperatures during the cooldown.

Long-term – Once ADS is actuated, water carryover out the ADS Stage 4 lines limits the potential core boron concentration buildup following a cold leg LOCA. The design of the AP1000 plant facilitates water discharge from the hot legs as follows:

- PXS recirculation flow capability tends to fill the hot legs and bring the water level up to the ADS Stage 4 inlet.

- ADS Stage 4 lines discharge at an elevation 0.91 to 1.22 meters (3 to 4 feet) above the containment water level.

With water carried out ADS Stage 4, the core boron concentration increases until the boron added to the core in the safety injection flow equals the boron removed in the water leaving the RCS through the ADS Stage 4 flow. The lower the ADS Stage 4 vent quality, the lower the core boron concentration buildup.

Long-term Results – Analyses have been performed (Reference 9.6.6-2) to bound the maximum core boron concentration buildup. These analyses demonstrate that highest ADS Stage 4 vent qualities result from the following:

- Highest decay heat levels

- Lowest PXS injection/ADS 4 vent flows, including high line resistances and low containment water levels

The long-term cooling analysis discussed in Section 9.6.6.2 is consistent with these assumptions. The ADS Stage 4 vent quality resulting from this analysis is less than 40 percent at the beginning of IRWST injection and reaches a maximum of less than 50 percent around the initiation of recirculation. It decreases after this peak, dropping to a value less than 8 percent at 14 days.

With the maximum ADS Stage 4 vent qualities, the maximum core boron concentration peaks at a value of about 7400 ppm at the time of recirculation initiation. After this time, the core boron concentration decreases as the ADS Stage 4 vent quality decreases, reaching 5000 ppm about

9 hours after the accident. The core boron solubility temperature reaches a maximum of 14.4°C (58°F) (at 7400 ppm) and quickly drops to 4.4°C (40°F) (at 5000 ppm). With these low core boron solubility temperatures, there is no concern with cold PXS injection water causing boron precipitation in the core. With the IRWST located inside containment, its water temperature is normally expected to be above these solubility temperatures. The minimum core inlet temperature is greater than the solubility temperature considering heatup of the injection by steam condensation in the downcomer and pickup of sensible heat from the reactor vessel, core barrel, and lower support plate.

The boron concentration water in the containment is initially about 2980 ppm. As the core boron concentration increases, the containment concentration decreases slightly. The minimum boron concentration in containment is greater than 2950 ppm. The solubility temperature of the containment water at its maximum boron concentration is 0°C (32°F).

With high decay heat values, the ADS Stage 4 vent flows and velocities are high. These high vent velocities result in flow regimes that are annular for more than 30 days. The annular flow regime moves water up and out the ADS Stage 4 lines. This flow regime is based on the Taitel-Dukler vertical flow regime map. Lower decay heat levels can be postulated later in time or just after a refuelling outage. Significantly lower decay heat levels result in lower ADS Stage 4 vent qualities. They also result in ADS Stage 4 vent flows/velocities that are lower. Even with low ADS Stage 4 vent flow velocities, the AP1000 plant will move water out the ADS Stage 4 operating as a manometer. Small amounts of steam generated in the core reduce the density of the steam/water mixture in the core, upper plenum, and ADS Stage 4 line as it bubbles up through the water. As a result, the injection head is sufficient to push the less dense, bubbly steam/water mix out the ADS Stage 4 line.

At the time recirculation begins, the containment level will be about 102.8 meters (109.3 feet) (for a non-DVI LOCA) and will be about 102.4 meters (108.0 feet) (for a DVI LOCA). Over a period of weeks after a LOCA, water may slowly leak from the flooded areas in containment to other areas inside containment that did not initially flood. As a result, the minimum containment water could decrease to 101.1 meters (103.5 feet). During recirculation operation following a LOCA and ADS actuation, the operators are guided to maintain the containment water level above the 102.1 meter (107 feet) elevation by adding borated water to the containment. In addition, if the plant continues to operate in the recirculation mode, the operators are guided to increase the level to 102.7 meters (109 feet) within 30 days of the accident. These actions provide additional margin in water flow through the ADS Stage 4 line. The operators are also guided to sample the hot leg boron concentration prior to initiating recovery actions that might introduce low temperature water to the reactor.

9.6.6.5 Conclusions

Calculations of AP1000 plant long-term cooling performance have been performed using the WCOBRA/TRAC model developed for the AP1000 design and described in Reference 9.6.6-2. The DEDVI case was chosen because it reaches sump recirculation at the earliest time (and highest decay heat). A window mode case at the minimum containment water level postulated to occur 2 weeks into long-term cooling was also performed.

The DEDVI small-break LOCA exhibits no core uncovery due to its adequate reactor coolant system mass inventory condition during the long-term cooling phase from initiation into containment recirculation. Adequate flow through the core is provided to maintain a low cladding temperature and to prevent any buildup of boric acid on the fuel rods. The wall-to-wall floodup case using the window mode technique demonstrates that effective core cooling is also provided at

the minimum containment water level. The results of these cases demonstrate the capability of the AP1000 plant passive systems to provide long-term cooling for a limiting LOCA event.

9.6.6.6 References

9.6.6-1 Westinghouse Documents WCAP-14601, Rev. 2 (Proprietary) and WCAP-15062, Rev. 2 (Non-Proprietary), "AP600 Accident Analyses - Evaluation Models," May 1998.

9.6.6-2 Westinghouse Documents WCAP-15644-P (Proprietary) and WCAP-15644-NP (Non-Proprietary), Revision 2, "AP1000 Code Applicability Report," March 2004.

9.6.6-3 Westinghouse Documents WCAP-15613 (Proprietary) and WCAP-15706 (Non-Proprietary), Revision 0"AP1000 PIRT and Scaling Assessment," March 2001.

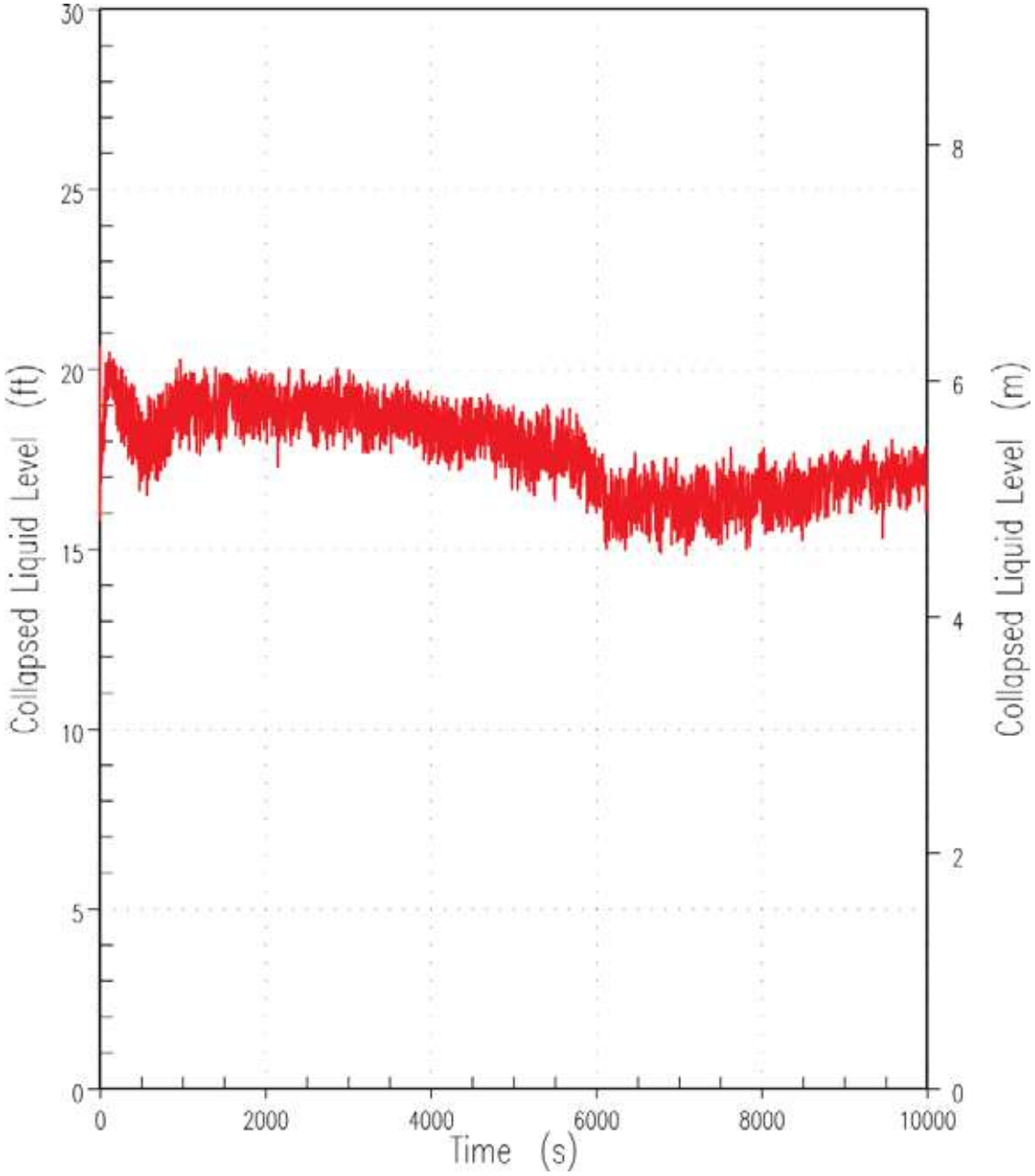


Figure 9.6.6-1. Collapsed Level of Liquid in the Downcomer (DEDVI Case)

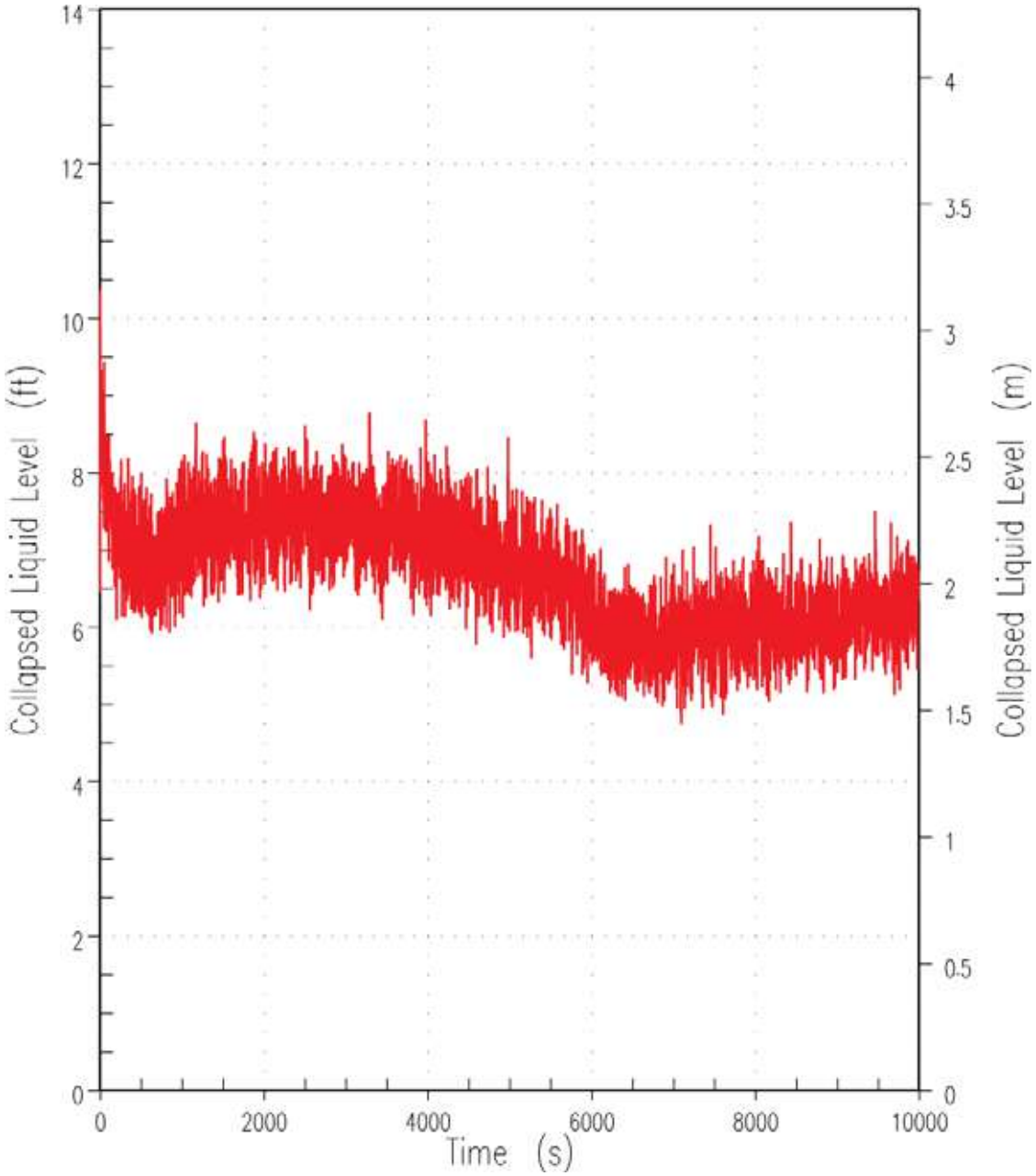


Figure 9.6.6-2. Collapsed Level of Liquid over the Heated Length of the Fuel (DEDVI Case)

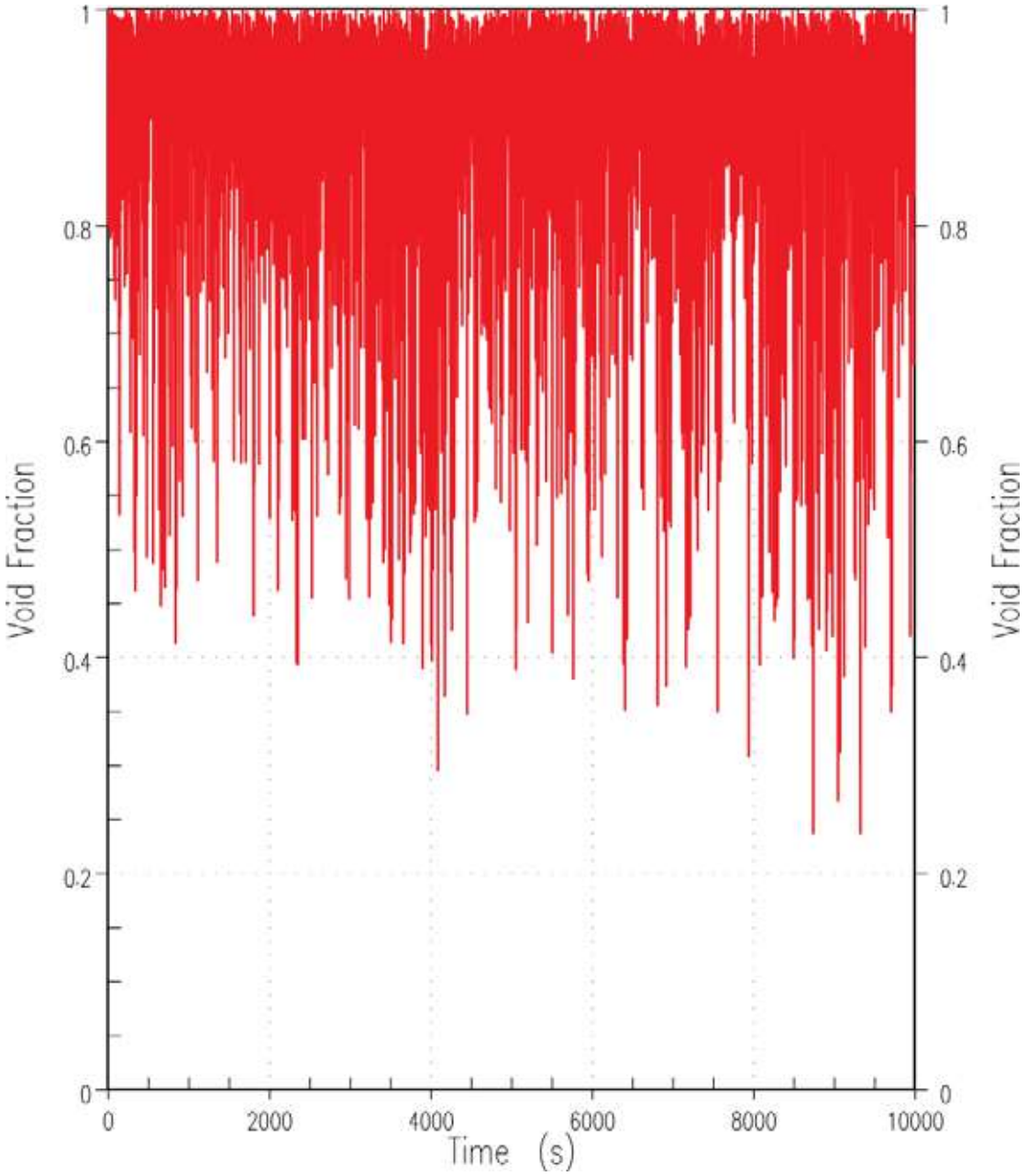


Figure 9.6.6-3. Void Fraction in Core Hot Assembly Top Cell (DEDVI Case)

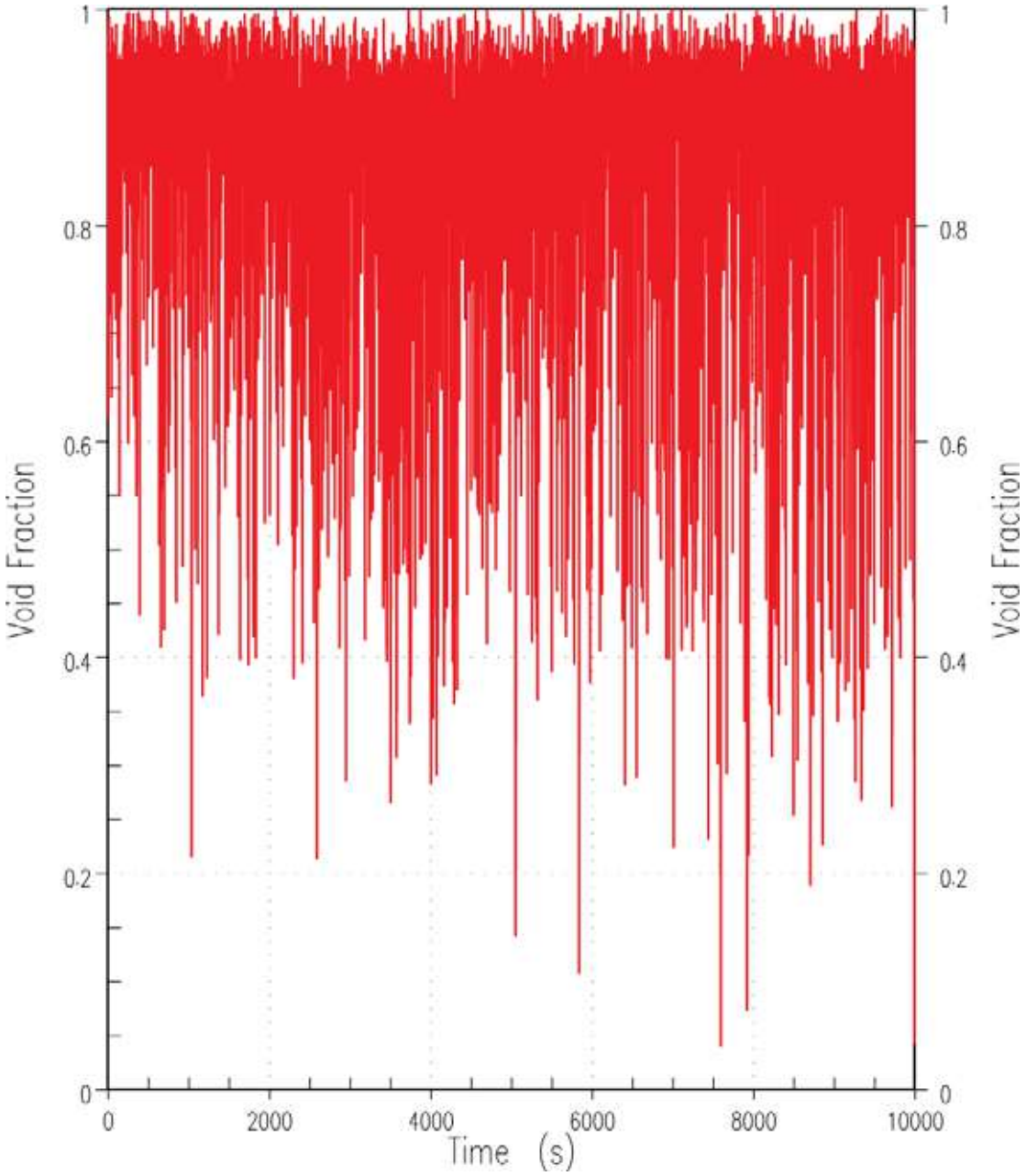


Figure 9.6.6-4. Void Fraction in Core Hot Assembly Second from Top Cell (DEDVI Case)

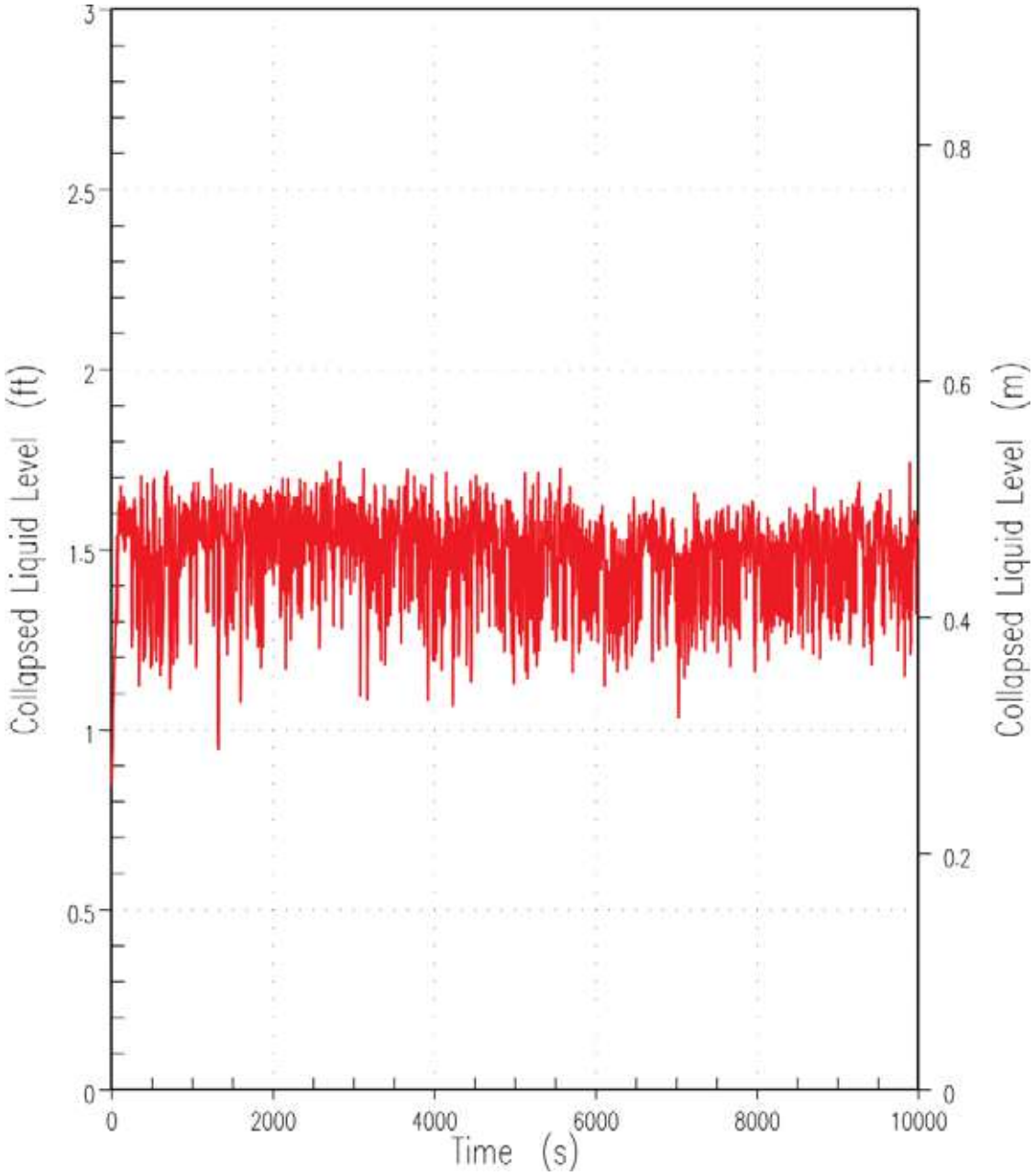


Figure 9.6.6-5. Collapsed Liquid Level in the Hot Leg of Pressuriser Loop (DEDVI Case)

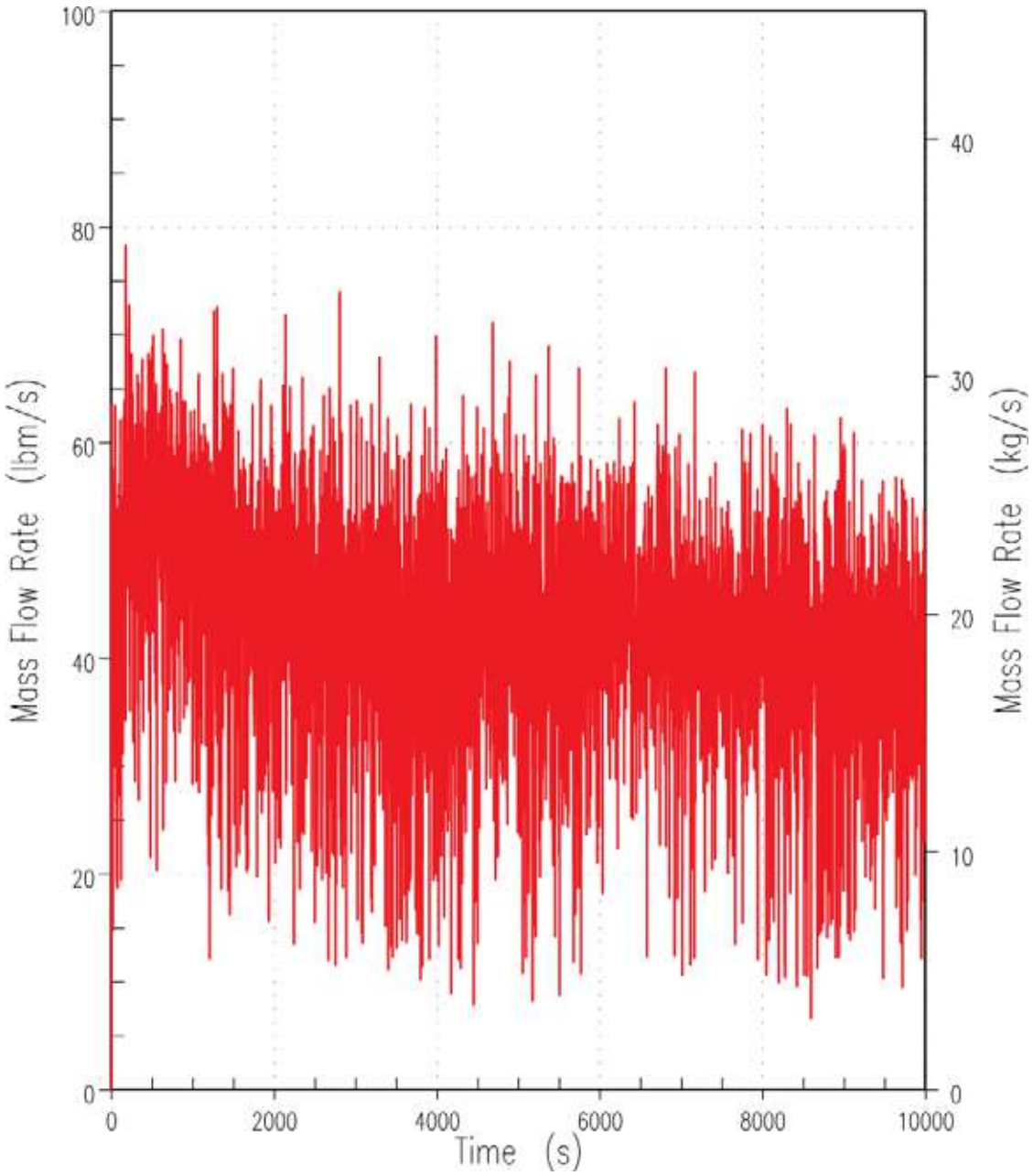


Figure 9.6.6-6. Vapour Rate out of the Core (DEDVI Case)

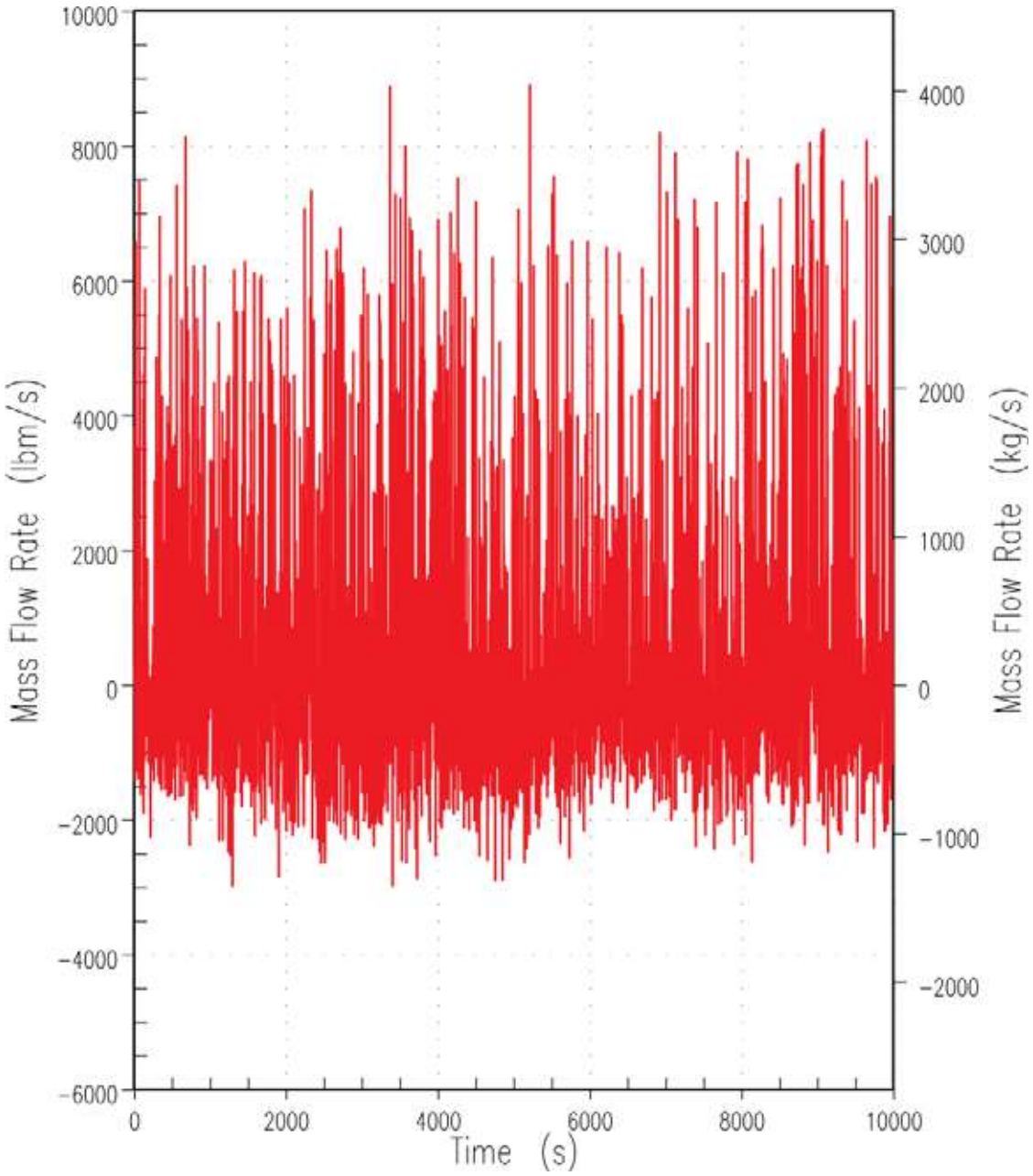


Figure 9.6.6-7. Liquid Flow Rate out of the Core (DEDVI Case)

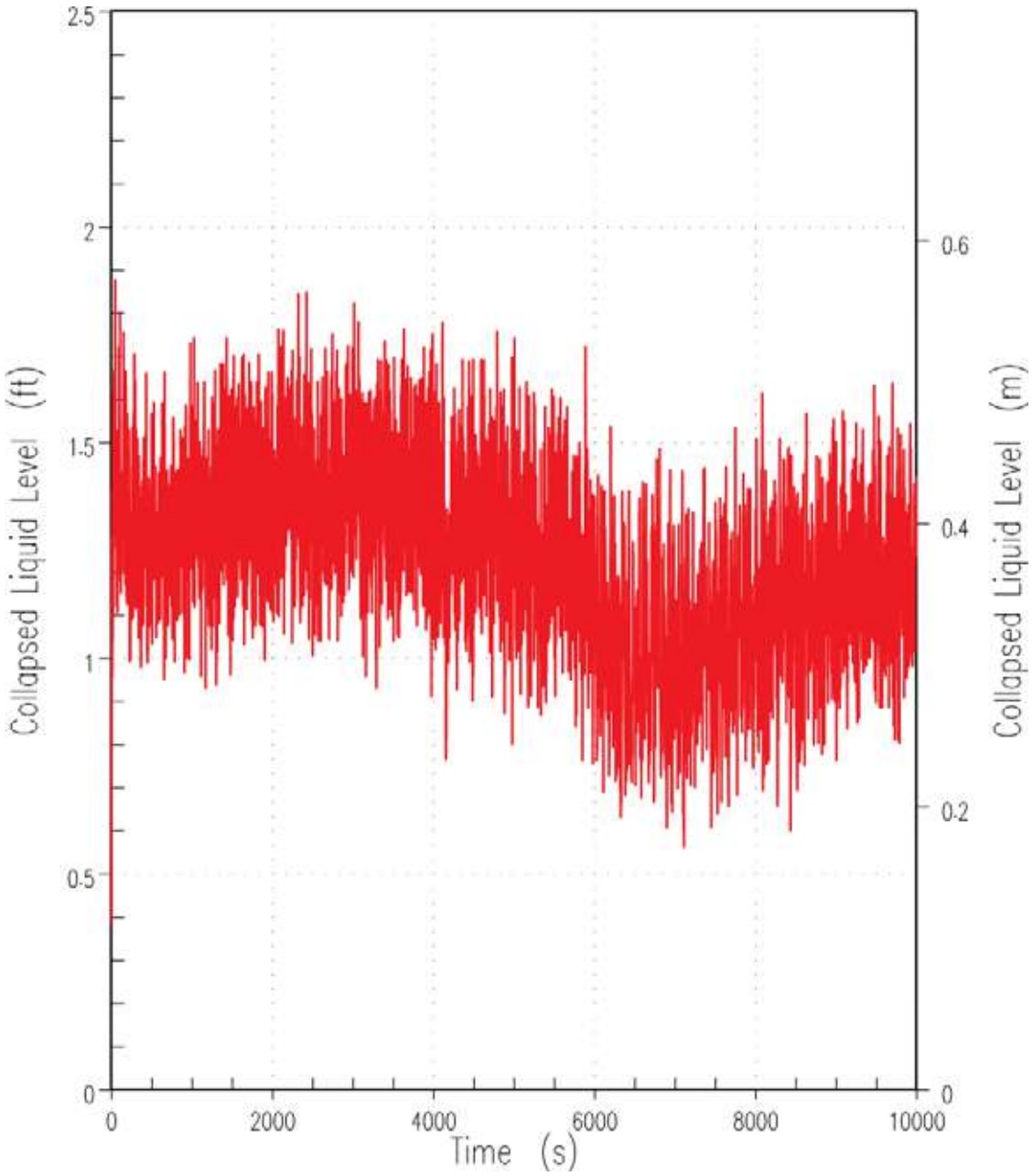


Figure 9.6.6-8. Collapsed Liquid Level in the Upper Plenum (DEDVI Case)

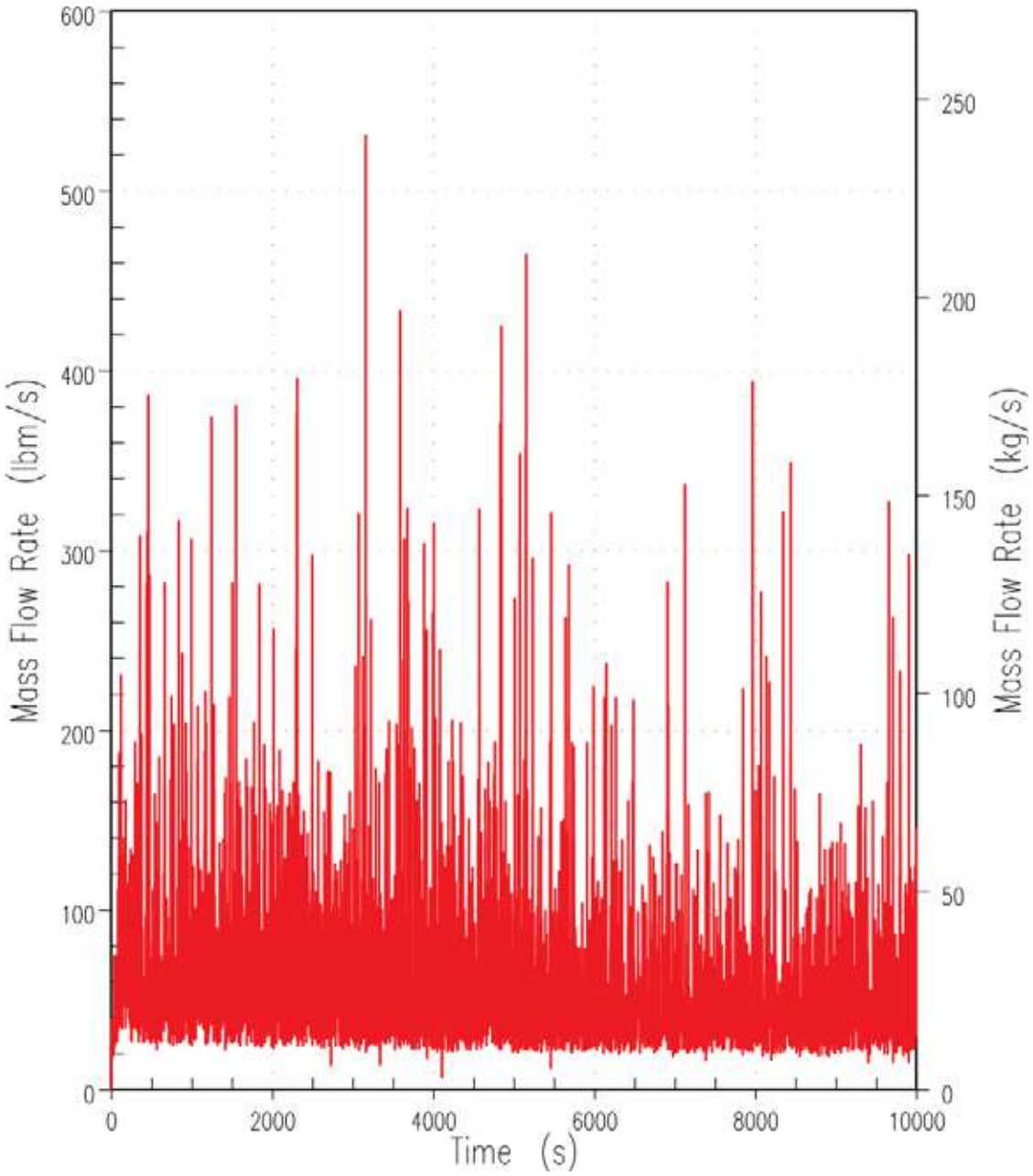


Figure 9.6.6-9. Mixture Flow Rate Through ADS Stage 4A Valves (DEDVI Case)

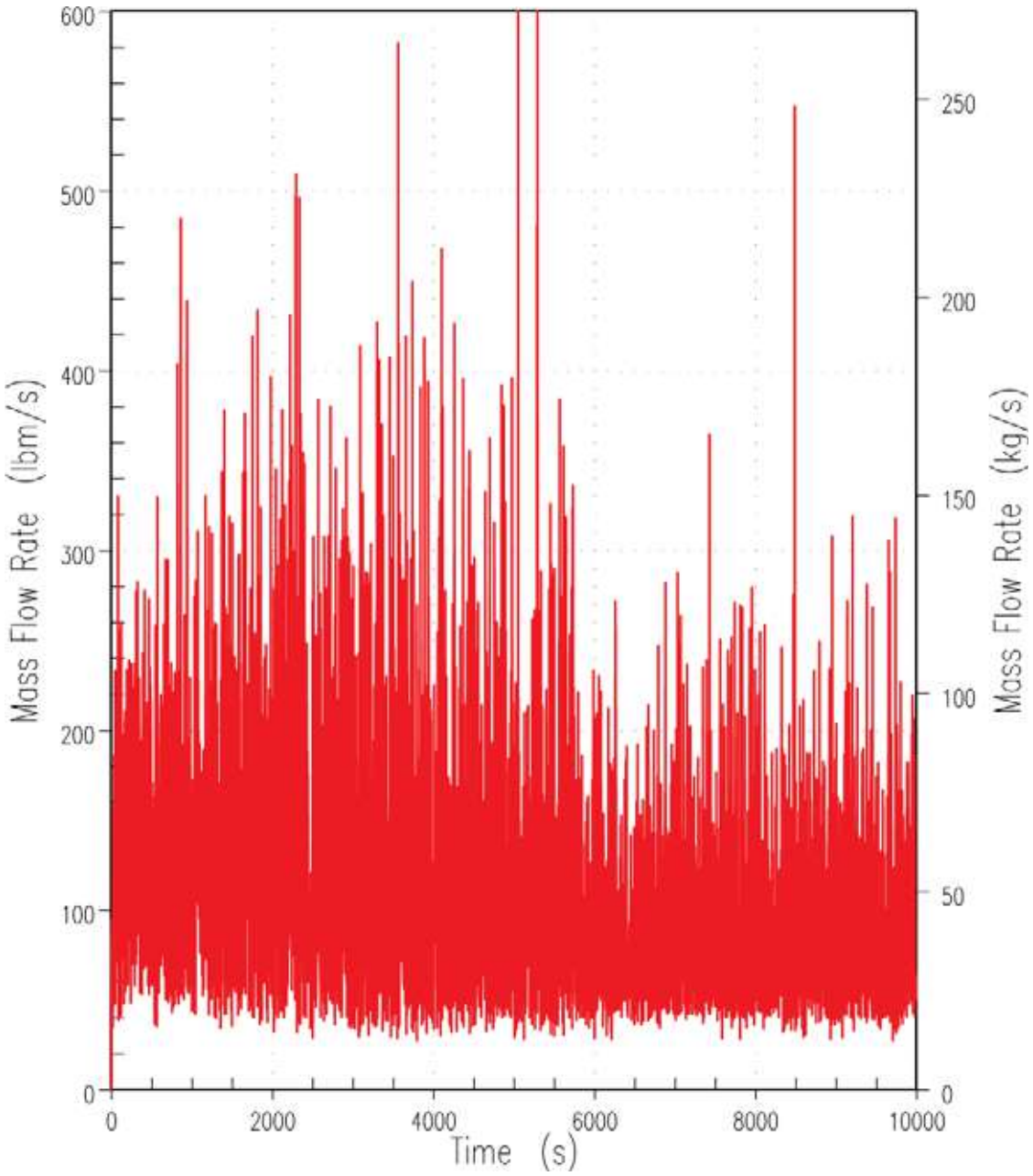


Figure 9.6.6-10. Mixture Flow Rate Through ADS Stage 4B Valves (DEDVI Case)

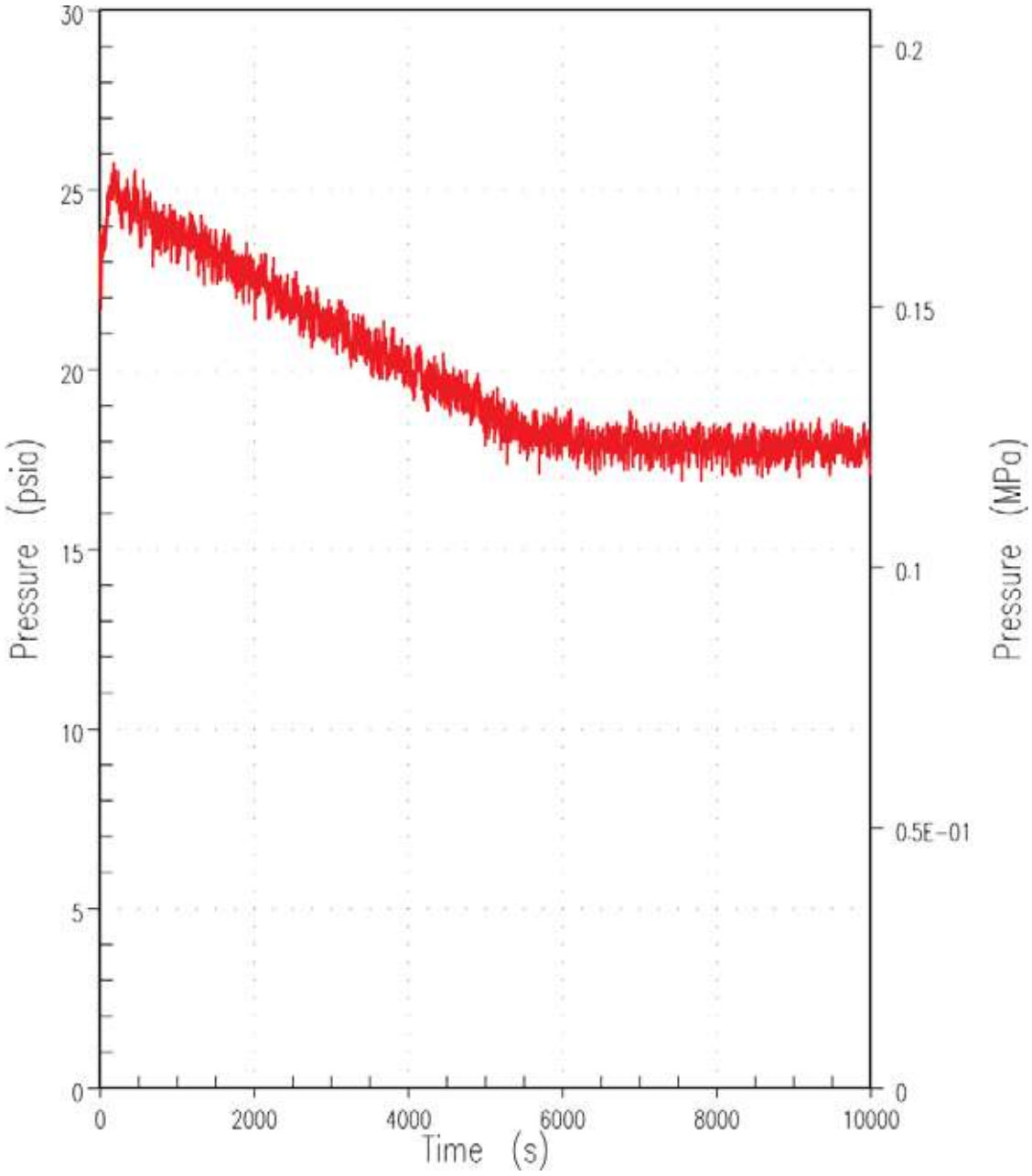


Figure 9.6.6-11. Upper Plenum Pressure (DEDVI Case)

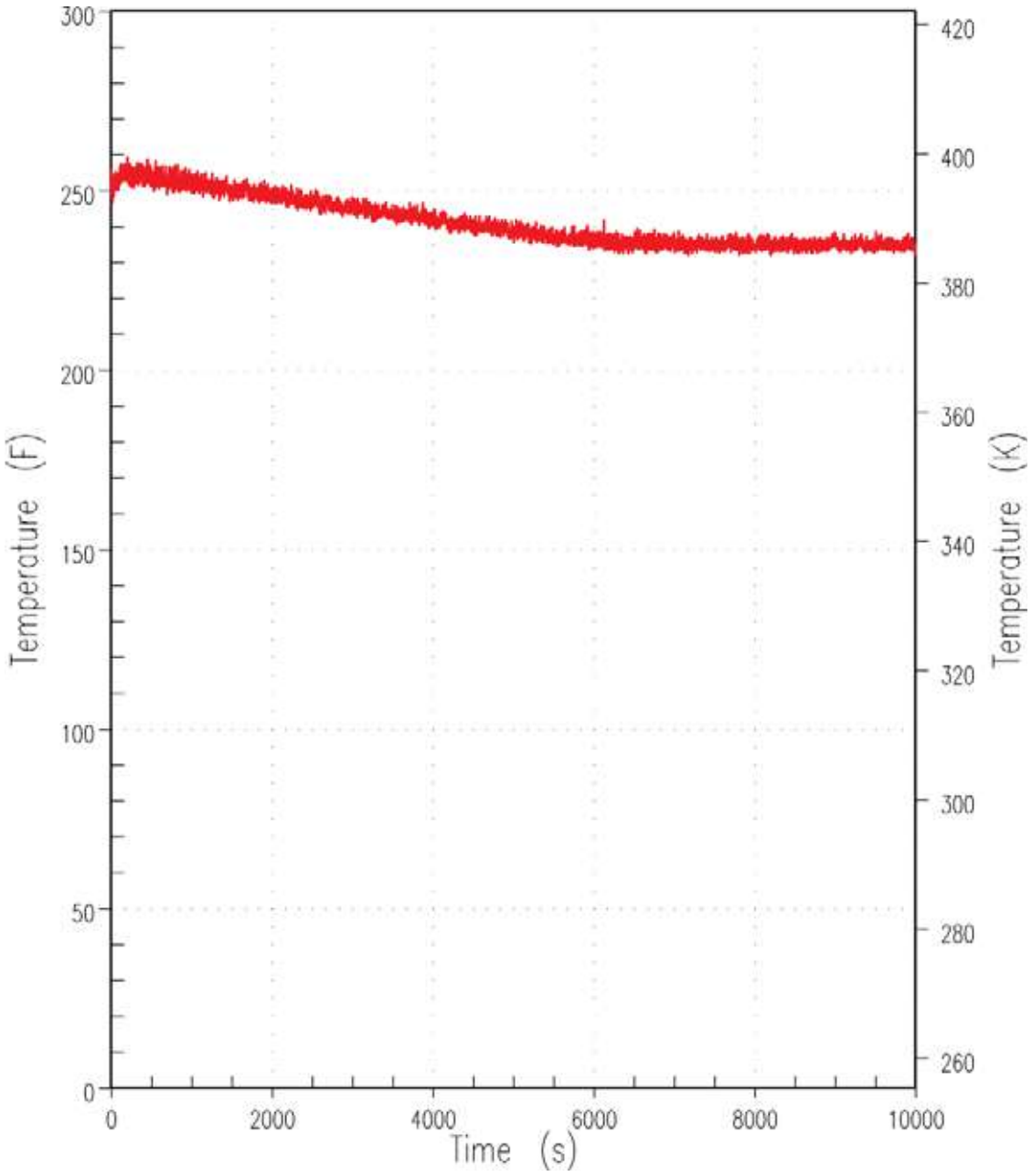


Figure 9.6.6-12. Peak Cladding Temperature (DEDVI Case)

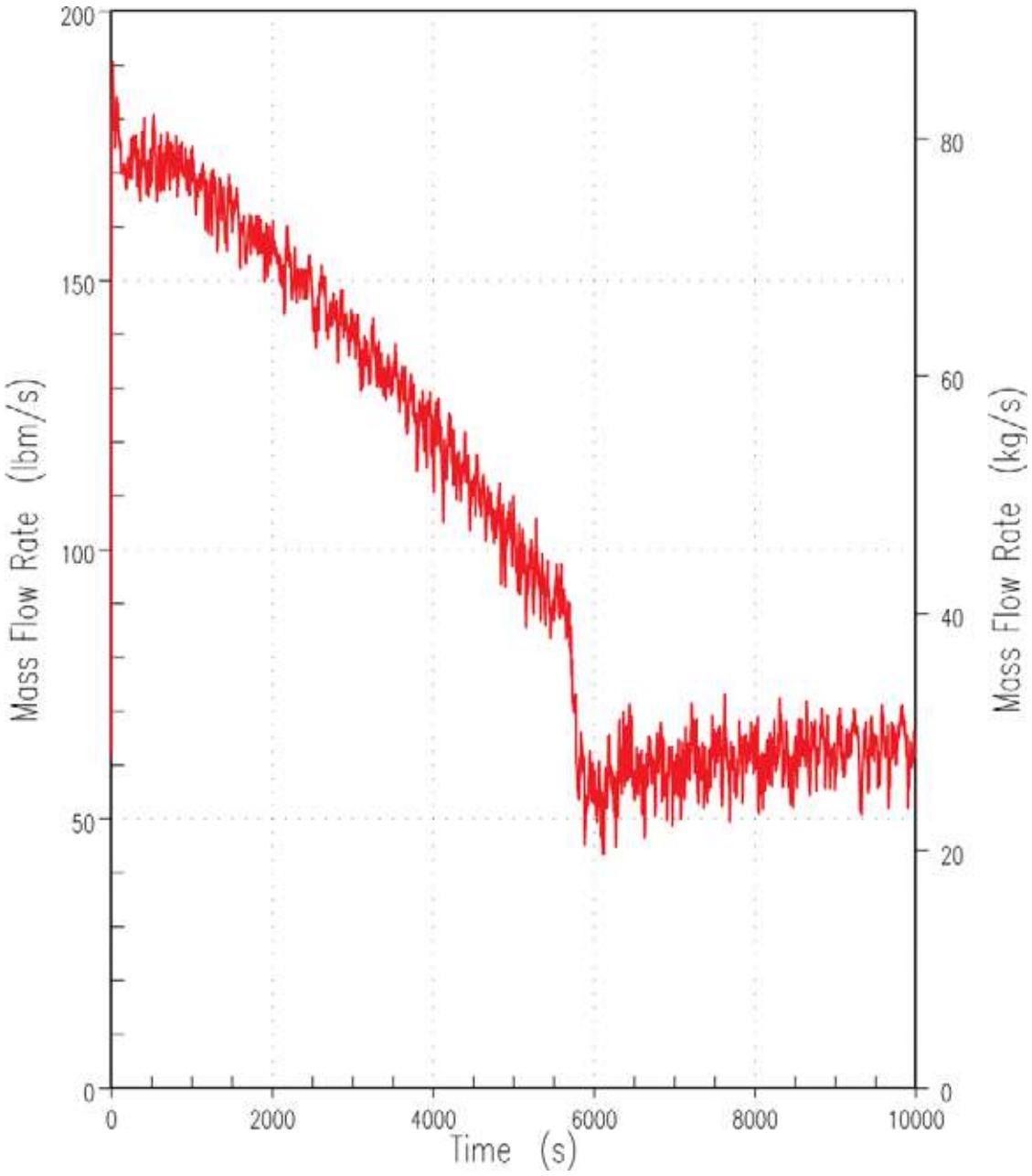


Figure 9.6.6-13. DVI–A Mixture Flow Rate (DEDVI Case)

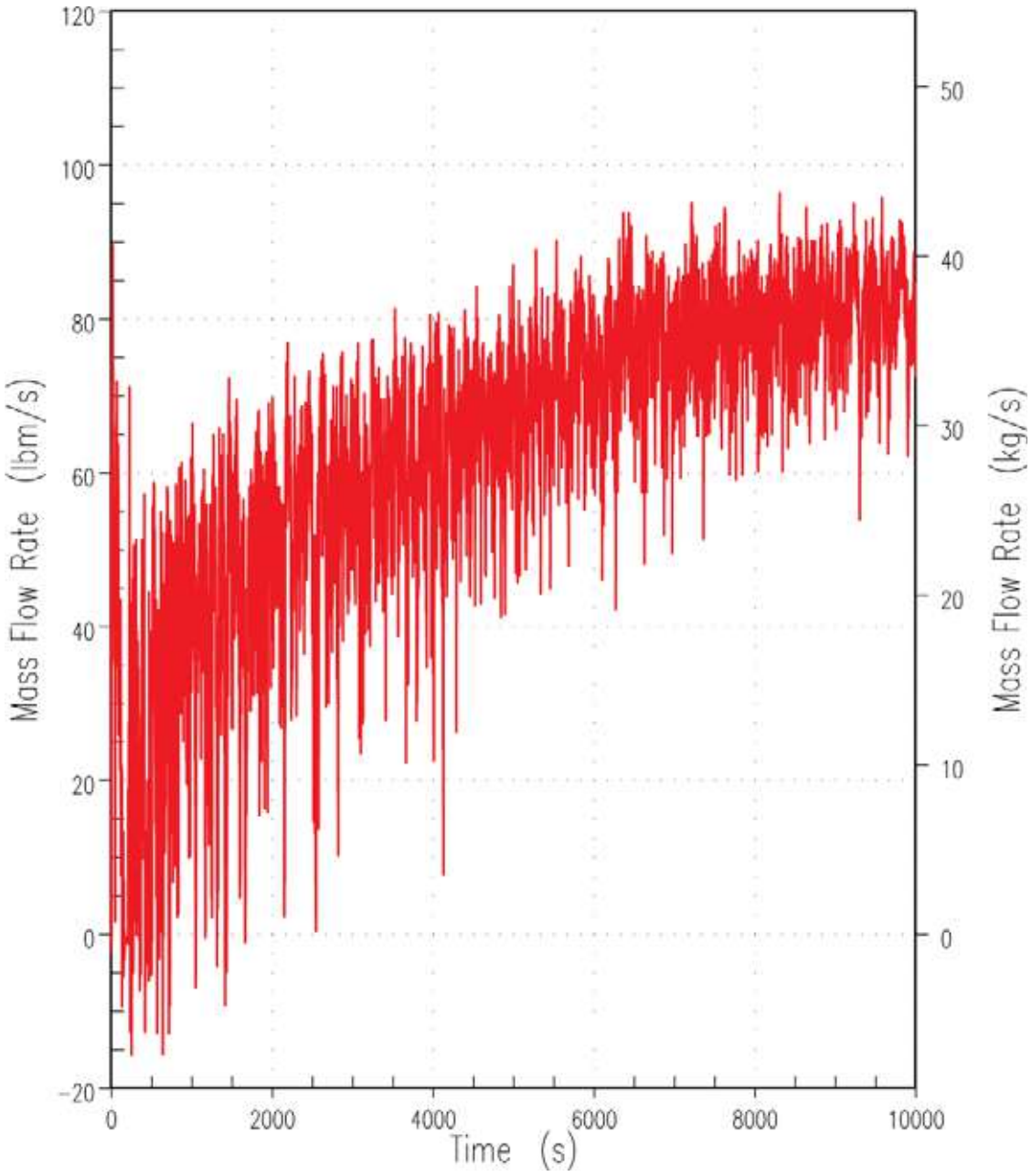


Figure 9.6.6-14. DVI–B Mixture Flow Rate (DEDVI Case)

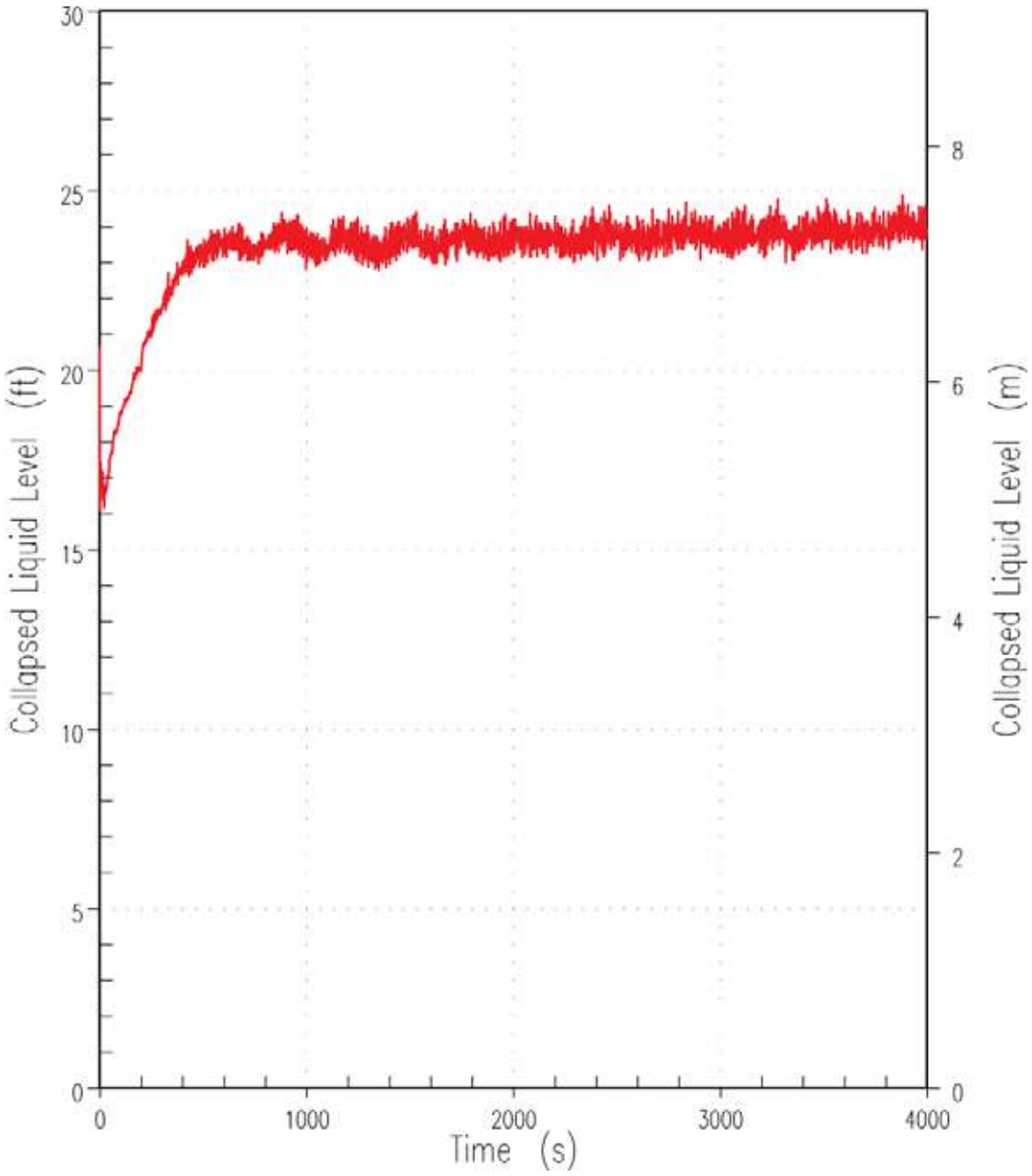


Figure 9.6.6-15. Collapsed Level of Liquid in the Downcomer (Wall-to-Wall Floodup Case) – 0.101 MPa (14.7 psia)

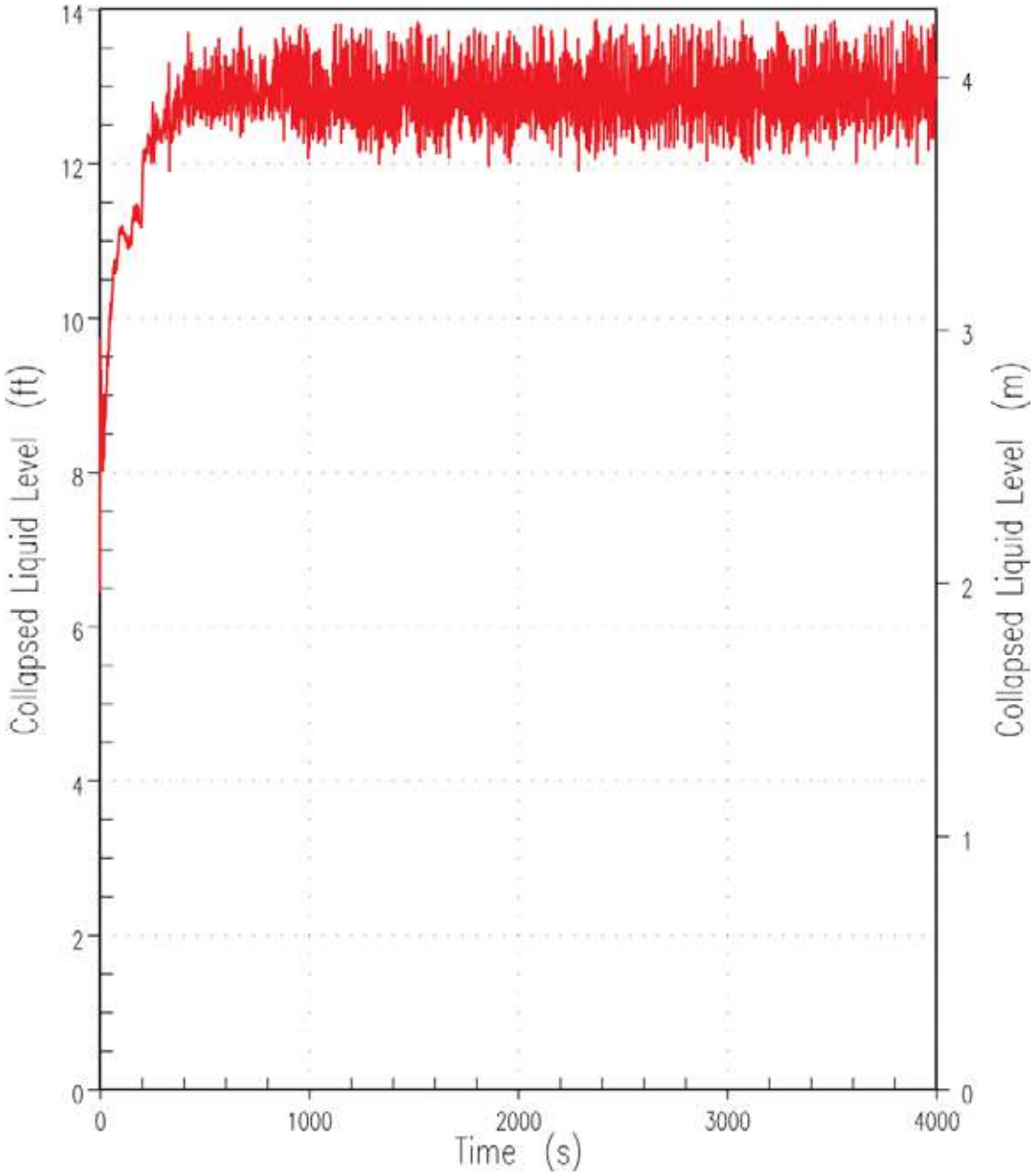


Figure 9.6.6-16. Collapsed Level of Liquid Over the Heated Length of the Fuel (Wall-to-Wall Floodup Case) – 0.101 MPa (14.7 psia)

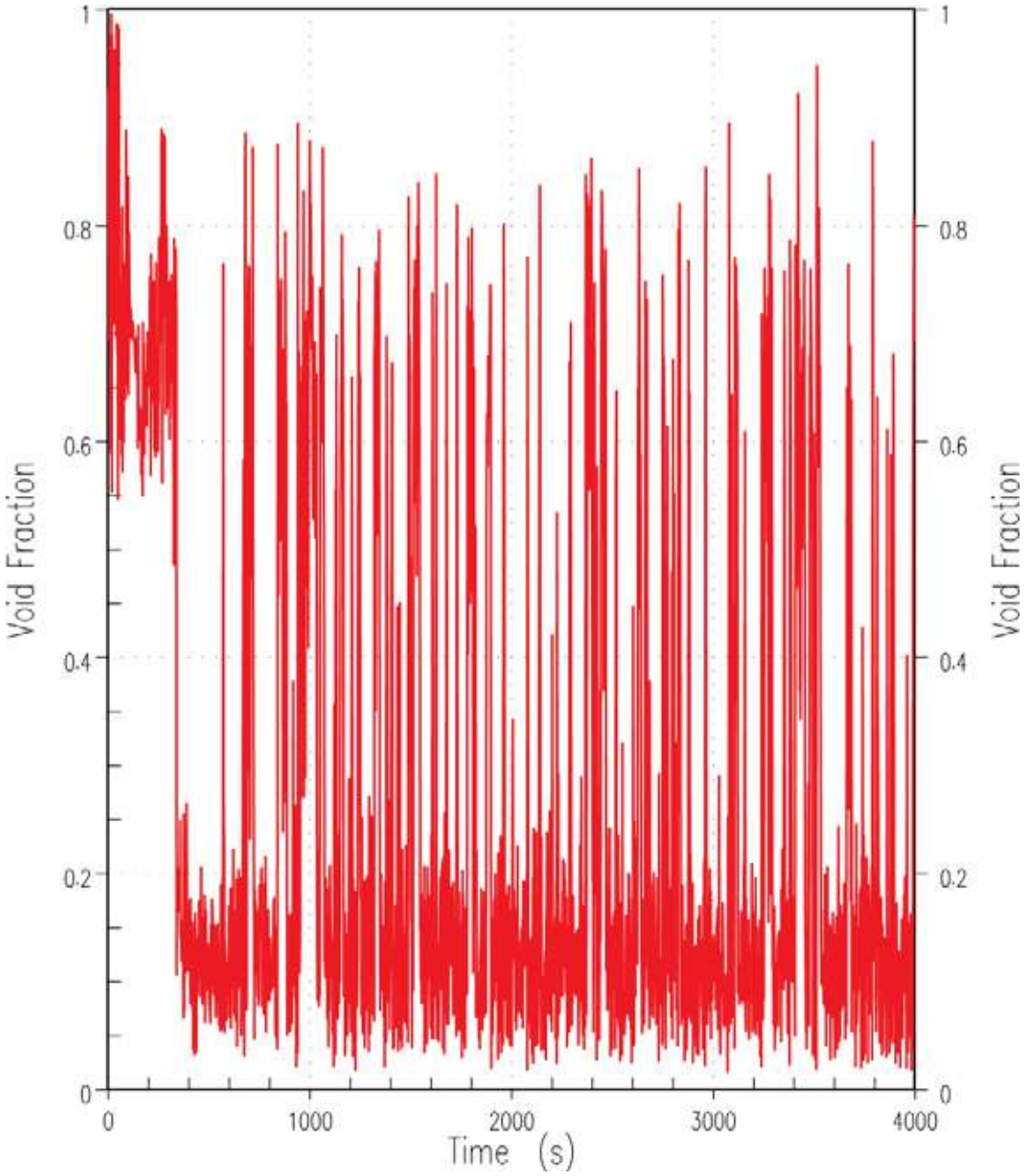


Figure 9.6.6-17. Void Fraction in Core Hot Assembly Top Cell (Wall-to-Wall Floodup Case) – 0.101 MPa (14.7 psia)

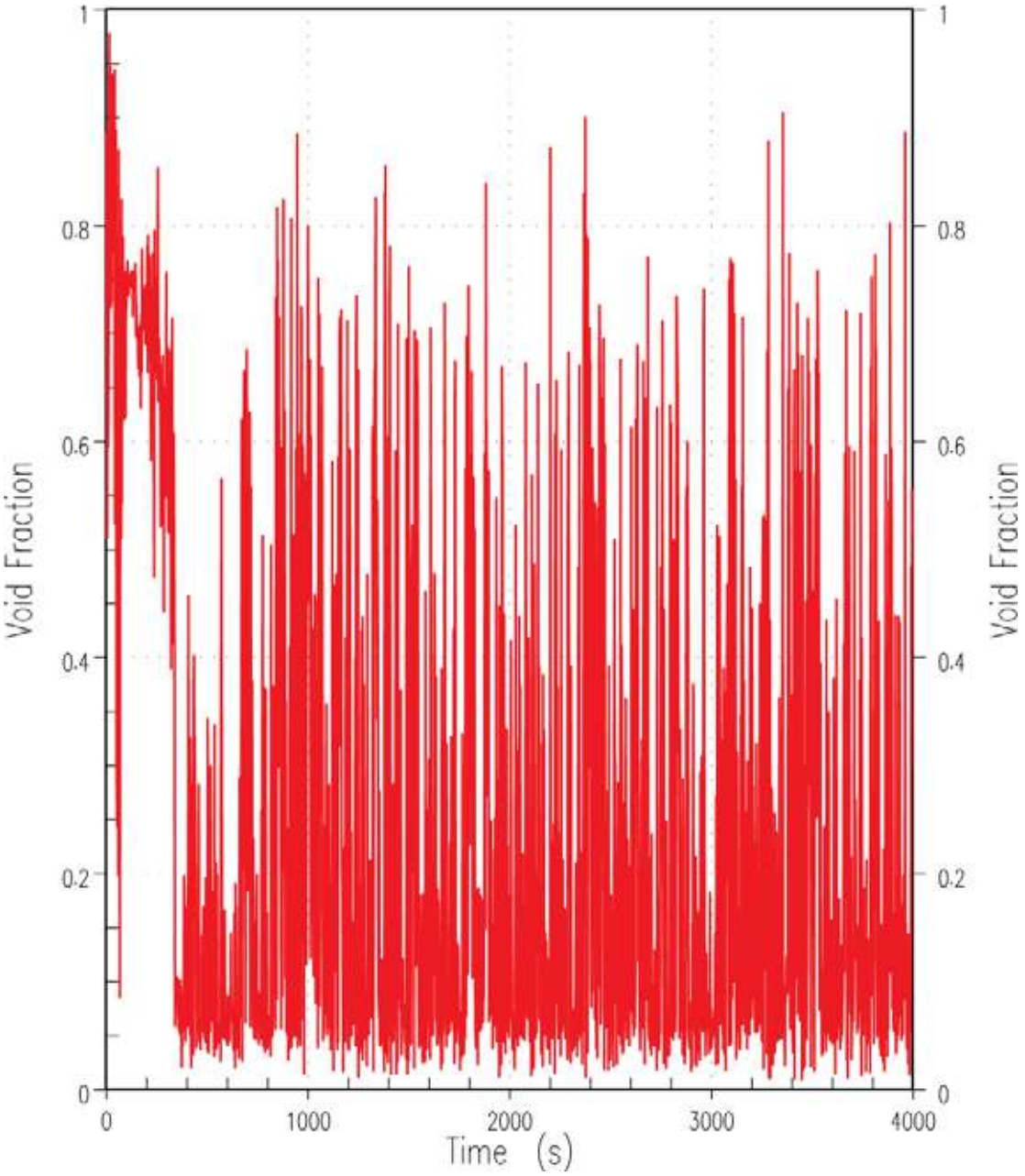


Figure 9.6.6-18. Void Fraction in Core Hot Assembly Second from Top Cell (Wall-to-Wall Floodup Case) – 0.101 MPa (14.7 psia)

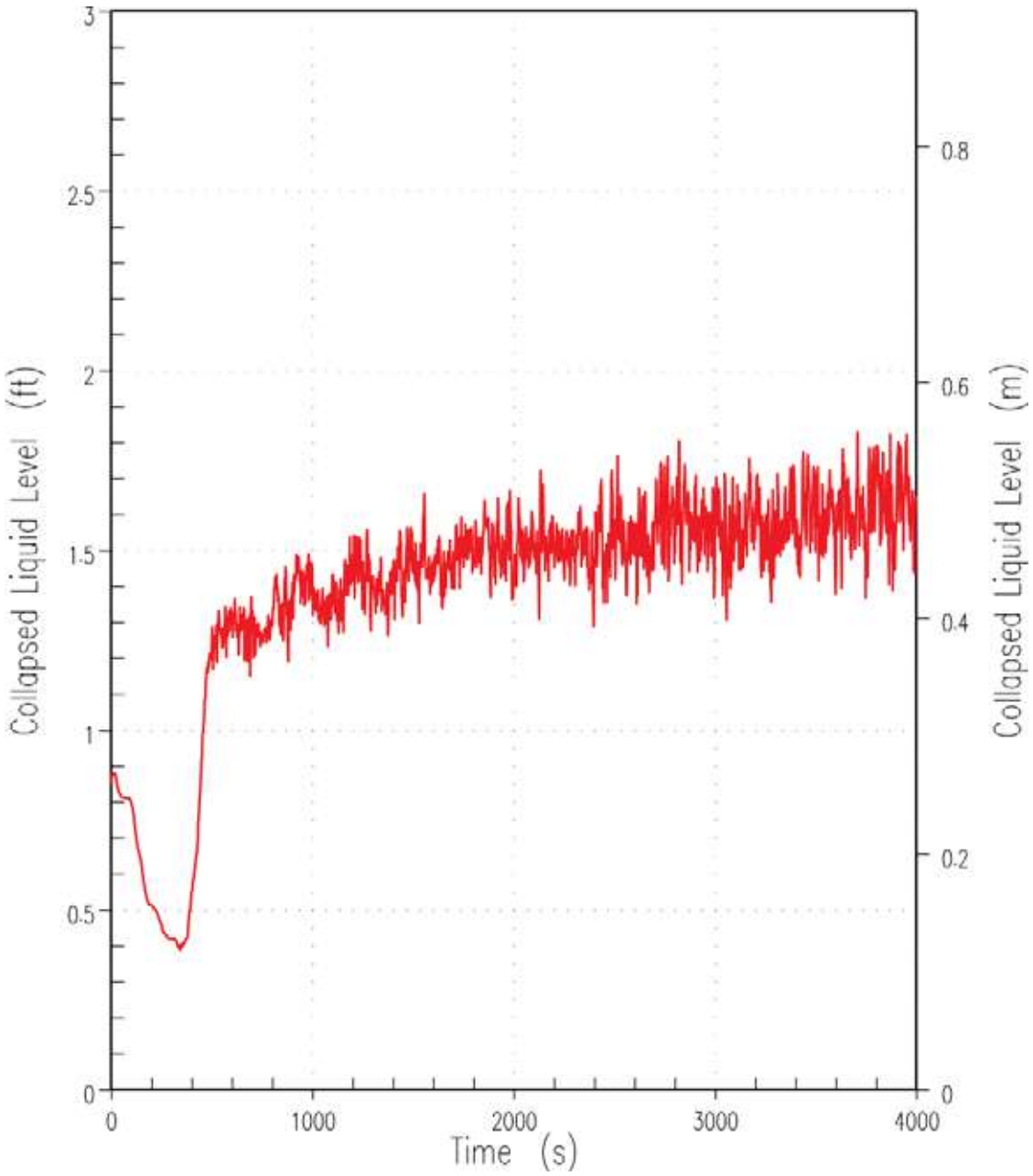


Figure 9.6.6-19. Collapsed Liquid Level in the Hot Leg of Pressuriser Loop (Wall-to-Wall Floodup Case) – 0.101 MPa (14.7 psia)

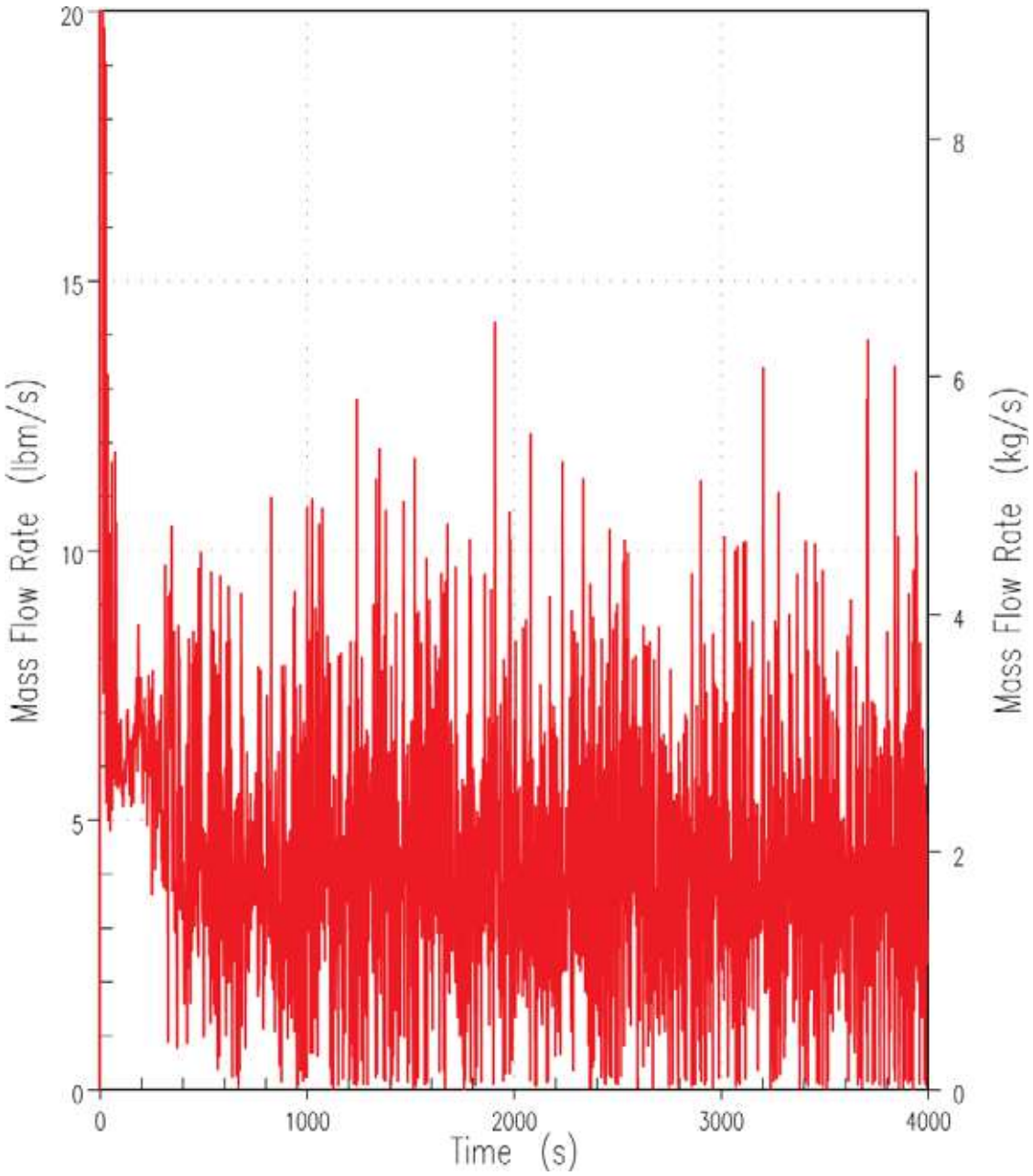


Figure 9.6.6-20. Vapour Rate out of the Core (Wall-to-Wall Floodup Case) – 0.101 MPa (14.7 psia)

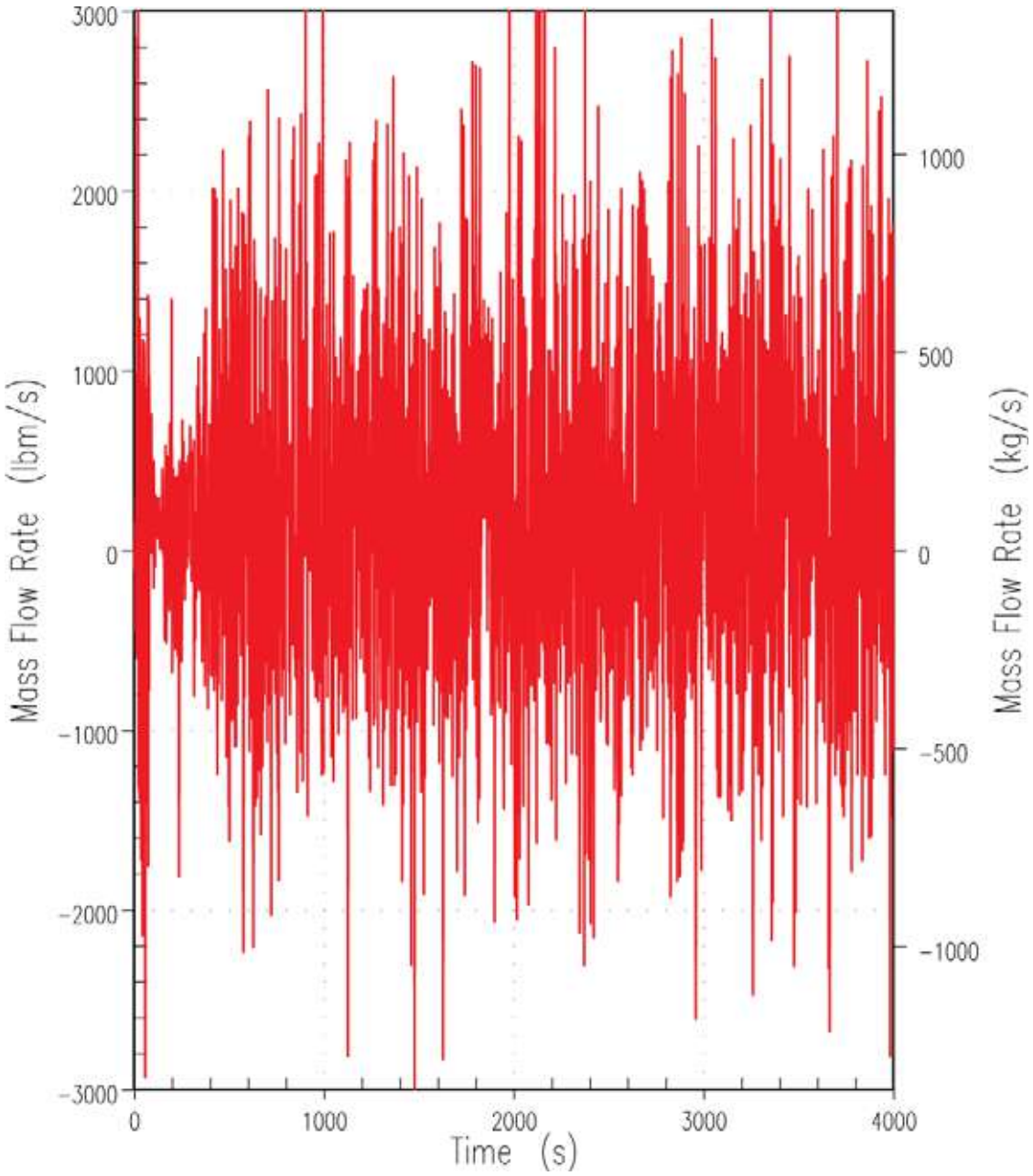


Figure 9.6.6-21. Liquid Flow Rate out of the Core (Wall-to-Wall Floodup Case) – 0.101 MPa (14.7 psia)

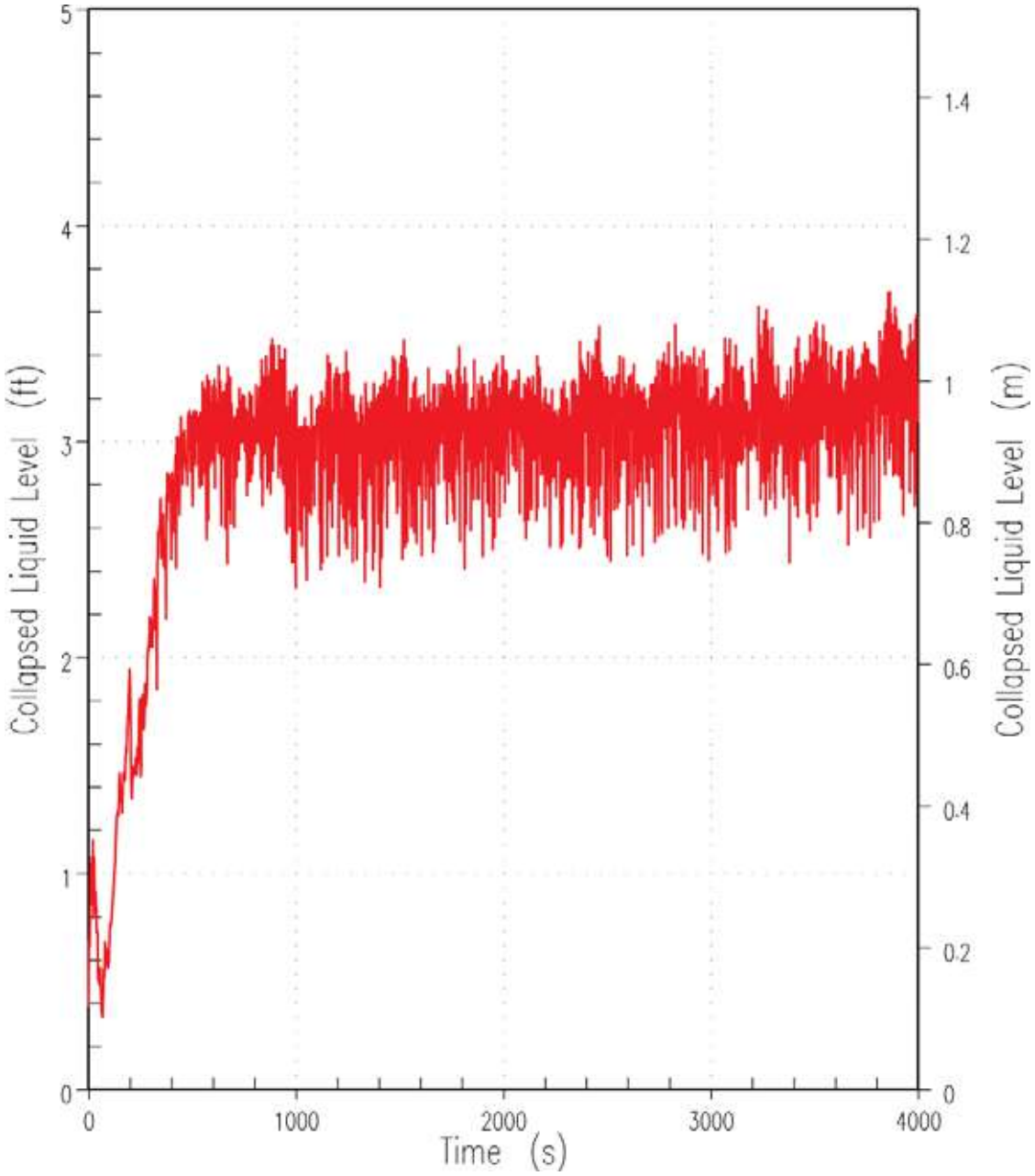


Figure 9.6.6-22. Collapsed Liquid Level in the Upper Plenum (Wall-to-Wall Floodup Case) – 0.101 MPa (14.7 psia)

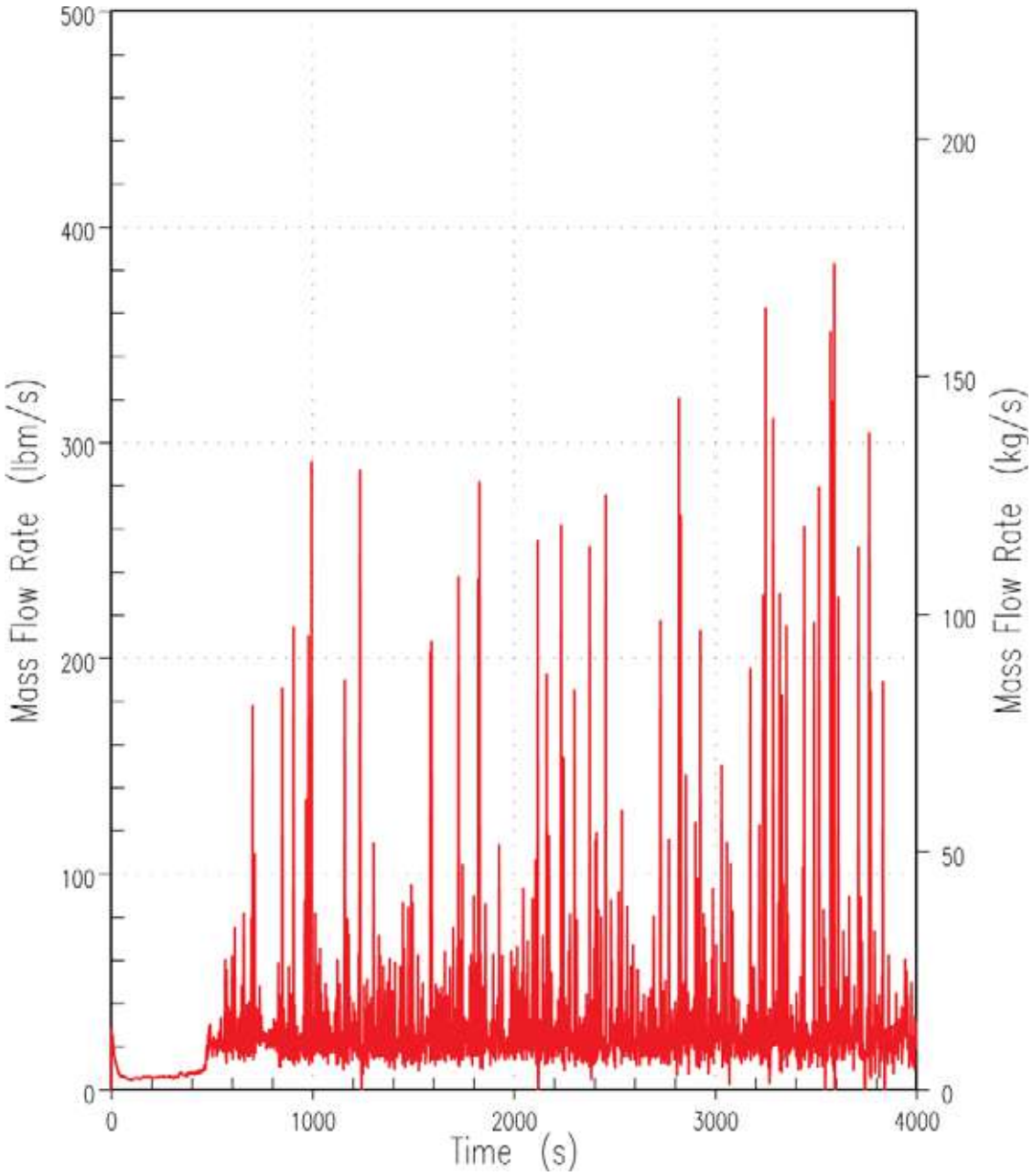


Figure 9.6.6-23. Mixture Flow Rate Through ADS Stage 4A Valves (Wall-to-Wall Floodup Case) – 0.101 MPa (14.7 psia)

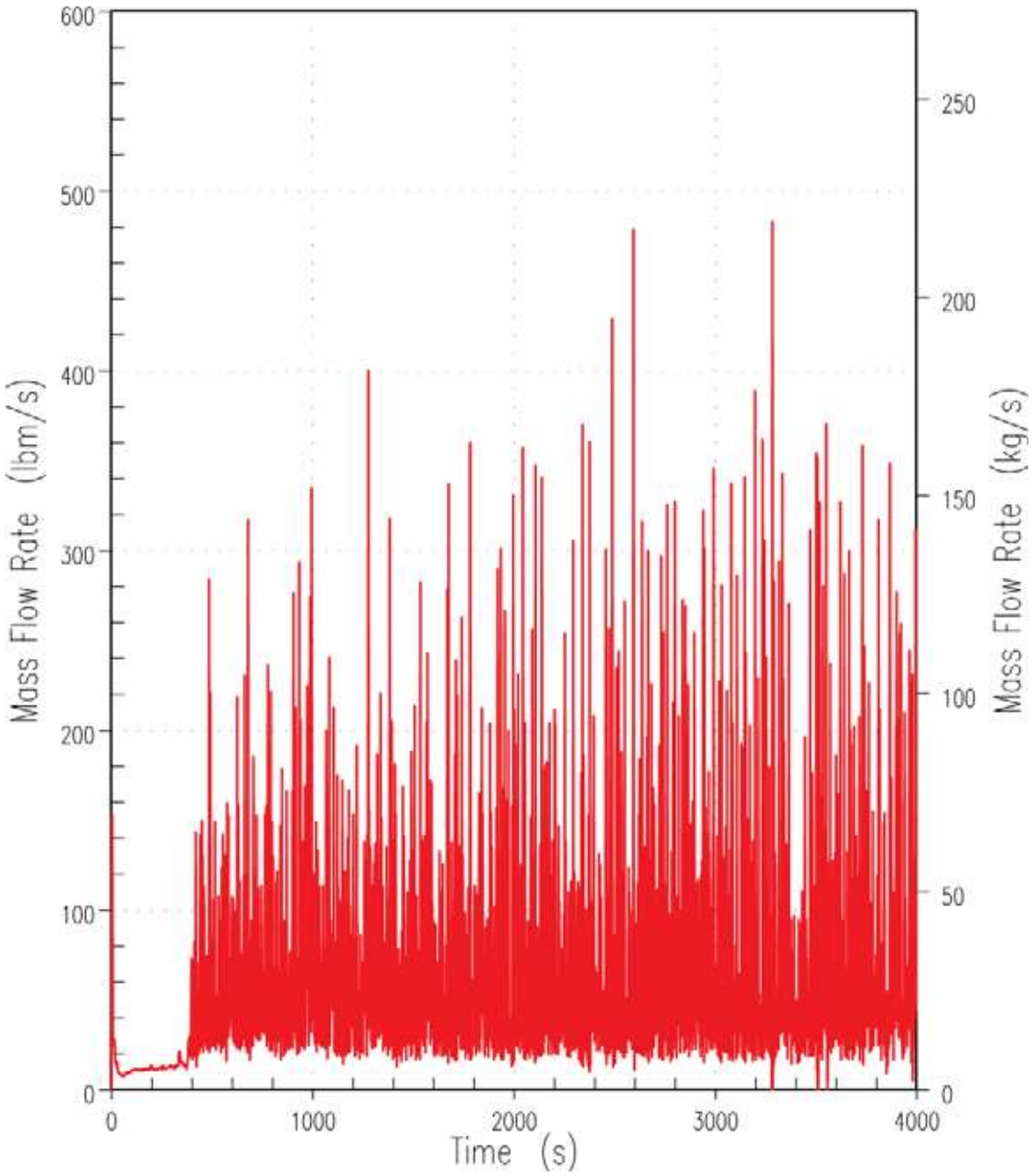


Figure 9.6.6-24. Mixture Flow Rate Through ADS Stage 4B Valves (Wall-to-Wall Floodup Case) – 0.101 MPa (14.7 psia)

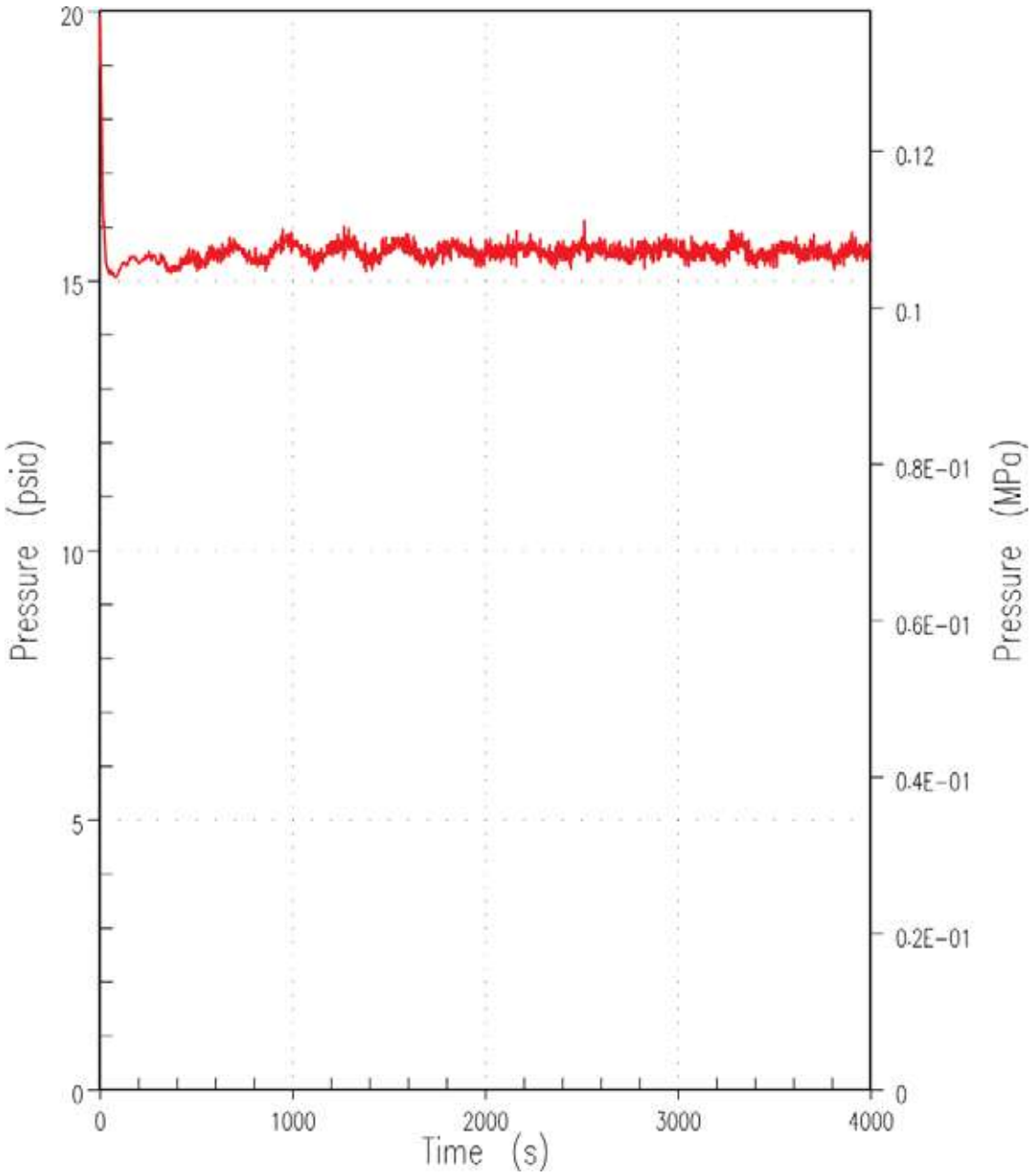


Figure 9.6.6-25. Upper Plenum Pressure (Wall-to-Wall Floodup Case) – 0.101 MPa (14.7 psia)

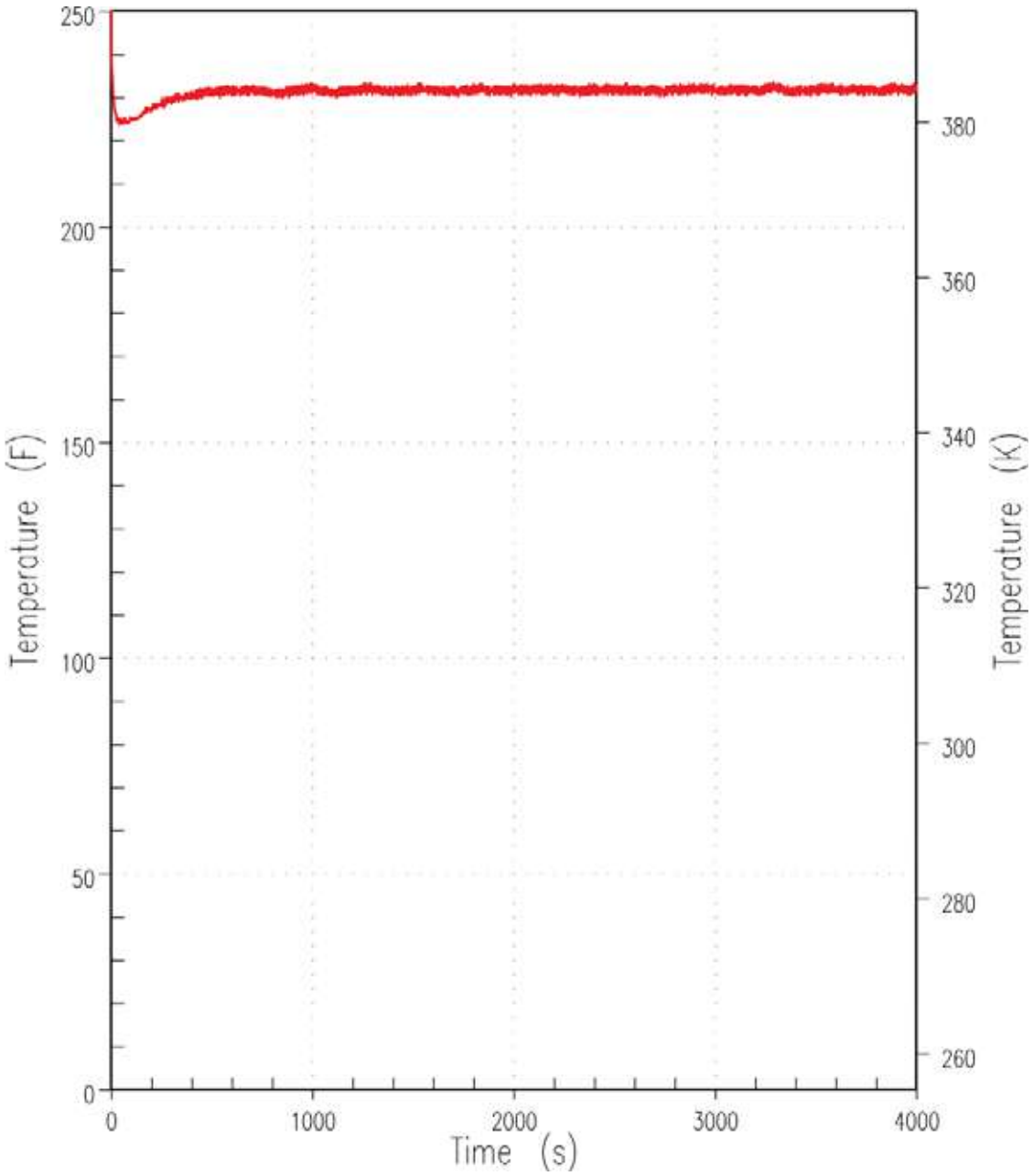


Figure 9.6.6-26. Hot Rod Cladding Temperature Near Top of Core (Wall-to-.Wall Floodup Case) – 0.101 MPa (14.7 psia)

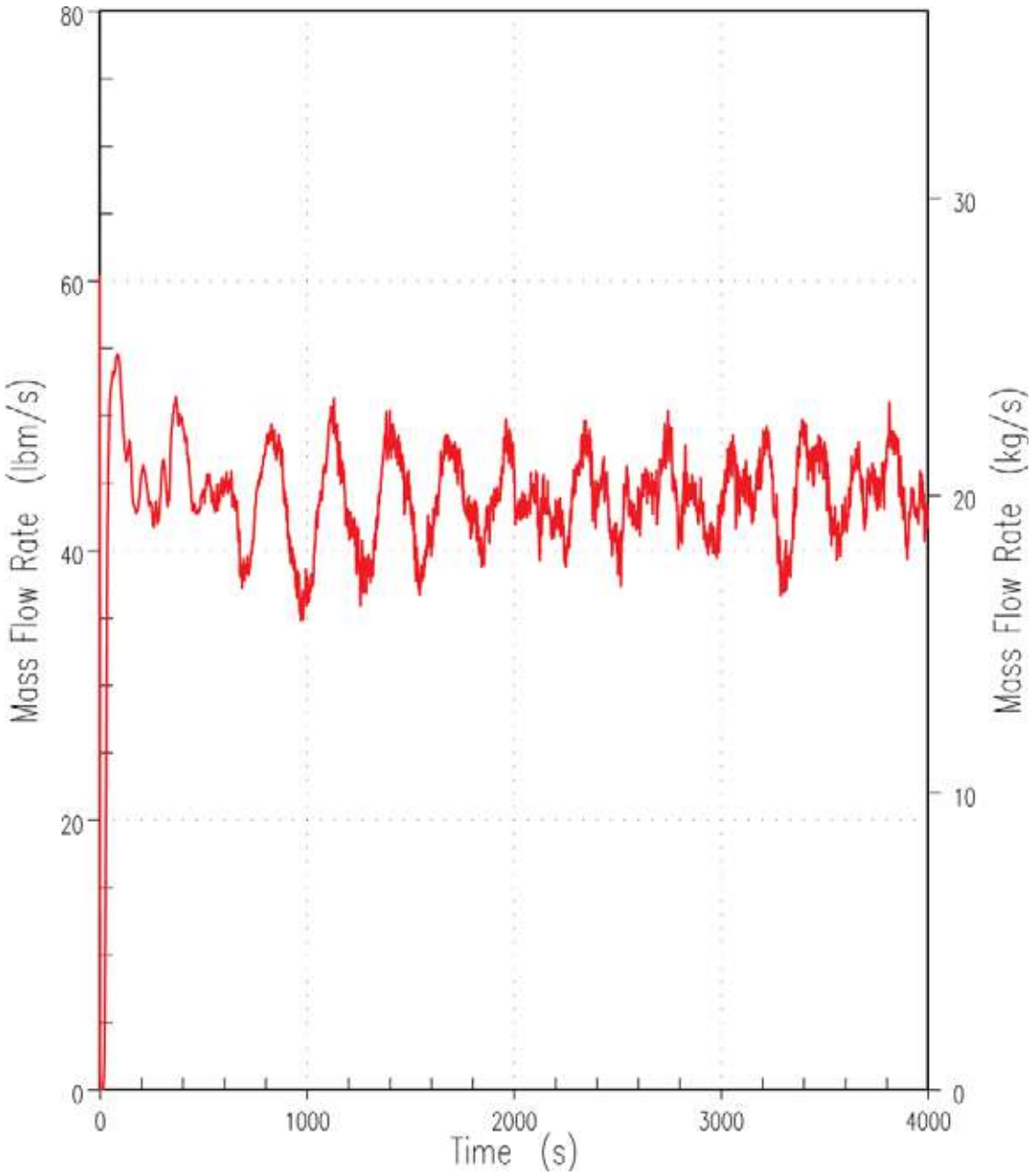


Figure 9.6.6-27. DVI-A Mixture Flow Rate (Wall-to-Wall Floodup Case) – 0.101 MPa (14.7 psia)

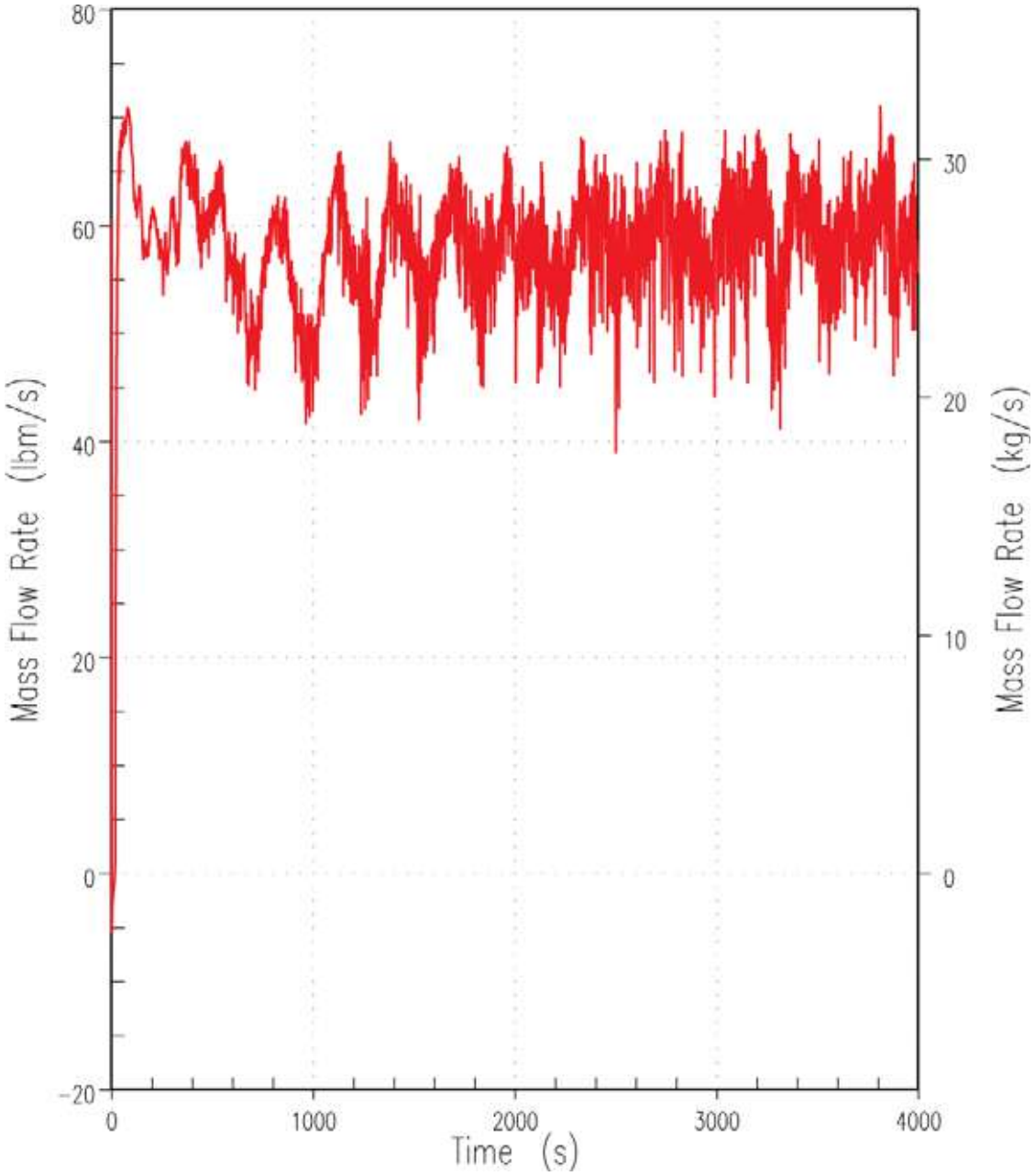


Figure 9.6.6-28. DVI-B Mixture Flow Rate (Wall-to-Wall Floodup Case) – 0.101 MPa (14.7 psia)

9.7 Spent Fuel Pool Fault Groups

9.7.1 Criticality Faults during Refuelling, Fuel Handling, and Fuel Storage

9.7.1.1 Introduction and Overview

This section assesses the criticality faults associated with refuelling, fuel handling, and fuel storage (faults 2.4.5 and 3.2.1-3.2.4 – see Appendix 8A).

9.7.1.1.1 Refuelling – Normal Operations

Refuelling is achieved by removing the integrated head package (IHP) from the RPV so that the fuel assemblies can be accessed. The reactor is deemed to be in the refuelling mode (Mode 6) once any of the head bolts are less than fully tensioned.

Both RNS pumps and heat exchangers remain operating during refuelling. As decay heat decreases and as fuel is moved to the SFP, one residual heat removal pump and heat exchanger may be taken out of service. However, the valves remain aligned should the need arise to start this pump quickly in case of a failure of the operating residual heat removal pump.

Then the refuelling cavity is flooded with borated water from the IRWST. The reactor upper internals are then removed and placed on a stand in the refuelling cavity. Fuel may now be removed from the core.

The fuel handling equipment is designed to handle the spent fuel assemblies underwater from the time they leave the reactor vessel until they are placed in a container for shipment from the site. Underwater transfer of spent fuel assemblies provides an effective and transparent radiation shield, as well as a reliable cooling medium for removal of decay heat. Boric acid in the water is a defence in depth measure to preclude criticality.

The refuelling cavity and the fuel storage area are connected by the fuel transfer tube which is fitted with a quick opening hatch on the canal end and a valve on the fuel storage area end and kept full of borated water at all times during fuel movement. The hatch is in place except during refuelling to provide containment integrity. The hatch or valve can be used to provide isolation during a refuelling outage. Fuel is carried through the tube on an underwater transfer car.

Fuel is moved between the RPV and the fuel transfer system by the refuelling machine. The fuel transfer system is used to move a fuel assembly and its associated core component between the containment building and the auxiliary building fuel handling area. After a fuel assembly is placed in the fuel container in the fuel transfer system, the lifting arm pivots the fuel assembly to the horizontal position for passage through the fuel transfer tube. After the transfer car transports the fuel assembly through the transfer tube, the lifting arm at that end of the tube pivots the assembly to a vertical position so that the assembly can be lifted out of the fuel container and placed in the spent fuel racks.

Fuel (both new and used) is moved back into the core using the reverse procedure to that for removing spent fuel from the core. Fuel is introduced into the refuelling cavity via the fuel transfer system and placed in the specified location in the core by the refuelling machine.

9.7.1.1.2 Fuel Storage – Normal Operation

The new and spent fuel storage areas are accessible to operating personnel.

New fuel assemblies received for refuelling are removed one at a time from the shipping container and moved into the new fuel assembly inspection area. After inspection, the accepted new fuel assemblies are stored dry in the new fuel storage rack. The rack is designed to store 72 fuel assemblies of the maximum design basis enrichment, and includes integral neutron absorbing material to maintain the required degree of sub-criticality. For the initial core load, some new fuel assemblies may be stored in the SFP. During fuel loading, new fuel is moved via the SFP to the reactor.

The SFP provides storage space, heat removal and shielding for spent fuel. The pool, which is constructed of reinforced concrete and concrete filled structural modules, is approximately 12.95 m (42.5 ft) deep and contains borated water with a nominal boron concentration of 2700 ppm. It has storage locations for 10 years of spent fuel storage, including 5 locations for damaged/defective fuel.

Spent fuel storage cells are composed of stainless steel boxes separated by a water gap, with fixed neutron absorber panels centred on each side. The steel walls define the storage cells, and stainless steel sheathing supports the neutron absorber panel and defines the boundary of the flux-trap water-gaps used to augment reactivity control. Stainless steel channels connect the storage cells in a rigid structure and define the flux-trap between the neutron absorber panels. Neutron absorber panels are installed on all exterior walls where a fuel assembly could be mislocated. For those areas where there is insufficient space to misplace a fuel assembly between the rack and the spent fuel pool wall, no neutron absorber is present. Radial neutron leakage compensates for the lack of exterior neutron absorber in these areas.

There are five locations to store defective fuel assemblies which are separated from each other by a water gap, similar to the rack design for normal storage locations. Additionally, they are separated from the surrounding storage cells by a large water gap. Therefore two neutron absorber panels separate the fuel assemblies in the defective storage locations from any other fuel assembly.

The full capacity of the pool is more than sufficient to hold an entire core off-load of 157 fuel assemblies.

In addition to the integral neutron absorbing material to preclude criticality the SFP contains soluble boron at a concentration controlled by Technical Specification limits (minimum 2300 ppm). This increases the margin to criticality.

9.7.1.1.3 Fuel Handling- Normal Operation

In the fuel handling area, fuel assemblies are moved about by the fuel handling machine, which is a gantry-style crane equipped with two hoists, one of which is used for lifting new fuel, the other for spent fuel. Initially, a short tool is used to handle new fuel assemblies, but the new fuel elevator must be used to lower the assembly to a depth at which the fuel handling machine can place the new fuel assemblies into or out of the spent fuel storage racks.

The fuel handling machine is used to handle new fuel assemblies in the rail car bay, new fuel rack, and new fuel elevator. The capacity of the fuel handling machine, while over the new fuel storage rack, is limited to lifting a fuel assembly, control rod assembly, and handling

tool. The new fuel storage rack is not accessed by the cask handling crane. This precludes the movement of loads greater than fuel components over stored new fuel assemblies.

During fuel handling operations, a ventilation system removes gaseous radioactivity from the atmosphere above the new fuel pit and SFP.

Spent fuel assemblies are lifted using a long (approximately 11 m (36.1 ft)) spent fuel handling tool, which ensures an adequate depth of water is maintained for radiation shielding.

The following procedure briefly outlines the typical steps of the operation to transfer spent fuel assemblies from the SFP to a shipping cask. It assumes that the cask loading pit has been previously filled with water and that the gate between the cask loading pit and the SFP has been opened:

- The transfer cask containing a clean, empty spent fuel canister is brought into the cask washdown pit. The spent fuel canister is removed as necessary and prepared for cask loading.

- The transfer cask/spent fuel canister are placed into the cask loading pit.

- The fuel handling machine is positioned over the specific fuel assembly to be shipped out of the spent fuel storage rack. The fuel assembly is picked up and transported into the cask loading pit. During the transfer process the fuel assembly is always maintained with the top of the active fuel at least 2.67 m (8.8 ft) below the water surface, to ensure adequate shielding from direct radiation.

- Once the fuel transfer process is complete, the lid is placed on top of the cask to provide the required shielding.

- The cask is then moved to the washdown pit and cleaned with demineralised water. Decontamination procedures can be started at this time.

- When the spent fuel canister closure and drying processes are complete, the transfer cask is prepared for transfer into a storage or shipping container as applicable.

The cask is lifted using the cask handling crane, which is a bridge crane mounted on two runway rails. It is typically used only when fuel movement activities associated with refuelling the reactor are not in progress. The cask handling crane's path is designed such that the cask cannot pass over the spent fuel pool, new fuel pit, or fuel transfer canal. This precludes the movement of loads greater than fuel components over stored fuel. For the unlikely event of a dropped cask on to a hard surface, consideration of integrity of fuel in the cask and consequences for criticality will be addressed in the cask safety case.

9.7.1.2 Fault Assessment

The faults are considered in two groups: those within the reactor containment and those outside the containment (i.e., in the auxiliary building). Note that the criticality safety of fuel in a new fuel cask or in a spent fuel cask (including dropped load events) will be demonstrated in the safety case for the relevant cask.

The following faults have the potential to present a criticality hazard during refuelling or fuel handling operations within the reactor containment:

Fault 2.4.1, Uncontrolled Rod Cluster Control Assembly Bank Withdrawal During Refuelling

When fuel assemblies are in the pressure vessel and the vessel head is not in place, k_{eff} will be maintained at or below 0.95 with control rods and soluble boron. Further, the fuel will be maintained sufficiently sub-critical that removal of the rod cluster control assembly bank will not result in criticality. The COLR will define the soluble boron concentration required to maintain the shutdown margin.

Fault 2.4.2, Inadvertent Loading of a Fuel Assembly in an Improper Position in Core During Refuelling

During refuelling, the boron concentration in the reactor is kept at such a level that fuel of any burnup can occupy its intended position in the core without challenging the criticality safety limits ($k_{eff} < 0.95$). If fuel were placed in an improper position in the core, it is expected that this would be noticed from monitoring the Inverse Count Rate Ratio derived from the source range detectors during fuel loading, especially if the margin to criticality were significantly reduced (k_{eff} approaching 1.0). If fuel assemblies of similar reactivity were interchanged so that it was not noticed during loading, this might create operational difficulties (e.g., with core power distribution) but there would be no safety issue. It is shown below that, for a reactor operating at power, a fuel misloading fault (Fault 3.1) is bounded by uncontrolled withdrawal of a single RCCA (discussed in Section 9.5).

Fault 2.4.3, Loss or Reduction of Boration in Refuelling Cavity due to:

- **Faulty boron concentration measurement**
- **Uncontrolled dilution/addition of unborated water (e.g., from Fire Protection System (FPS))**

Loss or reduction of boration would reduce the margin to criticality but would not cause a criticality event. In the refuelling cavity, fuel is only moved one assembly at a time in transit to the SFP; or stored in the in-containment fuel storage rack which is a 1x6 array of storage cells. Each storage location is surrounded by neutron-absorbing panels. A criticality assessment of the in-containment rack (Reference 9.7-14) shows that, when loaded with six new fuel assemblies in unborated water, the neutron multiplication factor (including biases and uncertainties) is $k_{eff} = 0.88$, i.e., it would be sub-critical with a large margin of safety below the criterion for safe operation under normal conditions ($k_{eff} < 0.95$).

The assessment referred to above (Reference 9.7-14) also includes a calculation for a single isolated fresh fuel assembly outside of the in-containment rack, in unborated water, and shows that $k_{eff} < 0.95$ for this case also. It is fully reflected but assumes no neutronic interaction with other fissile material. To ensure neutronic isolation, the in-containment storage rack has at least 254 mm (10 inches) of water separation from the sides of the rack. The design of the in-containment storage rack ensures this.

Therefore, a complete loss of boron in the refuelling cavity would not result in a criticality event.

Fault 2.4.4, Loss of Configuration of Reactor Core due to Dropped Loads (Including Integrated Head Package, or Upper Core Internals)

The heavy loads such as the vessel head would not fit inside the open reactor vessel and so could only damage at most the upper part of the fuel. The radiological consequences of this

event are dealt with as part of a separate fault group (Appendix 8A – dropped loads). Regarding the risk of criticality, all such scenarios are considered to be bounded by a dropped load onto the fuel assemblies in the SFP.

Fault 2.4.5, Dropped Fuel Assembly (Spent or New) Onto, or Into Reactor Core

The risk of a dropped fuel assembly onto the reactor core is dealt with as part of a separate fault group (dropped loads). Regarding the risk of criticality, all such scenarios are considered to be bounded by a dropped fuel assembly in the SFP, where there are potentially many more fuel assemblies stored.

Fault 2.4.6, Displacement of Control Rods

As with fault 2.11, the fuel will be maintained sufficiently sub-critical that displacement or complete removal of one or more rod cluster control assemblies will not result in criticality.

The following faults have the potential to present a criticality hazard when handling new or spent fuel outside the reactor containment:

Fault 3.1.8, Flooding of New Fuel with Unborated Water or Oil

- In new fuel assembly inspection area (with concrete reflection)
- In new fuel storage rack (dry buffer store)

The criticality assessment for the new fuel storage rack (Reference 9.7-15) shows that $k_{eff} < 0.95$ when the storage pit is fully flooded with unborated water (for the maximum load of 72 fuel assemblies with 5.0 weight percent U-235, and with full water reflection). Furthermore, if the water density is chosen for optimum moderation conditions, then $k_{eff} < 0.98$ so that the criterion for accident conditions is still met.

For a single fuel assembly in the inspection area flooded or sprayed with water, and with concrete reflection on two sides, the reactivity is expected to be less than for a fully loaded new fuel storage rack covered in water. This fault scenario is therefore screened out from further analysis.

Although oil is more moderating than water, the quantity of oil present in the fuel handling area (e.g., in lifting equipment) is not sufficient to significantly affect the margin to criticality of the new fuel, even if it leaked directly into the pit.

Fault 3.2.1, Loss or reduction of boration in SFP due to:

- Faulty boron concentration measurement
- Uncontrolled dilution/addition of unborated water (e.g., from FPS)

As an all region 1 style of fuel rack does not require the use of soluble boron or burnup credit to maintain criticality safety, the above fault is not a bounding fault.

Reference 9.7-13 calculates the maximum k_{eff} for the spent fuel racks filled with fresh fuel of maximum nominal initial enrichment of 4.95 weight percent U-235 without soluble boron. The results show that the maximum k_{eff} of the racks is less than 0.95 at a 95% probability at a 95% confidence level.

Fault 3.2.2, Loss of Configuration of Fuel in Storage Racks (e.g., Seismic or Dropped Load)

- Dropped fuel assembly lying on top of rack (toppled)
- Vertical misalignment of fuel assembly relative to fixed neutron absorber panels
- Change in rod pitch to a more reactive configuration (possibly outside rack)
- Distortion of rack geometry (e.g., bringing fuel assemblies closer together)
- Displacement of racks closer together, or with more concrete reflection

It is possible to drop a fresh fuel assembly on top of the SFP storage racks. In this case the physical separation between the fuel assemblies in the SFP storage racks is such that the dropped assembly must either enter a vacant storage location or remain lying on top of the racks.

For the case in which a fuel assembly is assumed to be dropped on top of a rack, Reference 9.7-13 shows that the fuel assembly will come to rest horizontally on top of the rack with a minimum separation distance from the active fuel region of more than 0.3 m (1 ft), which is sufficient to preclude neutron coupling (i.e., an effectively infinite separation). Consequently, the horizontal fuel assembly drop accident will not result in a significant increase in reactivity which remains below a k_{eff} of 0.95. Furthermore, the soluble boron in the spent fuel pool water increases the margin to criticality. This fault is not considered further as there are no consequences.

For a vertical drop of an assembly into a location that might be occupied by another assembly or that might be empty, Reference 9.7-13 concludes that a vertical impact onto another assembly would at most cause a small compression of the stored assembly, reducing the water-to-fuel ratio and thereby reducing reactivity. A vertical drop into an empty storage cell could result in a small deformation of the baseplate. The resultant effect would be the lowering of a single fuel assembly by the amount of the deformation. This could potentially result in a misalignment between the active fuel region and the neutron absorber. However, the amount of deformation for this drop would be small and restricted to a localised area of the rack around the storage cell where the drop occurs. Furthermore, the soluble boron in the spent fuel pool water assures that the true reactivity is always less than the limiting value for this dropped fuel accident. This fault is not considered further as there are no consequences.

Fault 3.2.3, Misplaced fuel assembly in SFP

- In space next to fuel racks
- Vertical misalignment of fuel assembly relative to fixed neutron absorber panels

The arrangement of the fuel storage racks in the pool and design of the racks physically prevents placement of an assembly outside the racks which would challenge criticality safety.

The spent fuel storage racks are qualified for the storage of fresh unburned fuel assemblies with the maximum permissible enrichment (4.95 weight percent U-235) in every location. Therefore the abnormal location of a new fuel assembly within normal cells is not an issue.

When fuel assemblies are lowered into the racks, it is conceivable that some part of an assembly could catch on the rack canister openings and not get fully lowered into position, leaving some portion of the fuel protruding above the fixed neutron absorber panels. However, if this happened to a single fuel assembly, it would not have criticality consequences because there would be no neighbouring fuel assemblies with which to couple.

It is considered incredible that this would happen to multiple adjacent fuel assemblies due to fuel handling controls. This fault is not considered further.

Fault 3.2.4, Increased Reactivity After Incomplete Repair of Fuel Assembly

- Some fuel rods removed and not replaced

If fresh fuel is found defective at delivery inspection and needs to be reconstituted it would not be handled at site. It would be sent back to the fabrication facility instead. The only other type of fuel assembly that needs to be reconstituted would be one with a leaking pin caused by in-reactor operation and would therefore have experienced burnup. It would be placed in one of the defective fuel racks on the side of the SFP. If a pin is removed it would be for the sole purpose of immediately replacing it with a steel dummy rod.

It is conceivable that fuel rods could be removed from a fuel assembly with the intention of later replacing them (e.g., with stainless steel rods), and that the fuel assembly may be left with one or more vacant positions until this is done and placed in a pool rack inadvertently. The likelihood of one of these assemblies being placed with the rest of the fuel with a pin removed is therefore very low. However, the increased reactivity effect of having removed a pin will be significantly smaller than the reduced reactivity effect due to the burnup that the assembly accrued. To get a significantly increased reactivity would require repair on low burnup fuel and multiple errors with vacant positions in the optimum locations, and this is considered very unlikely and not within the design basis. This fault is not considered further.

9.7.1.2.1 Bounding Fault for Design Basis Assessment

No fault is identified as bounding because no criticality faults increase reactivity above allowed levels. These faults are therefore screened out deterministically and no initiating event frequency, DB class, or response need be discussed.

9.7.1.2.2 ALARP Assessment

Note that while not necessary to maintain subcriticality the spent fuel pool boron concentration is measured manually, once every seven days. An automatic boron concentration monitor and alarm would provide a further indication to the operators of any dilution, at an earlier time than the manual measurements. However, it is most likely that other indications would occur first, e.g., a high SFP level. Any automatic system like this would have to be of high reliability and built to high standards, and the costs of providing such a system is considered disproportionate to the marginal improvement in risk as an additional defence in depth measure.

The rack design is such that, even if the racks were loaded with fresh fuel and/or boron concentrations assumed to be zero, the fuel would remain sub-critical. This physically safe design is considered ALARP.

9.7.2 Loss of Heat Removal Faults during Refuelling, Fuel Handling, and Fuel Storage

9.7.2.1 Introduction and Overview

This section assesses the loss of heat removal faults associated with refuelling, fuel handling and fuel storage in faults 3.2.5-3.2.9 and 3.2.10 – see Appendix 8A.

The AP1000 SFP design is based on a defence in depth approach that relies on both A-2 active systems and A-1 passive systems to provide protection against potential heat-up leading to damage of the stored fuel. In line with the AP1000 passive design philosophy, the active spent fuel pool cooling system (SFS) is a Class 2 safety system. The Class 2 cooling chain is designed not only to reliably support normal operation, but also to minimise the demand on the passive systems.

In case of multiple failures in the Class 2 cooling chain (SFS/RNS, CCS, SWS, their supporting systems, or AC power supplies), the principal means of ensuring cooling of the spent fuel is provided by the Class 1 inventory of water in the pool and additional Class 1 makeup sources that can provide passive makeup to the spent fuel pool. Following a postulated complete loss of the Class 2 cooling chain, the pool will heat up and boil off water, providing the necessary cooling to the spent fuel. The water above the fuel, even at reduced water levels, provides sufficient shielding since no operations immediately above or in the pool fuel handling area would be conducted. The Class 1 SFP water inventory is thus the principal means of fulfilling the Category A safety function of cooling and shielding the fuel in the SFP. Class 1 sources provide sufficient inventory to provide cooling for at least 72 hours (and in most cases, a much longer period of time).

When fuel is removed from the reactor after shutdown, the decay heat can be tens of kW per fuel assembly. The decay heat is removed by keeping the fuel continually immersed in water, which is typically cooled by the RNS when the fuel is inside containment or by the SFS when the fuel is in the spent fuel pool, which is in the Auxiliary Building, outside of containment. The SFP water temperature is normally limited to 49ºC (120ºF) during all plant operations. If one of the cooling trains fails during refuelling operations, this SFP temperature can be exceeded, but will be limited to 60ºC (140ºF). Furthermore, operation of any single train of SFS or RNS will prevent boiling from occurring in the SFP or in the refuelling cavity inside containment. Thus, the Class 2 SFS with the ability of the Class 2 RNS to also remove heat from the SFP minimises reliance on the operation of the Class 1 passive systems, structures, and components (SSCs). A brief description of the AP1000 spent fuel cooling methods is provided below.

Both the RNS and SFS are comprised of two redundant trains of equipment that are powered by redundant and separated power supplies. The RNS and SFS heat exchangers are cooled by the Class 2 CCS and SWS systems, which are also comprised of redundant trains that are powered by redundant and separated power supplies. Additionally, the associated supporting structures and piping that ensure fuel coverage are designed as seismic Class 1 SSCs. These SSCs include:

- The RNS pressure boundary (includes piping, valves, RNS side of heat exchangers, RNS pumps)
- SFS piping connected to the pool or other associated pits that are at elevations below the SFS pump suction and return piping connections to and from the pool
- The refuelling cavity
- The refuelling cavity seal
- The fuel transfer tube
- The fuel transfer canal

- The spent fuel pool
- The cask loading pit
- The cask washdown pit
- The spent fuel pool gates.

During normal plant operation, the SFP water is maintained at or below 49ºC (120ºF) by operation of either one of the two SFS cooling trains. The SFS train not being used for cooling is placed in standby and is available should the operating train of equipment become unavailable. Similarly, only one of the two trains of the CCS and SWS are normally required to operate. In addition, the CCS is designed such that either CCS pump can be operated and aligned to either CCS heat exchanger, and can cool either SFS heat exchanger. Likewise, the SWS is designed such that either SWS pump can be operated and aligned to either CCS heat exchanger, and the service water can be cooled by either SWS cooling tower. This flexibility in operation ensures that the failure of any active component in the SFS, CCS, and SWS will not interfere with normal SFP cooling, and that normal planned maintenance on these components can be performed without a significant loss in cooling reliability. The two CCS and SWS trains can also be segregated in the event of a passive failure such that no single piping failure can disable both trains. Additionally, either one of the two redundant, separated RNS trains can be aligned to cool the SFP should both SFS trains be unavailable, since the RNS pumps and heat exchangers are not operating during normal plant operation.

During plant cooldown operations and prior to the initiation of refuelling activities, both RNS trains are aligned to the RCS to remove the core decay heat, and both CCS and SWS trains operate to support RNS cooling. Typically, the decay heat from the fuel assemblies in the SFP is quite low at this time since the last core region removed from the core has had one whole fuel cycle for its decay heat to decrease. However, the RNS, CCS, and SWS are designed such that after RCS cooldown and preparations for refuelling, the operation of just one train of each system provides sufficient cooling to the RCS, such that one of the two RNS trains can be aligned to provide SFP cooling should both the operating train and standby train of the SFS become unavailable.

During the removal of the spent or used fuel from the reactor vessel, during the fuel transfer process, and during storage in the SFP, both the RNS trains and SFS trains are aligned to and operate to remove the core decay heat. Both CCS and SWS trains are also operated to support the RNS and SFS cooling functions. However, the RNS, SFS, CCS, and SWS are all designed such that only one of the two trains of each system is required to prevent boiling of the water in the reactor vessel and SFP. Therefore, adequate cooling to prevent boiling can be provided by aligning one RNS train to provide SFP cooling should both the operating train and standby train of the SFS become unavailable; or by one of two RNS trains providing cooling for the fuel inside the reactor containment and one of two SFS trains providing cooling for the fuel outside containment in the SFP and transfer canal.

Following a full core off-load (including an emergency core off-load), where all the fuel inside the reactor vessel is removed and placed in the SFP, any one of the four SFS and RNS cooling trains combined with any one of two CCS pumps, CCS heat exchangers, SWS pumps, and SWS cooling towers can provide sufficient SFP cooling to prevent boiling in the SFP.

Eventually (after a number of years), the decay heat is low enough to enable the spent fuel to be transferred to a spent fuel cask for ultimate disposal or storage in dry conditions. The

following sections address fault conditions in spent fuel cooling during refuelling (Mode 6) and throughout the time it is stored in the spent fuel pool.

Safety Case Overview

The AP1000 design provides sufficient inventory to ensure that the fuel assemblies located in the racks in the SFP will remain covered for at least 72 hours following all Design Basis Events, by a combination of initial inventory in the pool and available Class 1 makeup sources, assuming the un-availability of all non-Class 1 systems.

The analyses presented in Sections 9.7.2.3 and 9.7.2.4 demonstrate that adequate Class 1 inventory is provided to ensure coverage of fuel seated in the racks for at least 72 hours for all postulated breaks, even for breaks in Class 1 lines. A discussion is provided to explain how fuel being moved at the time of an event can be placed in the spent fuel racks. It is noted that for RNS breaks (Class 1), this makeup will have to be supplied via a Class 2 line, which is considered acceptable due to the frequency of the event and the significant time available (over 1 day) before any makeup is necessary. Additionally, for the vast majority of the fuel cycle, no SFP makeup is required to support having the 72 hours before the stored fuel is uncovered.

In addition to the provision of pool makeup from Class 1 sources, the AP1000 design provides a robust design of the Class 2 active cooling chain and of the Class 3 and general non-safety (GNS) systems that minimises the demands on the Class 1 passive systems

The analysis presented in Section 9.7.2.3 demonstrates that the Class 2 systems are designed such that no single failure can preclude the operation of the cooling chain, and multiple failures are necessary before the actuation of the passive systems is required. The design is such that the probability of onset of boiling is a DB1 fault (with an initiating event frequency ~1.0E-03 per year). For cases where boiling in the SFP occurs, the analysis presented in Section 9.7.2.3 shows that doses to the public and workforce would remain well below the Target 4 BSL.

Finally, Section 9.7.2.3.4 shows that the design provides additional defence in depth in that there are additional Class 2, 3, and GNS sources, with their own dedicated power supply (diverse from main AC and the standby Diesel Generators), that are available to provide makeup should there be a failure of both the Class 2 heat removal chain and the Class 1 makeup, or should makeup be required for an extended period of time beyond 72 hours.

9.7.2.2 Analysis of Faults

Two faults were identified from the fault schedule (Table 8A-2):

Fault ID	Description
3.2.5-3.2.9	Loss of Water Inventory from SFP
3.2.10	Loss of Spent Fuel Cooling Capability

Fault ID 3.2.10, the loss of spent fuel cooling capability will be addressed first in Section 9.7.2.3. Fault ID 3.2.5-3.2.9 is addressed in Section 9.7.2.4, which describes the protection against a postulated break in Class 1 and Class 2 lines.

9.7.2.3 Fault ID#3.2.10 – Loss of Spent Fuel Cooling Capability

9.7.2.3.1 Identification of Causes and Accident Description

This section provides an overview of the potential causes of a loss of SFP cooling and provides an integrated narrative to describe the interaction of the Class 1, 2 and 3 systems and the associated claims.

Section 9.7.2.3.2 discusses the normal spent fuel pool operation, including the Class 2 cooling chain and the associated train separation. Assuming an initiating event (e.g., loss of ac electrical power, or failure of a pump in the SFS/RNS/CCS/SWS systems), and assuming a series of failures in the Class 2 cooling chain (including the potential for common cause failures), a loss of pool cooling capability of the pool would result.

The unmitigated consequence of such a loss of cooling event is heatup and boil off of the water in the SFP. After a significant length of time (a day or more) fuel damage would occur resulting from fuel uncovery and the subsequent release of radioactivity. Section 9.7.2.3.3 describes how the pool inventory and other Class 1 passive systems provide protection against the potential for fuel uncovery. Section 9.7.2.3.4 provides a description of the additional lines of defence in depth, including Class 2 makeup that can be supplied to the pool. Considering that a loss of cooling would be due to the loss of the normal Class 2 cooling chain, these Class 2 sources are diverse, and rely on diverse and/or separated power supplies.

Finally, in Section 9.7.2.3.8, post fault recovery is described for a break in the Class 2 SFS suction/return piping, as well as the non-break scenario where the cooling chain is lost.

The following sections provide the analyses required to demonstrate the capability of each line of defence to achieve its objective.

9.7.2.3.2 Normal Spent Fuel Cooling and Overview of Class 2 Cooling Chain

The SFS consists of two mechanical trains of equipment. Each train includes one pump, one heat exchanger, and separate piping to and from the pool. During normal plant operation, only one of the SFS trains is needed to provide spent fuel pool cooling and purification. Therefore, if the operating train fails, the standby train can be brought into operation.

During refuelling, as fuel assemblies are unloaded from the core and moved into the pool, and for some time afterwards (based on the decay heat load), both SFS trains are in operation, but only one train is required to prevent onset of boiling conditions. Either RNS train can also be aligned to provide cooling for the SFS pool, provided it is no longer needed for normal shutdown cooling.

Both SFS and RNS reject heat to the CCS and SWS. All of these systems are normally powered by the main ac power system (ECS), but each SFS-RNS-CCS-SWS train and their supporting systems can also be powered by one of the two standby diesels (onsite standby power system (ZOS)) in the event of a loss of offsite electrical power and plant trip.

All of the systems discussed above are Class A-2, and provide a high reliability of spent fuel cooling. Multiple failures are required for a loss of heat removal to occur. The potential scenarios leading to a loss of cooling capability are:

- Loss of offsite power with plant trip (caused by failure of the rapid power reduction system) and subsequent failure of both trains of the onsite standby diesel generators

- Loss of both trains of SFS, plus the loss of both RNS trains
- Loss of both trains of CCS
- Loss of both trains of SWS
- Loss of both trains of the ECS
- Complete loss of the PLS

In the unlikely event of an extended loss of normal spent fuel pool cooling (i.e., loss of both trains of SFS and available train(s) of the RNS, or their supporting systems), it is likely that the fault can be identified and repaired before the onset of boiling in the SFP and certainly before there is any significant loss of SFP water inventory (i.e., mean time to return (MTTR) is lower than the time to onset of boiling or to significant water loss challenging fuel uncovery). Low spent fuel pool level alarms in the control room will alert the operator to initiate makeup water to the pool. If the non-seismically qualified sensor is functional, an alarm for low spent fuel pool level will alert the operators in the control room to makeup water in the SFP. In addition, alarms are provided from redundant Class 1 instrumentation to alert the operator to makeup to the pool and to alert the operator that the pool has reached the low level limit.

Loss of cooling in the refuelling cavity is bounded by the loss of spent fuel pool cooling since the amount of water in the spent fuel pool compared to the inventory of spent fuel (and decay heat) is much less than in the refuelling cavity. Also, the containment provides an additional barrier to any activity release if water is boiled in the refuelling cavity, compared with the spent fuel pool located outside the containment. In addition, the operation of the Class 1 PCS acts to condense the steam created if the refuelling cavity boils and the condensed steam is returned to the IRWST and can be re-used to remove core decay heat.

9.7.2.3.3 Class 1 Passive Cooling

During the first 72 hours after a loss of cooling event, any required makeup water is supplied from Class 1 seismically qualified sources that do not rely on ac power. If further makeup water is required after 72 hours, water from other onsite sources is made available to the spent fuel pool. The amount of makeup water to the pool required to ensure the 72 hours and 7 day cooling capability depends on the decay heat level of the fuel in the spent fuel pool and is provided as follows:

- When the calculated decay heat level in the spent fuel pool is less than or equal to 4.0 MW, no makeup is needed to achieve spent fuel pool cooling for at least 72 hours.
- When the calculated decay heat level in the spent fuel pool is greater than 4.0 MW and less than or equal to 5.0 MW, makeup from the Class 1 cask washdown pit is sufficient to achieve spent fuel pool cooling for at least 72 hours. A minimum level of 4.19 m (13.75 feet) in the cask washdown pit is provided for this purpose. Availability of this makeup source is controlled by Technical Specifications.
- When calculated decay heat level in the spent fuel pool is greater than 5.0 MW and less than or equal to 7.0 MW, makeup from the cask washdown pit and cask loading pit is sufficient to achieve spent fuel pool cooling for at least 72 hours. A minimum level of 4.19 m (13.75 feet) in the cask washdown pit is provided for this purpose. The cask

loading pit is maintained full during shutdown operations for this purpose. Availability of these water makeup sources are controlled by Technical Specifications.

- When the calculated decay heat level in the spent fuel pool is greater than 7.0 MW, makeup from the PCCWST is sufficient to achieve SFP cooling for at least 72 hours, and the combination of the PCCWST and the passive containment cooling ancillary water storage tank (PCCAWST) is sufficient to achieve spent fuel pool cooling for at least 7 days.

- When the decay heat level in the reactor is less than or equal to 7.0 MW, water is not needed for containment cooling for the first 72 hours and the PCCWST can be used for makeup to the spent fuel pool. The volume of water in this tank is sufficient to provide makeup for at least 72 hours, based on the highest heat load in the spent fuel pool. Between 72 hours and 7 days the tank can continue to provide makeup water as required until it is empty.

- When the decay heat level in the reactor is greater than 7.0 MW, the water in the PCCWST is reserved for containment cooling. Spent fuel pool makeup water is initially provided by the cask washdown pit or a combination of the cask washdown pit and cask loading pit depending on the heat load in the spent fuel pool according to Technical Specifications. After 72 hours, makeup water can be provided from the PCCAWST.

Alignment of the cask washdown pit and PCCWST is accomplished by positioning manual valves. Gravity driven flow from the cask washdown pit to the spent fuel pool is provided as the cask washdown pit water level will follow the spent fuel pool level. Gravity driven flow from the PCCWST is controlled by a manual throttle valve with local flow indication, which is set to achieve the desired flow when the makeup is initiated. The initial flow will be set based on the amount of decay heat in the SFP and the throttle valve can be adjusted to match the boiling conditions. This can be determined from the full-range level indicators displayed in the control room. The cask loading pit can be aligned to the spent fuel pool by opening the gate which separates these two pits.

After 72 hours, makeup water from the Class 2 PCCAWST can either be pumped to the PCCWST and then gravity fed to the spent fuel pool as discussed above, or the water can be pumped directly to the spent fuel pool. When the makeup water is pumped directly to the pool, the flow rate is controlled by the same manual throttle valve used to set the flow rate when providing gravity driven flow from the PCCWST.

It is expected that after 7 days other site water sources such as the fire protection system, demineralised water system, or water from offsite sources can be used to makeup SFP boiling for an extended time period. In addition, river or sea water may be used as makeup.

The following indications and alarms will alert the operator of a loss of normal spent fuel cooling:

- Spent fuel pool high temperature indication and high alarm – Safety Class B-3

- Spent fuel pool low-2 water level indication and low alarm – 3 way redundant Safety Class A-1 instrumentation

- Spent fuel pool low water level indication and low alarm – Safety Class B-3

- SFS pumps discharge flow indication and low alarm and/or SFS heat exchanger outlet temperature indication and high alarm – Safety Class B-3

- If the loss of SFP cooling was caused by failures in the CCS or SWS, there would be additional indications and alarms associated with those systems

After the operators become aware of the loss of cooling to the SFP, they would track the SFP temperature as it increased toward boiling. After boiling starts, they would track the SFP level as it decreased due to the boil-off. If the SFP is boiling, an additional indication and alarm may be generated by the spent fuel room air-activity monitor (Safety Class C-3). During this time the operators would attempt the recover Class 2 cooling. The SFP water level indication would be used to indicate when the operators would need to align an alternative makeup source.

9.7.2.3.4 Placement of Fuel in the Racks

Upon the loss of off-site power and notification from the control room or the pool visual level indicator, the operators involved with fuel movement in the fuel handling area assess the condition and the immediate actions needed to place a fuel assembly in a safe storage location.

A total time of less than one hour is assumed to perform the manual fuel move from the fuel transfer system upender to a defective fuel cell storage location. This time estimate is considered conservative and can be improved with the reduction of travel distance to place a fuel assembly fully down.

The fuel handling area will remain habitable with adequate lighting for greater than 2 hours with an averaged wet bulb global temperature (WBGT) of 35 °C (95°F) or less.

Completion of the operation would result in dose rates well below the appropriate Target 4 limits. The doses for the described event bound anticipated less limiting doses for other events, where spent fuel pool level is maintained until the onset of boiling.

Following safe placement of the fuel assembly, the fuel handling area (FHA) would be evacuated (Reference 9.7-11).

9.7.2.3.5 Post-72 Hour Cooling and Diverse Class 2/3 makeup sources

As stated in 9.7.2.3.3, the amount of makeup water needed to prevent fuel uncovery for at least 72 hours depends on the decay heat load in the SFP. This makeup is provided solely by Class 1 sources. In the unlikely event of an extended loss of cooling scenario, where post fault recovery has not occurred after 72 hours, the Class 2, 3, and GNS makeup sources are able to provide post-72 hour cooling capability. Furthermore, if there is a loss of cooling event coincident with a failure of a Class 1 passive makeup source, the sources described below provide a diverse means of ensuring adequate water level in the SFP, each with its own dedicated power supply.

Class 2 makeup water from the PCCAWST: Either one of the two Safety Class B-2 pumps powered by its corresponding ancillary diesel generator can provide makeup to the SFP. The ancillary diesels are a diverse power source separate from the standby diesel system. The pumps are located in the Seismic II portion of the Annex Building. Makeup water can be aligned to the pool through any of the following paths:

1. Directly into the SFP through the Class 1 RNS line

2. Through the Class 2 SFP Spray lines.
3. Indirectly to the SFP through the Class 1 RNS line by refilling the PCCWST

Note that the Class 2 Ancillary equipment is protected against hurricanes but is not protected from other limiting internal / external hazards. If these SSCs are not available then offsite equipment would be brought to the site and connected to Class 1 connections to provide the same functions.

Makeup from the FPS to SFP spray lines: One of the two Safety Class B-3 FPS tank packages can be used to provide at least 1893m^3 (500,000 US gallons) of makeup supply to the spray lines. The lead fire pump is electric motor-driven and the second pump, to be used if offsite power is lost, is diesel engine-driven. This is a dedicated fire protection diesel engine. This diverse source pumps water from the FPS storage tanks to the spray lines. In addition, upon actuation, up to 2366 l/min (625 gpm) of makeup water can be provided to refill the FPS tanks by the Raw Water System (RWS).

Flanged Connection to SFP spray lines: A Safety Class B-3 flanged connection, located outside of the fuel handling area, can also be used to provide makeup water to the SFP through the spray lines. This connection is powered by a dedicated, portable pump and will provide a diverse means of providing makeup to the SFP. The portable pump can be used to take suction from a fire hydrant on the southeast side of the plant or any other potable water source and discharge the water into the flange to connect to the SFP spray lines.

The above makeup sources can all be used if ac power is not available. If ac power is available, demineralised water transfer and storage system (DWS) and CVS water can also be supplied as makeup water to the SFP. The DWS water can be pumped through the SFS connection to the SFP, while the CVS makeup water can be pumped through the SFS connection or RNS connection to the SFP.

PCCAWST Flange Connection: A Class 2 flanged connection, which ties into the existing line PCS-PL-L064 between the PCCAWST and PCS-PL-V037, can also be used to provide makeug water for SFP and Containment cooling. A site-specific portable pump can be used to take suction from the PCCAWST flange connections and discharge to the PCS Class 1 flange connections to provide makeup water for SFP and Containment cooling.

9.7.2.3.6 Analysis of Effects and Consequences

There are two scenarios which may lead to a release of activity:

- Loss of all forced flow cooling leads to boiling of the pool which causes activity in the pool to be carried into the building atmosphere and the outside environment

- Boiling continues long enough and makeup is not supplied for the fuel to be uncovered, leading to fuel failure and a large release to the building and atmosphere.

This section addresses loss of cooling events due to the failures in the cooling chain, including a break in the non-seismic, non-Class 1 SFS suction/return piping. This is the only non-Class 1 piping that can lead to a loss of cooling in the event of a pipe break. Postulated breaks in Class 1 lines are discussed in Section 9.7.2.4.

9.7.2.3.7 Analysis Method

The analysis for the AP1000 spent fuel pool heatup, boiloff, and emergency makeup on loss of cooling is documented in APP-SFS-M3C-012 (Reference 9.7-10). This analysis supports the AP1000 design, but it only considers loss of cooling or a break of non-Class 1 lines. It does not assume a break in Class 1 lines and does not directly provide time to onset of boiling analysis. To support the UK safety case, additional analyses has been performed, covering a wider range of frequent and infrequent design basis conditions. These analyses are documented in UKP-SFS-M3C-012 (Reference 9.7-3).

The time to the onset of boiling and the time to fuel uncovery were calculated for a number of scenarios. The loss of cooling scenarios that have been investigated are defined below and are also described in Reference 9.7-3.

Emergency full core offload: This case assumes the maximum possible heat load in the SFP. It is assumed that a full core offload (157 assemblies) occurs just after the reactor has reached maximum power following a recent refuelling. When the full core is offloaded, all fuel storage positions are occupied.

Full core offload: Similar to the emergency full core case, this scenario assumes a full core (157 assemblies) has been recently transferred to a full SFP; however, in this scenario the offload takes place after a normal fuel cycle of 18 months.

Beginning of cycle: This case assumes that a refuelling outage has just finished and there are 69 recently offloaded assemblies in the SFP, along with the maximum number of long term fuel assemblies.

Middle of cycle: This case assumes that an event occurs during the middle of a normal fuel cycle of 18 months, with 69 recently offloaded assemblies and the maximum number of long term fuel assemblies.

The emergency full core offload is a very unlikely event, such that its occurrence coincident with loss of spent fuel cooling could be excluded on the double contingency principle. The remaining three cases conservatively evaluate different time in cycle conditions. In general, the refuelling cases considered – the emergency and full core offload – would only apply for a very small fraction of the fuel cycle (approximately 10-15 days every 18 months, or under 3%), while the cases at the beginning and middle of the cycle can be used to provide an estimate of average conditions during the vast majority of the cycle.

The calculations of the boiloff times and fuel uncovery times (Reference 9.7-3) include several conservative assumptions, designed to make the evaluation very conservative and simplify the evaluation methodology. Conservative assumptions include assuming increased core power and uncertainty in the decay heat, draindown of all connected water sources to the postulated break elevations, and event initiation at maximum normal pool temperature of 48.9° C (120°F). Further the top of fuel in the Spent Fuel Pool is assumed to be at elevation [ ][1] since that is the location of the level measurement instrumentation. The actual top of active fuel is located at elevation [ ].

1. Note that the basis for all elevations is set to 100 feet in US design and 100 m in metric design.

9.7.2.3.8 Analysis Results

Onset of Boiling Conditions Analysis

If a complete loss of cooling is assumed, there is a potential for SFP pool boiling. However, even during normal refuelling scenarios (with the whole core off loaded), it would take at least 3 hours for the pool to begin boiling. Figure 9.7.2-1 shows the results of the onset of boiling calculations for various times that the loss of cooling may occur. The available time to onset of boiling conditions is a function of when the event occurs during the fuel cycle. The boiling time is shortest during the portion of the refuelling outage where the entire recently discharged core is located in the pool. At end of the outage, only approximately 44% of the fuel assemblies removed from the reactor are left in the pool (69 assemblies are conservatively assumed to be discharged to the spent fuel pool and the remaining 88 assemblies returned to the core). During the subsequent operation of the plant, the spent fuel decay heat continues to decrease, such that at end of cycle the onset of boiling would take over 24 hours, after the complete loss of pool cooling capability occurs.

As discussed in the following section, actuation of the Class 1 passive pool makeup system will then prevent fuel uncovery in the bounding case for at least 72 hours, and a significantly longer time is provided for more credible conditions.

Fuel Uncovery Analysis

Table 9.7.2-1 shows the estimated times to fuel uncovery from the beginning of the transient for the scenarios identified above, relying solely on the initial inventory in the SFP and the associated pits. This is essentially the time available for operator action to align the makeup sources to prevent fuel uncovery. For each heat load, the time from the loss of SFP cooling to when the pool water inventory is reduced to the top of the fuel assemblies is listed. Both a loss of cooling event, with all lines intact, and a postulated break in a SFS Class 2 line are considered. Postulated breaks in Class 1 lines are discussed in Section 9.7.2.4.

Table 9.7.2-1 illustrates that for the “no break” and “Class 2 piping break” cases, abundant time is available for the operators to initiate water makeup to the SFP from Class 1 (or Class 2 and 3) water sources, and to restore the SFP cooling function. In fact, only during increased heat loads during and immediately following a refuelling scenario would any action be required to support the 72 hour safety claim.

In Case 2, a break in the SFS suction piping, the ability to cool the SFP using the normal Class 2 SFS cooling chain would be lost; however, the operator could align the SFP to an available RNS train, if either of the two trains is available. With at least 2 hours available until boiling starts, it is highly unlikely that a Class 2 SFS suction or return line piping break would lead to a boiling scenario, considering one of the two RNS trains can be used to cool the pool.

For the cases where the operator is required to provide initiate passive makeup, the Class 1 PCCWST could be aligned to achieve the 72 hour objective with abundant margin. The operator actions required to align the PCCWST consist of opening three manually operated valves. Once aligned, the PCCWST has a minimum of 2864 m^3 (756,700 US gallons) available for spent fuel pool makeup, enough to keep the fuel covered well past 72 hours.

Operator Actions

The robust design of the AP1000 ensures multiple pathways to provide Class 1 makeup from the PCCWST and additional Class 2 and 3 makeup from other diverse sources. The operator

actions required to align the various makeup sources are outlined in Table 2.4-3 of Reference 9.7-4.

9.7.2.3.9 Post Fault Recovery

The following post-accident recovery section below, along with Section 9.7.2.4.6 (Post Fault Recovery for infrequent pipe breaks), provide a general description of how the operators would deal with a loss of cooling event.

Loss of Cooling without a Pipe Break:

If a loss of cooling accident occurs without a pipe break, the recovery actions consist of maintaining sufficient level in the SFP while the cause of the loss of cooling accident is identified and fixed. Additional details on operations to restore cooling are provided in Reference 9.7-4.

Table 9.7.2-1 shows that during normal plant conditions, the operators will have at least 3 days to identify the cause of the problem and take corrective actions. During a refuelling outage, the operators will have at least 36 hours. The most likely cause of a loss of cooling is a station blackout or a loss of the CCS/SWS cooling chain. The MTTRs for these faults are significantly shorter than the 3 days and 36 hours for normal operation and refuelling, respectively.

Break of SFS Suction/Return Piping

The SFS return line to the SFP has a hole that is located below the operating deck elevation. This hole acts as a siphon break to prevent draining the pool in the event of an SFS return pipe break or equipment leak.

Because the Class 1 SFP connection to the RNS is below the SFS piping connections, even if the SFP pool level drops to the bottom of the SFS suction piping, an RNS pump and heat exchanger train can be aligned to the SFP to restore cooling capability. At least one of the two RNS trains would always normally be available as the first line of defence for an SFS pipe break. Additional detail on operations to restore cooling are provided in Reference 9.7-4.

9.7.2.3.10 Consequences Analysis for Onset of Boiling Conditions and Event Frequency

Dose Analysis

The following conservative assumptions are included in the dose analyses:

- The initial activity in the pool is based on the .025 mSv/hr (2.5 mRem/hr) dose rate limit at the pool surface. It is conservatively assumed that the entire dose is from I-131, the iodine nuclide with the greatest dose impact. It is, however, expected that most of the dose rate would actually be coming from cobalt, instead of iodine.

- It is conservatively assumed that the iodine escape rate coefficient increases by 2 orders of magnitude coincident with the loss of SFP cooling. It is however expected that the escape rate coefficient would remain approximately the same since the heat transfer from the fuel to the SFP water would not significantly increase. Additionally, the iodine that would be released over a 30-day period is assumed to be present in the pool at the onset of boiling. These conservatisms account for approximately 45% of the analysis source term.

- Iodine, when oxidised, becomes volatile and may enter the air above the SFP; other nuclides, except for noble gases, are non-volatile (i.e., particulate). It is conservatively assumed that 1% of the iodine becomes airborne. From Figure 11 of Reference 9.7-12, it can be seen that the fraction of iodine oxidised (and therefore assumed to be volatile) in a boric acid solution is less than 1% at 100 ºC (212°F). The iodine release rate is assumed to be proportional to the calculated steaming rate from the pool. Since the SFP boiling is a gradual process as opposed to flashing, the moisture carryover and resultant particulate release is assumed to be negligible and is therefore not modelled.

- The SFP iodine release is assumed to be a direct atmospheric release (e.g., everything that escapes the pool surface is assumed to be released to the environment). No credit is taken for the volume of the room in which the SFP is located. Atmospheric releases would be subject to dilution effects from the volume of the room and the exhaust rate from the room to the atmosphere

- Operation of the VAS and containment air filtration system (VFS) HVAC systems is not credited in the dose analysis. It is noted that for most expected normal operation conditions (e.g., not emergency core offload or during refuelling), even with the conservative assumptions identified herein, the VAS and VFS systems, if available, would be able to at least significantly delay, if not prevent, the actuation of the relief panels following onset of boiling conditions. This would extend the time before any postulated release to the environment occurs, and significantly reduce any such release.

While airborne crud contribution is not modelled in the evaluation of the radiological consequences of a SFP boiling event, the dose impact of crud in the SFP is expected to be very small (Reference 9.7-5).

As discussed in Section 4.1.2 of Reference 9.7-5 (Spent Fuel Pool Chemistry, UKP-GW-GL-081, Rev. 0, January 2011), a passive filtering capability is provided by the fuel handling area relief paths. This solution is considered ALARP as it resolves an uncertainty with a design change that is considered practical. The filters will be specified to ASME-AG-1, which requires a minimum efficiency of 99.97% when testing with 0.3μm particles. The conclusion is that with this additional filtration the boiling dose analysis remains bounding.

Reference 9.7-6 documents Westinghouse analyses for the doses at the site boundary and in the control room following a postulated extended pool boiling. Two cases are considered:

1. Emergency core offload case. The dose for the duration at the site boundary is reported as less than 0.3 mSv. The control room dose is calculated as less than 0.4 mSv. The assumptions considered in this case are consistent with the emergency core offload case described in Section 9.7.2.3.6 and Reference 9.7-4.

2. Normal At-Power Operation case. The dose at the site boundary is calculated as 0.04 mSv.[1] The control room dose is calculated as less than 3.0E-03 mSv (assuming main control room emergency habitability system (VES) in operation). The assumptions considered in this case are consistent with the beginning of cycle case described in Section 9.7.2.3.6 and Reference 9.7-4.

1. Note that the dose provided in Reference 9.7-6 for this case is calculated for the limiting 2 hours. The dose for the duration at the site boundary that is provided here has been conservatively estimated by multiplying the LPZ (low population zone) dose by the ratio of the EAB (exclusion area boundary) X/Q by the smallest LPZ X/Q used in the analysis, as 5.0-03 mSv * (5.1E-04/8.0E-05) = 4.0E-02 mSv. The site boundary X/Q used in Reference 9.7-6 bounds the value listed in Appendix 9A, Table 9A-5.

It is noted that even considering the emergency core offload case to conservatively bound refuelling, and for the normal at-power operation case to conservatively bound the rest of the cycle, the emergency core offload case only applies to approximately 3% of the time in cycle, while for the remaining 97% the very low doses calculated for a loss of spent fuel cooling during normal operation case would remain bounding. In all cases, the doses are below the limits of Chapter 8 for the appropriate event class.

Operators will not be allowed to re-enter fuel handling area during pool boiling after all fuel has been seated in the racks. Further, anyone attempting entry or residing in the area would notice that the building was full of steam; therefore, it is incredible that there would be any cumulative dose associated with workers in the immediate vicinity of the pool.

Event Frequency

The bounding fault as described above includes a seismic event sufficient to damage the SFS piping. This would be a rare event. More frequent events would be associated with failures leading to a loss of spent fuel cooling, due to system failures or loss of offsite power. In each of these cases, the SFS piping would remain intact and the initial water level would be higher than is conservatively assumed in the consequence assessment.

The following faults needs to be considered to establish a probability for the loss of cooling function provided by the A-2 systems:

- Loss of offsite power with plant trip and subsequent failure of both trains of the onsite standby diesel generators
- Loss of both trains of SFS, plus the loss of both RNS trains
- Loss of both trains of CCS
- Loss of both trains of SWS
- Loss of both trains of the ECS
- Complete loss of the PLS

A PSA has been conducted for loss of spent fuel pool cooling (Reference 9.7-7). The two main initiators leading to pool boiling, and eventually to fuel uncovery, are LOOP and Loss of Component Cooling/Service Water Systems (LCCW).

PSA studies conducted in Reference 9.7-7 have been revised in Reference 9.7-8 to take into account the UK specific SFP, RNS, CCS and SWS design and the latest reliability data from NUREG/CR-6928 (Reference 9.7-9). The Spent Fuel Pool boiling contribution from pipe breaks retained in the PSA study is less than 1.0E-05/yr.

The spent fuel pool boiling frequency contribution from loss of offsite power is calculated by multiplying the frequency of loss of offsite power used in Reference 9.7-8 (3.59E-02/yr. a DB2 fault) by the probability of failing to recover offsite power, and by the probability of failure of the diesels to start and run for 24 hours. The frequency calculated is less than 1.0E-05/yr.

The spent fuel pool boiling frequency contribution from loss of the SFS and RNS trains documented in Reference 9.7-8 is less than 1.0E-04/yr.

A frequency of 3.50E-04/yr. (Reference 9.7-8) has been calculated for the spent fuel pool boiling due to LCCW is calculated as a DB1 fault (Reference 9.7-8). This frequency takes into account the diverse FPS connection to the CCS that is able to provide a separate heat sink to significantly reduce the probability of SFP boiling. With at least 1230 m^3 (325,000 US gallons) of fire protection water available and 2366 l/min (625 gpm) of RWS makeup water available to the FPS, this diverse connection can sustain cooling for a heat load of approximately 8.8 MW (30 MBTU/hr) in the SFP. The RWS makeup water automatically supplies water to the FPS storage tank once a low level is reached. If FPS water is being used to cool the SFP, the PRHR HX or other Class 1 components could be activated to cool the RCS inside containment until CCW/CCS is restored.

The total frequency calculated for onset of boiling conditions, taking into account the various contributors described above, is approximately 5.0E-04/yr. classifies boiling as a DB1 fault (Reference 9.7-8).

Consequences Assessment

As discussed above, the unmitigated consequences of any event potentially leading to a loss of cooling is eventual fuel uncovery and fuel damage. The primary protection against fuel uncovery is provided by the Class 1 systems.

The analysis documented herein shows that the calculated doses (<< 1mSv) and the low probability of the event (DB1) are acceptable. The associated doses remain well below the limits of Chapter 8 for the appropriate event class.

9.7.2.3.11 Consequences Analysis for Extended Boiloff and Potential Fuel Uncovery

As the pool boils, the water inventory is slowly reduced. As shown in Table 9.7.2-1, for the majority of time in a fuel cycle (approximately 97% of the time), no operator action is needed before 72 hours. In the unlikely event that the operator has to perform an action before 72 hours, the operator has over 24 hours before additional makeup is required. The operator would align makeup from the Class 1 source to ensure water is maintained above the stored fuel for at least 72 hours. For non-refuelling scenarios, over 72 hours are available before any makeup to the SFP is needed to prevent stored fuel uncovery.

There are several diverse engineered means of making up the pool inventory and, the long timescale before fuel uncovery means that operator intervention with water being supplied from a number of alternative on-site sources or from public water source can be claimed. The non-Class 1 sources of water that do not rely on the plant ECS and therefore do not rely on offsite or on-site standby power include:

- The PCCAWST with the use of ancillary diesel generators to power the PCS recirculation pumps
- The FPS water storage tank with diesel driven FPS pump and fixed piping to add water directly to the pool
- Fire hydrant or potable water source through flanged connection to SFP spray lines
- Offsite water supplies as available

All of these sources can be initiated if there is a failure of the Class 1 sources or to maintain long term cooling of the SFP. There are also several additional sources of water that can be used, but rely on the plant ac electrical power (ECS) including:

- The FPS water storage tank with motor driven pump and fixed piping to add water directly to the pool.
- The DWS water storage tank with motor driven pumps and fixed piping to add water directly to the pool.
- The boric acid storage tank and DWS water storage tank with the CVS makeup pumps and fixed piping to add borated water directly to the pool.

Since the water loss from the SFP is due to boiling, the boron concentration in the pool would not be reduced to below normal levels by using unborated water to make up the inventory, so there is no criticality issue.

In summary, the Class 1 water inventory and makeup ensure at least 72 hours are available before fuel uncovery is challenged, even when a postulated loss of the complete A-2 cooling chain without recovery is assumed. As discussed in the next section, 'Event Frequency', this results in an extremely robust design, which is effective in achieving a very low frequency for fuel uncovery.

Additionally, it is be noted that, as a beyond design basis measure, the spent fuel pool sprays will be available to maintain fuel cooling in the event of loss of water immersion. This requires either the diesel driven FPS pump or the motor driven FPS pump and a standby diesel generator to be available and working. In addition, there is a gravity driven spray line to the pool provided from the PCCWST and a flanged connection to the spray lines for additional water sources to be supplied to the SFP. These sources of makeup can be initiated by manual operator action, but they have no flow control.

Event Frequency

The "AP1000 PRA Spent Fuel Pool Evaluation" (Reference 9.7-7) presents the initial PSA for the AP1000 SFP. Fault tree analysis was used to quantify an estimate of the SFP contribution to the AP1000 fuel damage frequency (FDF). The analysis includes development of success criteria and mitigation strategy used to provide cooling and water makeup to the SFP and fault tree quantification results. The FDF calculated for the SFP is expected to have a small effect on radionuclide releases at the plant boundary.

The AP1000 SFP FDF was calculated in Reference 9.7-7 to be less than 1.0E-9 per year. This analysis is judged to be conservative. It does not include the latest SFS, RNS, CCS and SWS design for UK (and therefore the newly calculated spent fuel pool boiling frequency contribution from the loss of CCS/SWS). This is significantly lower than the 1.0E-07/yr. cut-off for design basis events in the UK. Also no MTTRs are credited although results from Table 9.7.2-1 shows that in the worst scenario, more than 24 hours are available for the operators restore SFP cooling when SFP cooling is lost or before establishing a makeup water source.

The SFP is located outside the reactor containment building, and fuel damage in the SFP is, therefore, considered to result in a release outside containment. The comparable large release frequency (LRF) quantified in the "UK AP1000 Probabilistic Safety Assessment" is less than 1.0E-07 events per year (Section 10.4.11). The FDF value is less than 1 percent of the LRF

value. The FDF quantified for the SFP will result in a minimal increase in the source term values used for a Level 3 PSA analysis.

9.7.2.3.12 Conclusions

The AP1000 design provides robust Class 1 passive systems to backup the active Class 2 spent fuel cooling chain. As demonstrated in Section 9.7.2.3.7, not only is the initial pool inventory sufficient to provide abundant time before a potential for fuel uncovery is approached, but also several Class 1 makeup sources are available to the operator to provide makeup water to the SFP for well over the 72 hours claimed in the safety claim in Section 9.7.2.1. These multiple lines of defence are sufficient to reduce the probability of fuel damage to less than 1.0E-9/yr., which places it well beyond the design basis.

9.7.2.4 Fault ID#3.2.5-3.2.9 – Postulated Loss of Water Inventory from the SFP

9.7.2.4.1 Identification of Causes and Accident Description

The no-break and non-seismic piping break scenarios are already included in the analysis documented in Section 9.7.2.3. In this Section, other less likely, but potentially more severe, Class 1 breaks are considered.

The spent fuel storage facility is located within the seismic Category I auxiliary building fuel handling area. The walls of the spent fuel pool are an integral part of the seismic Category I auxiliary building structure and are therefore designed to withstand a design basis earthquake. The spent fuel pool racks are also seismic Category I. The fuel handling machine is a seismic Category II component and is evaluated to show that it does not collapse into the spent fuel pool as a result of a seismic event. The fuel handling machine is also designed to maintain its load carrying and structural integrity functions during a safe shutdown earthquake. The spent fuel cask handling crane is a single-failure proof, seismic Category 1 component. In addition, the cask handling crane rails are placed such that the crane cannot drop any load that would fall or topple into the spent fuel pool. Therefore, a design basis earthquake or credible dropped load would not cause serious damage to the pool wall or liner sufficient to cause a leak.

There are, however, a number of piping connections to the SFP, all of which are seismic Category I, except for the SFS pump suction lines from the pool and the SFS pump discharge lines returning to the pool. Therefore, damage to the SFS pump suction and return piping is within the design basis and could lead to a lowering of the pool water to the level of the SFS suction header, i.e., about [ ] below the normal water level. This is still [ ] above the top of the fuel stored in the pool. Note that the SFS pump discharge lines returning cooled water to the pool are each provided with a siphon break hole consistent with limiting the loss of pool water as described above. In the case of a pipe break of the SFS piping connected to the SFP caused by a seismic event, the water level would be lowered to the SFS pump suction piping connection and the SFS cooling capability would be lost, however an RNS train can be connected to the SFP to restore cooling capability. This scenario is discussed in Section 9.7.2.3.

Leakage from any of the other pipes connected to the SFP is considered to be a very low probability event. This is because, apart from the SFS pump lines, all piping connected to the pool is seismic Category I. These Class 1 lines connected to the open SFP will normally be at ~20% of their design pressure. Further, these lines are schedule 40 or greater which are capable of use in systems with higher design pressures and thereby provide significant margin against pipe rupture. Furthermore, they are not under the load path of any lifting machinery.

A break in a Class 1 pipe connected to the SFP is an infrequent event; however, these postulated breaks have been analysed to show that even under the worst possible scenarios, the AP1000 design provides a significant window of time before the fuel is uncovered: hence, considering the low probability of occurrence of these events, consequential fuel uncovery is not considered credible.

The possible postulated breaks of Class 1 piping that could lead to the pool draining are listed below:

- A break in the Class 1 RNS suction line (the return line has a siphon break to limit draindown)
- A break in the DN 150 mm (6 inch nominal) Fuel Transfer Canal (FTC) drain line (only if the FTC gate is open)
- A break in the DN 200 mm (8 inch nominal) CLP piping connection to RNS (only if the CLP gate is open)
- A break in the DN 50 mm (2 inch nominal) SFP makeup water piping connection to the common water supply/drain header

The only time the FTC gate is expected to be closed, is during maintenance, when the FTC needs to be emptied. The CLP gate is required to be open when the decay heat load in the SFP is greater than 5.0 MW. Note that a break in the DN 25 mm (1 inch nominal) SFP level instrumentation piping will not result in rapid pool draindown since these connections include a 9.5 mm (3/8 inch) diameter orifice to limit possible pool outflow. In addition, because of the low discharge flow rate and the accessibility of these instrument lines, operator action to plug the leaking line can be taken and this event is not considered further.

Figure 9.7.2-2 provides a sketch illustrating the relative position of these lines relative in the SFP.

All of the breaks considered would cause the SFP to drain to the [ ] elevation in different amounts of time. Due to the design of the Class 1 spent fuel pool piping, it can be argued that the probability of any of these breaks occurring is negligible.

A review of all the potential breaks identifies three potential limiting scenarios that need to be considered in a design basis analysis:

1. The first scenario considered is a Class 1 RNS suction line break. While the RNS suction line is connected at a relatively high elevation compared to other potential Class 1 break locations in the spent fuel pool, a break in this suction line could prevent safety class makeup from the PCCWST from being supplied to the SFP.

2. The second scenario considered is a break during refuelling outage of the DN 200 mm (8 inch nominal) Class 1 CLP piping connection. This is the largest line potentially connected to the SFP that could drain the SFP and leads to the fastest drain time to the [ ] elevation. It is noted that this break is postulated during refuelling with the CLP gate open and the entire core relocated to the spent fuel pool, thus maximizing the heat load. This is the fastest draindown scenario, but with the core in the spent fuel pool, the PCCWST is available to provide Class 1 makeup, as long as sufficient time for operator action can be shown.

3. The third scenario considered is a break during normal operation of the DN 150 mm (6 inch nominal) class 1 FTC drain line. This scenario presents a slightly slower drain time than the CLP line break discussed above and a significantly lower decay heat in the pool (since assemblies have been returned to the core), but this event is postulated during normal operation. In this mode of operation, PCCWST cannot be aligned to provide makeup to the SFP without breaking a Limiting Condition for Operation (LCO) required by Technical Specifications.

The analyses of these scenarios demonstrate that the 72 hour claim is met and that adequate time is provided for the operator to initiate Class 1 mitigation features.

9.7.2.4.2 Analyses of Consequences and Frequency of the Event

The failure of Class 1 lines is considered an infrequent event and an Incredibility of Failure (IoF) argument could be made for these lines. However, the AP1000 design is such to provide significant protection against these postulated events, with sufficient Class 1 makeup sources to ensure an extended grace period before additional actions are required. Hence, to simplify the licensing and operational impact an IoF argument is not made for these lines; instead analyses are performed to demonstrate acceptable consequences for these postulated events.

9.7.2.4.3 Analysis Method

The analysis methodology outlined in Section 9.7.2.3.6 was used for the analysis of these postulated breaks. For additional conservatism, all breaks are assumed to drain the SFP instantaneously to the postulated break level. This allows simplification of the analysis model, but it is a significant conservatism added to the analysis, as only water below the draindown elevation is credited in the transient. Furthermore, taking no credit for the steel and concrete heat sinks, the assumption of a minimum time (15 days) following shutdown, and no credit for the draindown time, all have a significant effect on the calculated time. The assumptions and analysis can be found in Reference 9.7-3.

It would be possible to develop a more realistic evaluation model and show significant additional margin, but given the extended grace periods demonstrated in the following sections, this is not considered necessary.

9.7.2.4.4 Analysis Results

The times until fuel uncovery are discussed below for the limiting cases identified in Section 9.7.2.4.1.

9.7.2.4.5 Postulated Breaks in Class 1 RNS Line

The frequency of an RNS break has been calculated at less than 1.0E-05/yr. in Reference 9.7-8, which is outside the design basis (more frequent than 1.0E-05 per year, Reference 9.7-2). This frequency was determined by measuring the length of pipe from the pool boundary to the first isolation valve and multiplying the length by the frequency of the pipe breaking per foot of pipe. This estimate ignores conservatisms that exist with respect to the operating pressure being ~1% of the design capability of the installed piping and there being very little thermal transients.

A postulated break in the Class 1 RNS suction line during an emergency full core offload will not uncover the fuel for at least 24 hours without any operator action. As expected, if the break occurs during a full core offload, during the beginning of a cycle, or during the middle of a cycle, even more time is required to boil-off the SFP water.

Table 9.7.2-2 provides the time available for the operator actions to align the Class 1 makeup sources to the Spent Fuel Pool. The break of the RNS lines means the PCCWST water cannot be supplied via the Class 1 RNS line; however, Class 1 makeup from the PCCWST can be supplied via the non-Class 1 SFP spray lines. This provides a passive means of supplying makeup to the SFP even if the Class 1 path has been broken. Although the SFP spray lines are not Class 1, given the frequency on the order of 1.0E-05 breaks/year, this capability is sufficient. In addition, with a minimum of 24 hours the operator has to align the passive Class 1 makeup source, the 72 hour requirement for Class 1 is satisfied in this case. In addition to the Class 1 passive makeup, makeup water can be provided through the spray lines by the PCCAWST (powered by ancillary diesel), FPS water tanks (powered by FPS diesel), and an outside water source through the flanged connection (powered by portable, site-specific pump). These diverse paths provide additional layers of defence against fuel uncovery and can be used to extend the 72 hours to at least 7 days.

Postulated Breaks in DN 200 mm (8 inch nominal) CLP Line During Refuelling

A postulated break in the DN 200 mm (8 inch) CLP line has the potential to drain the SFP to the bottom of the gate [ ]. In order for this to occur, the break would have to be located in a portion of the pipe between the CLP pool boundary and the first isolation valve. In addition, the CLP gate would have to be opened, which only occurs when the decay heat load in the SFP is greater than 5.0 MW. Taking into account the conditions necessary for the break to drain the pool (the amount of time in a cycle the gate is open and the length of pipe before the isolation valve), the frequency of the DN 200 mm CLP line breaking is well below the design basis cut-off.

Table 9.7.2-3 shows the time available for operator action assuming a break in the DN 200 mm CLP line that drains the pool to gate elevation occurs, Table 9.7.2-3 shows the time available for operator action.

In this break scenario, it is assumed that the break occurs at 150 hours after plant shutdown, when the full core of 157 assemblies has been offloaded from the reactor vessel and stored in the SFP. This maximises the heat load in the pool, but since the decay heat in the reactor for this scenario will be less than 7.0 MW (since the fuel is not in the reactor vessel but in the spent fuel pool), makeup water from the PCCWST is available for makeup to the faulted SFP. As shown in Table 9.7.2-3, over two hours, calculated with very conservative assumptions, are available before the operator needs to align the class 1 PCCWST water makeup, which is then sufficient to maintain the fuel covered for an extended period of time, well above 72 hours. Additional non-Class 1 makeup sources are also available, but this analysis shows that the initial inventory and the available makeup from Class 1 sources are sufficient to maintain the fuel covered for 72 hours.

Postulated Break in DN 150 mm (6 inch nominal) FTC Drain Line

The frequency of a break in the DN 150 mm FTC drain line, taking into account the length of pipe that would cause the pool to drain, is well below the design basis cut-off (Reference 9.7-8). Due to the fact that the FTC gate is normally open, the frequency of the break is greater than the DN 200 mm CLP line break; however, more time is available for the operator to initiate makeup.

The break analysed in Table 9.7.2-4 is assumed to occur during normal operation of the plant (but at the beginning of a new cycle to maximise the heat load in the pool); 360 hours after plant shutdown, while 69 freshly discharged assemblies reside in the SFP. The CLP gate is assumed to be closed, while the FTC gate is assumed to be open, as this is expected during

normal operation. In this case, the most limiting postulated break is the double ended guillotine rupture of the FTC drain line. Assuming the operator was not able to isolate the break from the SFP by closing the FTC gate, the water level would lower to the bottom of the gate [ ]. The operator would first try to align any of the non-Class 1 sources described in Section 9.7.2.3.4.

Should these steps prove unsuccessful, the Class 1 makeup from the PCCWST would be available. However, use of this makeup source would result in a violation of Technical Specification LCO 3.6.6. This LCO states that the operator would trip the reactor and bring the reactor to a safe shutdown conditions, according to the required steps.

The results in Table 9.7.2-4 show that, even for this limiting case, the initial pool inventory is sufficient to prevent fuel uncovery for over 4 hours, without reliance on any additional water source. It is noted that this case is analysed at the beginning of a cycle, and thus the calculated time to uncovery represents a minimum value during the fuel cycle.

During this time, if non-Class 1 makeup water sources are available, the operator would try to establish stable makeup from the non-Class 1 sources. However, if non-Class 1 makeup water sources are not available, the operator would proceed to shutdown the reactor and maintain it in a safe state using Class 1 and Class 2 systems, and provide makeup to the Spent Fuel Pool from the available Class 1 makeup water sources. The Class 1 makeup water sources ensure sufficient makeup water is available to protect the fuel in the Spent Fuel Pool for at least 72 hours. These sources are the normally isolated Cask Washdown Pit, Cask Loading Pit, and PCCWST. This extends the grace period provided by Class 1 sources only to over 72 hours.

Loss of Water in Refuelling Cavity due to CLP Line Break or FTC Drain Line Break

It is noted that when the fuel transfer tube is open during refuelling operations, postulated breaks in the FTC/SFP/CLP piping will result in the loss of some water from the Refuelling Cavity inside containment. The non-seismic portions of the SFS are isolated from the refuelling cavity on Low-2 Class A-1 spent fuel pool level sensors to preclude a decrease in Refuelling Cavity level below [ ]. Following such breaks, the operator has sufficient time to restore isolation of the Refuelling Cavity from the FTC/SFP/CLP by closing the manual gate valve on the FTC side of the fuel transfer tube, prior to significant heatup and subsequent boiling of the SFP water.

For postulated breaks in the Class 1 DN 150 mm (6 inch nominal) FTC drain line or the DN 200 mm (8 inch nominal) CLP line (if the CLP gate is open), the Refuelling Cavity water will transfer to the FTC as the FTC/SFP/CLP water level decreases. Since the fuel transfer tube is very large (76 cm (30 inch) in diameter) compared to the postulated breaks, the Refuelling Cavity water level will closely follow the decreasing water level in the FTC/SFP/CLP, and the rate of water loss from the entire FTC/SFP/CLP/Refuelling Cavity will be limited by the flow from the broken FTC or CLP line. The water level in the refuelling cavity decreases at a slower rate than it would for the postulated break of an RNS line outside containment described in Section 9.8.5.3. This is due to the large combined surface area of the FTC/SFP/CLP/Refuelling Cavity.

The loss of water from inside containment to the FTC, which would prolong the draindown of the SFP, is not considered in the SFP boiloff calculations. The boiloff calculations assume a more conservative scenario in which the water in the pool instantaneously drains to the gate elevation. The impact of these breaks on the ability to maintain cooling for fuel in the reactor vessel containment has not been analysed since they are bounded by the postulated break of an RNS line outside containment, described in Section 9.8.5.3.

The isolation on Low-2 spent fuel pool level automatically terminates the loss of water from the refuelling cavity; this bounds breaks in the non-seismic spent fuel pool suction line.

9.7.2.4.6 Post Fault Recovery

Recovery following these unlikely events is more complex than the recovery from more likely loss of cooling faults (as discussed in Section 9.7.2.3.7, and for which recovery is discussed in Section 9.7.2.3.8) due to the need to terminate the originating cause of the event. Once the break is isolated, the recovery is completed with the same actions described in Section 9.7.2.3.8. Additional details on operations to restore cooling are provided in Reference 9.7-4.

9.7.2.4.7 Conclusions

Even for postulated, infrequent breaks in Class 1 lines, sufficient water inventory and makeup are available to ensure at least 72 hours before any potential fuel uncovery. Refer to the additional conclusions stated in Section 9.7.2.3.12.

9.7.3 References

9.7-1 ONR "Safety Assessment Principles for Nuclear Facilities," Rev. 0, Office of Nuclear Regulation, 2014.

9.7-2 HSE T/AST/006, Issue 3, Technical Assessment Guide, "Deterministic Safety Analysis and the Use of Engineering Principles in Safety Assessment," Health and Safety Executive, July 2000.

9.7-3 Westinghouse Report UKP-SFS-M3C-012, Rev. B, "AP1000 Additional Investigation of Spent Fuel Pool Heatup, Boiloff and Emergency Makeup on Loss of Cooling to Support UK GDA Safety Case," September 2016.

9.7-4 Westinghouse Report UKP-GW-GL-077, Rev. 2, "AP1000® Spent Fuel Pool Faults," November 2016.

9.7-5 Westinghouse Report UKP-GW-GL-081, Rev. 0, "AP1000 Spent Fuel Chemistry," January 2011.

9.7-6 Westinghouse Report APP-SSAR-GSC-182, Rev. 2, "AP1000 Spent Fuel Pool Boiling Radiological Doses for the Advanced First Core," April 2016.

9.7-7 Westinghouse Report UKP-GW-GL-743, Rev. 1, "AP1000 PRA Spent Fuel Evaluation," January 2010.

9.7-8 Westinghouse Report UKP-PRA-GSC-002, Rev. A, "Spent Fuel Pool Boiling Frequency for the UK AP1000 PlantTM," January 2011.

9.7-9 NUREG/CR-6928, "Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants," Nuclear Regulatory Commission, February 2007.

9.7-10 Westinghouse Report APP-SFS-M3C-012, Rev. 5, "AP1000 Spent Fuel Pool Heatup, Boiloff, and Emergency Makeup on Loss of Cooling," April 2014.

9.7-11 Westinghouse Report UKP-FHS-M3R-001, Rev. A, "Report on Limiting Conditions for Manual Fuel Movement and ALARP Assessment," March 2016.

9.7-12 European Commission Report EUR 15615 EN, "Realistic Methods for Calculating the Release of Radioactivity following Steam Generator Tube Rupture Faults (A Consensus Document)," L.C.M. Dutton, et al, 1994.

9.7-13 Westinghouse Report APP-GW-GLR-029, Rev. 4, "AP1000 Spent Fuel Storage Racks Criticality Analysis," January 2013.

9.7-14 Westinghouse Report APP-FS06-N1C-001, Rev. 0, "AP1000 In-Containment Rack Criticality Analysis," February 2010.

9.7-15 Westinghouse Report APP-GW-GLR-030, Rev. 0, "New Fuel Storage Rack Criticality Analysis," May 2006.

Table 9.7-1. Not Used

Table 9.7.2-1. Complete Loss of SFP Cooling – SFP Boil-off Time to Top of Fuel (hrs)

Complete Loss of Spent Fuel Pool Cooling – SFP Boil-off Time to the Top of Fuel (hrs) (without additional Class 1 makeup)				
	SFP Contains Maximum Number of Assemblies Including:			
Event – Loss of all SFP Cooling with	**a) Emergency Full Core Offload**	**b) Refuelling with Full Core Offloaded**	**c) Beginning of Cycle (after 88 assemblies returned to core)**	**d) Middle of Cycle (after 88 assemblies returned to core)**
Case 1: No Pipe Breaks	>36 hours	>48 hours	> 72 hours	> 96 hours
Case 2: Class 2 SFS Suction Piping Break	>24 hours	>36 hours	> 72 hours	> 72 hours

Table 9.7.2-2. Time to Potential Fuel Uncovery Following a Postulated Break of the Class 1 SFP to RNS Pump SFP Cooling Line

	Emergency Full Core Offload	Refuelling with Full Core Offload in SFP	Beginning of Cycle (after 88 Assemblies Returned to Core)	Middle of Cycle (after 88 Assemblies Returned to Core)
Class 1 RNS Suction Piping Break	>24 hours	>24 hours	>48 hours	>72 hours

Table 9.7.2-3. Time to Potential Fuel Uncovery Following a Postulated Break in the Class 1 CLP Piping Connection to the RNS During a Refuelling Outage

Time to the Onset of Boiling (hrs)	> 1
Time to Boiloff to Top of Active Fuel [ ] Elevation (hrs)	> 2

Table 9.7.2-4. Time to Potential Fuel Uncovery Following a Postulated Break in the Class 1 FTC Drain Line Immediately after a Refuelling Outage

Time to the Onset of Boiling (hrs)	> 2
Time to Boiloff to Top of Active Fuel [ ] Elevation (hrs)	> 4

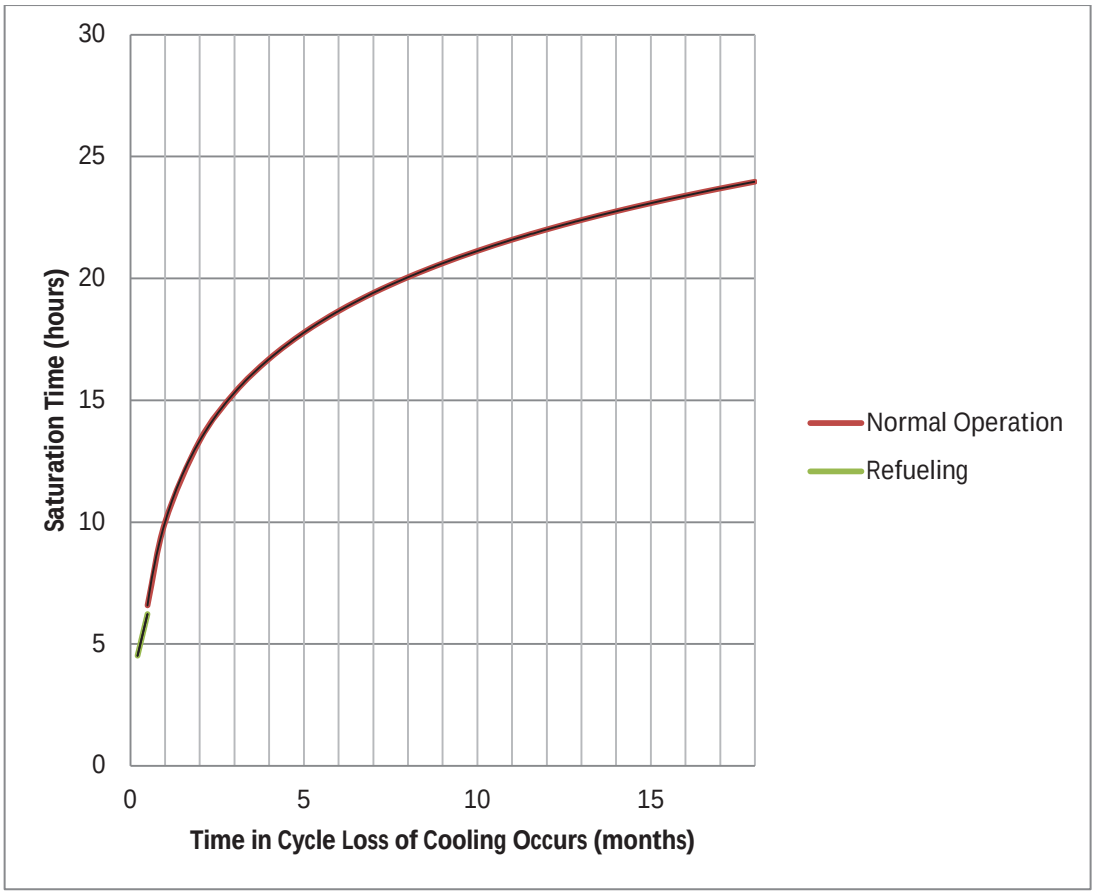


Figure 9.7.2-1. Time to Onset of SFP Water Boiling for Loss of Cooling Events (no break)

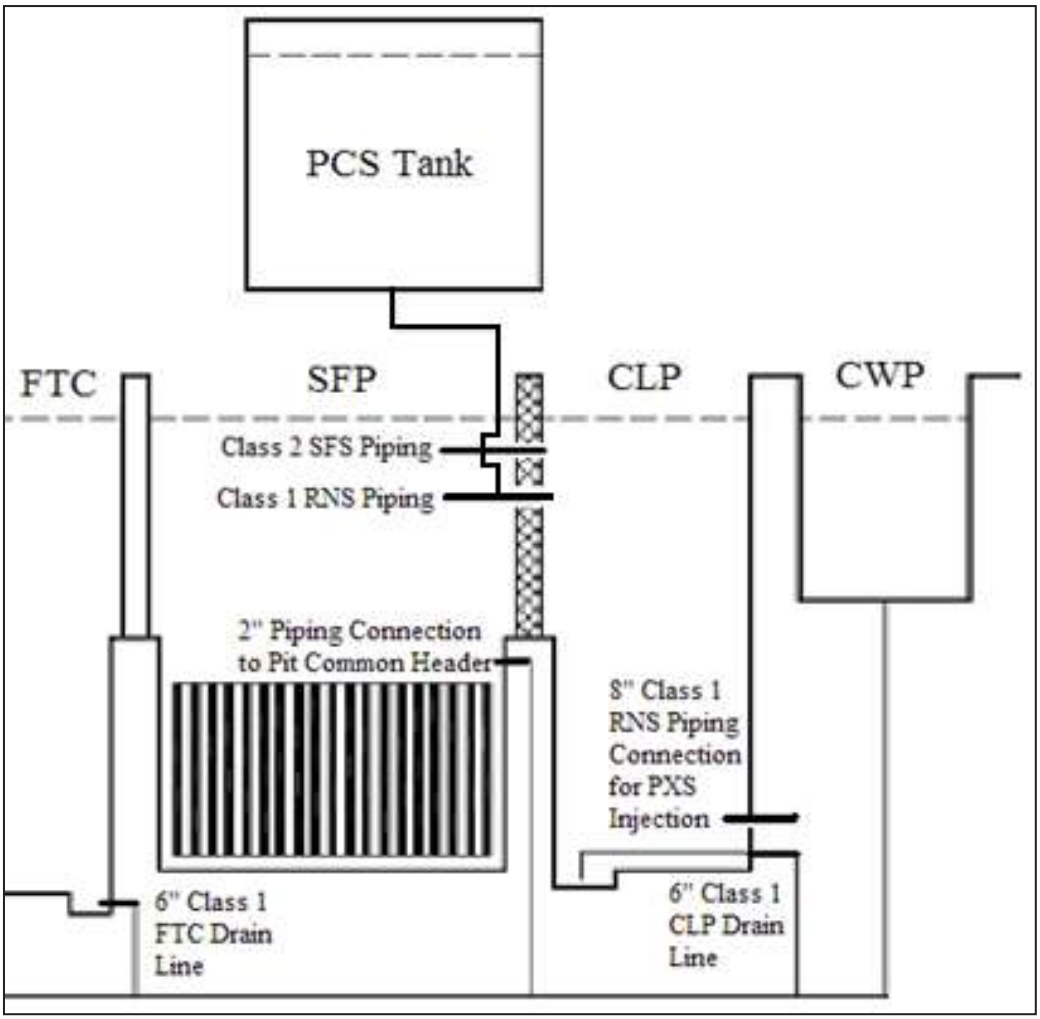


Figure 9.7.2-2. Sketch of SFP Class 1 Piping Connection

9.8 Shutdown Faults

9.8.1 Introduction and Overview

Table 9.8.1-1 provides a summary description of the AP1000 operating modes. The discussion in this Section is focused on Shutdown and Refuelling Modes, which are Modes 4, 5 and 6.

Westinghouse has considered shutdown operations in the design of the AP1000 nuclear power plant. The AP1000 defence-in-depth design philosophy to provide normally operating Class 2 active systems and passive Class 1 safety systems gives the AP1000 a greater degree of safety during shutdown operations as well as during normal power operation when compared to currently operating plants. This section presents and evaluates the AP1000 design features to address the issues of shutdown risk and shutdown safety. Potential faults during shutdown modes were evaluated to determine whether they are potentially limiting. The potentially limiting faults were analysed using design basis computer codes and methods, only crediting mitigation by A-1 features.

Potential faults in shutdown modes have been identified. The process of identifying potential faults in shutdown mode considers three different aspects:

1. Screening of at-power faults that are also applicable in shutdown modes
2. Potential faults that are specific to shutdown modes
3. Other faults that are generic to refuelling operation

One of the key aspects of shutdown evaluations is that, while shutdown events are typically covered by the analysis of at-power events, which are in general more limiting and designed to cover a full range of operating conditions from 0 to 100% power, different Class 1 safety systems are not available once certain shutdown conditions are reached. Therefore, an evaluation of shutdown events needs to be accompanied by a detailed assessment of the systems available and the procedures available.

To achieve this objective, the content of this section is therefore organised as follows:

- Section 9.8.2 – potential faults for each identified category are identified and organised.
- Section 9.8.3 provides a detailed description of systems designed to operate during shutdown conditions and for shutdown operations.

The following Sections are then dedicated to the documentation of the fault studies for shutdown faults:

- Section 9.8.4 is dedicated to the analysis of faults identified as at-power faults but which can also occur during shutdown.
- Section 9.8.5 covers potential faults that are specific to shutdown modes.

As is demonstrated in the following sections, for each of these groups of faults the AP1000 design provides multiple lines of defence, both through the Class 2 active systems and through the Class 1 passive systems. In the AP1000 design the fundamental function of the Class 2 systems is to reliably support normal operation and minimise the demand on the passive systems. The Class 1 systems provide the primary means of ensuring the safety

functions. These systems will not be used for normal operation of the plant. The combination of active defence in depth (Class 2) and passive features (Class 1) provides a robust design with multiple lines of defence.

Reliance on operator actions during shutdown modes is only credited when there is indication from Class 1 instruments and when there is at least 30 minutes for the operator to take action. These actions are specifically addressed in Sections 9.8.4 to 9.8.5 as part of the assessment of each potential fault identified.

9.8.2 Potential Faults during Shutdown Modes

The following three-step approach has been taken to ensure a rigorous evaluation of shutdown faults:

1. First, all at-power events identified in the fault schedule (Appendix 8A) are evaluated to (1) identify whether they are applicable to shutdown modes, as discussed in Section 9.8.1 and shown in Table 8A-2; (2) identify if applicable, what the plant response to the event will be, compared against the at-power response, and especially considering the availability of different Class 1 equipment credited in the accident mitigation during shutdown conditions; (3) provide a design basis analysis for the event. In most cases, this analysis is provided by already completed analyses of at-power events, but in some cases shutdown specific analyses may be required. Also, in some cases, multiple analyses, covering different shutdown modes, may be required due to different availability of Class 1 equipment. In these cases, separate cases are presented in the discussion covering different modes.

    a. A critical consideration for the evaluation of shutdown faults is the availability of different Class 1 engineered safety features during the different operating modes, as well as the plant specific design features designed specifically to address shutdown modes. Section 9.8.3 provides a summary description of AP1000 key design features relative to shutdown modes. Additionally, Table 9.8.3-1 provides a summary of the availability of relevant Class 1 systems over different shutdown modes.

    b. Section 1 of Table 8A-2 includes at-power design basis faults, and they have been re-evaluated for shutdown mode considerations.

    c. Section 9.8.4 provides a discussion and assessment of each fault in different shutdown modes. For each, reference to the fault schedule ID (Table 8A-2) for each fault is also provided.

2. During shutdown modes, the RNS is aligned to provide heat removal from the reactor coolant system. As such, potential faults specific to this mode of operation need to be identified and addressed.

    a. Section 2 of Table 8A-2 includes potential faults associated with RNS operation that are included in this assessment. It is noted that this table identifies all modes over which the fault is relevant, but mode-specific assessment may be required to consider the availability of different Class 1 equipment.

    b. Section 9.8.5 provides a discussion and assessment of each fault identified,and for each, reference to the fault schedule ID is provided.

3. Finally, additional faults associated with refuelling (Mode 6) are identified in Sections 2 and 3 of Table 8A-2.

    a. All of these faults have either been screened out (see Appendix 8A) or are discussed elsewhere in this chapter, as identified in Appendix 8A.

9.8.3 AP1000 Design Features to Address Shutdown Safety

The AP1000 has incorporated design features that address issues related to shutdown operations. This section provides a discussion of the RCS design features that are incorporated to address shutdown operations or that are important to minimizing the risk to plant safety during shutdown.

Table 9.8.3-1 provides a summary of the availability of Class 1 passive core cooling equipment during different operational modes.

Westinghouse has considered shutdown modes, shutdown alignments, and industry issues related to shutdown in the design of the AP1000 Class 1 and Class 2 systems designed to operate or be available during shutdown. This section provides descriptions of the important systems designed to operate during shutdown and includes specific design features that have been incorporated for shutdown operations with a discussion of their operating modes or alignment during shutdown.

In this section, references are made to the various AP1000 plant operating modes. The AP1000 plant operating modes are defined in Table 9.8.1-1. The mode definitions for the AP1000 design are similar to those of current Westinghouse PWRs, with the difference being the definition of Mode 4, safe shutdown.

In the AP1000, Mode 4 has been redefined as safe shutdown and corresponds to the range of RCS temperature between 215.6°C (420°F) and 93.3°C (200°F). The upper temperature limit corresponds to the RCS temperature that can be achieved by the passive Class 1 systems 36 hours after shutdown. The ability of the passive Class 1 systems to achieve Mode 4 within 36 hours is shown in Section 9C.3.1.1.1.

9.8.3.1 RCS Design Features for Shutdown

The AP1000 design has incorporated design features that address issues related to shutdown operations. This section provides a discussion of the RCS design features that are incorporated to address shutdown operations or that are important to minimizing the risk to plant safety during shutdown.

9.8.3.1.1 Loop Piping Offset

The RCS hot legs and cold legs are vertically offset. This permits draining of the steam generators for nozzle dam insertion with the hot leg level much higher than in traditional designs. The RCS must be drained to a level sufficient to provide a vent path from the pressuriser to the steam generators. This loop piping offset also allows an RCP to be replaced without removing the full core.

9.8.3.1.2 RCS Instrumentation Designed to Support Shutdown Operations

Instrumentation is provided to monitor the RCS process parameters as required by the PLS and PMS as discussed in Chapter 19. This section describes RCS instrumentation designed to accommodate shutdown operations.

9.8.3.1.2.1 RCS Hot Leg Level

There are four Class 1 RCS hot leg level channels, two located in each hot leg. These level indicators are provided primarily to monitor the RCS water level during mid-loop operation following shutdown operations. Each has a level tap on the bottom of the hot leg, and another tap on the top of the hot leg close to the steam generator at the high point of the tubing run. The level tap for the instrument in the hot leg with the RNS step-nozzle suction line connection is between the reactor vessel and the step-nozzle. Figure 9.8.2-1 shows a simplified sketch of the RCS level instruments.

These channels provide Class 1 signals for the following protection functions:

- Isolation of letdown on low level on a two-out-of-four basis.
- Actuation of fourth-stage ADS valves on low (empty) hot leg level on a two-out-of-four basis. Actuation of fourth-stage ADS causes actuation of IRWST injection.

These functions protect the plant during shutdown operations. Letdown isolation assists the operators when draining the RCS to a mid-loop level. If the operators fail to isolate letdown, these channels send a signal to close the letdown valves and stop the draining process.

In the event of a loss of the RNS during shutdown, coolant inventory could be boiled away. When the hot leg water level indicates that the loops are empty, IRWST injection and fourth-stage ADS are actuated 25 minutes after receipt of the empty hot leg level signal. See Section 9.8.5.3.2.2.

These channels also provide signals to the letdown flow control valve to control the drain rate of the RCS via the letdown line during the transition to mid-loop operation. When the hot legs are full, the drain rate can proceed at a high level. As the water level is reduced to the hot legs, the drain rate is automatically decreased to a rate of approximately 4.5 m^3/hr (20 gpm).

These channels are also used to generate the alarms on low hot leg water level. The alarm setpoints are selected to give the operator sufficient time to take manual actions that would prevent the automatic actuation described previously. Indication of these channels is available in the main control room. This variable is used by the operator to monitor the status of RCS inventory following an accident and is, therefore, classified as a post-accident monitoring system (PAMS) variable.

The accuracy and response time of the hot leg level instruments are consistent with the standard ESF actuation discussed in Section 19.2. Concerns related to potential problems of noncondensable gases in the hot leg level instrument lines that have been raised in industry have been addressed in the layout of the instrument lines. In addition, as the hot leg level instruments are provided primarily for shutdown operations, off-gassing due to sudden depressurisation of the RCS in shutdown modes is not a concern.

In the AP1000 design, draining of the RCS to mid-loop conditions is achieved in a controlled manner as discussed in Section 9.8.3.1.4. Due to the low RCS drain rate, and the RCS step-nozzle as discussed in Section 9.8.3.1.3, the amount of air-entrainment, and therefore RCS level perturbation during mid-loop, is negligible. Draining of the RCS is conducted in a quasi-steady-state, and the reliability of an accurate level reading is high.

9.8.3.1.2.2 Pressuriser Level

A fifth, non Class-1 (GNS), independent pressuriser level transmitter, calibrated for low temperature conditions, provides water level indication during startup, shutdown, and refuelling operations in the main control room and in the remote shutdown workstation. The upper level tap is connected to an ADS valve inlet header above the top of the pressuriser. The lower level tap is connected to the bottom of the hot leg. This provides level indication for the entire pressuriser and a continuous reading as the level in the pressuriser decreases to mid-loop levels during shutdown operations

9.8.3.1.2.3 RCS Hot Leg Wide-Range Temperatures

The RCS contains two Class 1 thermowell-mounted hot leg wide-range temperature detectors, one in each hot leg. The detectors' indication of RCS Hot Leg temperature below 93ºC (200°F) assures that inadvertent RCS venting does not occur during Reactor Head Vent Valve in-service testing during shutdown conditions. The orientation of the resistance temperature detectors enables measurement of the reactor coolant fluid in the hot leg when in reduced inventory conditions. Their range is selected to accommodate the low RCS temperatures that can be attained during shutdown. In addition, at least two incore thermocouple channels are available to measure the core exit temperature during mid-loop RNS operation. These two thermocouple channels are associated with separate electrical divisions.

9.8.3.1.2.4 Pressuriser Surge Line Temperatures

There are three Class 2 temperature detectors located on the RCS pressuriser surge line. These instruments monitor the pressuriser surge line fluid temperature during plant normal operations to detect thermal stratification in the surge line. Two of the temperature detectors are on a moderately sloped run approximately midway between the RCS hot leg and the pressuriser. One detector is on the bottom of the pipe and the other detector is on the top. The third detector is located on the pressuriser surge line close to the pressuriser nozzle. This detector is used to monitor cold water insurges to the pressuriser during transient operations.

The temperature is monitored at the three locations using strap-on resistance temperature detectors. Temperature indication is provided in the main control room. One low-temperature alarm is provided to alert the operator of thermal stratification in the surge line. This alarm is associated with the detector on the bottom of the pipe.

During shutdown operations, this temperature instrumentation will be monitored to detect possible surge line stratification. If stratification is detected, the operators can increase spray flow to increase the outsurge from the pressuriser and reduce stratification in the surge line.

9.8.3.1.3 Step Nozzle Connection

The AP1000 RNS uses a step-nozzle connection to the RCS hot leg. The step-nozzle connection has two effects on mid-loop operation. One effect is to lower the RCS hot leg level at which a vortex occurs in the residual heat removal pump suction line due to the lower fluid velocity in the hot leg nozzle. This increases the margin from the nominal mid-loop level to the level where air entrainment into the pump suction begins.

Another effect of the step-nozzle is that, if a vortex should occur, the maximum air entrainment into the pump suction as shown experimentally will be no greater than 5 percent (Reference 9.8-1). The RNS pumps can operate with 5% air-entrainment. As discussed in NUREG-0897 (Reference 9.8-2), low levels of air ingestion can be tolerated, and a pump inlet void fraction of 5% has been shown experimentally to reduce the pump head less than 15%. At this level of degradation, the RNS pumps would maintain decay heat removal. The

step-nozzle thereby precludes air binding of the pump and will allow for RNS pump operation with low water levels in the hot leg.

9.8.3.1.4 Improved RCS Draindown Method

During cooldown operations, the RCS water level is drained to a mid-loop level to permit steam generator draining and maintenance activities. The AP1000 has improved the reliability of draindown operations by incorporating a dedicated drain path, controlled in the main control room, to be used to reduce the water level in the RCS. In current plants, various drain paths can be used either locally or remotely from the control room. These drain paths include the Class 1 residual heat removal system, loop drain valves, and letdown. The result is that draining of the RCS can be difficult to control, and perturbations in water level can occur due to inadvertent system manipulations of which the operators are not always aware.

The AP1000 RCS drain path is via the CVS letdown line from the RNS cross-connect provided to maintain full RCS purification flow during shutdown. The letdown line flow control valve controls the letdown rate, which controls the RCS draindown rate. At the appropriate time during the cooldown, the operator initiates the draindown by placing the CVS letdown control valve into a refuelling draindown mode. At this time, the makeup pumps are turned off and the letdown flow control valve controls the drain rate to the liquid radwaste system at the initial maximum rate of approximately 22.7 m^3/hr (100 gpm). The rate is reduced once the level in the RCS is to the top of the hot leg. The letdown rate is manually controlled based upon the difference in flow instruments readings in the CVS letdown line and injection line. The letdown flow control valve as well as the letdown line containment isolation valve receives a signal to automatically close once the appropriate level is attained. Class 1 alarms actuate in the control room if the RCS level falls below the automatic letdown valve closure setpoint so that the operator is alerted to manually isolate the letdown line. Furthermore, an automatic isolation of the letdown line is actuated on low hot leg level via the Class 1 PMS. This draindown method provides a reliable means of attaining mid-loop conditions.

9.8.3.1.5 ADS Valves

The ADS stage 1, 2, and 3 valves, connected to the top of the pressuriser, are open whenever the CMTs are blocked during shutdown conditions while the reactor vessel upper internals are in place. This provides a vent path to preclude pressurisation of the RCS during shutdown conditions if decay heat removal is lost. This also allows the IRWST to automatically provide injection flow if it is actuated on a loss of decay heat removal. In addition, two of the four ADS fourth-stage valves are required to be available during reduced inventory operations to preclude surge line flooding following a loss of the RNS.

9.8.3.1.6 Steam Generator Channel Head

The AP1000 steam generator is a vertical-shell U-tube evaporator with integral moisture separating equipment. The generator is discussed in Appendix 20C.

On the primary side, the reactor coolant flow enters the primary chamber via the hot leg nozzle. The lower portion of the primary chamber is hemispherical and merges into a cylindrical portion, which mates to the tubesheet. This arrangement provides enhanced access to all tubes, including those at the periphery of the bundle, with robotics equipment. This feature enhances the ability to inspect, replace, and repair portions of the AP1000 unit compared to the more hemispherical primary chamber of earlier designs. The channel head is divided into inlet and outlet chambers by a vertical divider plate extending from the apex of the head to the tubesheet.

The reactor coolant enters the inverted U-tubes, transferring heat to the secondary side during its traverse, and returns to the cold leg side of the primary chamber. The flow exits the steam generator via two cold leg nozzles to which the reactor coolant pumps are directly attached.

The AP1000 steam generator channel head has provisions to drain the head. For minimizing deposits of radioactive corrosion products on the channel head surfaces and for enhancing the decontamination of these surfaces, the channel head cladding is machined or electropolished for a smooth surface.

The steam generator is equipped with permanently mounted nozzle dam brackets, which are designed to support nozzle dams during refuelling operations. The design pressure of the nozzle dam bracket and nozzle dam is selected to withstand the RCS pressures that can occur during a loss of shutdown cooling. The nozzle dam design pressure is at least 0.345 MPa abs (50 psia).

The AP1000 nozzle dams can be installed with the hot leg water level at the nominal water level for mid-loop operations. The nozzle dams can be inserted via the steam generator manway. The ADS valves connected to the pressuriser are open during all reduced inventory operations including nozzle dam installation, and provide a vent path to preclude pressurisation of the reactor coolant system following a loss of decay heat removal when the nozzle dams are installed.

9.8.3.2 PXS Design Features for Shutdown

A significant improvement in shutdown safety for the AP1000 design is the availability of a dedicated Class 1 system that can be automatically or manually actuated in response to an accident that can occur during shutdown. In current plants, the safety systems that mitigate the consequences of an accident are also the operating systems that are used for decay heat removal. In the AP1000 design, Class 2 active systems provide the first level of defence, while the passive Class 1 systems are available during shutdown modes to mitigate the consequences of an accident. This design approach results in a significant improvement in the AP1000 plant shutdown risk.

9.8.3.2.1 Core Makeup Tanks

The CMTs provide RCS makeup. During shutdown, the CMTs are available in Modes 3, 4, and 5, until the RCS pressure boundary is open and the pressuriser water level is reduced. During power operation, the CMTs are automatically actuated on various signals including a safeguards actuation signal (low RCS pressure, low RCS temperature, low steam line pressure, and high containment pressure) and on low pressuriser water level. See Chapter 19 for a description of the AP1000 PMS actuation logic. In shutdown modes, portions of the safeguards actuation signal are disabled to allow the RCS to be cooled and depressurised for shutdown. For instance, the low RCS pressure and temperature, and low steam line pressure signals are blocked in Mode 3 prior to cooling and depressurising the RCS. Therefore, during shutdown Modes 3, 4, and 5, the primary signal that actuates the CMTs due to a loss of inventory is the pressuriser level signal. In Mode 5, with the RCS open (in preparation for reduced inventory operations), the low pressuriser level signal is blocked prior to draining the pressuriser. Therefore, in Mode 5 with the RCS open, the CMTs are not required to be available and the RCS makeup function is provided by the IRWST.

The CMTs also provide an emergency boration function for accidents such as steam line breaks. However, the signals that provide the primary protection for this function (low steam line pressure, low RCS pressure, and low RCS temperature) are blocked in Mode 3 as discussed above. Prior to blocking these signals in Mode 3, the Technical Specifications

require that the RCS be sufficiently borated. For these events, the pressuriser level signal provides automatic actuation of the CMTs for a steam line break that might occur due to the RCS shrinkage that would occur.

9.8.3.2.2 Accumulators

The PXS accumulators provide safety injection following a LOCA. In Mode 3, the accumulators must be isolated to prevent their operation when the RCS pressure is reduced to below the set pressure of their contained nitrogen gas. The accumulator isolation valves are closed when the RCS pressure is reduced to 6.895 MPa gauge (1000 psig) to block their injection when the RCS pressure is reduced to below the normal accumulator pressure.

9.8.3.2.3 In-containment Refuelling Water Storage Tank

The IRWST provides long-term RCS makeup. During shutdown, the IRWST is available until Mode 6, when the reactor vessel upper internals are removed and the refuelling cavity flooded. At that time, the IRWST is not required, due to the large heat capacity of the water in the refuelling cavity.

The IRWST injection paths are actuated on a low-6 CMT water level. This signal is available in shutdown Modes 3, 4, and 5, with the RCS intact. When the RCS is open to transition to reduced inventory operations, the CMT actuation logic on low pressuriser level is removed, and the CMTs can be taken out of service. For these modes, automatic actuation of the IRWST can be initiated (on a two-out-of-two basis) on low hot leg level.

9.8.3.2.4 Passive Residual Heat Removal Heat Exchanger

The PRHR HX provides decay heat removal during power operation and is required to be available in shutdown Modes 3, 4, and 5, until the RCS is open. In these modes, the PRHR HX provides a passive decay heat removal path. It is automatically actuated on a CMT actuation signal, which would eventually be generated on a loss of shutdown decay heat removal, as shown in the analysis provided in Section 9.8.4. In modes with the RCS open (portions of Mode 5 and Mode 6), decay heat removal is provided by “feeding” water from the IRWST and “bleeding” steam from the ADS.

9.8.3.2.5 Reduced Challenges to Low-Temperature Overpressure Events

Another design feature of the PXS that reduces challenges to shutdown safety is the elimination of high-head safety injection pumps in causing low temperature overpressure events. In current plants, during water solid operations that may be necessary to perform shutdown maintenance, the high-head safety injection pumps are a major source of cold overpressure events. To address this, plants are required to lock out safety injection pumps to prevent them from inadvertently causing a cold overpressure event. This eliminates a potential source of safety injection for a loss of inventory event that could occur at shutdown. With the AP1000 PXS, the CMTs are not pressurised above RCS pressure and are, therefore, not capable of causing a cold overpressure event. Therefore, they are not isolated until the pressuriser is drained for mid-loop. Low-temperature overpressure events are discussed in Section 9.8.4.5.1.

9.8.3.2.6 Containment Recirculation Screens

The PXS containment recirculation screens may have to function in the longer-term during a shutdown accident that results in ADS operation. Effective screen design, plant layout, and other factors prevent clogging of these screens by debris during such accident operations.

- Two very large interconnected screens are provided.
- A significant delay is provided between the accident/ADS stage opening and the initiation of recirculation (at least 2 hours).
- Deep flood up levels are provided post ADS operation (9.4 m (31 ft) of water above the lowest level in containment and 7.8 m (25.5 ft) above floors around screens).
- Bottom of screens are located well above the lowest containment level (4.1 m (13.5 feet)) as well as the floors around them (0.6 m (2 feet)).
- Top of screens are located well below the containment floodup level (~3 m (~10 ft) from top screens to minimum flood level).
- Screens have protective plates located no more than 0.38 m (1 foot, 3 inches) above the top of the screens and extend at least 2.7 m (8 feet, 11 inches) in front and 2.1 m (7 feet) to the side of the screens.
- Screens have conservative flow areas to account for plugging. Operation of the Class 2 normal residual heat removal pumps with suction from the IRWST and the containment recirculation lines is considered in sizing screens. Note that adequate PXS performance can be supported by one screen with more than 90 percent of its surface area completely blocked.
- During recirculation operation, the velocity approaching the screens is very low, which limits the transport of debris.
- Each screen has a fine screen.
- Technical Specifications require the screens to be inspected during each refuelling outage.
- A cleanliness program limits the amount of foreign materials that might be left in the containment following refuelling and maintenance outages and become debris during an accident.

9.8.3.2.7 Containment System

9.8.3.2.7.1 Containment Closure at Shutdown.

The AP1000 has addressed the issue of containment closure at shutdown and incorporated the following requirements in the Technical Specifications. In shutdown Modes 3 and 4, containment status is the same as at-power. Specifically, containment integrity is required, the major equipment hatches are closed and sealed, and containment air locks and isolation valves are operable.

In Modes 5 and 6, containment closure capability is required during shutdown operations when there is fuel inside containment. Containment closure is required to maintain, within containment, the cooling water inventory. Due to the large volume of the IRWST and the reduced sensible heat during shutdown, the loss of some of the water inventory can be accepted.

In Modes 5 and 6, there is no potential for steam release into the containment immediately

following an accident. Steam release into containment could occur only after heatup of the IRWST due to PRHR HX operation (Mode 5 with RCS intact), after heatup of the RCS with direct venting to the containment (Mode 5 with reduced RCS inventory or Mode 6 with the refuelling cavity not fully flooded), or after heatup of the RCS and refuelling cavity (Mode 6 with refuelling cavity fully flooded). To limit the magnitude of cooling water inventory losses and because local manual action may be required to achieve containment closure, the containment hatches, air locks, and penetrations must be closed prior to steaming into containment.

9.8.3.2.7.2 Containment Equipment Hatches

The containment equipment hatches, which are part of the containment pressure boundary, provide a means for moving large equipment and components into and out of containment. If closed, the equipment hatch is held in place by at least four bolts. If open, each equipment hatch can be closed using a dedicated set of hardware, tools, and equipment. A self-contained power source is provided to drive each hoist while lowering the hatch into position. Large equipment and components may be moved through the hatches as long as they can be removed and the hatch closed prior to steaming into the containment.

9.8.3.2.7.3 Containment Air Locks

The containment air locks, which are also part of the containment pressure boundary, provide a means for personnel access during Modes 1, 2, 3, and 4 unit operation. Each air lock has a door at both ends. The doors are normally interlocked to prevent simultaneous opening when containment operability is required. The interlocks are necessary for the Personnel Airlock to be operable. In the event that the interlock is broken in Modes 1-4 (or a door is broken) the Personnel Airlock must be closed and locked, otherwise containment would be considered breached. Although some containment penetrations can be opened during normal operation, the Personnel Airlock cannot be. The interlock can only be disengaged in Modes 5 & 6. If a door is broken, or the interlock has failed, the airlock must be closed and locked.

During periods of unit shutdown when containment closure is not required, the door interlock mechanism may be disabled, allowing both doors of an air lock to remain open for extended periods when frequent containment entry is necessary. Temporary equipment connections (for example, power or communications cables) are permitted as long as they can be removed to allow containment closure prior to steaming into the containment.

9.8.3.2.7.4 Containment Penetrations

Containment penetrations, including purge system flow paths, which provide direct access from containment atmosphere to outside atmosphere must be isolated or isolatable on at least one side. Isolation may be achieved by an operable automatic isolation valve or by a manual isolation valve, blind flange, or equivalent.

9.8.3.2.7.5 Containment Spare Penetrations

Containment spare penetrations, which also provide a part of the containment boundary, provide for temporary support services (electrical, I&C, air, and water supplies) during Modes 5 and 6. Each penetration is flanged and normally closed. During periods of plant shutdown, temporary support systems may be routed through the penetrations; temporary equipment connections (for example, power or communications cables) are permitted as long as they can be removed to allow containment closure prior to steaming into the containment.

The spare penetrations must be closed or, if open, capable of closure prior to reaching boiling

conditions within reactor coolant system. Temporary containment penetrations that may be employed during shutdown modes must have a design pressure equal to the containment design pressure of 0.407 MPa gauge (59 psig).

9.8.3.2.7.6 Fuel Transfer Canal

The fuel transfer canal may be opened to provide for the transfer of new and spent fuel into and out of containment during Modes 5 and 6. At times when the canal is opened, it must be isolatable on at least one side by closure of the flange within containment or the gate valve outside containment.

9.8.3.3 AP1000 Class 2 Systems Design Features to Address Shutdown Safety

In the following sections the SGS, main and startup feedwater system (FWS), CVS and RNS features are discussed. It is especially the RNS, and its associated Class 2 cooling chain (CCS and SWS) and supporting systems (e.g., onsite standby Diesel Generators), that will be most relevant to the fault analyses discussed in the following sections.

9.8.3.4 Steam Generator and Feedwater Systems Design Features for Shutdown

This section discusses the AP1000 steam generator system (SGS) and the FWS designs as they relate to shutdown operations.

9.8.3.4.1 Feedwater Control

The AP1000 provides improvements in feedwater control that minimizes the probability of loss of feedwater transients during low power and shutdown modes. The main feedwater pumps are capable of providing feedwater during all modes of operation, including plant startup and standby conditions. In addition, the startup feedwater pumps are automatically started in the event that the main feedwater pumps are unable to continue to operate. The startup feedwater pumps are also automatically loaded on the diesels for operation following a loss of offsite power, during operating modes when the steam generators can be used for decay heat removal.

9.8.3.4.2 Safety Actuation in Shutdown Modes

The AP1000 design has Class 1 actuations associated with the SGS that are operable during shutdown modes. These include the PRHR HX actuation on low steam generator level during shutdown modes, and this is discussed in Section 9.8.4.2.3. Also included is the isolation of the main steam line on a high (large) negative rate of change in steam pressure. This Class 1 signal is provided to address a steam line break that could occur in Mode 3. If actuated, this signal causes the MSIVs to close to terminate the blowdown of the SGS following a steam line break. This signal is placed into service below the setpoint that disables the low steam line pressure signal (P11) that actuates steam line isolation. When the operator manually blocks the low steam line pressure signal, the steam line high pressure-negative rate signal is automatically enabled.

This steam line high pressure-negative rate signal is operable during Mode 3 when a secondary side break or stuck open valve could result in the rapid depressurisation of the steam line(s). In Modes 4, 5, and 6, this function is not needed for accident detection and mitigation. Section 9.8.4.1.3 discusses steam line break events that could occur in shutdown modes.

9.8.3.4.3 Steam Generator Cooling in Shutdown Modes

The secondary side of the steam generators can be cooled during shutdown by circulating their contents through the blowdown system to prevent heat transfer from the steam generators to the primary system. This feature reduces the challenges to low-temperature overpressure events. During RCS water-solid operation, heat input from the steam generators is capable of challenging the low-temperature relief valve. The Technical Specifications prevent the operators from starting an RCP with the steam generator secondary side temperature more than 27.8°C (50°F) higher than the primary side, with the pressuriser water-solid. With the RCS water-solid, the heat input that could occur would cause the system to be pressurised to the setpoint of the low-temperature overpressure relief valve in the RNS.

When the RCPs are operating, the secondary side of the steam generator is cooled by steaming to the MSS. Once the RNS is aligned, and steaming to the MSS is decreased, the secondary side of the steam generators is cooled by operation of the RNS. However, once the RCPs are tripped, water does not circulate through the primary side of the tubes and the secondary side of the steam generators remains at elevated temperature. With the ability to circulate the secondary side via the blowdown system, the AP1000 design reduces the probability that an RCP would be started with the secondary side of the generator at elevated temperature.

The AP1000 design has also incorporated steam generator fluid thermocouples to monitor the temperature of the fluid in the secondary side of the steam generator. This improves the ability of the operators to monitor this temperature to prevent them from inadvertently starting an RCP with the secondary side at elevated temperatures.

9.8.3.4.4 Normal Residual Heat Removal System

The AP1000 has incorporated various design features to improve shutdown safety. The RNS features that have been incorporated to address shutdown safety are described in this section.

9.8.3.4.4.1 RNS Pump Elevation and NPSH Characteristics

The AP1000 RNS pumps are located at the lowest elevation in the auxiliary building. This location provides the RNS pumps with a large available net positive suction head (NPSH) during all modes of operation including RCS mid-loop and reduced inventory operations. The large NPSH provides the pumps with the capability to operate during most mid-loop conditions without throttling the RNS flow. If the RCS is at mid-loop level and saturated conditions, some throttling of a flow control valve is necessary to maintain adequate net positive suction head for the RNS pumps. The RNS pumps can be restarted and operated with RCS conditions that might occur following a temporary loss of RNS cooling.

The plant piping configuration, piping elevations and routing, and the pump characteristics allow the RNS pumps to be started and operated at their full design flow rates in most conditions without the need to reduce RNS pump flow to meet pump NPSH requirements. This reduces the potential failure mechanism that exists in current PWRs, where failure of an air-operated control valve can result in pump runout and cavitation during mid-loop operations.

9.8.3.4.4.2 Self-Venting Suction Line

Most of the RNS pump suction line is sloped upward from the pump to the RCS hot leg. In the level portions of piping, there are no local high points. This eliminates potential problems

with refilling the pump suction line if an RNS pump is stopped due to pump cavitation and/or excessive air entrainment. With the self-venting suction line, the line will refill and the pumps can be immediately restarted once an adequate level in the hot leg is re-established.

9.8.3.4.4.3 IRWST Injection via the RNS Suction Line

During shutdown modes, initiating events such as the loss of the Class 2 RNS are postulated. Such events would require IRWST injection as discussed in Section 9.8.3.2, and as shown in the accident analyses provided in Section 9.8.4. For initiating IRWST injection, the operation of PXS squib valves in the IRWST injection line is required. However, the operators can use the RNS pump suction line that connects to the IRWST to provide controlled IRWST injection. This flow path, shown in Figure 9.8.2-2, connects the IRWST directly to the RCS via the RNS hot leg suction isolation valves and provides a diverse method for IRWST injection. In addition, it would be the preferred method of providing IRWST injection because the flow would be controllable by the operation of the IRWST suction line isolation valve. The RNS isolation valve is equipped with a throttle capability to provide the operators with the capability to control the injection flow via this path. The operator would monitor the RCS hot leg level while controlling flow through this valve. This path provides IRWST injection regardless of whether the RNS pumps are operating.

9.8.3.4.4.4 Codes and Standards/Seismic Protection

The entire RNS pressure boundary is classified as Safety Class 1 and thus as seismic Category I.

9.8.3.4.4.5 Increased Design Pressure

The portions of the RNS from the RCS to the containment isolation valves outside containment are designed to the operating pressure of the RCS. The portions of the system downstream of the suction line containment isolation valve and upstream of the discharge line containment isolation valve are designed so that its ultimate rupture strength is not less than the operating pressure of the RCS. The design pressure of the RNS is 6.205 MPa gauge (900 psig), which is 40 percent of operating RCS pressure.

9.8.3.4.4.6 Normal Residual Heat Removal System Relief Valve

An inside containment RNS relief valve is connected to each residual heat removal pump suction line. Each valve is designed to provide low-temperature, overpressure protection of the RCS. The valves, connected to the high-pressure portion of the pump suction lines, reduce the risk of overpressurising the low-pressure portions of the system.

9.8.3.4.4.7 Reactor Coolant System Isolation Valve

The RNS contains isolation valves in the pump suction lines from the RCS. These motor-operated containment isolation valves are designed to the RCS pressure. They provide an additional barrier between the RCS and lower pressure portions of the RNS.

9.8.3.4.4.8 Features Preventing Inadvertent Opening of Isolation Valves

The RCS isolation valves are interlocked to prevent their opening at RCS pressures above 3.103 MPa gauge (450 psig). The power to these valves is administratively blocked during normal power operation.

In addition, these valves are interlocked with the RNS/IRWST isolation valves to prevent their opening with the RNS open to the IRWST. This precludes the blowdown of the RCS to the IRWST through the RNS upon system initiation.

9.8.3.4.4.9 RCS Pressure Indication and High Alarm

The AP1000 RNS contains an instrumentation channel that indicates pressure in each normal residual heat removal pump suction line. A high-pressure alarm is provided in the main control room to alert the operator to a condition of rising RCS pressure that could eventually exceed the design pressure of the RNS.

9.8.3.4.5 Chemical and Volume Control System

The AP1000 CVS is a Class 2 system. However, portions of the system are Class 1 and perform Class 1 functions, such as containment isolation, termination of inadvertent RCS boron dilution, RCS pressure boundary preservation, and isolation of excessive makeup.

Boron dilution events during low power modes can occur for a number of reasons, including malfunctions of the reactor makeup control system. Regardless of the cause, the protection is the same. The CVS is designed to avoid and/or terminate boron dilution events by automatically closing either one of two series, Class 1 valves in the demineralized water supply line to the makeup pump suction to isolate the dilution source. Additionally, the suction line for the CVS makeup pump is automatically realigned to draw borated water from the boric acid tank. The automatic boron dilution protection signal is Class 1 and is generated upon any reactor trip signal, source-range flux multiplication signal, low input voltage to the Class 1 IDS battery chargers, or a safety injection signal.

The safety analysis of boron dilution accidents is provided in Section 9.4.6 and is discussed in Section 9.8.4.4.5. For dilution events that occur during shutdown, the source-range flux-doubling signal is used to isolate the line from the demineralized water system by closing the two Class 1 remotely operated valves. The three-way pump suction control valve aligns the makeup pumps to take suction from the boric acid tank and, therefore, stops the dilution. For diverse mitigation of boron dilution events at shutdown, a DAS actuation based on the intermediate range nuclear instrumentation (IRNI) results in a trip of the RCPs and RNS pumps, isolation of boron dilution sources, and CMT actuation. Boron addition following CMT actuation results in a negative reactivity addition and terminates the event.

For refuelling operations, administrative controls are used to prevent boron dilutions by verifying that the valves in the line from the demineralized water system are closed and locked. These valves block the flow paths that can allow unborated makeup water to reach the RCS. Makeup required during refuelling uses borated water supplied from the boric acid tank by the CVS makeup pumps.

During refuelling operations (Mode 6), two source-range neutron flux monitors are operable to monitor core reactivity. This is required by the plant Technical Specifications. The two operable source-range neutron flux monitors provide a signal to alert the operator to unexpected changes in core reactivity. The potential for an uncontrolled boron dilution accident is precluded by isolating the unborated water sources. This is also required by the plant Technical Specifications.

9.8.4 AP1000 Safety Evaluation of Postulated Initiating Events at Shutdown

This section reviews each of the at-power faults identified for evaluation with respect to lower power and shutdown modes in Section 1 of Table 8A-2.

9.8.4.1 Increase in Heat Removal from the Primary System

9.8.4.1.1 Feedwater System Malfunctions Which Increase Heat Removal from the Primary System (Faults 1.15.13 – 1.15.14a)

Faults that decrease feedwater temperature or increase feedwater flow can be postulated in the feedwater system. These faults could increase heat removal from the primary system, which reduces RCS temperature. The reduction in RCS temperature could lead to an increase in core power generation (due to a negative moderator temperature coefficient) and result in a reduction in margin-to-core design limits. Unchecked, excessive feedwater flow could also result in overfilling the steam generators.

Discussions and analyses, initiated from Modes 1 and 2, of RCS cooldowns caused by feedwater system malfunctions are presented in Sections 9.1.1 and 9.1.2. Section 9.1.1 covers reductions in feedwater temperature, and Section 9.1.2 covers increases in feedwater flow. These faults are categorised as DB2 frequent faults for Modes 1 and 2, which are the limiting initial conditions for feedwater system induced RCS cooldown transients. Assuming a reduction in frequency of $1/20^{th}$ for the same event at shutdown conditions, these faults would be categorised as DB1 infrequent faults for shutdown modes,

Protection against feedwater system induced cooldown transients is provided by the PMS through automatic functions that trip the reactor and isolate the feedwater system. The protection functions are available in all modes during which the feedwater system is in operation. Reactor trip signals include overpower ΔT, high power-range nuclear flux, high intermediate-range nuclear flux, or high source-range nuclear flux. The PMS closes the main feedwater control valves on low-1 RCS average temperature signal. The PMS also closes the main feedwater isolation valves and trips the booster/main feedwater pumps when RCS average temperature decreases below the low-2 RCS T_{avg} setpoint. These protection functions are arranged to detect symmetrical plant transients with a channel out of service and a single channel failure.

Additional PMS functions are provided to detect and protect against asymmetrical feedwater system malfunctions. Automatic reactor trip, closure of the main feedwater control and isolation valves, closure of the startup feedwater control and isolation valves, tripping of the booster/main feedwater pumps, and tripping of the startup feedwater pumps occur if the level in a single steam generator is above the High-3 water level setpoint. Similar actions occur if cold leg temperature in a single RCS loop decreases below the Low-2 T_{cold} setpoint. The High-3 steam generator level setpoint is active in Modes 1 through 4 unless the various feedwater valves are closed. This ensures that the steam generators cannot inadvertently be overfilled. The Low-2 T_{cold} signal is available in Modes 1 through 3. In Mode 3 prior to blocking the Low-2 T_{cold} signal, the RCS must be borated to cold shutdown conditions, in accordance with the plant Tech Specs. With the RCS borated, no feedwater malfunction can be postulated to cool the RCS such that a core power excursion would occur.

The feedwater malfunction associated with a drop in feedwater temperature is less severe as power level is decreased. Normal operating feedwater temperature decreases as plant power level decreases. Therefore, if a fault suddenly reduces the feedwater temperature, the maximum change in feedwater temperature will occur if the plant is operating at full power.

In Modes 2 and below, feedwater entering the steam generators is routed through the startup feedwater control valves. The maximum achievable flow rate through the startup feedwater path is much less than when flow is being controlled by the main feedwater control valves. Therefore, failure of a main feedwater control valve in Mode 2 and below is not likely. The

assumption of a failed open startup feedwater control valve, in Mode 2 and below, will result in a relatively slow transient due to low feedwater flow rate.

The most severe RCS cooldowns caused by feed system malfunctions will occur in Modes 1 or 2. In Modes 3 or 4, RCS cooldowns due to feedwater malfunctions would be precluded, inconsequential, or less severe than in Modes 1 or 2. In Modes 5 and 6, any cooldown caused by feedwater system malfunction is meaningless because the RCS is already cold, and the RNS system effectively decouples the steam generators from the core. The analyses presented in Section 9.1 bound the consequences of this class of events initiated in the shutdown modes.

Because the primary and secondary circuits remain intact and offsite power remains available, there is no release of activity to the environment. Therefore, the radiological consequences of these events presented in Sections 9.1.1.4 and 9.1.2.4 for the release of activity resulting from a case where offsite power is lost are limiting compared to the event occurring in lower modes.

Thus, this event during any shutdown mode is less limiting than the at-power conditions for which a design basis analysis is provided. In addition, due to the likelihood of these faults occurring at shutdown conditions being categorised as an infrequent fault, diverse mitigation is not explicitly required. However, since the required protection functions are available in all modes of operation, for both primary and diverse mitigation considerations, and no further discussion is provided here.

9.8.4.1.2 Excessive Increase in Secondary Steam Flow (Faults 1.15.18 and 1.15.18a)

An excessive increase in secondary steam flow (excessive load increase) is caused by a rapid increase in steam flow that results in a power mismatch between the reactor core power and the steam generator load demand. The PLS is designed to accommodate a 10-percent step load increase in steam flow in the range of 25 to 100 percent of full power. Analyses results for a 10-percent step increase in steam flow are presented in Section 9.1.3. The analyses are performed for Mode 1 from full-power initial conditions. Depending upon the plant and PMS characteristics (setpoint uncertainties), a reactor trip signal may or may not be generated for an excessive load increase from full power.

This fault is categorised as a DB2 frequent fault for occurrences in Modes 1 and 2. Assuming a reduction in frequency of $1/20^{th}$ for the same event at shutdown conditions, these faults would be categorised as DB1 infrequent faults for shutdown modes,

An excessive load increase in Mode 1 is considered limiting because an excessive load increase at full power will put the plant at the highest achievable power level. Load increases at less than full power, or during startup (Mode 2), will not reach as high a power level. The excessive load increase, in Mode 2, will not be as severe as the Mode 1 excessive load increase.

In Mode 3, the excessive load increase may be considered to be a simple steam release because there can be no load, per se, when the turbine is off-line and the core is subcritical. The Mode 3 load increase will be less limiting than the Mode 1 or Mode 2 case because the core is already subcritical. Automatic safeguards actuation signals may not be available if blocked by the operator (blocking is necessary to depressurise and cool down the RCS). However, the RCS must be borated to meet shutdown margin requirements at cold shutdown (93.3°C [200°F]) prior to blocking automatic safeguards actuation signals to prevent a return to criticality in the event of a cooldown.

The Mode 4 situation is bounded by Mode 3 because pressure and temperature conditions in

the primary and secondary systems are reduced. At some point in Mode 4, the RNS will be placed in service. In Modes 5 and 6, the RNS should be in operation. Any steam release will have little or no effect upon the core.

Because the primary and secondary circuits remain intact and offsite power remains available, there is no release of activity to the environment. Therefore, the radiological consequences of this event presented in Section 9.1.3.4 for the release of activity resulting from a case where offsite power is lost are limiting compared to the event occurring in lower modes.

Thus, this event during any shutdown mode is less limiting than the at-power conditions for which a design basis analysis is provided. In addition, due to the likelihood of this fault occurring at shutdown conditions being categorised as an infrequent fault, diverse mitigation is not explicitly required. However, since the required protection functions are available in all modes of operation, for both primary and diverse mitigation considerations, and no further discussion is provided here.

9.8.4.1.3 Steamline Breaks (Faults 1.15.19, 1.21.1 – 1.21.3. and 1.22.1 – 1.22.2a)

This section includes both DB2 frequent faults (spurious opening of a SG relief valve) and DBL infrequent faults (postulated design basis break of the main steam line) events. Assuming a reduction in frequency of $1/20^{th}$ for the same event at shutdown conditions, these faults would be categorised as DB1 infrequent faults or beyond design basis for shutdown modes.

The spurious opening of a steam generator safety or relief valve is a DB2 event and referred to as a credible steam line break. This event affects the core like a load increase but different analysis assumptions are applied. The credible steam line break is usually assumed to be an unisolatable, uncontrolled steam release, which causes a non-uniform core cooldown (typical of an open safety valve) during the period immediately following a reactor trip which inserts all but the most reactive RCCA. The resulting reactivity excursion may be large enough to overcome the shutdown margin and return the core to critical, especially when there is little or no decay heat (with power peaking in the region of the stuck RCCA). The credible steam line break is analysed in Mode 2, and the results are presented in Section 9.1.4. The assumptions used in the analysis lead to a more severe, post-trip transient than will result from a load increase initiated in Mode 1.

In Mode 1, prior to reactor trip, the transient characteristics of an inadvertent opening of a steam generator safety or relief valve are similar to the excessive load increase. A reactor trip signal, if needed, may result from overpower ΔT logic. After the reactor trip, the concern becomes a possible return to criticality with the most reactive RCCA stuck in the fully withdrawn position, leading to high local power levels. However, a post-trip return to criticality is less likely when this event occurs in Mode 1 than in Mode 2 because there will be more decay heat present, which tends to retard the cooldown.

In Mode 3, results are expected to be better than the Mode 2 case because pressure, temperature, and flow conditions will be less limiting. An occurrence in Mode 4 will be less severe than in Modes 2 or 3 due to the lower initial RCS temperature, and an effective decoupling of the secondary system from the primary system as the RCPs are removed from service and the RNS is started. Automatic safeguards actuation signals are available through Mode 3, until the RCS is borated and the automatic safeguards signals are blocked (see excessive load increase discussion). Both CMTs continue to be available for automatic actuation on low-2 pressuriser level or manual actuation through Mode 4 with the RCS not being cooled by the RNS (see Technical Specification LCO 3.5.2). In Mode 4 with the RNS

in operation and in Mode 5 with the RCS pressure boundary intact, one CMT is available for actuation if needed.

Any cooldown in Modes 5 and 6 caused by depressurisation of the secondary system is meaningless because the RCS is already cold, and the RNS system effectively decouples the steam generators from the core.

The steam line rupture is a DBL infrequent fault event, producing a greater uncontrolled steam release than the spurious opening of a steam generator safety valve (described above), but the relative effects in the various modes and requirements for protection equipment are the same. This is the most severe cooldown event.

The radiological consequences of these events presented in Sections 9.1.4.4, 9.1.5.4, and 9.1.6.4 are limiting because the coolant temperature, secondary side releases and RCS activity concentrations (including consideration of iodine spikes) bound those that would exist in the other modes.

Thus, this event during any shutdown mode is less limiting than the at-power conditions for which a design basis analysis is provided, as discussed above. In addition, due to the likelihood of these faults occurring at shutdown conditions being categorised as an infrequent or beyond design basis fault, diverse mitigation is not explicitly required. However, since the required protection functions are available in applicable modes of operation, for both primary and diverse mitigation considerations, no further discussion is provided here.

9.8.4.1.4 Inadvertent PRHR HX Operation (Faults 1.15.15 – 1.15.17)

Inadvertent actuation of the PRHR HX causes an injection of relatively cold water into the RCS. This produces a reactivity insertion in the presence of a negative moderator temperature coefficient. Because the PRHR HX is connected to only one RCS loop, the cooldown resulting from its actuation is asymmetric with respect to the core. Inadvertent actuation of the PRHR HX could lead to an asymmetric power increase and a reduction in margin-to-core design limits.

A limiting analysis of an inadvertent actuation of the PRHR HX heat exchanger is presented in Section 9.1.7. The analysis is initiated in Mode 1 from hot full-power conditions, where this fault is categorised as a DB2 frequent fault; this is the most limiting case. This fault is also categorised as a DB2 frequent fault during shutdown conditions due to the initiator, a valve misalignment, being just as likely at any time of operation.

The PRHR HX heat transfer rate is a function of the inlet temperature to the heat exchanger and the flow rate through the heat exchanger. PRHR HX heat transfer rate is higher with high flow rates and high inlet temperatures. Therefore, the maximum heat removal rate will occur when the plant is at full-power condition with forced RCS flow and a high hot leg temperature. At plant full-power conditions, the PRHR HX heat removal rate is approximately 10 percent of full power. At HZP conditions with natural circulation, heat removal by the PRHR HX is approximately 1.5 percent to 2 percent of full power.

The heat sink for the PRHR HX is the IRWST, in which the heat exchanger is submerged. Prior to actuation of the PRHR HX, the fluid within the heat exchanger is in thermal equilibrium with the fluid in the IRWST. Thus, the PRHR HX is initially filled with relatively cold fluid which is at containment ambient temperature. When the PRHR HX is actuated, the initial fluid outsurge is fluid at containment ambient temperature. Once the original fluid in the PRHR HX is purged, the out-flow temperature trend of the heat exchanger is set by the temperature entering the heat exchanger from the RCS hot leg minus the temperature drop

through the heat exchanger. Thus, the outlet fluid temperature is limited by the cooling capacity of the PRHR HX.

In Mode 3, because the reactor is subcritical, inadvertent actuation of the PRHR HX produces a less severe power excursion than if the reactor is at power or at HZP with the reactor just critical. If in Mode 3 below no-load temperature, the cooldown caused by the actuation of the PRHR HX results in the cold leg temperature dropping below the Low-2 T_{cold} safeguards signal setpoint. This function actuates a reactor trip, initiates boration by the CMTs, and most importantly, trips all the RCPs. When the RCPs trip, natural circulation flow begins in the RCS and the PRHR HX loop. When natural circulation flow is initiated, the heat removal capability of the PRHR HX decreases to approximately 1.5 percent of full power and the severity of the transient is minimized. With the RCS in natural circulation, the cooldown rate of the RCS is also slowed. If criticality is obtained, boration by the CMTs will bring the core subcritical again.

The Low-2 T_{cold} safeguards signal may be blocked by the operator in Mode 3 to allow plant depressurisation and cooldown to lower modes. However, prior to blocking the Low-2 T_{cold} safeguards signal, the RCS is borated to the shutdown margin requirements at cold shutdown (93.3°C [200°F]). Therefore, in Mode 3 with safeguards signals blocked or in Mode 4, cooldown of the RCS by inadvertent actuation of the PRHR HX will not result in a reactivity excursion, which produces a power increase.

In Modes 5 and 6, the RCS will be borated such that a cooldown-induced power excursion could not be postulated. The RCS will be at (93.3°C [200°F]) or less, and with initial RCS temperatures this low, no significant cooling of the RCS by inadvertent actuation of the PRHR HX could be postulated.

Because the primary and secondary circuits remain intact and offsite power remains available, there is no release of activity to the environment. Therefore, the radiological consequences of this event presented in Section 9.1.7.4 for the release of activity resulting from a case where offsite power is lost are limiting compared to the event occurring in lower modes.

Thus, this event during any shutdown mode is less limiting than the at-power conditions for which a design basis analysis is provided. Since the required protection functions are available in all modes of operation, for both primary and diverse mitigation considerations, no further discussion is provided here.

9.8.4.2 Decrease in Heat Removal by the Secondary System

9.8.4.2.1 Loss of Load, Turbine Trip, Inadvertent MSIV closure, and Loss of Condenser Vacuum (Faults 1.12.8 – 1.12.11, 1.16.7, and 1.18.1)

Discussions and analyses of the consequences of loss of load, turbine trip, inadvertent closure of MSIVs, or loss of condenser vacuum are presented in Sections 9.2.2 through 9.2.5. These DB2 frequent fault events are characterized by a rapid reduction in steam flow from the steam generators. This results in an increase in steam pressure and a heatup of the primary side if the reactor power is not reduced. The effects of the primary to secondary power mismatch during these events are mitigated by tripping the reactor and opening secondary and primary side safety valves. The severity of these events is increased if the primary to secondary power mismatch is increased. Therefore, the most severe results occur if the plant is initially operating in Mode 1 at maximum-rated plant power conditions rather than lower power conditions. The turbine is off-line below Mode 1 and transients related to turbine-related faults cannot occur.

In Modes 2, 3, or 4, the plant may be removing decay heat by dumping steam to the condenser. In Mode 4 when the RCS is below 176.7°C (350°F), decay heat is removed using the RNS. In Modes 2, 3, or 4, the transient response to a loss of condenser vacuum or inadvertent MSIV closure is bounded by the turbine trip analysis from full power because the power mismatch is low. Decay heat removal can still be accomplished by the steam generators through atmospheric steam relief through PORVs if available or through steam generator safety valves, which are available through Mode 4 (see Technical Specification LCO 3.7.1). Additionally, decay heat can be removed with the PRHR HX, which is available through Mode 5 with the RCS intact (see Technical Specifications LCO 3.5.4 and 3.5.5).

In Mode 5, with RCS open, and in Mode 6, the event is clearly not applicable.

The initiating event does not result in fuel damage and the primary and secondary circuits remain intact. The radiological consequences of this event presented in Section 9.2.3.4 for the release of activity resulting from a case where offsite power is lost are limiting compared to the event occurring in Modes 3 or 4 because the coolant temperature, secondary side releases and RCS activity concentrations bound those that would exist in the other modes. In Modes 4 or 5 with the RNS in operation there is no release of activity to the environment because offsite power remains available.

Thus, this event during any shutdown mode is less limiting than the at-power conditions for which a design basis analysis is provided. Since the required protection functions are available in all modes of operation, for both primary and diverse mitigation considerations, no further discussion is provided here.

9.8.4.2.2 Loss of ac Power (Faults 1.19.1 and 1.19.2)

A discussion and an analysis of a loss of ac power event are provided in Section 9.2.6. The loss of ac power, which is a DB2 frequent fault in all modes, results in the loss of forced primary coolant flow and the loss of main feedwater flow. This results in a heatup and pressurisation of the RCS. If the reactor is at power, the event is mitigated by tripping the reactor. The reactor may be automatically tripped on low RCP speed, low RCS flow, low steam generator level, or several other primary side heatup signals. Also reactor trip may occur due to the loss of power to the control rod drive mechanisms.

Following reactor trip, the PRHR HX is activated for decay heat removal. Automatic PRHR HX actuation on low steam generator level is available in Modes 1 through 3 and in Mode 4 when the RCS is not being cooled by the RNS. The most limiting case for loss of ac power would be if the plant were at full rated power. This will result in the highest decay heat levels and stored energy in the RCS and the heat removal capability of the PRHR HX will be maximized. In Modes 4 or 5 with the RNS in operation, the plant response to a loss of ac power is the same as the loss of RNS cooling discussed in Section 9.8.5.

The radiological consequences of this event presented in Section 9.2.6.4 are limiting compared to the event occurring in Modes 3 or 4 because the coolant temperature, secondary side releases and RCS activity concentrations bound those that would exist in the other modes. In Modes 4 or 5 with the RNS in operation, the radiological consequences of a loss of ac power are the same as the loss of RNS cooling discussed in Section 9.8.5.1.3.3.

Thus, this event during any shutdown mode is less limiting than the at-power conditions for which a design basis analysis is provided. Since the required protection functions are available in all modes of operation, for both primary and diverse mitigation considerations, no further discussion is provided here.

9.8.4.2.3 Loss of Normal Feedwater (Faults 1.16.1 – 1.16.3, 1.17.1, and 1.20.1 – 1.20.2)

The main feedwater system is in operation during Modes 1 and 2. The startup feedwater system is used in Mode 2 below approximately 2 percent power, in Mode 3, and in Mode 4 before the RNS is aligned. In Mode 4 with the RNS aligned and in Modes 5 and 6, the feedwater system is not used, and therefore, loss of feedwater events is irrelevant. The 'corresponding' shutdown event is the loss of RNS cooling, which is discussed and analysed in Section 9.8.5

A discussion and an analysis of a loss of normal feedwater event from rated full-power conditions are provided in Section 9.2.7; it is categorised as a DB2 frequent fault. The loss of normal feedwater flow results in a heatup and pressurisation of the RCS. If the reactor is at-power, the event is mitigated by tripping the reactor on low steam generator level.

Following reactor trip, the PRHR HX is activated for decay heat removal. Automatic PRHR HX actuation on low steam generator level is available in Modes 1 through 3 and in Mode 4 when the RCS is not being cooled by the RNS. The most limiting case for a loss of normal feedwater is with the plant initially at full rated power. This case will have the highest decay heat levels and stored energy in the RCS and the heat removal capability of the PRHR HX will be maximized. The analysis initiated from full power bounds cases initiated from the shutdown modes.

Because the primary and secondary circuits remain intact and offsite power remains available, there is no release of activity to the environment. Therefore, the radiological consequences of this event presented in Section 9.2.7.4 for the release of activity resulting from a case where offsite power is lost are limiting compared to the event occurring in lower modes.

Thus, this event during any shutdown mode is less limiting than the at-power conditions for which a design basis analysis is provided. Since the required protection functions are available in all modes of operation, for both primary and diverse mitigation considerations, no further discussion is provided here.

9.8.4.2.4 Feedwater System Pipe Break (Faults 1.16.8 – 1.16.10)

Depending upon the size of the break and plant operating conditions, the break could cause either an RCS heatup or an RCS cooldown. The cooldown aspects are less severe than a steam line break, which is discussed in Section 9.8.4.2.3 and is not considered in the following discussion.

The main feedwater system is in operation during Modes 1 and 2. The startup feedwater system is used in Mode 2 below approximately 2 percent power, in Mode 3, and in Mode 4 before the RNS is aligned. In Mode 4 with the RNS aligned and in Modes 5 and 6, the feedwater system is not used, and therefore, a loss of feedwater caused by a feedwater system pipe break will not cause a heatup of the RCS.

A discussion and an analysis of a DBL infrequent fault feedwater system pipe break from rated full-power conditions are provided in Section 9.2.8. A rupture of a feedwater system pipe results in a loss of feedwater flow causing a heatup and pressurisation of the RCS. If the reactor is at-power, the event is mitigated by tripping the reactor on low steam generator level.

Following reactor trip, the PRHR HX is activated for decay heat removal. Automatic PRHR HX actuation on low steam generator level is available in Modes 1 through 3 and in

Mode 4 when the RCS is not being cooled by the RNS. The most limiting case for a feedline break occurs with the plant at full rated power. This case will have the highest decay heat levels and the highest stored energy in the RCS and the heat removal capability of the PRHR HX will be maximized.

The radiological consequences of this event presented in Section 9.2.8.4 are limiting because the coolant temperature, secondary side releases and RCS activity concentrations bound those that would exist in the other modes.

Thus, this event during any shutdown mode is less limiting than the at-power conditions for which a design basis analysis is provided. Since the required protection functions are available in all modes of operation, for both primary and diverse mitigation considerations, no further discussion is provided here.

9.8.4.3 Decrease in Reactor Coolant System Flow Rate

9.8.4.3.1 Partial and Complete Loss of Forced RCS Flow (Faults 1.13.1 – 1.13.3)

A partial loss of forced RCS flow may be caused by a mechanical or an electrical failure in an RCP or from a fault in the power supply to the pumps. An RCP failure will result in only the loss of a single RCP. A fault in the power supplies for the RCPs could result in the loss of one, two, or all four RCPs. These faults are categorised as DB2 frequent faults for Modes 1 and 2.

The loss of one or more RCPs reduces the heat removal rate from the primary to the secondary coolant system and thereby causes a heatup in the RCS. The heatup of the RCS results in an increase in RCS pressure and a decrease in margin-to-core design limits (that is, DNB). An occurrence at full power will produce a greater and more rapid heatup than at part-power conditions or low-power conditions in Mode 2. Therefore, for evaluating the maximum RCS pressure or the minimum DNB ratio, analyses are performed at full-power conditions. Analyses for partial loss of forced RCS flow transients are presented in Section 9.3.1. Analyses for a complete loss of flow are presented in Section 9.3.2. These analyses bound loss of flow events initiated in other modes.

Protection for loss of forced RCS flow events is provided by tripping the reactor. This reduces reactor power and preserves margin-to-DNB limits. The AP1000 PMS includes a reactor trip on low RCS flow in any cold leg and a reactor trip on low RCP speed in any two of four RCPs. These two reactor trips are used to detect all possible partial and complete loss of RCS flow transients. Opening of the pressuriser safety valves in conjunction with the reactor trip prevents overpressurisation of the RCS.

Below Mode 2, when the core is subcritical, forced RCS flow is not needed because margin-to-DNB is not an issue. It is common to have one or more RCPs out of service below Mode 2 because full RCS flow is no longer needed. In Modes 3 through 5, LCO 3.4.5 of the Technical Specifications requires that all four RCPs need to be operating if the reactor trip breakers are closed, to ensure that DNB limits are not exceeded, in the event RCCAs are inadvertently withdrawn. If the trip breakers are open and RCCA withdrawal is precluded, no RCPs are required to be operating in Modes 3 through 5. Note that RCPs are not operated in Mode 6.

Following reactor trip in loss of forced RCS flow events, decay heat removal is required. The PRHR HX or the steam generators can be used for decay heat removal. In the event of a complete loss of forced RCS flow, RCS natural circulation is adequate to remove core decay heat. This is demonstrated by the loss of ac power analysis presented in Section 9.2.6.

Because the primary and secondary circuits remain intact and offsite power remains available, there is no release of activity to the environment. Therefore, the radiological consequences of these events presented in Sections 9.3.1.4 and 9.3.2.4 for the release of activity resulting from a case where offsite power is lost are limiting compared to the event occurring in lower modes.

Thus, this event during any shutdown mode is less limiting than the at-power conditions for which a design basis analysis is provided, as discussed above. Since the required protection functions are available in applicable modes of operation, for both primary and diverse mitigation considerations, no further discussion is provided here.

9.8.4.3.2 Reactor Coolant Pump Shaft Seizure or Break (Faults 1.13.11 – 1.13.12a)

An RCP shaft seizure or break results in a partial loss of forced RCS flow, and is categorised as a DB1 infrequent fault. The results are similar to partial loss of flow events discussed in Section 9.8.4.3.1 except that the rate of flow reduction is much more rapid if an RCP shaft breaks or seizes. Like the partial loss of flow, a locked or broken RCP shaft reduces the heat removal rate from the primary to secondary coolant system and thereby causes a heatup of the RCS. An occurrence at full power produces the most severe heatup transient. The discussion for the partial loss of flow with respect to limiting modes and protection is applicable to the RCP shaft seizures or breaks.

Analyses and evaluation of RCP shaft seizures and breaks for Mode 1, from full-power conditions, are provided in Sections 9.3.3 and 9.3.4. The analyses bound events initiated from the shutdown modes for reasons discussed in Section 9.8.4.3.1.

Because the primary and secondary circuits remain intact and offsite power remains available, there is no release of activity to the environment. Therefore, the radiological consequences of this event presented in Section 9.3.3.4 for the release of activity resulting from a case where offsite power is lost are limiting compared to the event occurring in lower modes.

Thus, this event during any shutdown mode is less limiting than the at-power conditions for which a design basis analysis is provided, as discussed above. Since the required protection functions are available in applicable modes of operation, no further discussion is provided here.

9.8.4.4 Reactivity and Power Distribution Anomalies

9.8.4.4.1 Uncontrolled RCCA Bank Withdrawal from a Subcritical Condition (Faults 1.15.1 – 1.15.3)

An uncontrolled RCCA bank withdrawal from a subcritical condition could cause a reactivity excursion, which if not terminated by a reactor trip, could result in DNB. Section 9.4.1 presents an analysis for the uncontrolled RCCA bank withdrawal from a subcritical condition in Mode 2, which is categorised as a DB2 frequent fault. Assumptions are used that make the analysis bound an occurrence in Modes 2, 3, 4, or 5. Specific conservative assumptions are made for the number of RCPs operating, the reactor trip functions credited, initial RCS temperature, and the magnitude of the reactivity excursion.

A single failure in the rod control system could cause the withdrawal of only one bank, and its withdrawal rate would be expected to be slower than the maximum rod speed possible when in automatic rod control. The analysis assumes the simultaneous withdrawal of the combination of two sequential RCCA banks having the greatest combined worth at the

maximum possible speed.

LCO 3.3.1 of the AP1000 plant Technical Specifications gives the operational requirements for reactor trips. The source-range high neutron flux trip must be in operation in Modes 3, 4, and 5 if the reactor trip breakers are closed. If the reactor trip breakers are open, then an RCCA withdrawal is precluded from occurring. The source-range high neutron flux trip is available in Mode 2 if power is below the P-6 interlock. In these instances, the source-range high neutron flux trip would be available to terminate the event, by tripping any withdrawn and withdrawing rods, before any significant power level could be attained. Therefore, DNB would be precluded. The intermediate-range high neutron flux reactor trip is also available in Mode 2. The analysis assumes that reactor trip does not occur until the power-range (low setting) high neutron flux setpoint is reached. No credit is assumed in the analysis for the source-range high neutron flux reactor trip or the intermediate-range high neutron flux reactor trip.

LCOs 3.4.4 and 3.4.5 of the AP1000 Technical Specifications give the operation requirements for RCPs. LCO 3.4.4 specifies that all four RCPs must be operating whenever the reactor trip breakers are closed in Modes 1 through 5. Rod control is not applicable in Mode 6.

The RCS temperature is assumed to be at the HZP value in the analysis. This is more limiting than that of a lower initial system temperature for DNB and core kinetics feedback calculations.

These conservative assumptions result in the core returning to critical and generating power before reactor trip occurs. The analysis presented in Section 9.4.1 bounds the inadvertent RCCA bank withdrawal from a subcritical condition transient in Modes 2 through 5.

Because the primary and secondary circuits remain intact and offsite power remains available, there is no release of activity to the environment, as indicated in Section 9.4.1.3.

Thus, this event during any shutdown mode is less limiting than the at-power conditions for which a design basis analysis is provided, as discussed above. Since the required protection functions are available in applicable modes of operation, for both primary and diverse mitigation considerations, no further discussion is provided here.

9.8.4.4.2 Uncontrolled RCCA Bank Withdrawal at Power (Fault 1.15.4)

By definition, this transient is only applicable to Mode 1.

9.8.4.4.3 RCCA Misalignment (Faults 1.15.5 – 1.15.5c)

RCCA misalignment events are analysed in Section 9.4.3. RCCA misalignment events include the following:

- One or more dropped RCCAs (DB2 frequent fault)
- Statically misaligned RCCA (DB2 frequent fault)
- Withdrawal of a single RCCA (DB1 infrequent fault)

Assuming a reduction in frequency of $1/20^{th}$ for the same event at shutdown conditions, these faults would be categorised as DB1 infrequent faults or beyond design basis for shutdown modes. These events may result in core radial power distribution perturbations, which may cause allowable design power peaking factors and DNB design limits to be exceeded. Therefore, these events are a concern only in the at-power modes, and the severity will be

increased at high power. If the reactor is subcritical, DNB will not be a concern.

Following the dropping of one or more RCCAs while at-power, core power will immediately be reduced. The reduced core power and the continued steam demand to the turbine causes a reactor coolant temperature decrease. If the reactor is in manual control, the core power rises due to moderator feedback to the initial power level at a reduced core inlet temperature. If the reactor is in automatic control, the control system detects the drop in power and initiates withdrawal of a control bank. Power overshoot above the initial power level may occur as the control system withdraws a bank. Following dropping of one or more RCCAs, the most severe results occur when the control system overshoots the initial power level in conjunction with a perturbation in the radial power distribution. This is the most limiting case for this event, and the results are presented in Section 9.4.3. If the reactor is in any of the subcritical modes, dropping RCCAs will not result in any power transient.

As in the case of dropped RCCAs, statically misaligned RCCAs have no effect in the absence of a critical neutron flux and are not a concern below Mode 2. The most limiting case, and analysis, is for Mode 1 which also bounds Mode 2 operation.

The most limiting case for the withdrawal of a single RCCA is an occurrence while in Mode 1. An occurrence in any of the subcritical modes will have no effect. The shutdown margin requirements are specified in LCO 3.1.1 of the AP1000 Technical Specifications. The shutdown margin requirements are determined assuming the most reactive RCCA is fully withdrawn from the core. Therefore, no single RCCA withdrawal initiated from the subcritical modes will insert enough reactivity to attain criticality.

Because the primary and secondary circuits remain intact and offsite power remains available, there is no release of activity to the environment. Therefore, the radiological consequences of these events presented in Sections 9.4.3.4.1 and 9.4.3.4.2 for the release of activity resulting from a case where offsite power is lost are limiting compared to the event occurring in lower modes.

Thus, this event during any shutdown mode is less limiting than the at-power conditions for which a design basis analysis is provided, as discussed above. In addition, due to the likelihood of these faults occurring at shutdown conditions being categorised as an infrequent or beyond design basis fault, diverse mitigation is not explicitly required. However, since the required protection functions are available in applicable modes of operation, for both primary and diverse mitigation considerations, no further discussion is provided here.

9.8.4.4.4 Startup of an Inactive Reactor Coolant Pump at an Incorrect Temperature (Fault 1.15.6)

This event is precluded from occurring during at-power modes by Technical Specifications. Startup of an inactive RCP while in any of the subcritical modes will have relatively little effect upon core temperature because there will be little or no temperature difference between the loops. Section 9.4.4 discusses the consequences of this event for the AP1000 design.

9.8.4.4.5 Chemical and Volume Control System Malfunction That Results in a Decrease in the Boron Concentration in the Reactor Coolant (Faults 1.15.7 – 1.15.9)

Boron dilution analyses and evaluations for Modes 1 through 5 are provided in Section 9.4.6. Therefore, the design basis analysis documented therein already covers shutdown Modes 3 to 5, which are categorised as DB2 frequent faults.

In Mode 6, administrative controls (operating procedures, system interlocks, and PLS control

logic) isolate the RCS from potential sources of unborated water by locking closed specified valves (DWS header isolation valves, CVS Makeup Flow Containment penetration isolation valves, and the 3-way blend valve) in the CVS, and thereby preclude an uncontrolled boron dilution transient. All of these valves are Class 1 with the exception of the 3-way blend valve, which is C-3. The isolation of all unborated water sources is required by the plant Technical Specifications. Makeup needed during refuelling is supplied from the boric acid tank which contains borated water.

Because the primary and secondary circuits remain intact and offsite power remains available, there is no release of activity to the environment. Therefore, the radiological consequences of this event presented in Section 9.4.6.4 for the release of activity resulting from a case where offsite power is lost are limiting compared to the event occurring in lower modes.

Since the required protection functions discussed in Section 9.4.6 are available in applicable modes of operation, for both primary and diverse mitigation considerations, no further discussion is provided here.

9.8.4.4.6 Inadvertent Loading of a Fuel Assembly in an Improper Position (Fault 1.15.10)

Fuel loading errors – such as inadvertent loading of one or more fuel assemblies into improper positions, having a fuel rod with one or more pellets of the wrong enrichment, or having a fuel assembly with pellets of the wrong enrichment – may result in power shapes in excess of design values. Section 9.4.7 presents Mode 1 results for this event which bound the results for operation in Mode 2. This event is meaningful only if the reactor is at-power and, therefore, not applicable in the subcritical Modes of 3 through 6.

9.8.4.4.7 RCCA Ejection (Faults 1.15.11 and 1.15.12)

Analyses for RCCA ejections in Mode 1 and Mode 2 are presented in Section 9.4.8, and these are categorised as DB1 infrequent faults. The cases analysed in Section 9.4.8 are the most limiting cases. The shutdown margin requirements are specified in LCO 3.1.1 of the AP1000 plant Technical Specifications. The shutdown margin requirements are determined assuming the most reactive RCCA is fully withdrawn from the core. Therefore, the ejection of a single RCCA initiated from the subcritical modes would not insert enough reactivity to attain criticality.

9.8.4.5 Increase in Reactor Coolant Inventory (Faults 1.12.1 – 1.12.5)

An increase in RCS inventory could be caused by inadvertent actuation of the CMTs or by malfunctions in the CVS system, both of which are categorised as DB2 frequent faults. Assuming a reduction in frequency of $1/20^{th}$ for the same event at shutdown conditions, these faults would be categorised as DB1 infrequent faults for shutdown modes. Analyses of events that increase the RCS inventory are provided in Section 9.5. Section 9.5.1 presents the analysis results for inadvertent actuation of the CMT. Section 9.5.2 contains results from the analysis of a CVS malfunction which increases RCS inventory. These events do not present a challenge to core design limits. If unchecked, these events could lead to overfill of the pressuriser and possible loss of reactor coolant from the system. The increase in pressuriser water volume is slow during these events and is determined by the injection rate, core decay heat produced, and heat removal rate from the RCS. While the pressuriser safety valves may open, the steam relief from the pressuriser safety valves is low and no serious challenge to the RCS pressure boundary occurs (if the pressuriser does not fill).

The analyses for these events are performed with the plant initially in Mode 1 at full-power

conditions. This results in the maximum amount of stored energy in the plant and in the maximum core decay heat. If the plant was assumed to be at part power, or in the subcritical modes, the amount of stored energy and decay heat will be significantly reduced.

If a spurious "S" signal occurs causing the CMTs to be actuated, the reactor is also tripped and the PRHR HX is also actuated. The CMTs will begin injecting cold, borated fluid into the RCS. The injected fluid expands as it is heated in the RCS by decay heat. The expansion is counteracted by decay heat removal through the PRHR HX. The severity of the expansion is increased with higher decay heat levels.

Malfunctions in the CVS, which add excess inventory to the RCS, are protected against by the inclusion of automatic CVS isolation functions in the PMS. If a safeguards signal has occurred (which also would activate the CMTs), the CVS is automatically isolated if the pressuriser level exceeds the high-1 pressuriser level setpoint. Above the high-1 pressuriser level setpoint, there is a high-2 pressuriser level setpoint, which also isolates the CVS. The high-2 pressuriser level function is not interlocked with the safeguards signal. The high-2 function protects in situations where the reactor is at-power or a safeguards signal has not occurred. The high-2 pressuriser level function is available in Modes 1 through Mode 3 and in Mode 4 when the RNS is not operating. These functions effectively prevent overfilling of the pressuriser when the CVS acts alone or where CVS interacts to also cause the CMTs to be actuated.

Isolation of CVS on high-2 pressuriser level is available in Modes 1 through 4 until the plant is operating on RNS. There are applications where the RCS may be filled water-solid when the RNS is in operation. In Modes 4, 5, and 6 when the RNS is in operation, low-temperature overpressure protection (LTOP) of the RCS pressure boundary is provided by the RNS relief valve(s). A discussion of this is provided in Section 9.8.4.5.1, below.

Because the primary and secondary circuits remain intact and offsite power remains available, there is no release of activity to the environment. Therefore, the radiological consequences of these events presented in Sections 9.5.1.4 and 9.5.2.4 for the release of activity resulting from a case where offsite power is lost are limiting compared to the event occurring in lower modes. In the event of RCS inventory loss through the RNS relief valve(s) at lower modes, the radiological consequences would be bounded by an RNS line break scenario (See Section 9.8.5.3).

Thus, this event during any shutdown mode is less limiting than the at-power conditions for which a design basis analysis is provided, as discussed above. Since the required protection functions are available in applicable modes of operation, for both primary and diverse mitigation considerations, no further discussion is provided here.

9.8.4.5.1 Low Temperature Overpressure Protection

For the AP1000 design, an RNS suction relief valve is located in each of the two RNS trains, immediately downstream of the RCS suction isolation valves. Each of these relief valves protects the RNS from over pressurisation and provides LTOP for the RCS components when an RNS train is aligned to the RCS to provide decay heat removal during plant shutdown and startup operations. The RNS relief valves are sized to provide LTOP by limiting the RCS and RNS pressure to less than the steady-state pressure limit. Section 17.5.7.2 provides a discussion of the LTOP design bases.

Typically, during normal operations, both RNS trains will be in use during plant cool-downs because that would significantly reduce the duration of the outage compared to use of a single train. In addition, the Short Term Availability Controls prohibit entering reduced inventory

Modes of operation without both RNS trains operable. With both RNS trains operable, there is single failure tolerance for the RNS relief valves.

Although unlikely, it is possible for the plant to enter Modes 4 and 5 with only one RNS train operable. In this case there is no failure tolerance for the RNS relief valves; however, this situation is acceptable because:

- It is unlikely to be in a shutdown condition with only one RNS train operable.
- It is unlikely to have a cold over pressure event in the AP1000 plant.
    - Unlike other PWRs, the AP1000 design does not have any high head safety injection pumps; whereas other PWRs typically have two to four. These pumps are a major source of potential cold over pressure.
    - The AP1000 design only has two CVS makeup pumps and they inject through a common cavitating venturi, which limits their combined makeup. Other PWRs typically have three such pumps and no cavitating venturi.
    - Most of the time during shutdown conditions there is a steam bubble in the pressuriser or the RCS is vented to the containment. Even with just a pressuriser steam bubble, the operator would have time to isolate the water makeup before having a cold over pressure event.
- The RNS relief valves are simple and reliable valves.
    - They are simple spring loaded designs with no C&I controls, valve operators, or power supplies.
    - These UK Safety Class 1 valves undergo extensive equipment qualification testing and additional in-service testing during plant operation.
        - Same valve type as those used for pressuriser steam generators, and elsewhere. Single failures are not considered credible in any of these applications, consistent with the ASME code.
- In the unlikely multi-failure event where only one RNS train was in service, a CVS pump spuriously operated without RCS letdown, and the RNS relief valve failed, core cooling would not be lost.
    - The limiting failure would be a rupture of the RNS piping outside containment. This is a design basis fault (Table 8A-2, faults 2.3.1-2.3.3) where the ADS valves would be opened and the RNS automatically isolated using Class 1 SSCs.

9.8.4.6 Decrease in Reactor Coolant Inventory

9.8.4.6.1 Inadvertent Opening of a Pressuriser Safety Valve or Inadvertent Operation of the Automatic Depressurisation System (Fault 1.5.2)

Section 9.6.1 includes analyses and evaluations of the inadvertent opening of a pressuriser safety valve, a DB1 infrequent fault, or the inadvertent operation of the ADS, a beyond design basis fault.

When analysed as depressurisation events, inadvertent opening of primary side relief valves, if the reactor is at-power, could result in exceeding core design limits, specifically DNB criteria. Violation of DNB criteria is not a realistic concern if the reactor is in any of the subcritical modes. Therefore, these events are analysed in Mode 1 at the maximum rated power and the analysis performed bounds cases initiated from Mode 2. These events bound events that can occur at shutdown.

The inadvertent ADS event is analysed as a loss-of-coolant accident in Mode 1 to demonstrate acceptance to the limits specified in 9.6.5. As described in Section 9.6.5, this

analysis is a "no-break" small-break LOCA calculation. The inadvertent opening of the 4-inch (102 mm) nominal size ADS Stage 1 valves is a situation that minimizes the venting capability of the RCS. Only the ADS valve vent area is available; no additional vent area exists due to a break. This case examines whether sufficient vent area is available to completely depressurise the RCS and achieve injection from the IRWST without core uncovery. The case analysed at-power bounds the inadvertent ADS during shutdown because the lower decay heat levels at shutdown reduce the challenge to the ADS vent capacity. More limiting loss-of-coolant accidents at shutdown are described in Section 9.8.5.

The radiological consequences of this event presented in Section 9.6.1.4 are limiting because the assumed consequential fuel damage bounds that which could result in the other modes.

Thus, this event during any shutdown mode is less limiting than the at-power conditions for which a design basis analysis is provided, as discussed above. Since the required protection functions are available in applicable modes of operation, no further discussion is provided here.

9.8.4.6.2 Failure of Small Lines Carrying Primary Coolant Outside Containment (Fault 1.9.2)

This DB2 frequent fault event is reported in Section 9.6.2 as the rupture of a primary coolant sample line; the radiological consequences of this event are analysed during Mode 1 because the coolant temperature and activity concentrations bound those that would exist in the other modes. Concerning shutdown risk, the consequences of a sample line break during Modes 2, 3, 4, or 5 are no more severe than if the accident occurs during Mode 1 operation.

Assuming a reduction in frequency of $1/20^{th}$ for the same event at shutdown conditions, this fault would be categorised as a DB1 infrequent fault for shutdown modes. As discussed above, this event during any shutdown mode is less limiting than the at-power conditions for which a design basis analysis is provided. In addition, due to the likelihood of this fault occurring at shutdown conditions being categorised as an infrequent fault, diverse mitigation is not explicitly required. However, since the required protection functions are available in applicable modes of operation, for both primary and diverse mitigation considerations, no further discussion is provided here.

9.8.4.6.3 Steam Generator Tube Rupture (Faults 1.11.1 – 1.11.3)

The DB2 cliff edge frequent fault SGTR analysis presented in Section 9.6.3 is the limiting case with respect to offsite doses. Assuming a reduction in frequency of $1/20^{th}$ for the same event at shutdown conditions, this fault would be categorised as a DB1 infrequent fault for shutdown modes. The analysis was performed at full power because this results in the maximum offsite dose. The key inputs from the thermal-hydraulic SGTR analysis to the offsite dose analysis are the amount of primary to secondary break flow and the steam released from the ruptured steam generator. Both of these will be significantly reduced at lower power levels and in lower modes of operation. Also the RCS activity concentrations (including consideration of iodine spikes) bound those that would exist in the other modes.

A margin to overfill analysis is presented in Section 9.6.3. The analysis is performed to demonstrate margin to steam generator overfill with no operator actions modelled. This is necessary because the dose analysis does not include consideration of water relief from the ruptured steam generator PORV/main steam safety valve (MSSV). This margin to steam generator overfill analysis was supported by the assertion that an analysis with operator actions modelled will also demonstrate margin to overfill. The overfill analysis with no operator actions discussed in Section 9.6.3 was initiated at full power. WCAP-10698-P-A (Reference 9.8-3) indicates that margin to overfill is reduced when the SGTR is initiated at

zero power because of the higher initial steam generator secondary liquid inventory. WCAP-10698-P-A concludes that zero power and lower mode SGTR overfill analyses are not limiting, based primarily on more rapid operator responses expected in those conditions. This is discussed further in the Appendices to WCAP-10698-P-A. When operator actions are credited for SGTR mitigation for the AP1000 design, the plant behaves in a manner comparable to a standard Westinghouse PWR and the conclusions of WCAP-10698-P-A apply.

When operator actions are not relied upon and only the automatic RCS cooling and depressurisation are credited, margin to overfill would still be maintained for SGTR events initiated at lower power levels and lower modes despite the increased initial steam generator secondary side inventory corresponding to the lower initial power assumption. This is because the automatic protection system actions that prevent overfill are independent of the operator actions. For operating plants, there is a set period of time from the start of the event until the operator can reverse the trend toward filling the steam generator. Therefore, the initial margin to overfill directly impacts the final margin. For the AP1000 design, the primary cooldown and depressurisation occur automatically when the PRHR HX is actuated on a low pressuriser pressure "S" signal or low pressuriser level CMT actuation signal. The primary pressure may still be held up by the CVS, until it is isolated on a high steam generator level signal. For the AP1000 design, a higher initial steam generator water level results in the CVS flow being terminated earlier.

In Mode 4, the PRHR HX actuation is provided only by the low pressuriser level signal. Although this results in delayed cooling and depressurisation, margin to steam generator overfill is still maintained. The increase in mass in the secondary side of the ruptured steam generator is directly related to the reduction in pressuriser water level, because (once the CVS is isolated on high steam generator water level) there is no source of makeup to the RCS. The steam generator secondary side can accommodate the amount of fluid initially contained in the pressuriser and still retain a significant amount of margin to steam generator overfill. The PRHR HX will, therefore, be actuated on low pressuriser water level in sufficient time for the PRHR HX to cool and depressurise the primary and terminate break flow before steam generator overfill will occur.

In Modes 5 and 6, the RCS pressure and temperature are reduced; thus, an SGTR event is not considered credible. In summary, this event during any shutdown mode is less limiting than the at-power conditions for which a design basis analysis is provided, as discussed above. In addition, due to the likelihood of this fault occurring at shutdown conditions being categorised as an infrequent fault, diverse mitigation is not explicitly required. Since the required protection functions are available in applicable modes of operation no further discussion is provided here.

9.8.4.6.4 Loss-of-Coolant Accident Events in Shutdown Modes (Faults 1.2.1 – 1.2.3, 1.4.1 – 1.4.3, 1.6.1, 1.7.1, 1.8.1 – 1.8.4, 1.9.1 – 1.9.2, and 1.10.1)

Section 9.6 presents a spectrum of break sizes of the postulated LOCAs at the full-power operating condition. Other things being equal, the reduction in power to decay heat levels associated with shutdown mode operations will make all LOCA events less limiting than those analysed at full power and reported in Section 9.6. However, as the plant proceeds through shutdown modes of operation, various PXS equipment are removed from service at identified points in time. One particularly significant action in the elimination of PXS equipment in the course of taking the AP1000 plant to cold shutdown, is the isolation of the accumulators at 6.895 MPa gauge (1000 psig). This procedural action reduces the capability of the PXS to mitigate LOCAs. For assessing the adequacy of the remaining PXS

components to mitigate postulated LOCA events, the limiting double-ended cold-leg guillotine (DECLG) break, analysed in Section 9.6.4, is analysed assuming it occurs immediately after the isolation of the accumulators (this results in limiting conditions as it maximises decay heat, since the time from shutdown is shorter, and the initial temperature and pressure are higher). The analysis is performed using the AP1000 Large-Break LOCA WCOBRA-TRAC model used for the at-power Design Basis Accident analysis. Only Class 1 systems are modelled in the analysis of this event.

Depressurisation of the AP1000 primary system during shutdown operations will be performed with the same care taken to avoid the flashing of liquid in the core and upper head that is taken by current operating plants. Prudent plant operation dictates that subcooling margin be retained as pressure is reduced. Therefore, since the AP1000 plant shutdown operations will be conducted in a prudent, controlled manner, it is anticipated that the RCS temperature will be near the 215.6°C (420°F) lower limit of Mode 3 when the accumulators are isolated.

For these analyses, the plant was assumed to be shut down in Mode 3 at steady-state conditions of 6.895 MPa gauge (1000 psig) and 218.3ºC (425°F) with the accumulators isolated. An initial pressure of 6.895 MPa gauge (1000 psig) is assumed because this is the highest pressure with the accumulators isolated and a hot-leg temperature of 218.3ºC (425°F) is the highest expected temperature when the pressure is 6.895 MPa gauge (1000 psig). The decay heat level is determined at 2.78 hours after reactor shutdown based on the time estimate to cool down the plant from full-power operation to 218.3ºC (425°F) at a cooldown rate of 27.8°C (50°F) per hour. The low pressuriser pressure safeguards signal is also assumed to be disabled because the initial pressure is below the setpoint.

Note, the assumed temperature of 218.3ºC (425°F) reflects normal operating practice, and is approximately 40ºC (72°F) lower than the maximum allowable hot leg temperature required by operating procedures to ensure RCS subcooling. However, the assumption is not expected to have a large impact on the analysis results.

The standard plant shutdown LOCA analyses are limited to a Mode 3 large-break LOCA due to the fact that this fault has the highest level of decay heat with accumulators unavailable, the largest break size, and thus the most severe depressurisation and loss of coolant. This fault is expected to be more limiting than a smaller break loss of coolant accident and/or a LBLOCA at any other lower mode. These expectations will be confirmed during site licensing and documented accordingly.

9.8.4.6.4.1 Double-Ended Cold-Leg Guillotine

The DECLG break is analysed using the WCOBRA/TRAC computer code and the AP1000-specific noding, which is based on the AP600 noding, presented in WCAP-14171, Revision 2 (Reference 9.8-4). Table 9.8.4-1 summarises the results.

This case models the double-ended rupture of one of the two cold legs in the RCS loop without the PRHR HX at a pressure of 6.895 MPa gauge (1000 psig) just after the accumulators are isolated. Only the CMTs and IRWST are available to deliver PXS flow. Analysis of this break evaluates the ability of the plant to withstand a large LOCA during shutdown with associated conditions and equipment availability. The nominal discharge coefficient (1.0) is modelled. The analysis is performed with conservative decay heat in alignment with that used in the at-power design basis analysis, and Technical Specification/Core Operating Limits Report maximum peaking factors.

The break is assumed to open instantaneously at 0.0 seconds. The subcooled discharge from

the broken cold leg (Figure 9.8.4-1) causes a rapid RCS depressurisation (Figure 9.8.4-2). In Figure 9.8.4-1, the positive flow direction is the normal operation direction. The reversal of flow entering the vessel to flow out of the break is shown. Due to High-1 containment pressure, an "S" signal is generated at 2.2 seconds. Following a 2.0-second delay, the isolation valves on the CMT and PRHR HX outlet lines begin to open. The reactor coolant pumps trip at 9.5 seconds.

Within a few seconds, the collapsed liquid level drops within the upper plenum due to voiding (Figure 9.8.4-3). The downcomer collapsed liquid level (Figure 9.8.4-4) quickly falls below the elevation of the cold legs; the elevation of the top of the core is 6.26 meters (20.54 feet) above the bottom of the reactor vessel.

CMT injection from both tanks replenishes the RCS mass inventory. Injection from the CMTs as the RCS pressure declines terminates the PCT transient because the stable injection of water from the CMTs exceeds the break flow. The core collapsed level refills are as shown in Figure 9.8.4-5. The draining of the CMTs is delayed by condensation occurring at the top of the tank (Figure 9.8.4-7); the CMT connected to the broken cold leg via the balance line does not begin to drain until the end of blowdown. The maximum PCT value is approximately 910°C (1671°F) for this bounding break size as shown in Figure 9.8.4-6, and all the acceptance criteria are met.

The radiological consequences of these events presented in Section 9.6 are limiting because the assumed consequential fuel damage bounds that which could result in the other modes.

9.8.4.6.4.2 DBA Credited SSCs

For the design basis evaluation of this DB1 infrequent fault, no claim is placed on systems which are not Class 1. The PMS provides the following:

- CMTs and containment isolation on High-2 containment pressure
- ADS 1-4 on Low CMT level
- IRWST injection on Low CMT level (via ADS 4 actuation signal)
- Containment recirculation on Low IRWST level
- PCS on High-2 containment pressure

9.8.5 AP1000 Safety Evaluation of Faults Specific to Shutdown Modes

9.8.5.0 Introduction and Overview of Faults

Section 2 of Table 8A-2 includes identification of potential faults to be considered that are specific to shutdown modes. As discussed in the review of postulated initiating events in Section 9.8.4, these faults are associated with the alignment of the RNS system to provide decay heat removal in Modes 4, 5 and 6. With RNS operation, most of the protection and transient evolution discussed for the at-power events is not applicable, and hence specific design basis analyses have been performed.

9.8.5.0.1 Failure of RNS during Mode 4 and 5, with RCS intact (Fault 2.1.2)

Section 9.8.5.1 provides the design basis analysis for this case. In Table 8A-2, this fault is identified as a frequent fault (DB2) and as such diverse core cooling analysis cases are required.

To bound all potential initiating events, the following assumptions are made in the design basis analysis:

a. The initiating event is postulated as a loss of offsite power, followed by a complete failure of the Class 2 cooling chain (e.g., loss of both DG trains or loss of both RNS trains, or loss of both SWS/CCS trains). Thus, only Class 1 features are credited in the analysis.

b. The worst initiating conditions are assumed from Mode 4 operation including the highest RCS temperatures and decay heat.

c. The worst assumptions relative to availability of Class 1 features between Mode 4 and Mode 5 (with RCS intact) are made. These are summarised by Table 9.8.3-1.

9.8.5.0.2 Failure of RNS during Mode 5 and 6, with RCS open (Faults 2.1.3 and 2.1.4)

Section 9.8.5.2 provides the design basis analysis for this case and bounds faults 2.1.3 and 2.1.4. In Table 8A-2 this fault is identified as an infrequent fault (DB1).

To bound all potential initiating events, the following assumptions are made in the design basis analysis:

a. The initiating event is postulated as a loss of offsite power, followed by a complete failure of the Class 2 cooling chain (e.g., loss of both DG trains, or loss of both RNS trains, or loss of both SWS/CCS trains). Thus, only Class 1 features are credited in the analysis.

b. The worst initiating conditions are assumed from Mode 5 operation including the highest RCS temperature and decay heat consistent with reduced RCS inventory.

c. The worst assumptions relative to availability of Class 1 features between Mode 5 (with RCS open) and Mode 6 are made. These are summarised by Table 9.8.3-1.

9.8.5.0.3 Loss of Coolant Accidents Involving RNS (Fault 2.3.1 – 2.3.3)

Section 9.8.5.3 provides the design basis analysis for this case and bounds faults 2.3.1-2.3.3. In Table 8A-2 this fault is identified as an infrequent fault. This section discusses postulated breaks in the RNS piping during RNS operation in shutdown Modes 4, 5, and 6. Breaks in the RNS inside containment are bounded by the MBLOCA (Faults 1.4.1 – 1.4.3) in Modes 4, 5, and 6 presented in Section 9.8.4.6.4. For breaks outside of containment, the break flow is lost and is therefore unavailable for containment recirculation flow, so the scenario is not bounded by an MBLOCA inside containment. This section therefore provides the analysis of RNS breaks outside of containment.

9.8.5.1 Failure of RNS During Mode 4 and 5, with RCS intact (Fault 2.1.2)

9.8.5.1.1 Identification of Causes and Accident Description

For this analysis, it is assumed that the RNS has just been placed in operation at 2 hours after reactor shutdown with the RCS at 176.7°C (350°F) and 2.76 MPa gauge (400 psig). It is assumed that a loss of offsite power occurs, followed by a failure of the Class 2 cooling chain, resulting in a loss of flow through the RNS, and thus, in a loss of RNS cooling. The MSS is assumed to be unavailable for heat removal during the event except for the MSSVs. The steam generator secondary side is assumed to be at saturated conditions for 176.7°C (350°F) with the normal water level. Because the Mode 4 plant conditions assumed for the analysis are more limiting than Mode 5 conditions, this analysis also bounds a loss of RNS cooling in Mode 5 when the RCS is intact.

It is assumed that only one CMT is available for injection because Technical Specifications permit one CMT to be taken out of service in Mode 4. If both CMTs are available, the overall results should be similar, although the timing of the event will be affected by the additional injected makeup mass. Even though all of the fourth-stage ADS valves are available in Mode 4, the Technical Specifications permit one of the fourth-stage ADS valves to be out of service in Mode 5 when the RCS is intact. Thus, it was assumed that only three of the fourth-stage ADS valves are available for operation to bound the equipment availability in Mode 5. In addition, one of the three available fourth-stage ADS valves is assumed to fail to open on demand as the single failure, consistent with the single failure assumption used for the full power small-break LOCA analyses. The assumption of a failure of one ADS fourth-stage valve is more important than the number of CMTs available considering that the RCS has so little stored energy and decay heat.

One design basis case was analysed. This case credits the PMS, PRHR, CMT, ADS 1, 2, 3, and 4, IRWST injection and containment recirculation. As such it allows for automatic safety system actuation on a low pressuriser level signal later in the event. Until this time, the primary mechanism for removing decay heat is boiling off the RCS inventory and venting through one RNS relief valve.

Two diverse cases are provided, including a primary diverse case and a backup diverse case. The primary case credits the PMS, CMT, ADS 1, 2, 3, and 4, IRWST injection and containment recirculation. As such it allows for automatic safety system actuation on a low pressuriser level signal. Until this time, the primary mechanism for removing decay heat is boiling off the RCS inventory and venting through one RNS relief valve. The diverse case credits DAS and PRHR. Manual operator action is credited at 1800 seconds (30 minutes) after the loss of RNS cooling. With the more reasonable assumptions appropriate for diverse cases the PRHR is able to successfully cool the core without the need for ADS.

9.8.5.1.2 DBA and Diverse Credited SSCs for Accident Mitigation

For this fault, the available SSCs credited are listed in fault 2.1.2 in Table 8A-2. All of these SSCs are Class 1 except for the Class 2 DAS in the Backup Diverse case.

For the DBA, the PMS provides the following:

- No reactor trip is required, as the reactor is already shutdown
- PRHR, CMTs, and containment isolation on Low-2 pressuriser level
- ADS 1-4 on Low CMT level

- IRWST injection on Low CMT level (via ADS 4 actuation signal)
- Containment recirculation on Low IRWST level
- PCS on High-2 containment pressure.

For the primary diverse case, the PMS provides the following:

- No reactor trip is required, as the reactor is already shutdown
- CMTs, and containment isolation on Low-2 pressuriser level
- ADS 1-4 on Low CMT level
- IRWST injection on Low CMT level (via ADS 4 actuation signal)
- Containment recirculation on Low IRWST level
- PCS on High-2 containment pressure.

For the backup diverse case, the DAS provides the following:

- No reactor trip is required, as the reactor is already shutdown.
- Manual PRHR actuation
- PCS and containment isolation on High containment temperature

9.8.5.1.3 Analysis of Effects and Consequences

9.8.5.1.3.1 DBA Case - Automatic Safety Injection Actuation

The accident analysed is a loss of RNS cooling, which is assumed to result in a complete loss of heat removal for the RCS. The sequence of events for this analysis is presented in Table 9.8.5-1. The loss of RNS cooling occurs at 2 hours after reactor shutdown.

Following the loss of RNS cooling, there is no active mechanism for heat removal from the RCS. The core decay heat generation causes the reactor coolant temperature and pressure to increase. Although the MSS is assumed to be unavailable for heat removal (with the exception of the MSSVs), the steam generators represent a heat sink that slows the rate of heatup of the reactor coolant. The fluid temperature at the core outlet for the transient is shown in Figure 9.8.5-1. The reactor coolant heatup causes the system pressure to increase, as shown in Figure 9.8.5-2, until the pressure reaches the RNS relief valve setpoint of 3.45 MPa gauge (500 psig) at approximately 2.19 hours. The normal relieving capacity of one RNS relief valve is 225 m^3/hr (991 gpm) at 3.79 MPa (550 psig), and the pressure is maintained at the relief valve setpoint as the temperature continues to increase and reactor coolant is discharged from the relief valve. Flow out the relief valve is shown in Figure 9.8.5-3. The expansion of the water due to the coolant temperature increase also causes the pressuriser level to increase slightly as shown in Figure 9.8.5-4.

The loss of reactor coolant through the relief valve is not sufficient to remove the core decay

heat, and the reactor coolant temperature continues to increase until the core outlet temperature reaches saturation near the relief valve setpoint at approximately 2.73 hours. The generation of steam in the core causes the system pressure to increase above the RNS relief valve setpoint and the pressuriser level to continue to increase. A mixture level begins to form in the upper plenum at approximately 2.74 hours and drops to the top of the hot-leg elevation as shown in Figure 9.8.5-5. At about 2.88 hours, enough mass has been discharged such that a mixture level also forms in the downcomer (Figure 9.8.5-6) and the downcomer two-phase level begins to decrease. As the boiling front moves lower and lower into the core, more steam generation occurs and the pressure continues to increase. Once the entire core length is boiling, the upper plenum mixture level is within the hot-leg perimeter. There is a brief period of two-phase discharge out the RNS relief valve when the upper plenum mixture level drops near the bottom of the hot leg at approximately 4 hours. Following this period there is sufficient steam generation due to the loss of the heat sink that vapour is able to flow into the pressuriser and promote pressuriser draining.

As the pressuriser level decreases, a CMT actuation signal is generated automatically on low pressuriser level. Following a 2.0-second delay, the isolation valves on the available CMT tank delivery lines begin to open and CMT injection flow is initiated at approximately 4.23 hours as shown in Figure 9.8.5-7. This signal also trips the RCPs. The opening of the PRHR HX isolation valve on a CMT actuation signal starts the flow through the heat exchanger. The CMT injection and PRHR actuation causes the reactor coolant pressure to decrease below the RNS relief valve setpoint, and the loss of reactor coolant is terminated at approximately 4.37 hours. As the CMT level decreases (Figure 9.8.5-8), the first-stage ADS setpoint at 67.5 percent volume is reached and flow initiates at 4.36 hours. The second-stage and third-stage ADS valves also open following the timer delays for the actuation of the second-stage and third-stage ADS valves. The vapour and liquid flow through the ADS valves (Figures 9.8.5-9 and 9.8.5-10) results in a rapid depressurisation of the reactor coolant system. The CMT reaches the fourth-stage ADS setpoint of 20 percent volume and two of the four fourth-stage paths open at 4.53 and 4.55 hours. As noted previously, it is assumed that one of the fourth-stage paths is out of service and one path is assumed to fail as the single active failure. The vapour and liquid flow through the fourth-stage ADS paths (Figures 9.8.5-11 and 9.8.5-12) further reduces the pressure to the point where IRWST injection begins at approximately 4.73 hours (Figure 9.8.5-13).

The CMT and IRWST injection reverses the decrease in the core stack and downcomer mixture levels as shown in Figures 9.8.5-5 and 9.8.5-6, respectively. As shown in Figure 9.8.5-5, the core stack mixture level is maintained above the elevation of the top of the core active fuel (6.26 m [20.54 feet] above the bottom of the reactor vessel) throughout the transient. At the end of the transient, the core stack mixture level has been restored to within the hot-leg perimeter and the downcomer mixture level has been restored to the DVI nozzle elevation. The fluid temperature at the core outlet has also been reduced and is being maintained at less than 121.1°C (250ºF). As shown in Figure 9.8.5-14, the reactor coolant mass inventory twice reaches a minimum of approximately 55,000 kg (122,000 lbm) and then 48,000 kg (106,000 lbm) when the CMT and IRWST injection then increase the inventory. The reactor coolant mass inventory has stabilized near 65,000 kg (144,000 lbm) at the end of the transient. Thus, it is concluded that the consequences of a loss of RNS in Modes 4 and 5 with the RCS intact are acceptable.

9.8.5.1.3.2 Primary Diverse Case – Automatic Safety Injection Actuation

This case has not been analysed at this time. However, it is fully expected to be successful because, as compared to the design basis case:

- A reduction of decay heat margin to be in line with that used for all other non-LOCA

faults. The analysis currently uses the more restrictive LOCA decay heat margin.
- An increase in the time assumed when RNS is initially aligned to cool RCS. It is currently conservatively assumed to occur faster than any realistic plant schedule would allow.
- The single failure of one ADS stage four valve to open need not be assumed since a CCF of the PRHR is assumed.

Since the PRHR HX is not credited in this diverse case, that will tend to shorten the time window available for action after the loss of RNS. However, this difference is more than compensated for by the above noted analysis improvements. As further evidence, the diverse core cooling case for loss of main feedwater (presented in Section 9.2.7.3.2) also credits core cooling by passive feed and bleed. This case credits a similar set of SSCs (PMS, CMTs, ADS, IRWST injection and Containment recirculation). The only difference in credited SSCs is that both CMTs are available to inject instead of one; however, this is offset by a higher RCS initial temperature and initial decay heat levels as well as early ADS actuation.

9.8.5.1.3.3 Backup Diverse Case – Manual PRHR HX actuation

This case has not been analysed at this time. However, it is fully expected to be successful because, as compared to the design basis case:

- A reduction of decay heat margin to be in line with that used for all other non-LOCA faults. The analysis currently uses the more restrictive LOCA decay heat margin.
- An increase in the time assumed when RNS is initially aligned to cool RCS. It is currently conservatively assumed to occur faster than any realistic plant schedule would allow.
- PRHR HX performance will be improved and more realistic, as it currently is artificially degraded for DBA SBLOCA analyses to conservatively account for uncertainties.

In this case, ADS is not credited so the PRHR HX by itself must limit the RCS mass loss out the RNS relief valve(s) and prevent core uncovery. The above differences significantly improve the PRHR HX performance. Over time, as RCS mass is lost, the hot legs will void, which will allow steam to enter the PRHR HX. In this mode of operation the PRHR HX heat transfer is enhanced by two effects. One is the greater density difference between hot water and steam, and the other is the higher heat transfer coefficient for steam condensation compared with water. This functionality was examined in detail in support of the frequent fault SBLOCA diversity analyses (See Section 9.6.5.3.4.2).

9.8.5.1.3.4 Radiological Consequences

The radiological consequences of a postulated loss of RNS cooling are evaluated.

9.8.5.1.3.4.1 Source Term

There is no fuel damage as a result of the accident. Therefore, the only activity available for release is that present in the primary coolant. The initial reactor coolant system noble gases, alkali metals, and iodines concentrations are assumed to be those associated with the equilibrium operating limit for primary coolant iodine activity. This evaluation conservatively includes consideration of an iodine spike that has resulted in an increased level of iodine in the reactor coolant. This spike is assumed to have resulted from the plant shutdown, cooldown and depressurisation associated with the transition from power operation to shutdown cooling. This spike is considered unlikely and not required for consideration in the accident dose calculations. Despite this the spike has been included in this evaluation. This spike has been included even though it is not a normal occurrence and increased clean

up would be initiated in response to its occurrence such that by the time an accident occurs there would no longer be an elevated iodine concentration.

9.8.5.1.3.4.2 Release Pathways

Failures of the RNS to cool the RCS would result in boiling of the RCS and the steam generated would be released to containment (directly if the RCS is open and via vent paths if the RCS is closed). The doses resulting from failures of the RNS are conservatively estimated assuming all activity in the RCS becomes airborne in containment. The resulting doses therefore bound failures of the RNS in both non-drained and drained conditions.

It is assumed that following a loss of RNS cooling containment would be closed prior to initiation of RCS boiling. Prior to allowing containment to be opened the standard practice would be to perform an assessment of the potential for boiling if a loss of cooling would occur and only open containment if this evaluation shows that sufficient time would be available to re-close containment before RCS boiling. It is noted that the plant Technical Specifications, Limiting Condition for Operation 3.6.8, includes requirements that open equipment hatches, air lock doors and spare penetrations can be closed prior to steaming into the containment. This provides a high level of confidence that a loss of RNS would not result in a release of significant RCS activity without containment being isolated.

9.8.5.1.3.4.3 Dose Calculation Models

The models used to calculate offsite and control room doses are provided in Appendix 9A.

9.8.5.1.3.4.4 Analytical Assumptions and Parameters

The assumptions and parameters used in the dose analysis are listed in Table 9.8.5-5. Instead of a detailed analysis the dose is conservatively estimated by comparing the activity that could become airborne in containment following a loss of RNS to that modelled in the LOCA analysis presented in Section 9.6.4.4 and calculating a proportional change in the doses.

9.8.5.1.3.4.5 Doses

The conservatively estimated maximum doses for all relevant pathways (inhalation, cloudshine, and groundshine) are as follows:

- Offsite dose: 0.225 mSv Worker dose: 0.326 mSv

These doses are within the Target 4 BSL for frequent faults (1 mSv offsite and 20 mSv onsite) as required for the loss of RNS in Modes 4 or 5 with the RCS closed. Therefore, these doses also support the infrequent fault Target 4 BSL for the loss of RNS in Modes 5 and 6 with the RCS open.

9.8.5.1.3.5 ALARP Evaluation

For this fault, Class 1 SSCs has been shown to be adequate to meet DB requirements. In addition, since this fault is classified as DB2, diverse mitigation is provided. The diverse mitigation uses Class 1 SSCs except for the C&I which is Class 2.

As discussed in Chapter 9.0.15, the standard AP1000 design has incorporated ALARP considerations throughout its development. Furthermore, the standard AP1000 plant design incorporates numerous features that reduce shutdown risk as discussed in Section 9.8.3. One of the more important features is reduced containment leak paths (fewer penetrations,

improved isolation valves, backup DAS actuation, and passive containment cooling) and the ability to close containment during shutdowns. In addition, the current risk of a large radioactivity release during shutdown conditions is significantly less than the SAP Target 8 BSO.

The radiological consequences presented to cover this fault (See Section 9.8.5.1.3.4) are slightly above the Target 4 BSO. However, the analysis performed during the Generic Design Assessment (GDA) has considerable conservatism, as the current analysis is an evaluation using a more limiting event. A commitment exists to update all radiological consequences analyses during site licensing. There are reasonable adjustments to be incorporated into the analysis for the loss of RNS faults that will bring the resultant doses below the Target 4 BSO. These include performing an event specific analysis rather than a comparison evaluation to more limiting faults.

Additionally, there are a number of conservatisms in the presented thermal hydraulic analyses that could be adjusted in order to demonstrate additional margin with respect to acceptance criteria. These include a reduction in decay heat margin for this fault to be in line with that used for all other non-LOCA faults and use of more realistic PRHR performance for the diverse cases.

Nonetheless, several potential enhancements have been identified for further evaluation in site licensing to confirm risks have been reduced ALARP. These potential enhancements include:

- A Technical Specification change to adjust the point when RNS is initially aligned to cool the RCS; specifically, to consider limiting RNS alignment to a point with a specific decay heat level. This would allow for a mechanistic, yet still conservative, timing assumption to be included in the presented analyses. Currently, RNS alignment is conservatively assumed to occur faster than any realistic plant schedule would allow.
- Consideration of instituting an automatic start of PRHR via DAS on a lower high hot leg temperature setpoint during shutdown conditions. This would primarily benefit the diversity evaluation for this fault.

Accounting for the ALARP considerations that went into the AP1000 design development, its low risk profile, and the expected demonstration of meeting the Target 4 BSO during site licensing as discussed above, making further improvements to the design are expected to be grossly disproportionate to the risk reduction that might be achieved. As a result, the current design with the above potential enhancements is considered ALARP.

9.8.5.2 Failure of RNS during Mode 5 and 6, with RCS Open (Faults 2.1.3 and 2.1.4)

9.8.5.2.1 Identification of Causes and Accident Description

For this analysis, it is assumed that the RNS is in operation in Mode 5 at 24 hours after reactor shutdown with the ADS Stage 1, 2, and 3 valves open and the RCS vented to the IRWST (see Table 9.8.3-1). The reactor coolant temperature is assumed to be at 71.1°C (160°F), and the pressuriser pressure is assumed to be at atmospheric pressure plus the elevation head in the IRWST, or 0.125 MPa abs (18.2 psia). The steam generator secondary side is assumed to be drained, and thus, there is no secondary heat sink for this case. It is assumed that the CMTs and the PRHR are not available because the Technical Specifications permit them to be taken out of service in Mode 5 with the RCS open. It is also assumed that only two of the fourth-stage ADS valves are available for potential use by the operators because the Technical Specifications permit two of the fourth-stage ADS valves to be out of

service in Mode 5 when the RCS is open. In addition, one of the two available fourth-stage ADS valves is assumed to fail to open on demand as the single failure. The Technical Specifications also permit one of the two IRWST injection paths to be out of service in Mode 5 with the RCS open, and thus, only one of the IRWST injection paths is assumed to be available.

It is assumed that a loss of offsite power occurs, followed by a complete loss of the Class 2 cooling chain, resulting in a loss of RNS flow, and thus a loss of RNS cooling. The sequence of events for this analysis is presented in Table 9.8.5-2.

9.8.5.2.2 DBA Credited SSCs

For the DBA, no claim is placed on systems which are not Class 1. The PMS provides the following:

- No reactor trip is required, as the reactor is already shutdown.
- ADS 4 on Low hot leg level; no ADS 1-3 actuation is required as the valves are already open in Mode 5 with the RCS open and Mode 6. Only 1 of 4 ADS-4 valves is assumed available (2 out of service and 1 single failure).
- IRWST injection on Low hot leg level
- Containment recirculation on Low IRWST level
- PCS and containment isolation on High containment temperature

9.8.5.2.3 Analysis of Effects and Consequences

9.8.5.2.3.1 Mode 5 RCS Open Prior to Draining

For this case, the loss of RNS cooling is conservatively assumed to occur at 24 hours; this is the earliest timing of an RCS open condition and leads to the most highest initial decay heat and the most limited venting capability to the RCS. The loss of RNS cooling causes the failure of the normal RCS cooling mechanism. Core decay heat generation then results in an increase in the reactor coolant temperature. The fluid temperature at the core outlet for the transient is shown in Figure 9.8.5-18. The core outlet fluid temperature increases steadily until approximately 24.61 hours when saturation temperature is reached and voiding is initiated in the core. Because the RCS is vented to the IRWST via the already open ADS Stages 1, 2, and 3, the pressure initially remains constant until approximately 24.5 hours as shown in Figure 9.8.5-19. As the void generation in the system increases, the vapour flow through ADS Stages 1, 2, and 3 is not sufficient to maintain the pressure. The pressure increases to approximately 0.410 MPa abs (59.5 psia), and then begins to decrease. As shown in Figure 9.8.5-20, the pressuriser level also increases as the reactor coolant temperature increases. The level subsequently reaches the top of the pressuriser as a result of the steam generation in the system. As shown in Figures 9.8.5-21 and 9.8.5-22, a mixture of steam and water is discharged via ADS Stages 1, 2, and 3 after the pressuriser fills.

The continued loss of reactor coolant through ADS Stages 1, 2, and 3 causes the pressure to begin to decrease at approximately 25 hours. The core outlet temperature is at saturation and also begins to decrease as the pressure decreases. A mixture level begins to form in the upper plenum at approximately 24.65 hours, and the level begins to decrease, as shown in Figure 9.8.5-23, as the voiding continues in the system. At about 24.70 hours, enough mass has been discharged that a mixture level forms in the downcomer (Figure 9.8.5-24) and the

downcomer level also begins to decrease. The pressuriser level does not decrease significantly due to an increasing void fraction in the pressuriser.

As the voiding in the core continues, the core stack mixture level continues to decrease as shown in Figure 9.8.5-23. The mixture level in the hot legs begins to decrease after 24.66hours (Figure 9.8.5-25). The hot legs are approximately empty by 25.16 hours. Hot leg empty is the normal signal for opening the fourth-stage ADS valves and to initiate IRWST injection when the systems are aligned for automatic actuation[1]. It is also the indication that will prompt operators to actuate the fourth-stage ADS valves and as such, it is assumed that the operator will initiate manual action shortly before 25.20 hours (following a two minute delay) to open the fourth-stage ADS valves and to open the IRWST flow path to permit IRWST injection when the downcomer pressure is sufficiently low. Discharge through one of the fourth-stage ADS valves is initiated at 25.20 hours as shown in Figures 9.8.5-26 and 9.8.5-27. As noted previously, one of the two available fourth-stage ADS paths is assumed to fail to open as the single active failure. The flow through the fourth-stage ADS path results in a further reduction in the pressuriser pressure and a rapid decrease in the pressuriser level. The downcomer pressure is also reduced to the point where IRWST injection is initiated at approximately 25.35 hours (Figure 9.8.5-28).

The IRWST injection reverses the decrease in the core stack and downcomer mixture levels as shown in Figures 9.8.5-23 and 9.8.5-24, respectively. As shown in Figure 9.8.5-23, the core stack mixture level is maintained well above the elevation of the top of the core active fuel (6.26 m [20.54 feet] above the bottom of the reactor vessel) throughout the transient. At the end of the transient, the core stack mixture level has been restored to approximately the middle of the hot-leg elevation. The fluid temperature at the core outlet has also been reduced to approximately 121.1°C (250°F). As shown in Figure 9.8.5-29, the reactor coolant mass inventory reaches a minimum of approximately 55,000 kg (122,000 lbm) and then begins to increase as a result of the IRWST injection. Thus, it is concluded that when the appropriate operator action is performed, one ADS Stage 4 valve is effective in reducing system pressure so that the consequences of a loss of RNS in Mode 5 with the RCS vented are acceptable.

9.8.5.2.3.2 Mode 5 Mid-Loop Operation

This additional case presented is a conservative analysis of a loss of RNS cooling during reduced inventory conditions (i.e., minimum inventory). During Mode 5, prior to draining to mid-loop conditions, from a water solid initial condition the operator manually opens the ADS Stages 1 through 3 paths to the IRWST. With the RCS “open,” the operator could then proceed to slowly drain the RCS to “mid-loop” conditions for performing steam generator maintenance or other maintenance that requires a reduced RCS water level. Before the operator starts draining to “mid-loop”, it is postulated that a loss of decay heat removal via the Class 2 RNS occurs. A loss of RNS cooling at this time is selected because it is the earliest time the RCS could be placed into a reduced inventory (that is, RCS open) condition. In addition, the backpressure on the reactor vessel, due to the presence of water in the pressuriser, is higher at this time. This presents the most challenging condition for the ADS to depressurise the RCS to IRWST cut-in pressure. This transient represents the most limiting “surge line flooding” scenario, a term commonly used for operating plants to refer to the phenomenon associated with water in the pressuriser and surge line causing a high backpressure in the RCS. For these operating plants this potentially challenges the ability of the low head safety injection systems to inject properly.

[1] This automatic actuation has a 25 minute delay; the manual actuation discussed in this analysis is in advance of the automatic actuation.

For a loss of the RNS during mid-loop operations, calculations have been performed to determine the time until core uncovery would occur. The results of these calculations are presented in Table 9.8.5-3. A loss of RNS cooling during mid-loop results in a heatup of the core to saturation, followed by a boiling off of the coolant to the IRWST via the ADS Stages 1, 2, and 3 valves. The conditions in the RCS following IRWST and fourth-stage ADS actuation are similar to the other cases in this evaluation. As shown in Table 9.8.5-3, the operator has at least 42 minutes from the loss of RNS cooling until the onset of core uncovery to manually actuate the IRWST and ADS Stage 4. In general, when considering appropriate operator action to mitigate the event, the results of a loss of RNS during mid-loop conditions are similar, but slightly less severe than the other cases presented in this evaluation due to the lower levels of decay heat and to the absence of the initial water inventory in the pressuriser. This serves to reduce the surge line flooding phenomenon that degrades the depressurisation capability of the ADS Stages 1 through 3 vent paths.

9.8.5.2.3.3 Radiological Consequences

The radiological consequences presented in Section 9.8.5.2.3.3 for the frequent fault loss of RNS faults also bound those for the infrequent fault scenarios.

9.8.5.2.3.4 ALARP Evaluation

The ALARP evaluation presented in Section 9.8.5.1.3.5 for the frequent fault loss of RNS scenarios also applies to these infrequent fault scenarios.

9.8.5.3 Loss of Coolant Accidents Involving RNS (Faults 2.3.1 – 2.3.3)

9.8.5.3.1 Identification of Causes and Accident Description

As discussed in Section 9.8.5.0.3, this section discusses postulated breaks in the RNS piping during RNS operation in shutdown Modes 4, 5, and 6. These faults are categorised as infrequent faults (DB1). The analysis presented below assumes that the RNS is isolated 30 minutes after the break occurs which is consistent with operator action. The plant has automatic Class 1 RNS isolation which is not credited here but the analysis will be revised during site licensing to incorporate the automatic actuation logic added to the design.

For a postulated RNS break outside the containment while in Modes 4 and 5 with the RCS pressure boundary intact, the RCS would lose inventory through the postulated break and the pressuriser water level would decrease. A low pressuriser level signal will automatically actuate the CMTs. When the RCS cold legs void, the CMTs would begin to drain and eventually ADS Stages 1, 2, 3, and later ADS Stage 4 would be actuated on low CMT level signals. The ADS Stage 4 signal would actuate IRWST injection and would also isolate the containment and RNS. The automatic RNS and containment isolation on an ADS Stage 4 signal reduces the RCS inventory lost outside containment and increases the inventory margin for passive containment recirculation over that shown in this analysis.

For a reduced inventory case in Modes 5 and 6 with the RCS pressure boundary open in the event of an RNS break outside the containment, the RCS would lose inventory. On low hot leg level, ADS Stage 4 and IRWST injection would be actuated. The ADS Stage 4 signal also isolates the RNS and containment. Technical Specifications require that the equipment hatches, containment air locks, and containment spare penetrations shall be capable of being closed before steaming into the containment. Therefore, RNS and containment isolation on an ADS Stage 4 signal and containment penetrations isolation will preserve enough inventory in case of RNS leakage to allow passive containment recirculation.

9.8.5.3.2 DBA Credited SSCs

For the DBA, no claim is placed on systems which are not Class 1. In Modes 4 and 5 with the RCS intact, the PMS provides the following:

- No reactor trip is required, as the reactor is already shutdown
- CMT on Low-2 pressuriser level
- ADS 1-4 on Low CMT level
- IRWST injection and containment isolation (including RNS) on Low CMT level (via ADS 4 actuation signal)
- Containment recirculation on Low IRWST level
- PCS on High-2 containment pressure.

In Mode 5 with the RCS open, the PMS provides the following:

- No reactor trip is required, as the reactor is already shutdown.
- ADS 4, IRWST injection, and containment isolation (including RNS) on Low hot leg level
- Containment recirculation on Low IRWST level
- PCS on High-2 containment pressure

In Mode 6, the PMS provides the following:

- No reactor trip is required, as the reactor is already shutdown.
- Manual actuation of ADS 4, IRWST injection, containment recirculation, and RNS isolation
- PCS and containment isolation on High-2 containment pressure.

9.8.5.3.3 Analysis of Effects and Consequences

9.8.5.3.2.1 Mode 4 and 5 with RCS Pressure Boundary Closed

For a postulated RNS break outside containment in these plant Modes, the RCS will lose inventory through the postulated break and the pressuriser water level will decrease. A low pressuriser level signal will automatically actuate the CMTs. Once the RCS level has decreased such that the cold legs void, the CMTs will also start to drain. When the CMTs have drained to approximately 71 percent of their volume, ADS stages 1, 2 and 3 will be actuated. Following the actuation of ADS stages 1, 2, and 3, ADS stage 4 and IRWST injection will be opened when the CMTs have drained to approximately 25 percent of their volume. ADS stage 4 actuation would also initiate automatic containment and RNS isolation.

To assess the capability of the plant to address this postulated RNS break, an analysis has been performed and the results show that the calculated containment water level is 102.41 m

(107.92 ft)[2], whereas the minimum-required containment water level to support passive containment recirculation is 102.39 m (107.85 ft). The minimum calculated containment water level is coincident with operator action at 30 minutes. Significant conservative assumptions in the analysis are included in this result. For example, the assumption of a constant break flow calculated according to the event initial conditions instead of allowing break flow to vary as conditions change. In addition, the automatic isolation signal for the RNS was not credited. With the minimum level maintained, no core damage will occur and long-term core cooling is ensured. This analysis demonstrates that sufficient time is available for the operator action before the loss of mass from the RCS and IRWST could challenge the long-term cooling capability. The sequence of events for this case is contained in Table 9.8.5-4.

9.8.5.3.2.2 Mode 5 with RCS Pressure Boundary Open

The RCS water level is initially assumed to be at mid loop (approximately 80% level of the Hot Legs). An RNS pipe break outside of the containment would quickly drain the RCS hot leg. A low Hot Leg level signal automatically actuates ADS Stage 4 and IRWST injection after a 25-minute time delay. The time delay is intended to allow for personnel that might be inside the containment to leave and also to close up the containment (as required by the Tech Spec). During this 25 minute time delay core cooling would be provided by heatup of the water in the reactor coolant system (below the mid loop level. The 25 minute time delay allows for the operators to assess the situation and determine what has happened and whether the event was a failure that caused loss of cooling or was caused by a pipe break. In the event of a pipe break, the operators would likely isolate the RNS manually in advance of the time that the low HL level signal would automatically open ADS 4 and initiate IRWST injection. Also note that the RNS is arranged in two separate trains such that a RNS pipe break would not disable both trains of RNS. If the faulted RNS train could be identified, it would be possible to isolate the faulted train and (after adding water to the RCS) to use the intact RNS to provide core cooling. If this was not achieved, IRWST injection and ADS stage 4 would provide feed and bleed cooling. When the IRWST level decreased, containment recirculation would be initiated to establish the long-term cooling mode. PCS operation would auto-actuate on high containment pressure to limit the containment pressure.

It was calculated that within 25 minutes, collapsed water level in the reactor vessel would be between the top core elevation, 98.24 m (94.22 ft) and bottom hot leg elevation 99.99 m (99.96 ft), thus conservatively ensuring that the core remains covered and no significant clad heatup would occur.

Containment water level is determined with a partial IRWST volume (the calculation assumes that during 5 minutes, the time difference between low hot leg level being reached and when operator action is needed, IRWST injection is lost through the postulated break) and volume corresponding to the top core elevation. It was shown that the containment water level is above the minimum required. This demonstrates that for Mode 5 with RCS open, passive recirculation will be established providing long term core cooling.

9.8.5.3.2.3 Mode 6 with Refuelling Cavity Flooded

In this case, a RNS break would drain water out of the Refuelling Cavity (RC) through the RCS via the removed Reactor Vessel head. The initial limiting break flow of 17.03 m^3/min (4500 gpm), assumed to remain constant, was used to determine how much of the reactor

2. Note that the basis for all elevations is set to 100 feet in US design and 100 m in metric design.

coolant inventory would drain out before the manual operator action would need to be claimed. It was shown that the final RC level, 107.74 m (125.41 ft), is well above the RV flange when the operator isolates the RNS break. After that time, the water in the RCS and RC heats up until it starts to boil. After boiling starts, the steam flows to and pressurises the containment, which results in automatic actuation of the PCS. The PCS water drains on the outside of the containment, cooling the containment shell and condensing the steam inside the containment.

The steam condensate is routed back from the containment shell to the IRWST through the PXS downspouts and gutters. In addition, it will be necessary for the operators to open one IRWST injection line. This will allow the water that is accumulating in the IRWST to return to the RCS to prevent the RCS from losing too much inventory. This establishes long term cooling and an equilibrium between IRWST and refuelling cavity levels.

It is also important to note that the configuration alignment of the reactor internals will impact the accident transient. In the event that internals are installed, ADS stage 4 actuation would be required to maintain sufficient depressurisation of the core. If the internals are removed, ADS stage 4 actuation is not required due to the large open area available to prevent pressurisation.

Consequently, long term core cooling for this Mode is ensured.

9.8.5.3.2.4 Radiological Consequences

The radiological consequences of a postulated break in RNS piping outside containment are evaluated.

9.8.5.3.2.4.1 Source Term

There is no fuel damage as a result of the accident. Therefore, the only activity available for release is that present in the primary coolant. The initial reactor coolant system noble gases, alkali metals, and iodines concentrations are assumed to be those associated with the equilibrium operating limit for primary coolant iodine activity. This evaluation conservatively includes consideration of an iodine spike that has resulted in an increased level of iodine in the reactor coolant. This spike is assumed to have resulted from the plant shutdown, cooldown and depressurisation associated with the transition from power operation to shutdown cooling. This spike is considered unlikely and not required for consideration in the accident dose calculations. Despite this the spike has been included in this evaluation. This spike has been included even though it is not a normal occurrence and increased clean up would be initiated in response to its occurrence such that by the time an accident occurs there would no longer be an elevated iodine concentration.

9.8.5.3.2.4.2 Release Pathways

It is assumed that the RNS pipe breaks outside containment and the break flow path is assumed to allow all of the activity in the RCS to be discharged into the auxiliary building. This assumption provides for a conservative dose calculation. A portion of the iodine and alkali metal activity, and all of the noble gas activity, transferred outside containment is assumed to become airborne.

9.8.5.3.2.4.3 Dose Calculation Models

The models used to calculate offsite and control room doses are provided in Appendix 9A.

9.8.5.3.2.4.4 Analytical Assumptions and Parameters

The assumptions and parameters used in the analysis are listed in Table 9.8.5-6. The limiting worker dose reported is the control room operator dose conservatively calculated neglecting actuation of the main control room emergency habitability system (VES) even though the setpoint would be reached.

9.8.5.3.2.4.5 Doses

The conservatively estimated maximum doses for all relevant pathways (inhalation, cloudshine, and groundshine) are as follows:

- Offsite dose: 52 mSv Worker dose: 323 mSv

These doses are within the Target 4 BSL for infrequent faults with IEF<1E-04 (100 mSv offsite and 500 mSv onsite). This analysis is significantly conservative due to assumptions that do not credit mechanistic and/or realistic limitations to the radiological consequences, such as:

- Maximum possible iodine spike
- Complete discharge of the initial RCS activity (i.e., no credit for containment isolation)
- No credit for delay, plate-out, or hold-up of radioactivity within the auxiliary building prior to being released to the environment
- No credit for the operation of the Class 2 HVAC system
- No credit for the Class 1 MCR HVAC system, VES

9.8.5.3.2.5 ALARP Evaluation

For this fault, Class 1 SSCs has been shown to be adequate to meet DB requirements.

As discussed in Chapter 9.0.15, the standard AP1000 design has incorporated ALARP considerations throughout its development. Furthermore, the standard AP1000 plant design incorporates numerous features that reduce shutdown risk as discussed in section 9.8.3. One of the more important features is reduced containment leak paths (fewer penetrations, improved isolation valves, backup DAS actuation, and passive containment cooling) and the ability to close containment during shutdowns. In addition, the current risk of a large radioactivity release during shutdown conditions is significantly less than the SAP Target 8 BSO.

The radiological consequences presented for this fault (See Section 9.8.5.3.2.4) are less than the Target 4 BSLs, but above the BSO. However, the analysis performed during GDA has considerable conservatism, and a commitment exists to update all radiological consequences analyses during site licensing. There are reasonable adjustments to the analysis for the RNS LOCA faults that will bring the resultant doses closer to the Target 4 BSO. However, due to the direct release of primary coolant outside of containment, it is not expected for the doses to be reduced below the BSO value. Considerations for improving the radiological consequences analyses include:

- Reduction of the assumed RCS activity levels to more realistic, but appropriately conservative, values based on more recent operating experience
- Reduction of the RCS mass loss assumed outside containment by crediting the automatic isolation of RNS
- Crediting Class 1 VES operation to reduce the worker doses

- Crediting reduction in offsite doses provided by Auxiliary Building structure

The adoption of a two train separated RNS system design reduces the likelihood of this fault and improves the mitigation capability. The use of two trains with smaller pipe diameters slows the inventory loss in the event of a line break, and the ability to use the two trains independently allows for continued cooling without reliance on the Class 1 passive safety systems by isolating the damaged train (if possible). Additionally, several enhancements have been identified for further evaluation in site licensing to confirm risks have been reduced ALARP. These potential enhancements include:

- A Technical Specification change to adjust the point when RNS is initially aligned to cool the RCS; specifically, to consider limiting RNS alignment to a point with a specific decay heat level. This would allow for a mechanistic, yet still conservative, timing assumption to be included in the presented analyses. Currently, RNS alignment is conservatively assumed to occur faster than any realistic plant schedule would allow.
- Improvement to the automatic RNS isolation functionality to reduce the RCS mass loss outside containment.
- Updates to the standard AP1000 plant Technical Specifications, which currently only require VES to be operable during Modes 1 – 4 as well as any time irradiated fuel is being moved. Specifically, adding an operability requirement during Mode 5 when there is high RCS activity would have a significant improvement to worker doses.

Accounting for the ALARP considerations that went into the AP1000 design development, its low risk profile, and the expected demonstration of improvements to the radiological consequences discussed above, making further improvements to the AP1000 design are expected to be grossly disproportionate to the risk reduction that might be achieved. As a result, the current design with the above potential enhancements is considered ALARP.

9.8.6 Conclusion

In order to demonstrate the plant shutdown safety case has reduced plant risk ALARP, a systematic evaluation of the AP1000 design with respect to faults during shutdown operations was provided. As demonstrated in this section, the plant is designed to mitigate events that can occur during all shutdown modes. All faults have demonstrated primary mitigation using only Class 1 SSCs, and where necessary, frequent faults also include demonstration of diverse mitigation using mostly Class 1 SSCs and supplemented with limited use of Class 2 SSCs.

The risk of core damage as a result of an accident that may occur during shutdown has been demonstrated to be acceptably low. In addition, conservatively calculated radiological consequences are within the Target 4 BSLs. The standard AP1000 plant design incorporates numerous features that reduce shutdown risk as discussed in Section 9.8.3. Nonetheless, while evaluating the shutdown safety case during GDA, additional design enhancements were incorporated in order to ensure that plant shutdown risks were reduced ALARP:

- Automatic containment and RNS isolation occur upon receipt of an ADS stage 4 signal in order to limit the amount of RCS coolant that could be lost in the event of an RNS line break outside of containment (Section 9.8.5.3)
- Automatic isolation of CVS dilution sources, CMT actuation, RCP trip, and RNS pump trip via a DAS connection to the intermediate range ex-core detectors to prevent a return to criticality during a boron dilution event at shutdown (Section 9.8.4.4.5)
- Adoption of a two train separated RNS system design, which provides reduced RNS pipe sizes as well as increasing the likelihood of continued RNS operation in the event of a

line break.

These features will be credited in analysis updates going forward in site licensing. Additional improvements that will be evaluated during site licensing that might further reduce shutdown risk ALARP include:

- Consideration of using an alternate RNS isolation signal so that less RCS inventory is discharged outside containment and only the faulted RNS train is isolated. One possibility would be the low Pressuriser level signal. Another might be high RNS train flow rates or large differences in train flow rates.
- Changes to the Technical Specifications to require the VES to be operable during Modes 4, 5, and 6 except when the RCS activity is low. Selection of what is sufficiently "low" will require a balance the need for VES planned maintenance, in-service inspections, in-service testing, avoidance of undesirable power reductions of the plant only to restore VES operability (in case of failures) with the reduction in post-accident MCR doses.
- Justification of using a lower RCS activity level (iodine spike) for RNS breaks based on more recent operating experience. This may be reflected in the plant design via a Technical Specification change that would preclude RNS operation with RCS activity levels above a specified limit.

9.8.7 References

9.8-1 Westinghouse Letter DCP/NRC0124, APWR-0452, "AP600 Vortex Mitigator Development Test for RCS Mid-loop Operation," July 6, 1994.

9.8-2 NUREG-0897, Rev. 1, "Containment Emergency Sump Performance," U.S. Nuclear Regulatory Commission, October 1985.

9.8-3 Westinghouse Documents WCAP-10698-P-A (Proprietary) and WCAP-10750-A (Non-Proprietary), "SGTR Analysis Methodology to Determine the Margin to Steam Generator Overfill," August 1987.

9.8-4 Westinghouse Documents WCAP-14171, Rev. 2 (Proprietary) and WCAP-14172, Rev. 2 (Non-Proprietary), "WCOBRA/TRAC Applicability to AP600 Large-Break Loss-of-Coolant Accident," March 1998.

Table 9.8.1-1. Definition of Operational Modes

Modes	Title	Reactivity Condition (K_{eff})	% Rated Thermal Power[1]	Average Reactor Coolant Temperature (°C (°F))
1	Power Operation	≥ 0.99	> 5	NA
2	Startup	≥ 0.99	≤ 5	NA
3	Hot Standby	< 0.99	NA	> 215.6 (420)
4	Safe Shutdown[2]	< 0.99	NA	215.6 (420) ≥ T_{avg} T_{avg} > 93.3 (200)
5	Cold Shutdown[2]	< 0.99	NA	≤ 93.3 (200)
6	Refuelling[3]	NA	NA	NA

Notes:

1. Excluding decay heat
2. All reactor vessel head closure bolts fully tensioned
3. One or more reactor vessel head closure bolts less than fully tensioned

Table 9.8.3-1. Availability of Class 1 Passive Core Cooling Equipment During Operational Modes

Equipment	Availability				
	Mode 1-2	Mode 3	Mode 4	Mode 5	Mode 6
CMTs	Y	Y(1)	Y(1, 2)	Y(1, 2) – RCS closed N(3) – RCS Open	N(3)
Accumulators	Y	N(4)	N(4)	N(4)	N(4)
IRWST	Y	Y	Y	Y(5)	N(6)
PRHR	Y	Y(7)	Y(7)	Y(7) – RCS closed N(8) – RCS Open	N(8)
ADS 1-3	Y	Y	Y	Y(9)	Y(9)
ADS 4	Y	Y	Y	Y(10)	Y(10)

Notes:

1. In shutdown modes, portions of the safeguards actuation signal are disabled to allow the RCS to be cooled and depressurised for shutdown and the primary signal that actuates the CMTs due to a loss of inventory is the pressuriser level signal.
2. In Mode 4 and 5, with RNS aligned and RCS closed, operation is allowed with 1 (rather than both) CMTs aligned. See also Section 9.8.5.0.1.
3. In Mode 5 with the RCS open, the CMTs are not required to be available and the RCS makeup function is provided by the IRWST.
4. In Mode 3, the accumulators must be isolated to prevent their operation when the RCS pressure is reduced to below their set pressure. The accumulator isolation valves are closed when the RCS pressure is reduced to 1000 psig (6.895 MPa gauge).
5. When the RCS is open to transition to reduced inventory operations, the CMT actuation logic on low pressuriser level is removed, and the CMTs can be taken out of service. For these modes, automatic actuation of the IRWST can be initiated (on a two-out-of-two basis) on low hot leg level. Also, in this mode only one injection flow path and one containment recirculation flow path are required to be available.
6. The IRWST is available until Mode 6, when the reactor vessel upper internals are removed and the refuelling cavity flooded. At that time, the IRWST is not required, due to the large heat capacity of the water in the refuelling cavity. Also, in this mode only one injection flow path and one containment recirculation flow path are required to be available.
7. In these modes, the PRHR HX provides a passive decay heat removal path. It is automatically actuated on a CMT actuation signal
8. In modes with the RCS open (portions of Mode 5 and Mode 6), decay heat removal is provided by “feeding” water from the IRWST and “bleeding” steam from the ADS.
9. The ADS first-, second-, and third-stage valves, connected to the top of the pressuriser, are open whenever the CMTs are blocked during shutdown conditions while the reactor vessel upper internals are in place. This provides a vent path to preclude pressurisation of the RCS during shutdown conditions if decay heat removal is lost.
10. Two of the four ADS fourth-stage valves are required to be available during reduced inventory operations to preclude surge line flooding following a loss of the RNS.

Table 9.8.4-1. Double-Ended Cold-Leg Guillotine Break – Sequence of Events

Event	Time (seconds)
Break open	0.0
"S" signal receipt	4.2
RCPs start to coast down	9.5
CMT draindown begins (CMT connected to intact cold leg)	25
CMT draindown begins (CMT connected to broken cold leg)	65
Lower plenum refilled	180

Table 9.8.5-1. Loss of RNS Cooling in Mode 4 with RCS Intact – Sequence of Events for Primary Case

Event	Automatic Actuation Time (hours)
Loss of RNS cooling	2.00
RNS relief valve flow starts	2.19
CMT and PRHR actuated	4.23
ADS Stage 1 flow starts	4.36
ADS Stage 2 flow starts	4.37
RNS relief valve flow terminated	4.37
ADS Stage 3 flow starts	4.40
ADS Stage 4 flow starts	4.53
IRWST injection starts	4.73

Table 9.8.5-2. Loss of RNS Cooling in Mode 5 and 6 with RCS Open – Sequence of Events

Event	Time (hours)
Loss of RNS cooling	24.00
Hot leg empty	25.16
ADS Stage 4 flow initiated	25.20
IRWST injection starts	25.35

Table 9.8.5-3. Evaluation of a Loss of RNS at Mid-loop with no IRWST Injection

Time After Shutdown	Time to Boiling	Time to Empty Hot Leg	Time to Core Uncovery
28 hours	3 minutes	20 minutes	42 minutes

Table 9.8.5-4. LOCA Involving RNS – Sequence of Events

Event	Approximate Time (minutes)
LOCA involving RNS	0.0
CMT actuation/injection	0.1
ADS Stage 1 actuation	4.7
ADS Stage 4 actuation	13.6
IRWST injection starts	13.7
Manual RNS isolation	30.0

Table 9.8.5-5. Parameters Used In Evaluating The Radiological Consequences Of A Loss of RNS Cooling

Reactor coolant iodine activity	Assumed shutdown spike up to 5.18E8 Bq/kg (14 μCi/g) dose equivalent I-131 (a factor of 56 times the iodine values in Table 9A-1)
Reactor coolant noble gas activity	Equal to the operating limit for reactor coolant activity of 2.6E9 Bq/kg (70 μCi/g) dose equivalent Xe-133 (see Table 9A-1)
Reactor coolant alkali metal activity	Design basis activity (see Table 9A-1)
Reactor coolant mass	2.95E5 kg (6.5E5 lbm)
RCS Activity Airborne fractions Iodines Noble gases Alkali metals	 1.0 1.0 1.0
Containment Volume	5.83E4 m^3 (2.06E6 ft^3)
Fraction of fuel rods assumed to fail	0.0
Removal Coefficients(1) Elemental Iodine Organic Iodine Particulates	 1.7 (hr^{-1}) 0.0 (hr^{-1}) 0.5 (hr^{-1})
Containment Leakage Rate 0-24 hours 24-720 hours	 0.1 (%/day) 0.05 (%/day)
Offsite atmospheric dispersion factors	See Table 9A-5
Control room modelling	See Appendix 9A

Note:

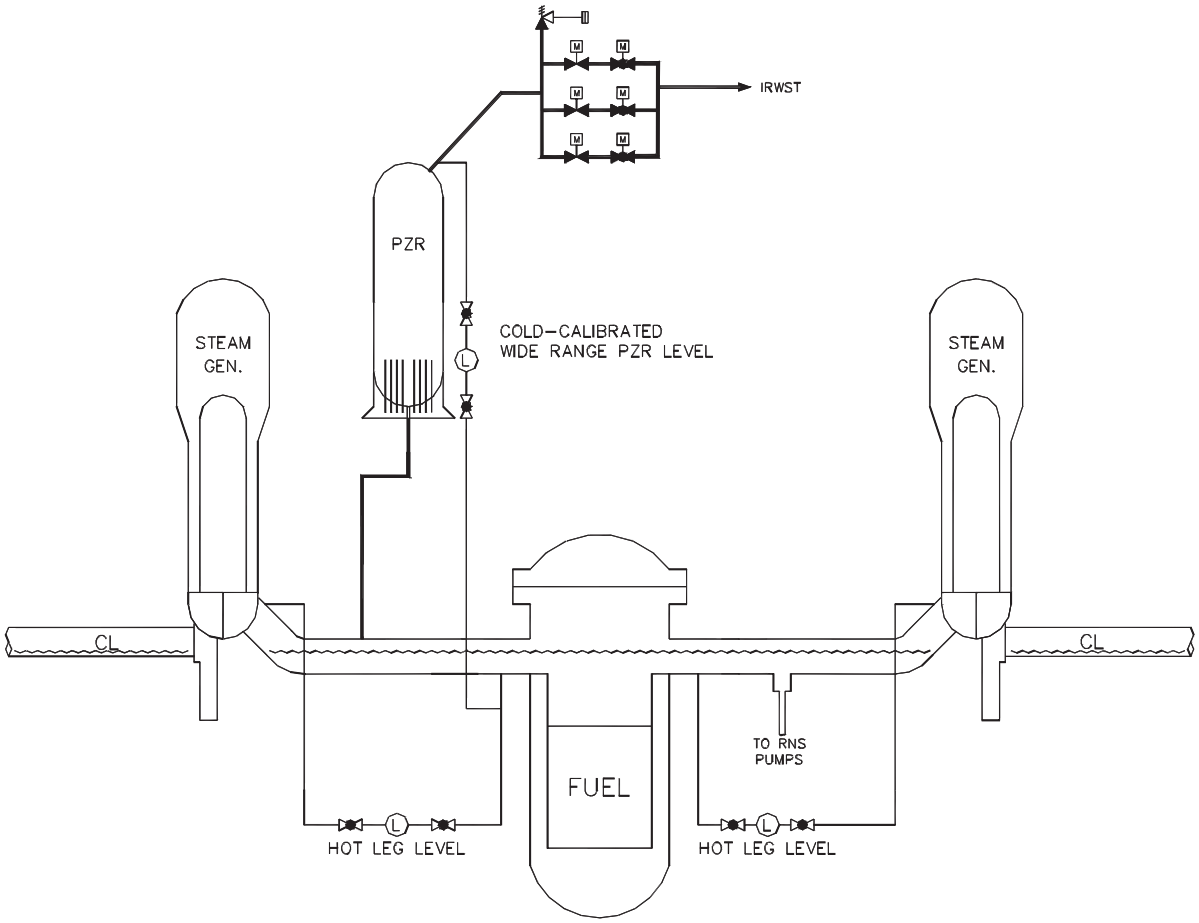
1. Elemental iodine removal is modelled until a DF of 200 is reached. Particulate removal is modelled until a DF of 1.0E4 is reached.

Table 9.8.5-6. Parameters Used In Evaluating The Radiological Consequences Of An RNS Pipe Break Outside Containment

Reactor coolant iodine activity	Assumed shutdown spike up to 5.18E8 Bq/kg (14 μCi/g) dose equivalent I-131 (a factor of 56 times the iodine values in Table 9A-1)
Reactor coolant noble gas activity	Equal to the operating limit for reactor coolant activity of 2.6E9 Bq/kg (70 μCi/g) dose equivalent Xe-133 (see Table 9A-1)
Reactor coolant alkali metal activity	Design basis activity (see Table 9A-1)
Reactor coolant mass	2.95E5 kg (6.5E5 lbm)
RCS Activity Airborne fractions Iodines Noble gases Alkali metals	 0.1 1.0 0.1
Fraction of fuel rods assumed to fail	0.0
Offsite atmospheric dispersion factors	See Table 9A-5
Control room modelling(1)	See Appendix 9A

Note:

1. The limiting control room operator dose calculation conservatively neglected actuation of the (VES) even though the setpoint would be reached.



Note: Hot leg level indication was improved during GDA to have two level indications being available on each hot leg where this figure currently shows one. This figure will be updated during site licensing to reflect the updated design.

Figure 9.8.2-1. Reactor Coolant System Level Instruments Used During Shutdown

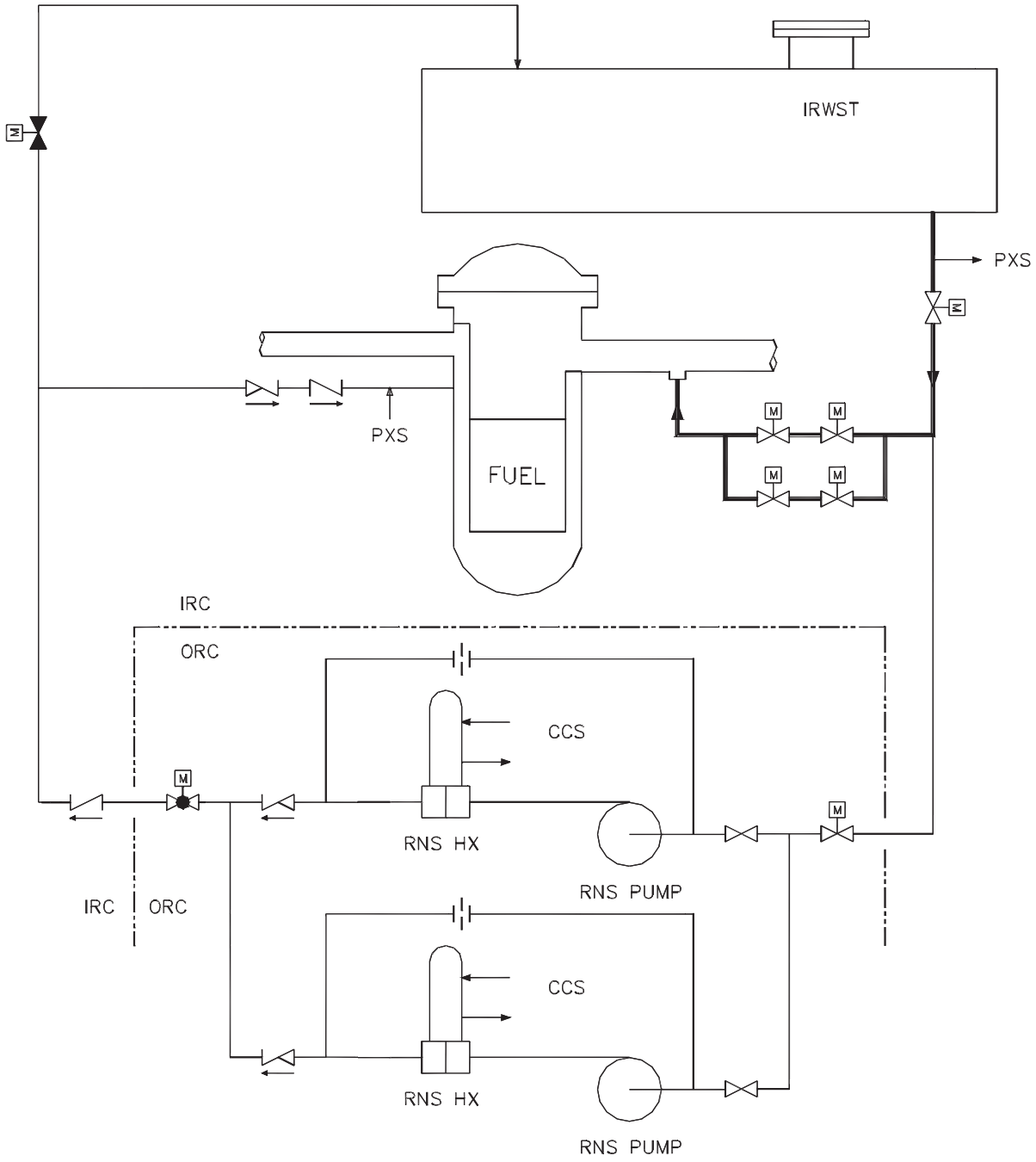


Figure 9.8.2-2. IRWST Injection Flow Path

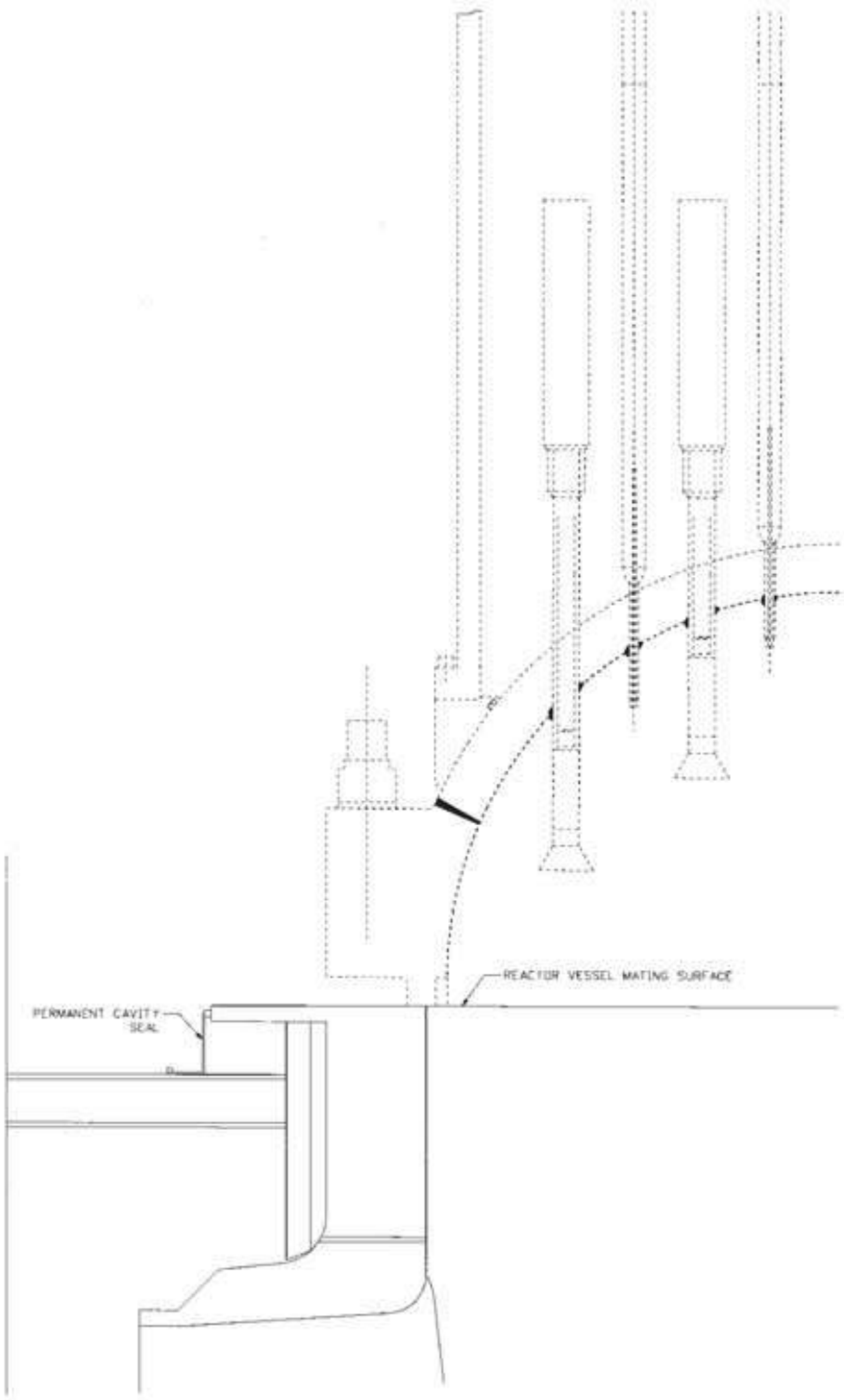


Figure 9.8.2-3. AP1000 Permanent Reactor Cavity Seal

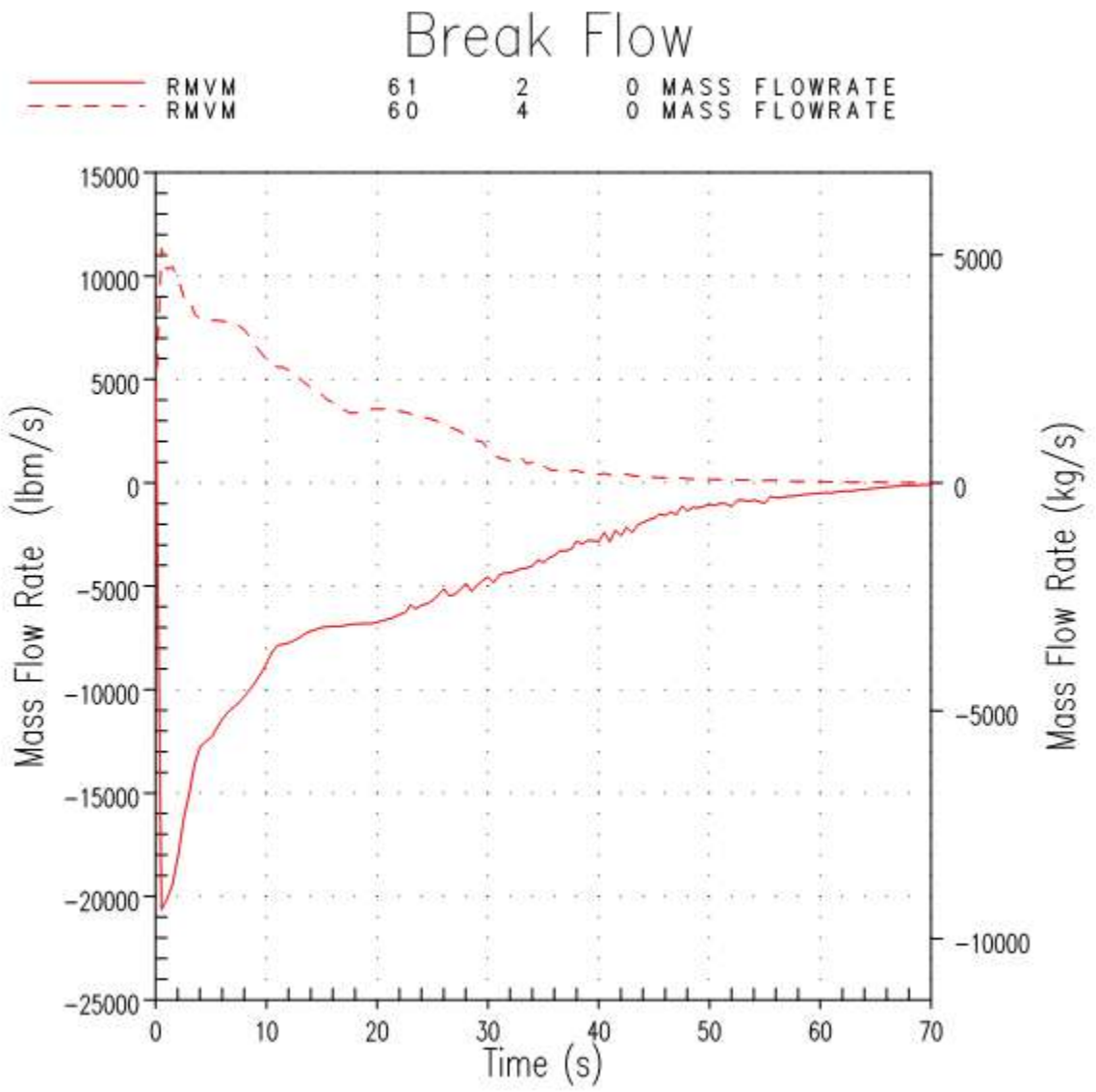


Figure 9.8.4-1. Mode 3 DECLG Break, Break Flow Rates, Vessel and RCP Sides

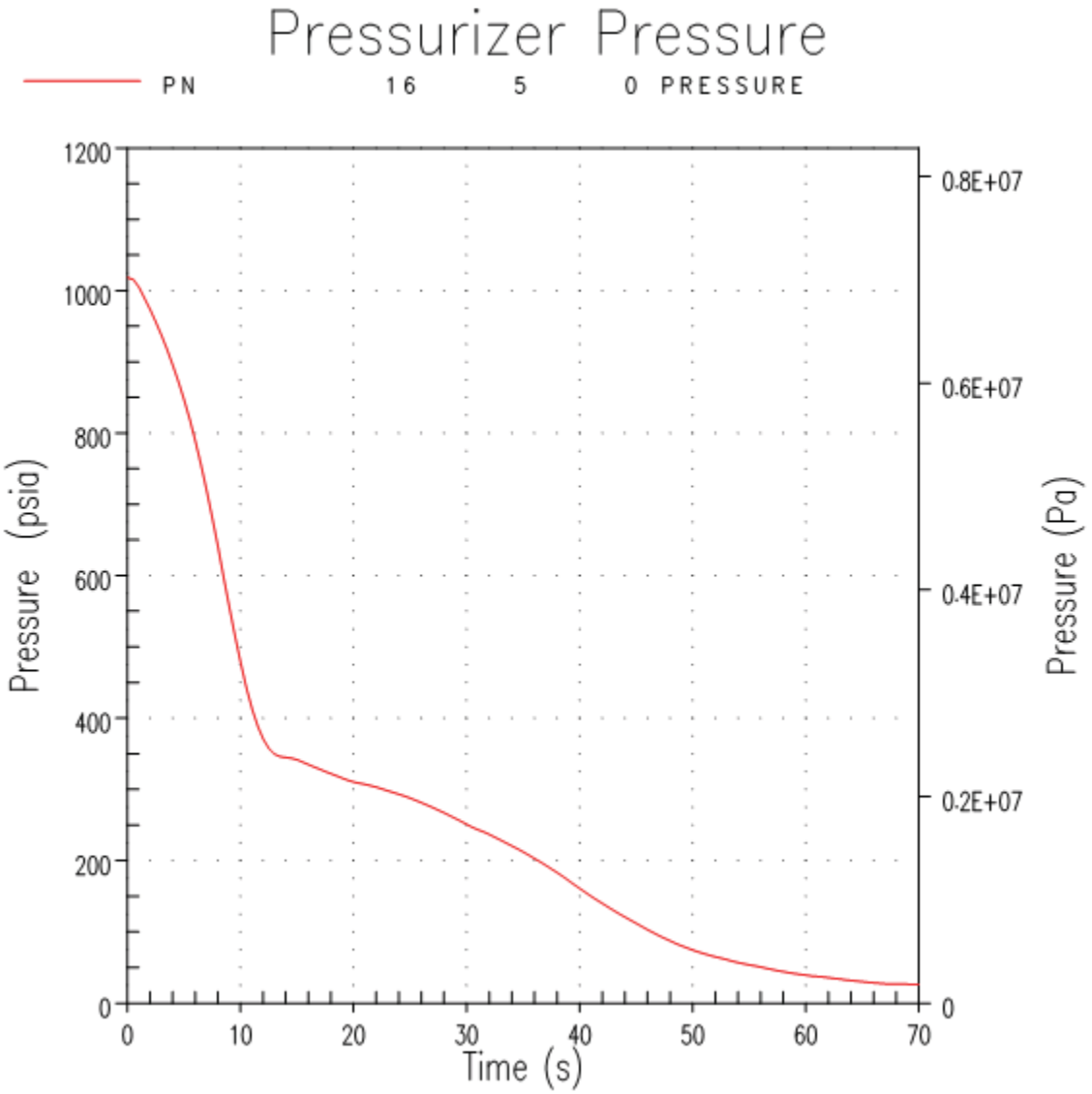


Figure 9.8.4-2. Mode 3 DECLG Break, Pressuriser Pressure

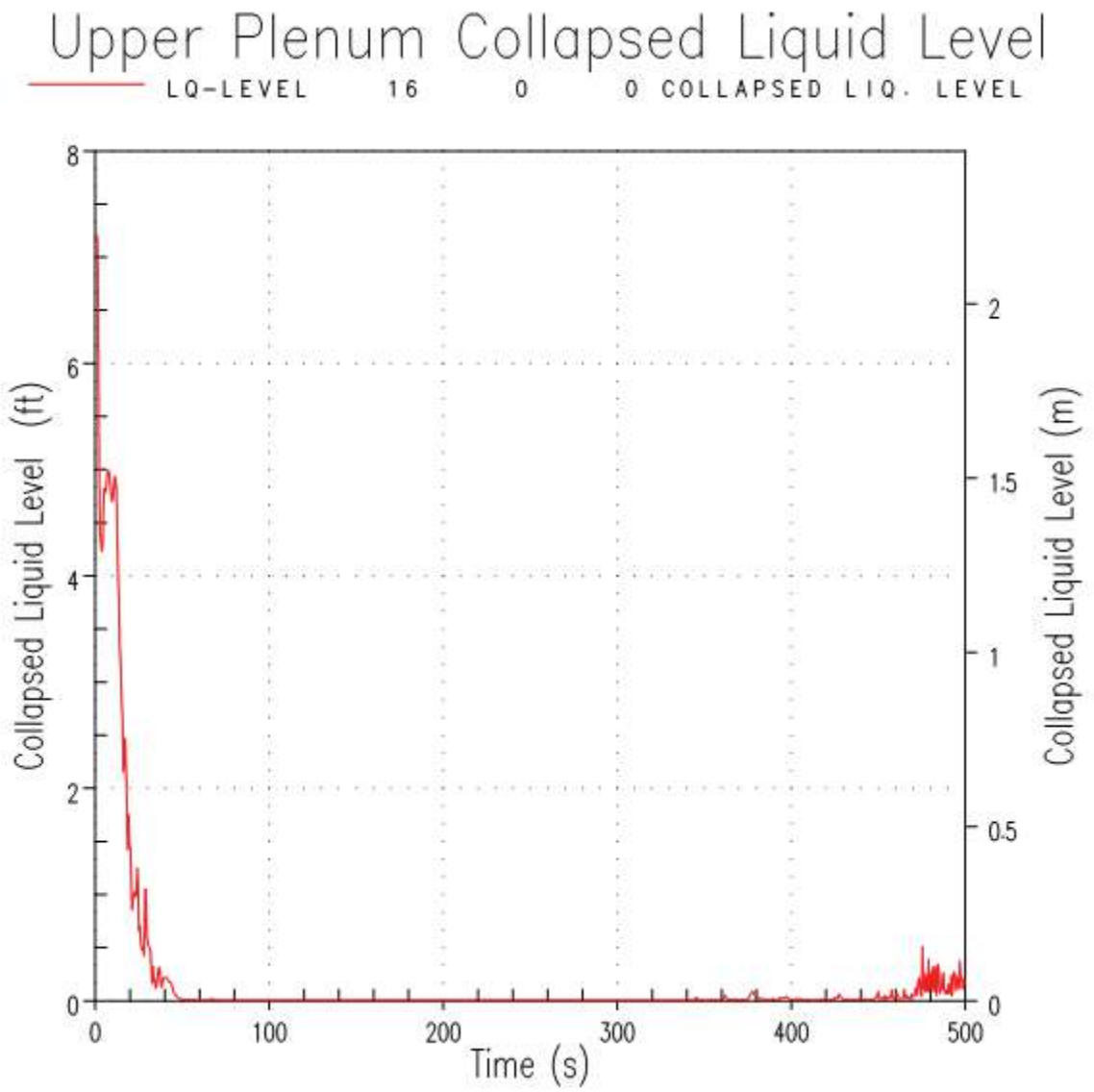


Figure 9.8.4-3. Mode 3 DECLG Break, Upper Plenum Collapsed Liquid Level

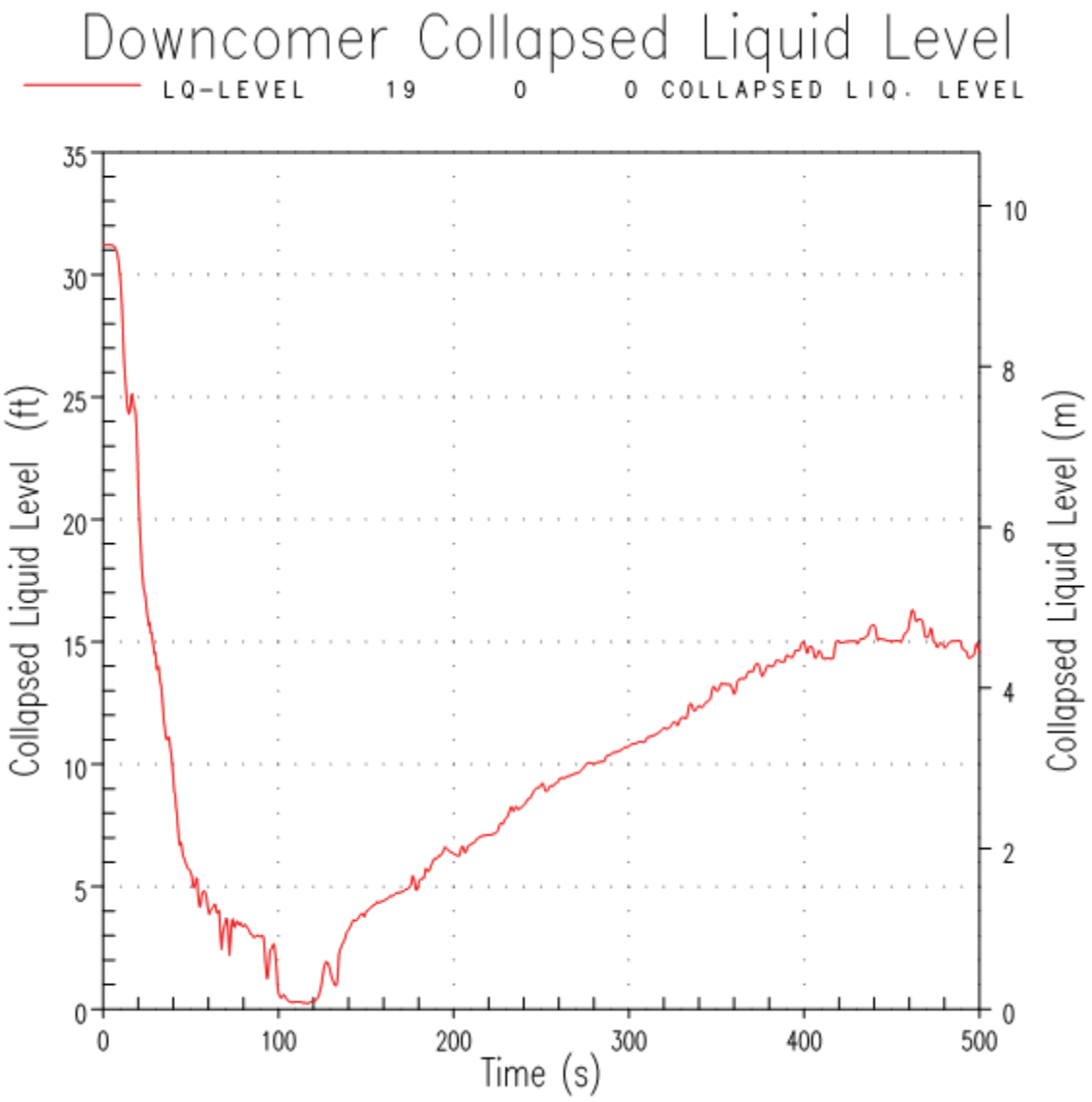


Figure 9.8.4-4. Mode 3 DECLG Break, Downcomer Collapsed Liquid Level

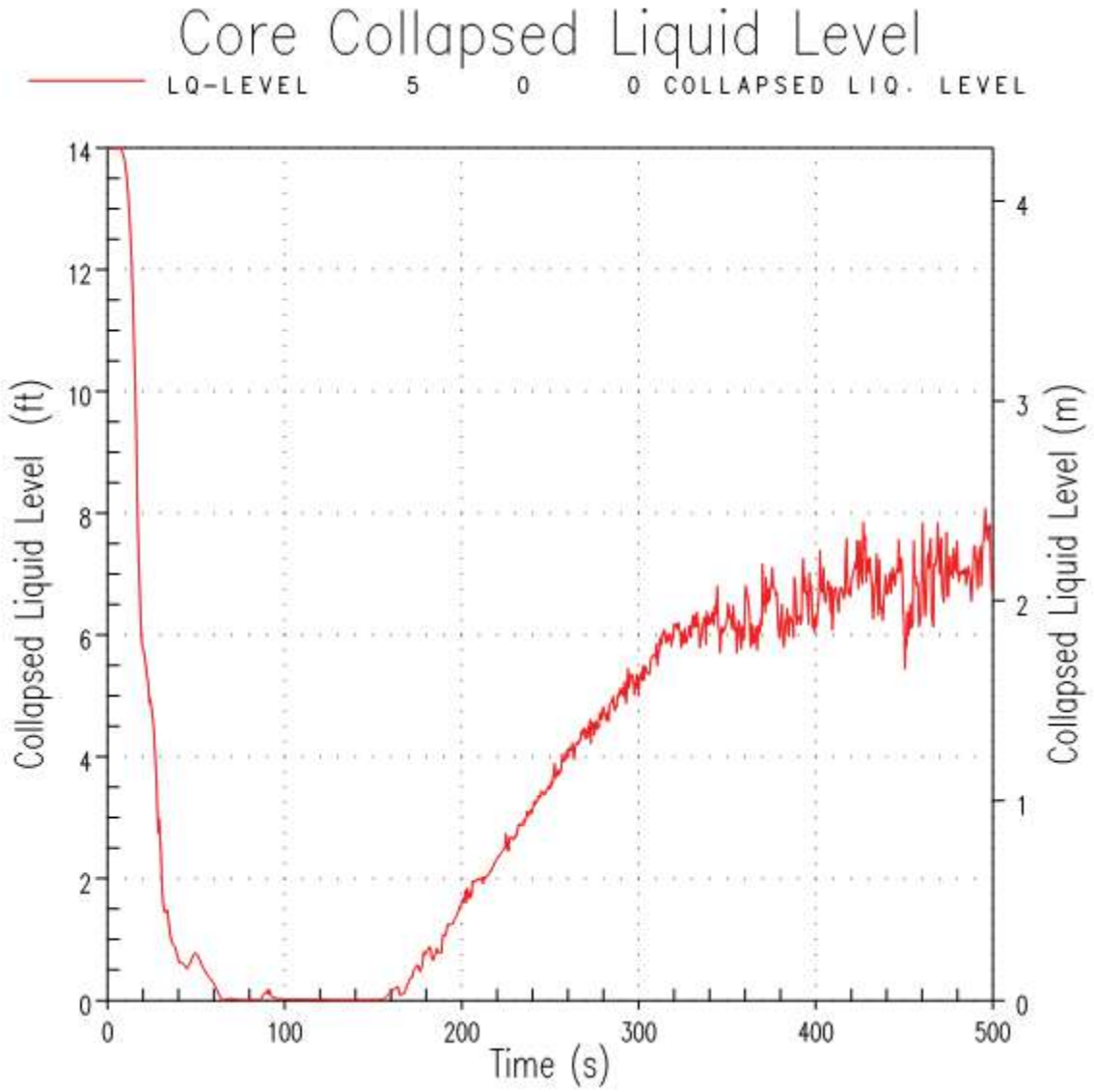


Figure 9.8.4-5. Mode 3 DECLG Break, Core Collapsed Liquid Level

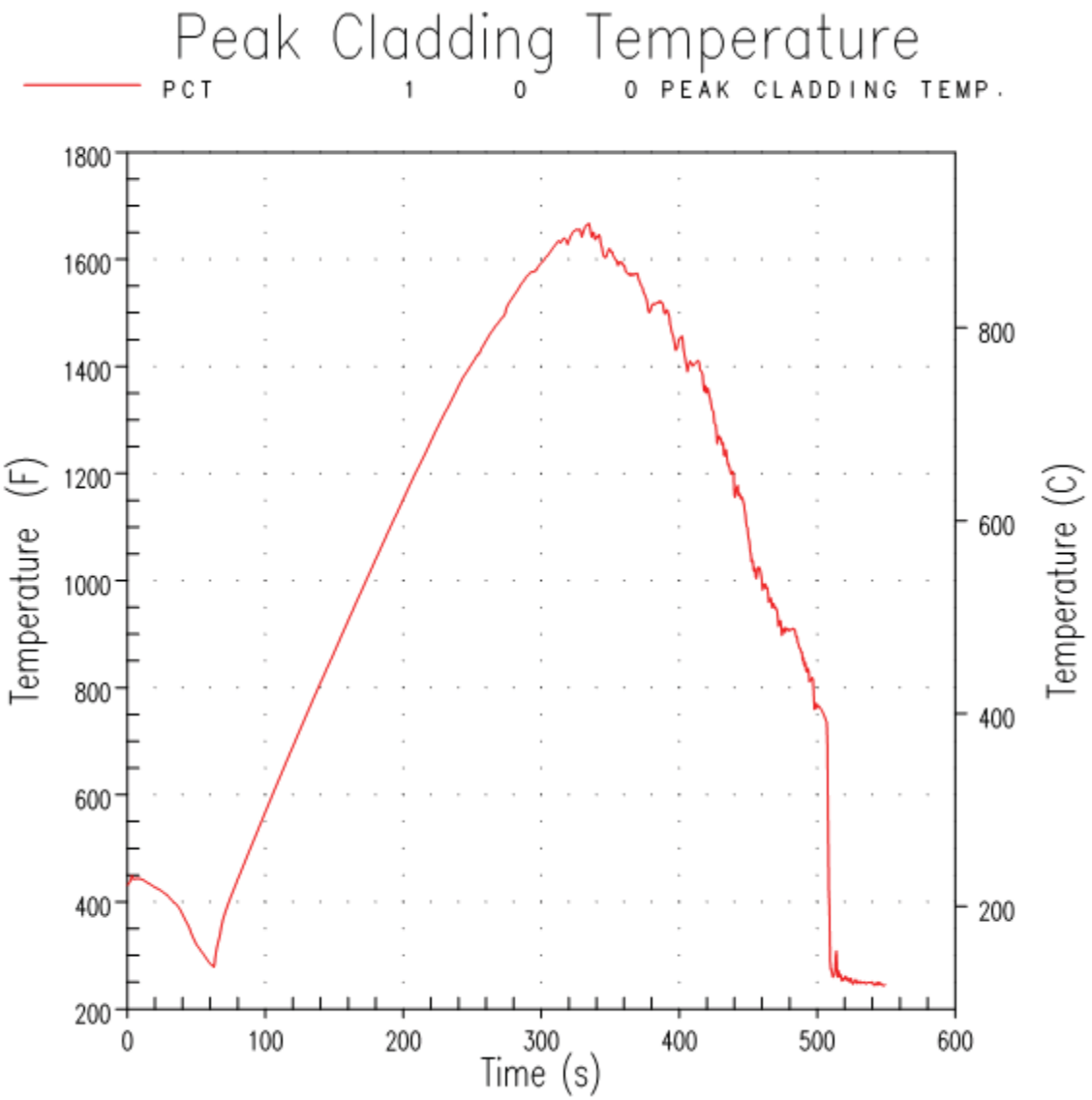


Figure 9.8.4-6. Mode 3 DECLG Break, Peak Cladding Temperature

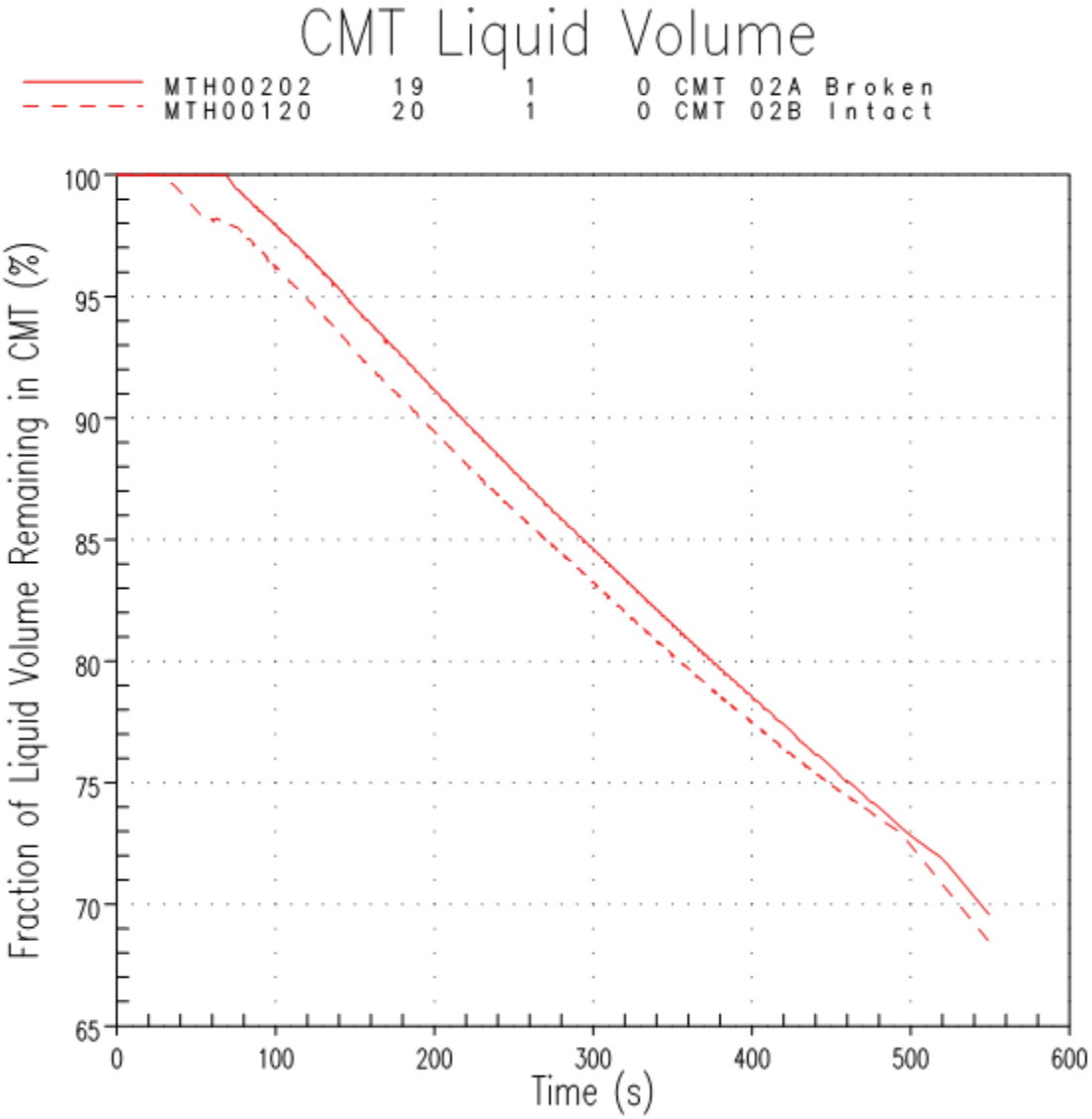


Figure 9.8.4-7. Mode 3 DECLG Break, CMT Liquid Volume

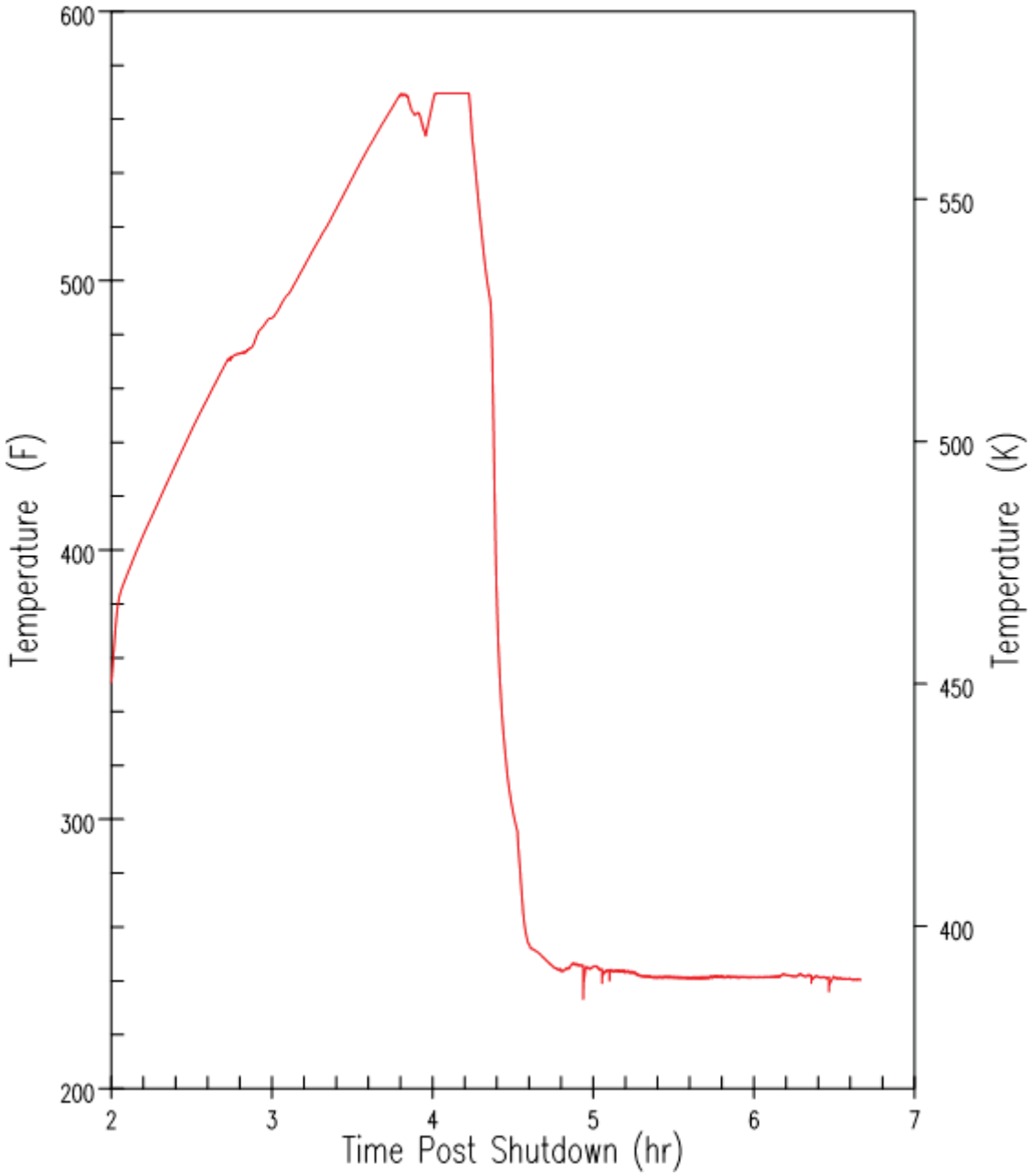


Figure 9.8.5-1. Core Outlet Temperature, Loss of RNS in Mode 4 with RCS Intact

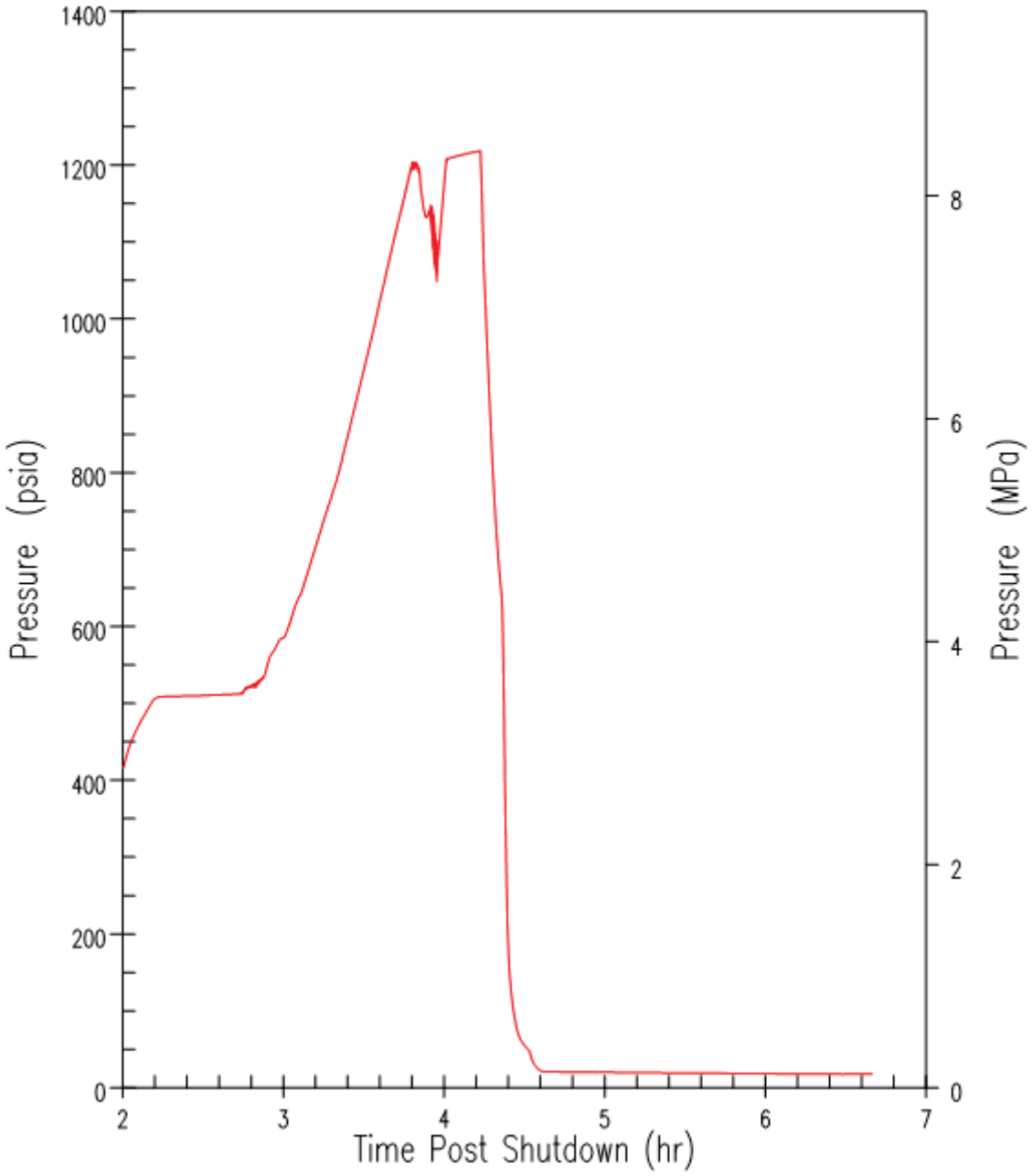


Figure 9.8.5-2. Pressuriser Pressure, Loss of RNS in Mode 4 with RCS Intact

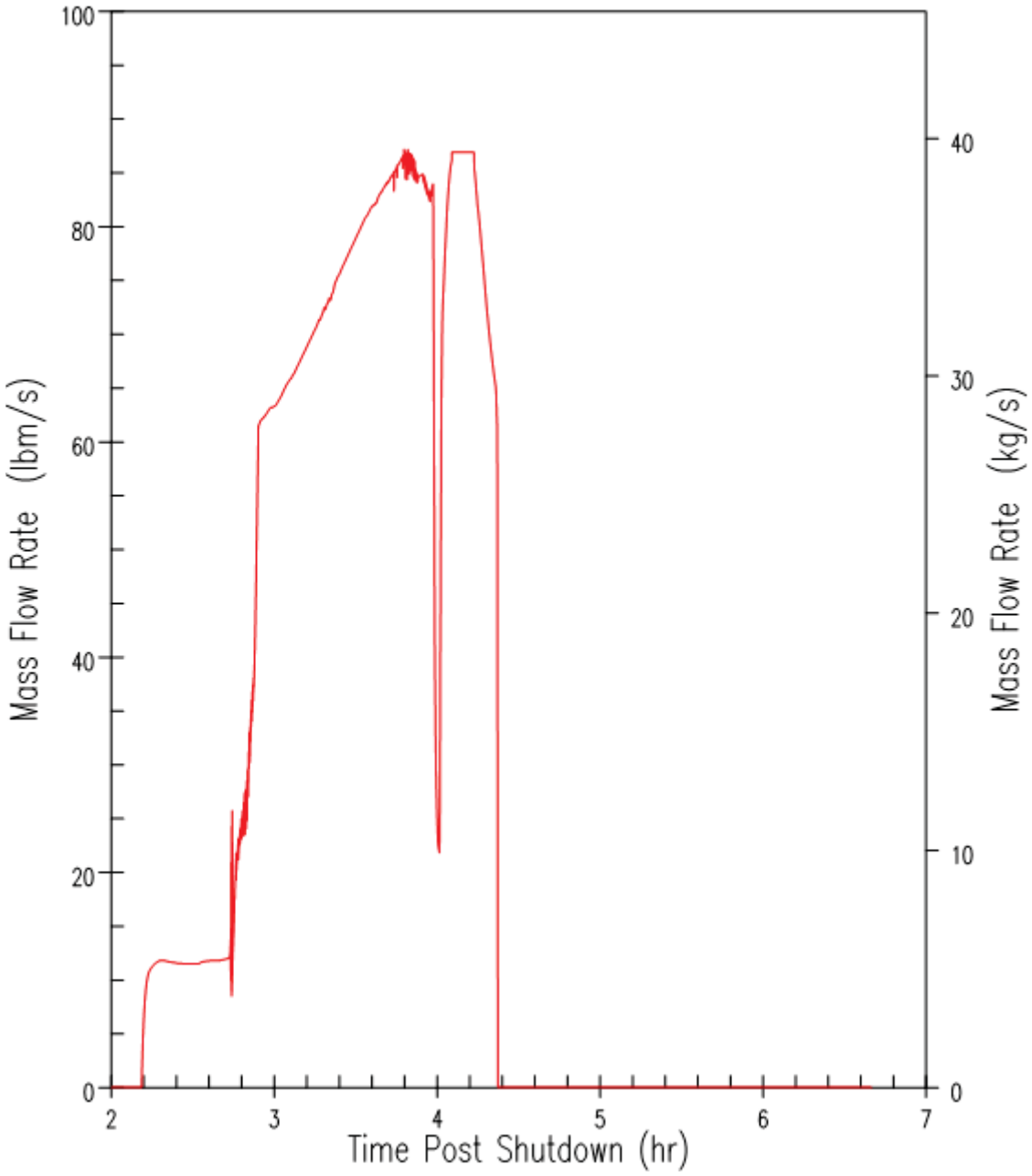


Figure 9.8.5-3. RNS Relief Valve Flow, Loss of RNS in Mode 4 with RCS Intact

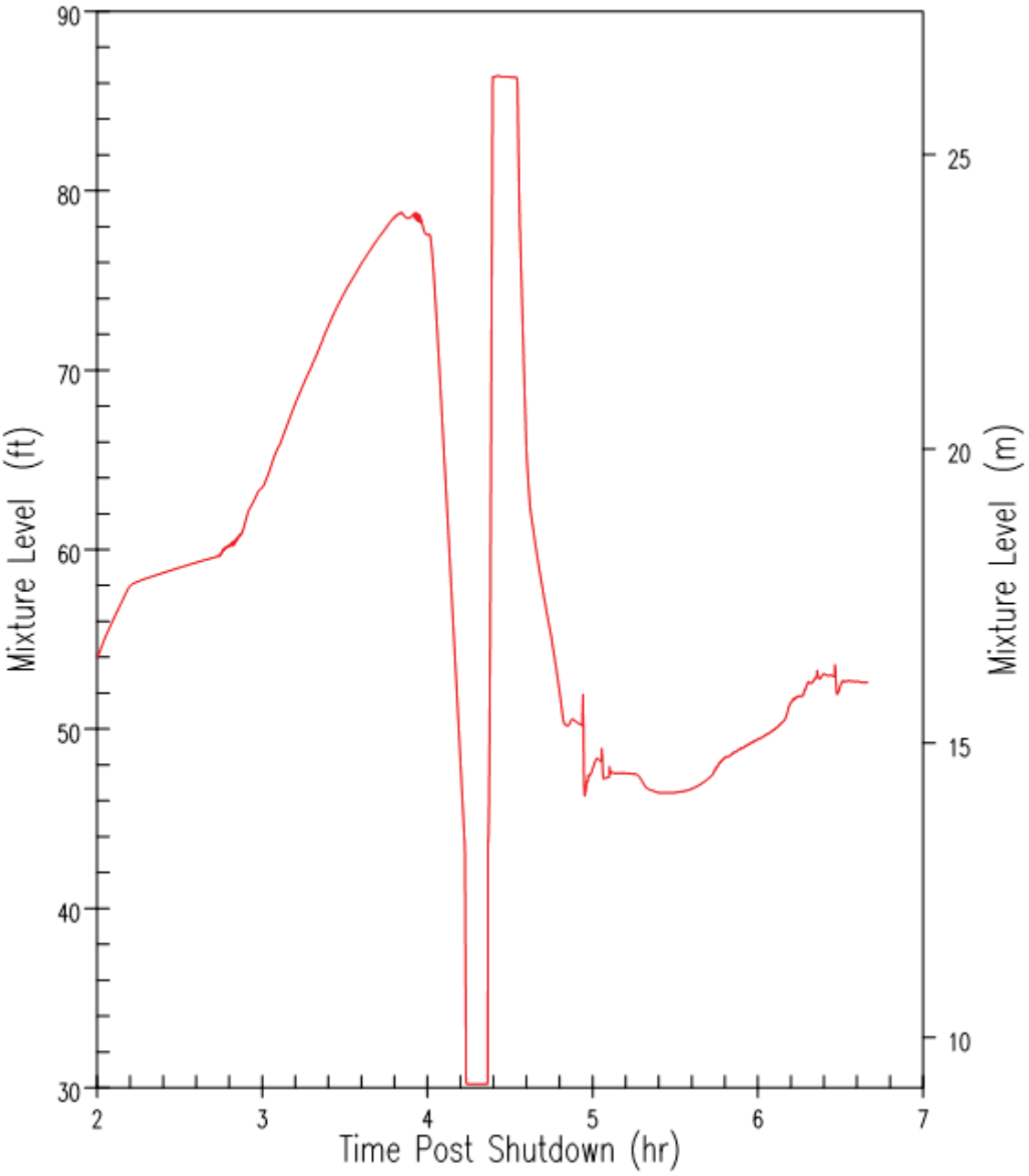


Figure 9.8.5-4. Pressuriser Mixture Level, Loss of RNS in Mode 4 with RCS Intact

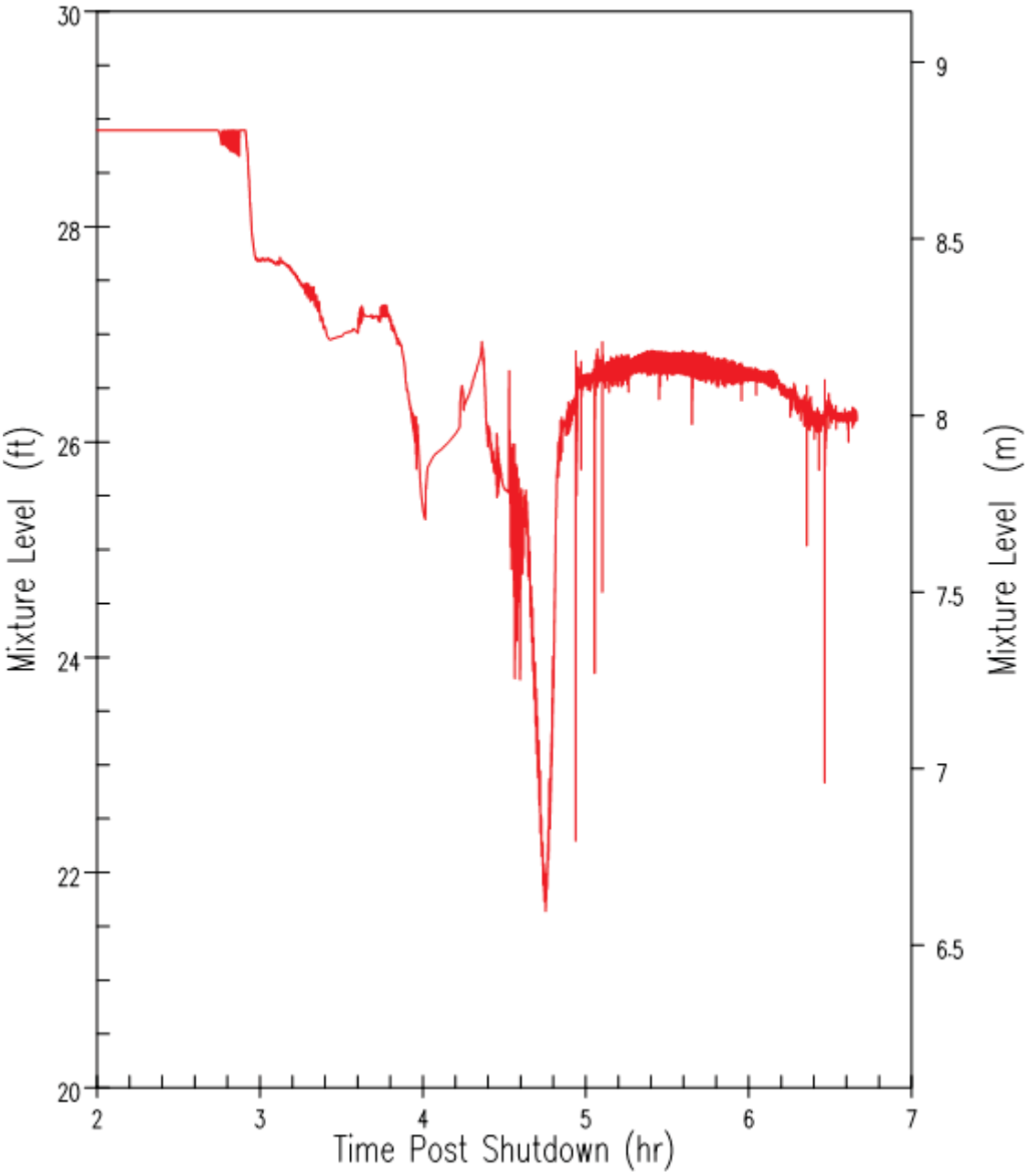


Figure 9.8.5-5. Core Stack Mixture Level, Loss of RNS in Mode 4 with RCS Intact

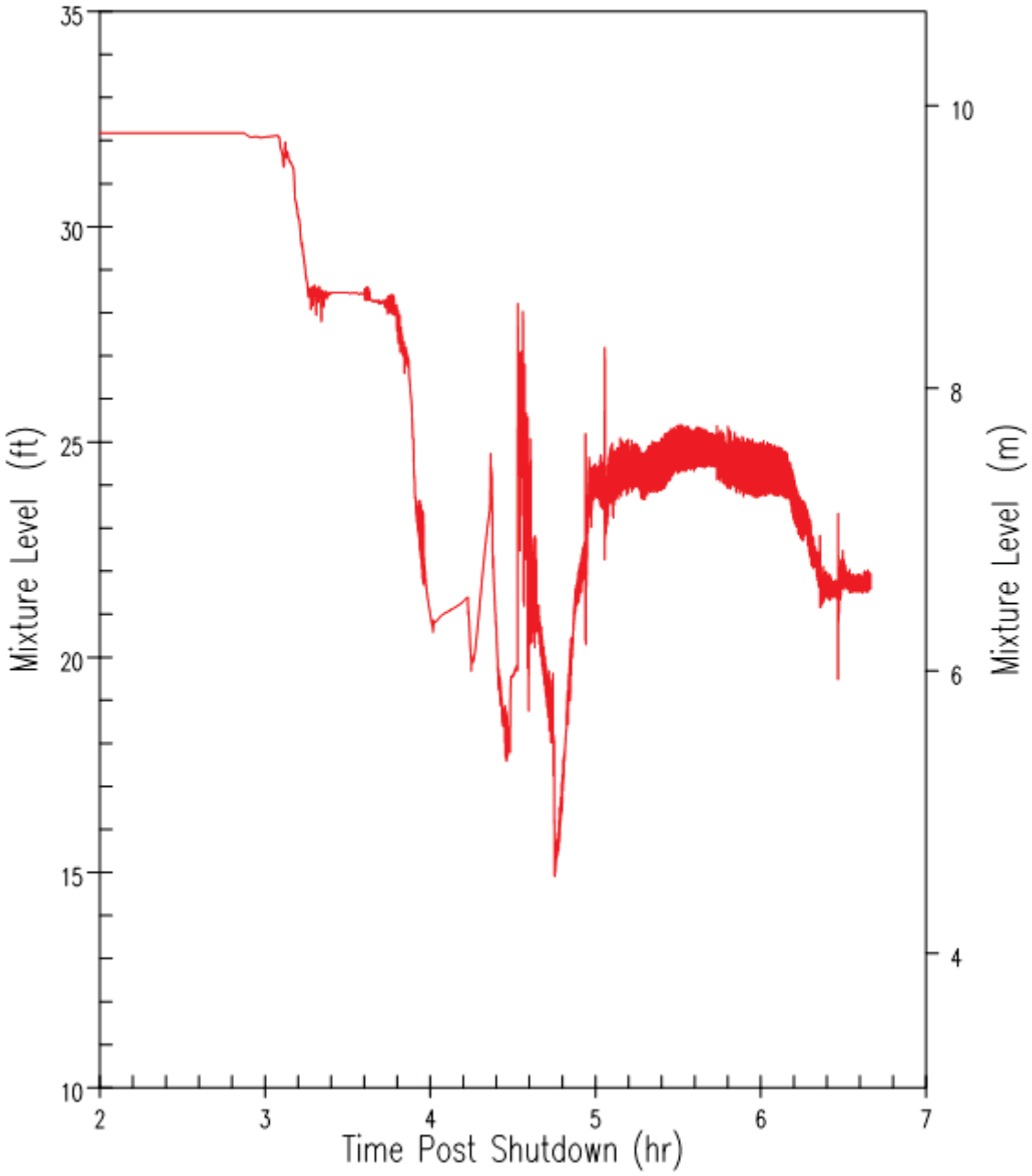


Figure 9.8.5-6. Downcomer Mixture Level, Loss of RNS in Mode 4 with RCS Intact

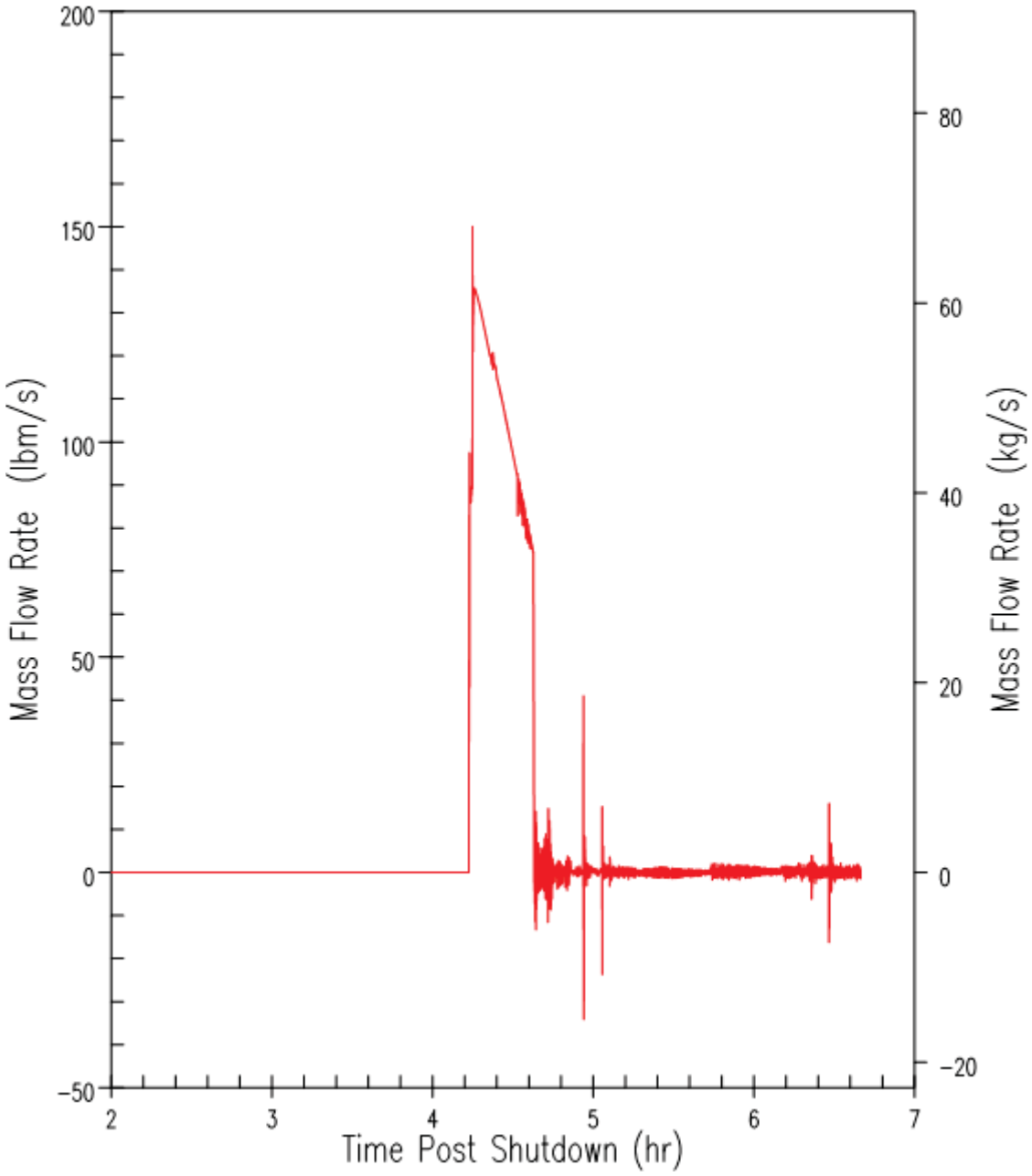


Figure 9.8.5-7. CMT to DVI Flow, Loss of RNS in Mode 4 with RCS Intact

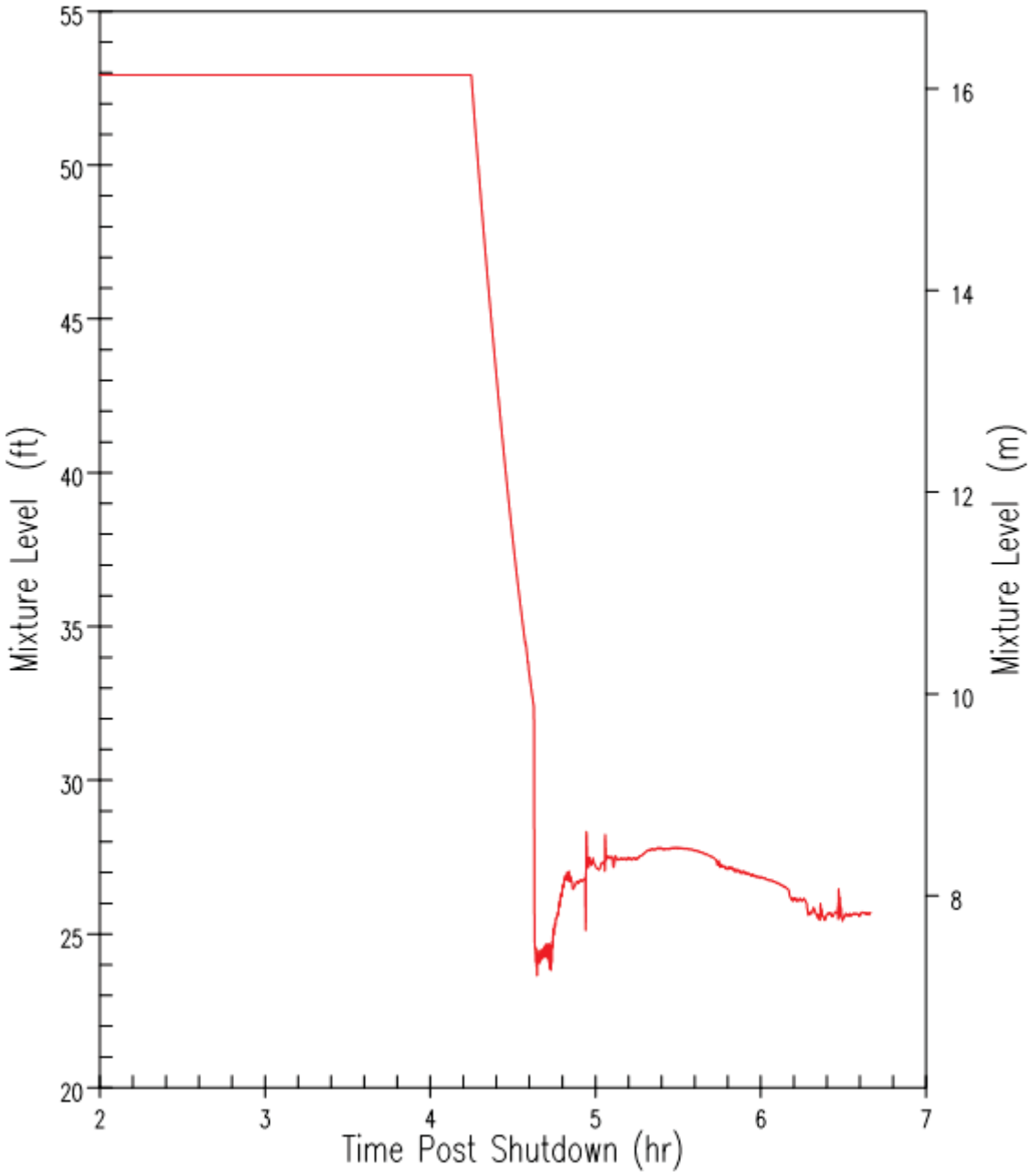


Figure 9.8.5-8. CMT Mixture Level, Loss of RNS in Mode 4 with RCS Intact

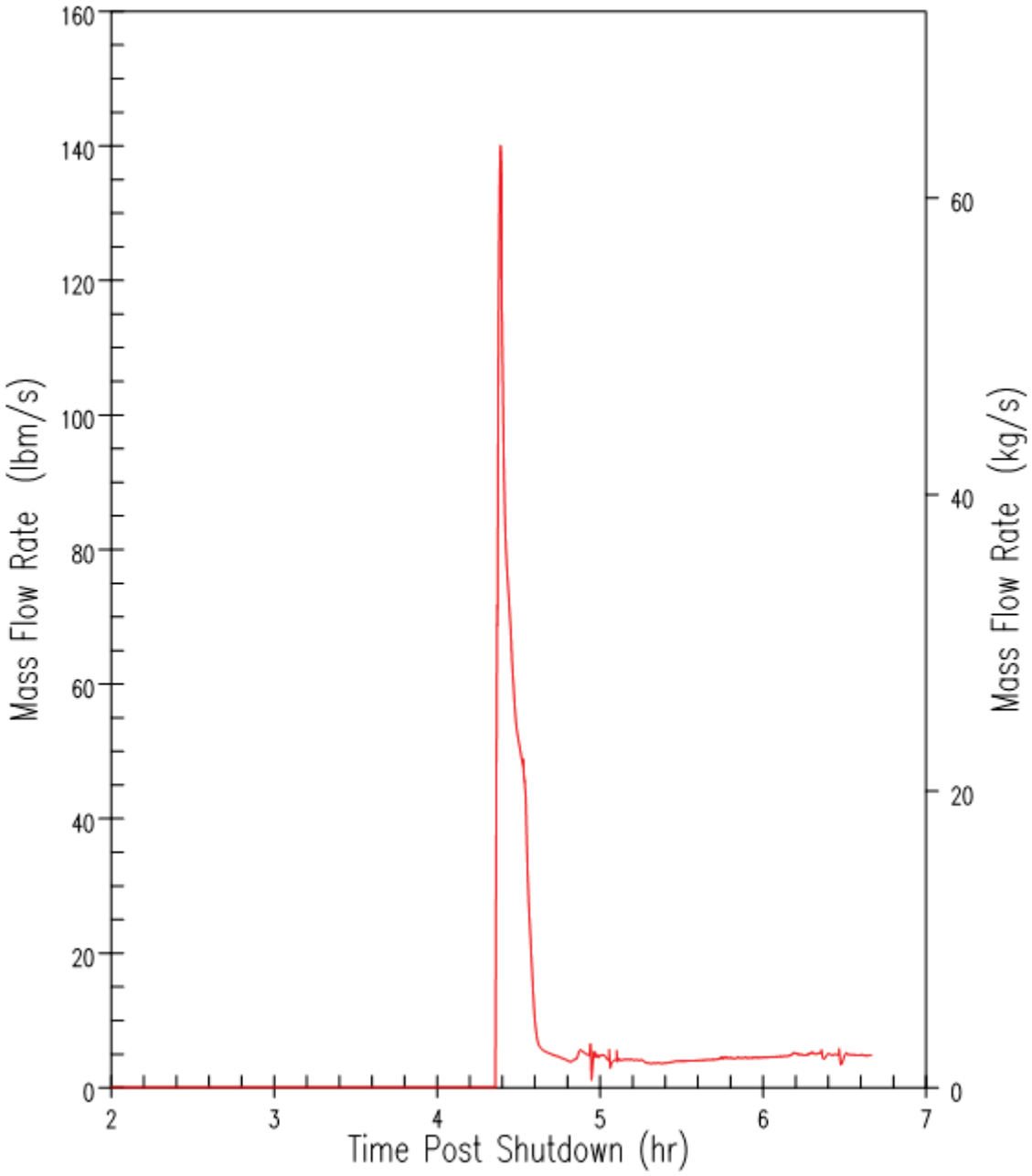


Figure 9.8.5-9. ADS Stages 1-3 Vapour Flow, Loss of RNS in Mode 4 with RCS Intact

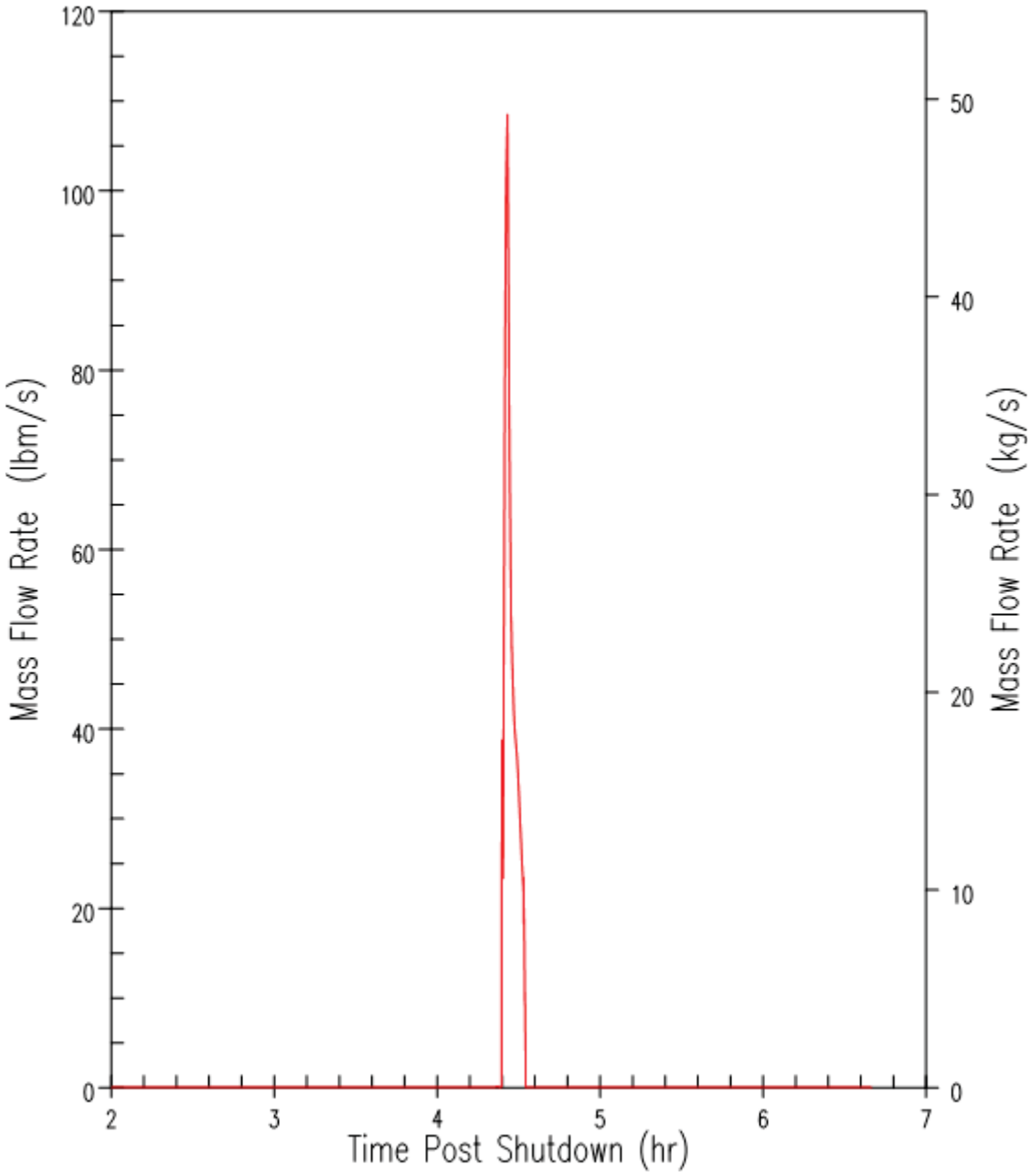


Figure 9.8.5-10. ADS Stages 1-3 Liquid Flow, Loss of RNS in Mode 4 with RCS Intact

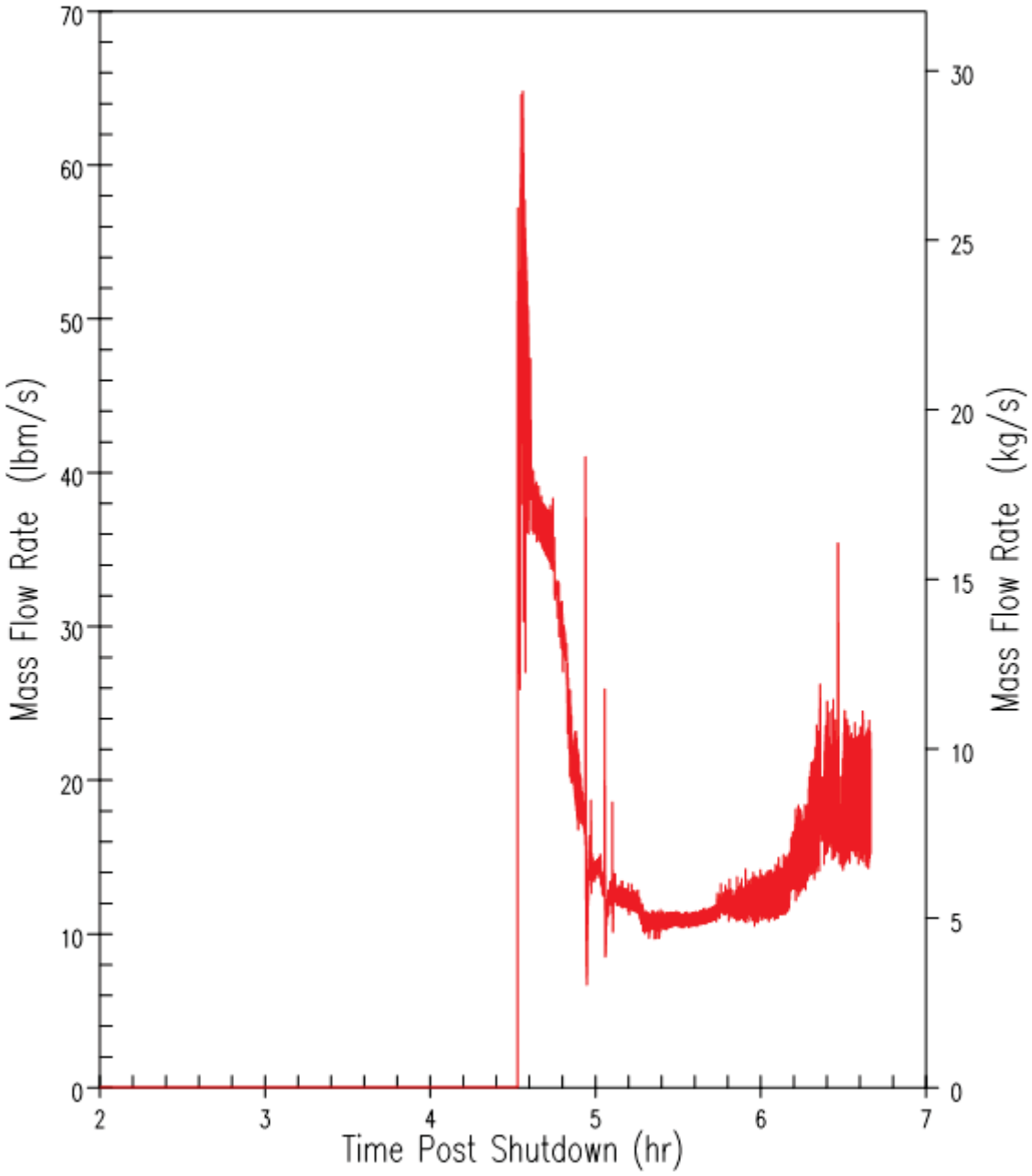


Figure 9.8.5-11. ADS Stage 4 Vapour Flow, Loss of RNS in Mode 4 with RCS Intact

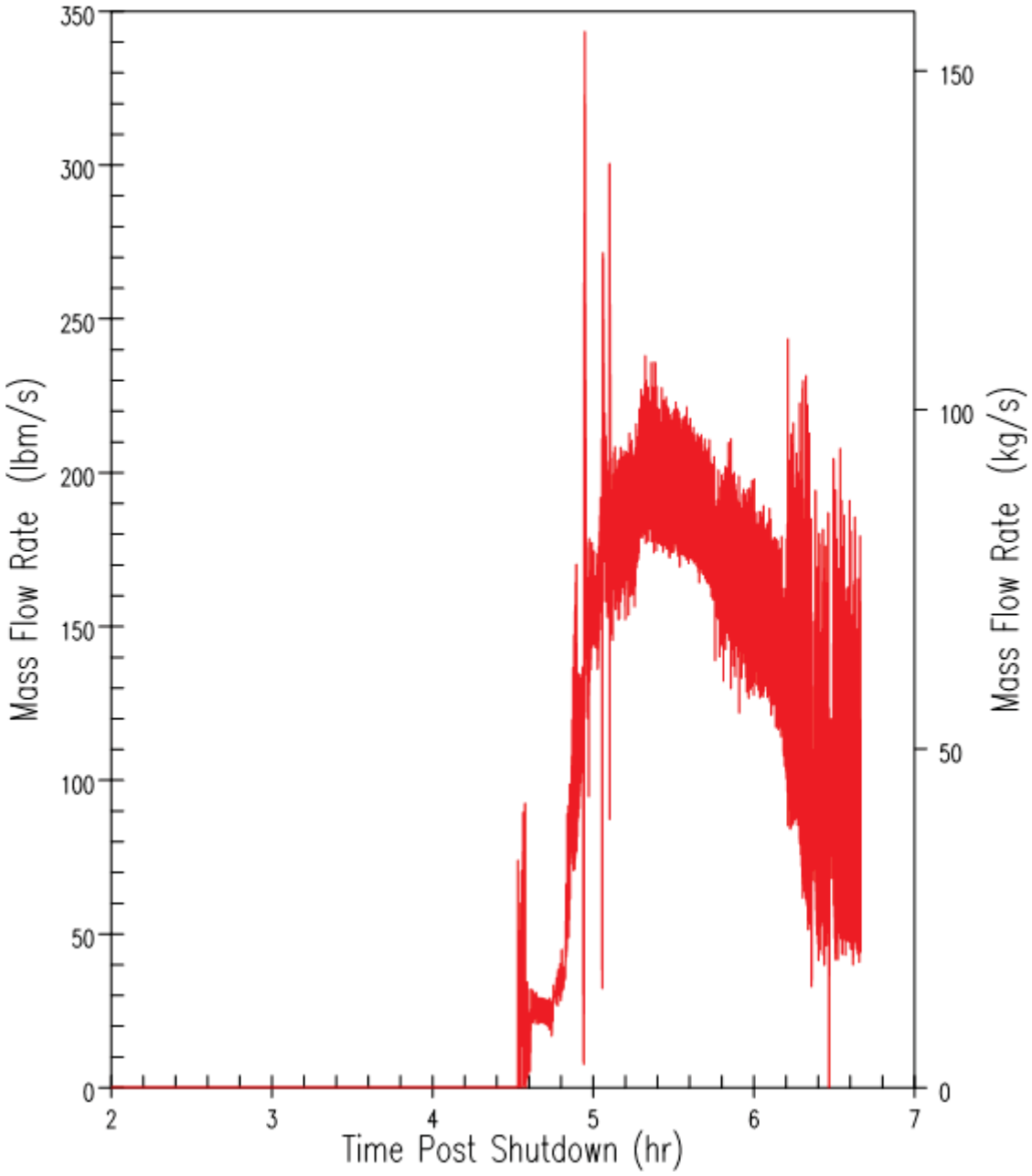


Figure 9.8.5-12. ADS Stage 4 Liquid Flow, Loss of RNS in Mode 4 with RCS Intact

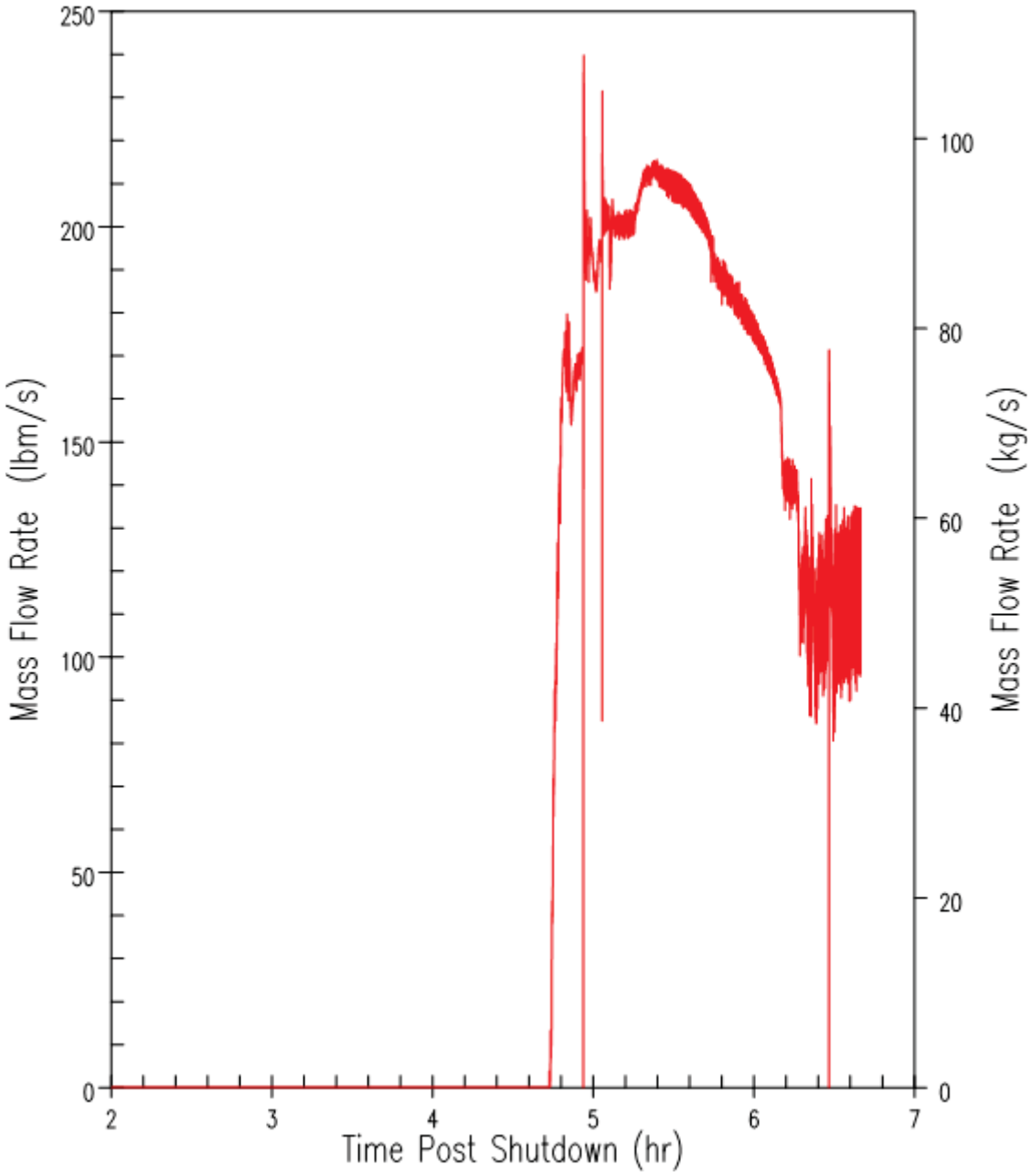


Figure 9.8.5-13. Total IRWST Injection Flow, Loss of RNS in Mode 4 with RCS Intact

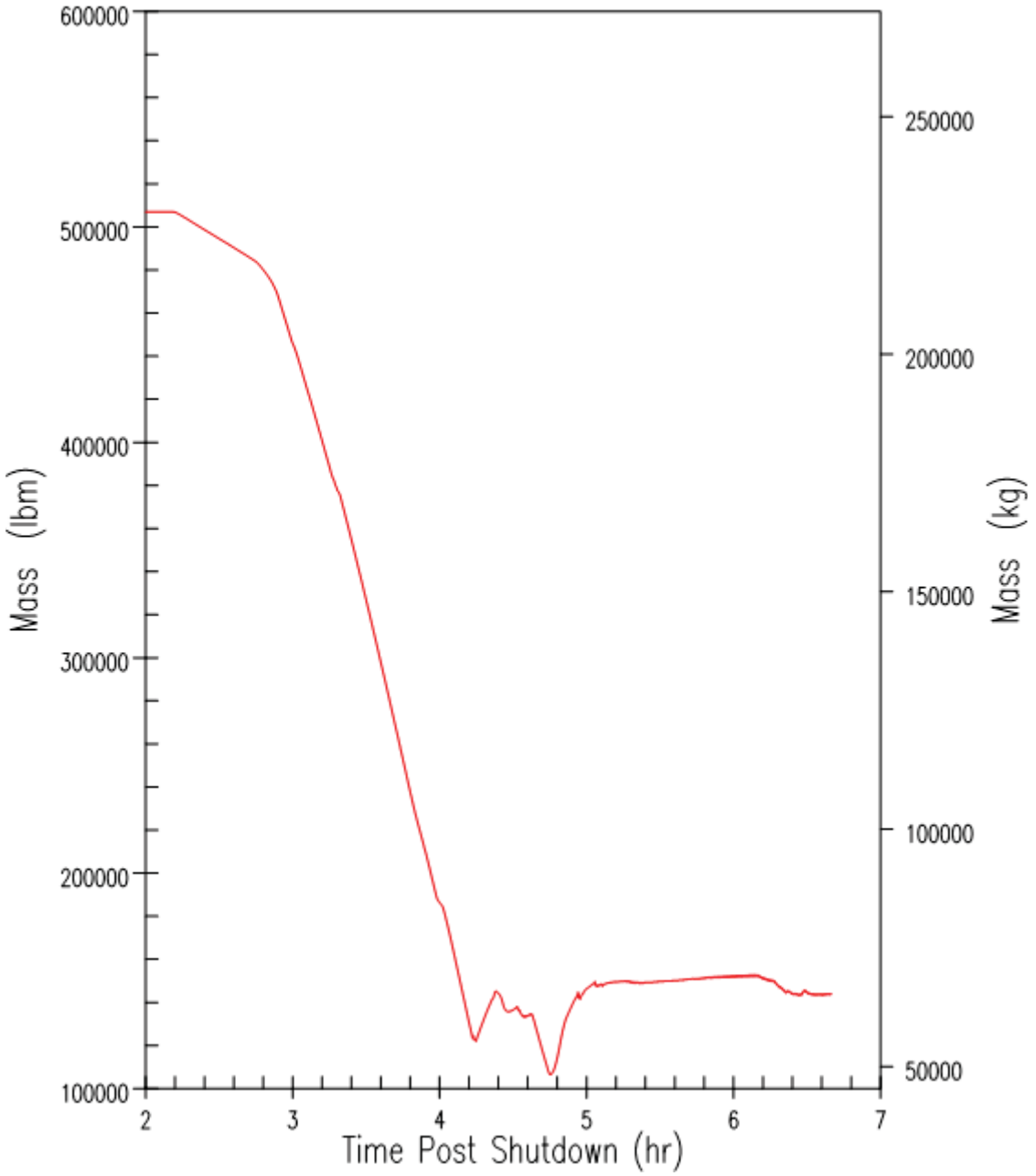


Figure 9.8.5-14. Primary Mass Inventory, Loss of RNS in Mode 4 with RCS Intact

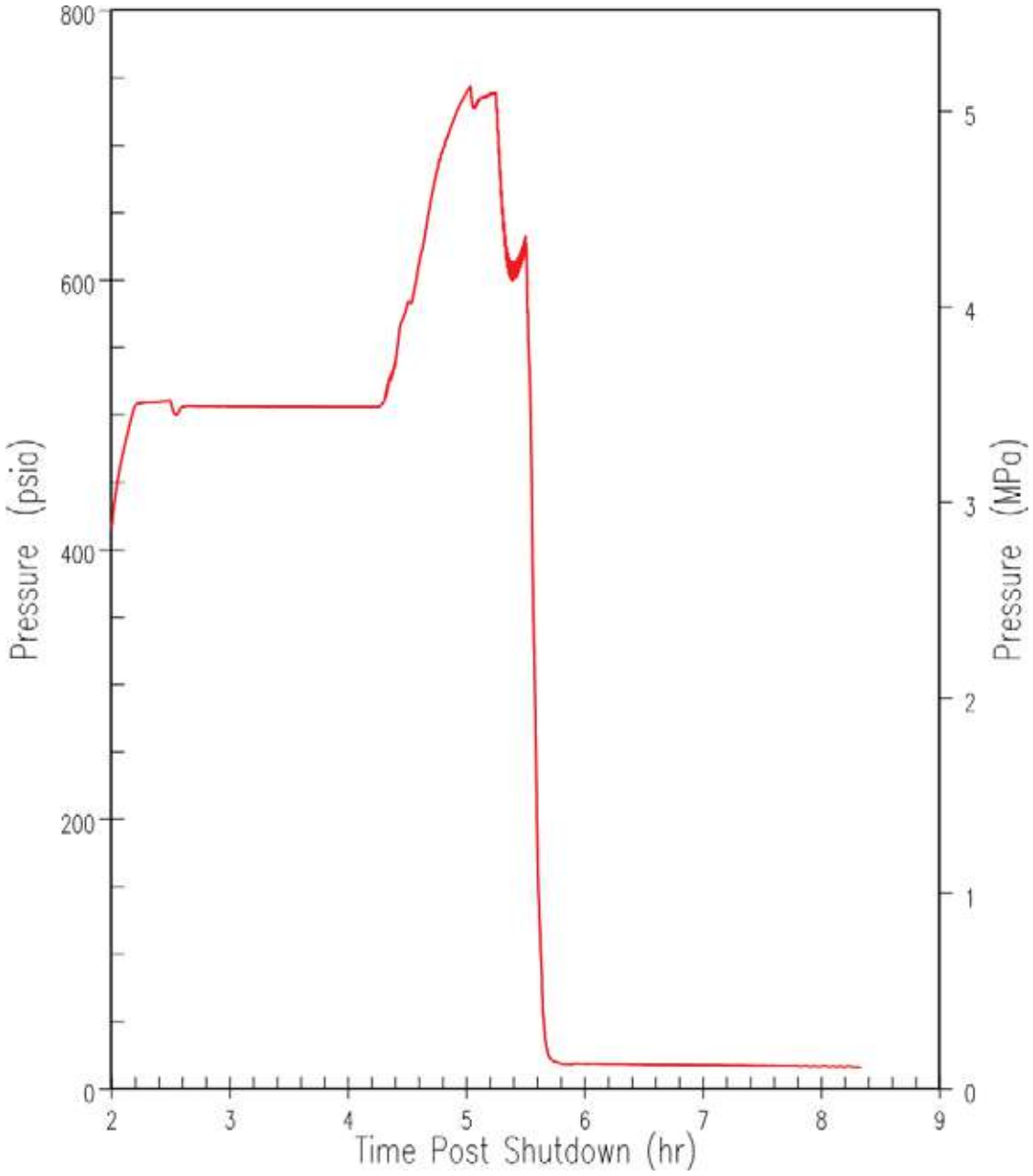


Figure 9.8.5-15. Pressuriser Pressure, Loss of RNS in Mode 4 with RCS Intact, Manual Safety System Actuation at 1800 Seconds

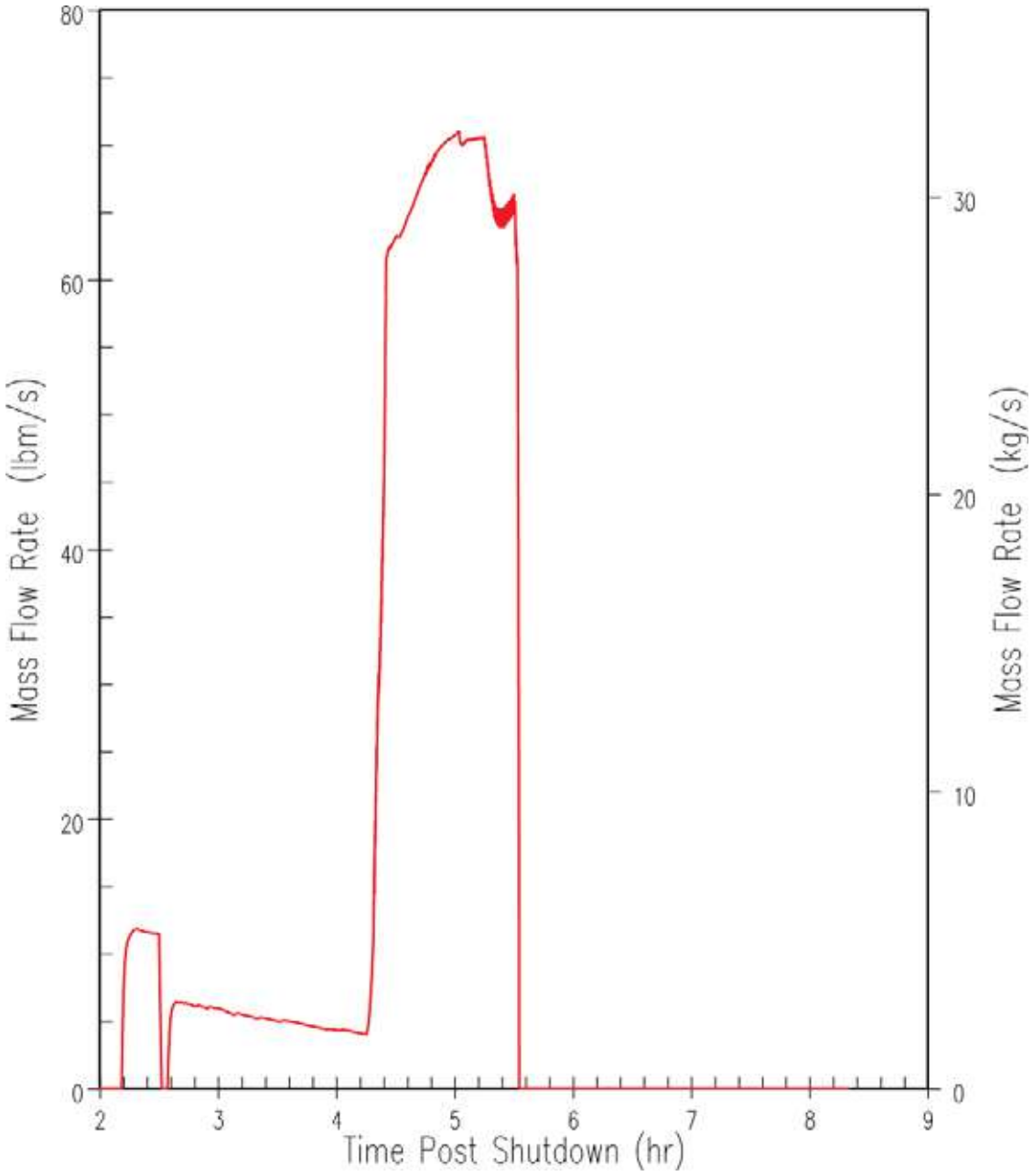


Figure 9.8.5-16. RNS Safety Valve Flow, Loss of RNS in Mode 4 with RCS Intact, Manual Safety System Actuation at 1800 Seconds

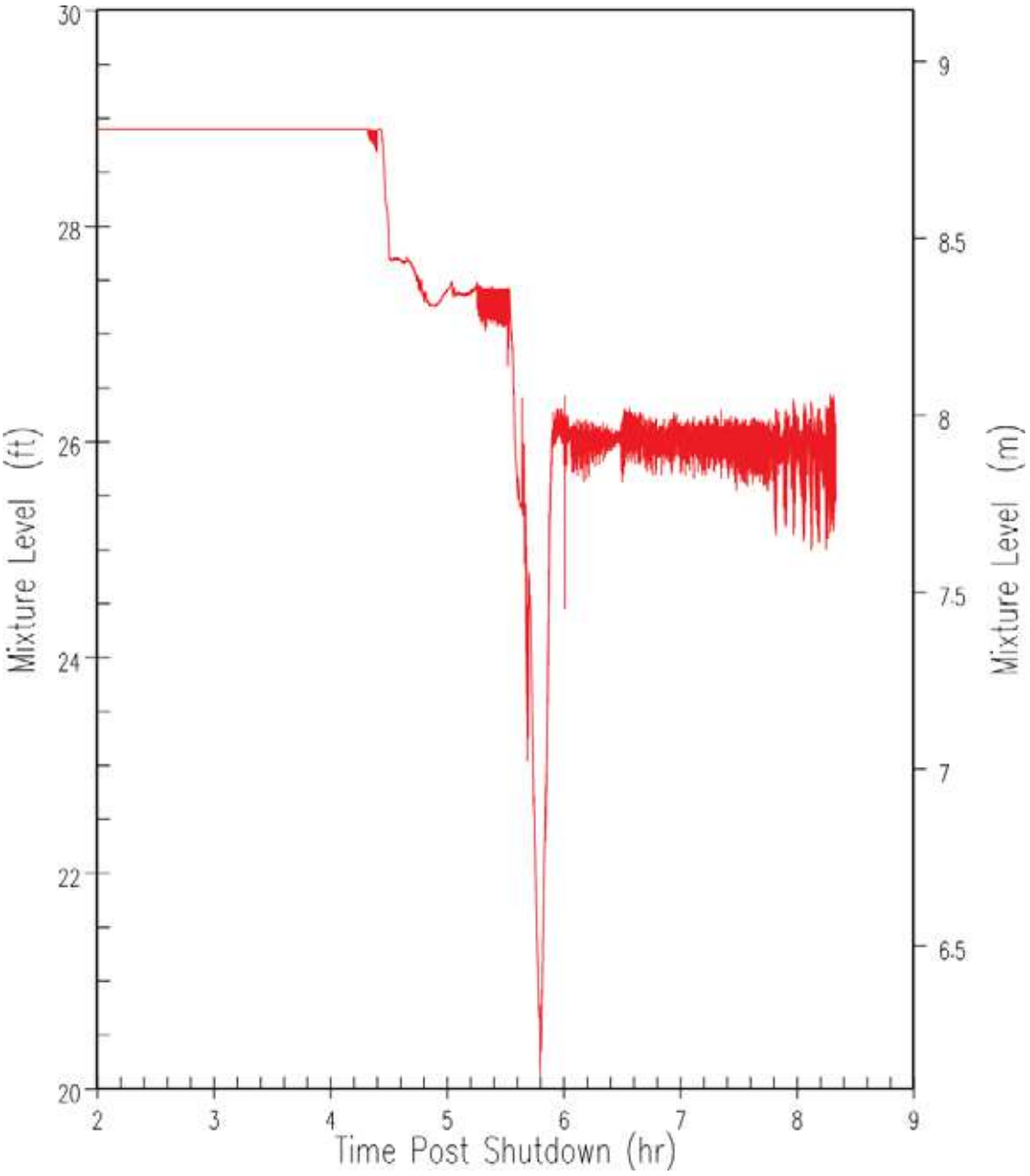


Figure 9.8.5-17. Core Stack Mixture Level, Loss of RNS in Mode 4 with RCS Intact Manual Safety System Actuation at 1800 Seconds

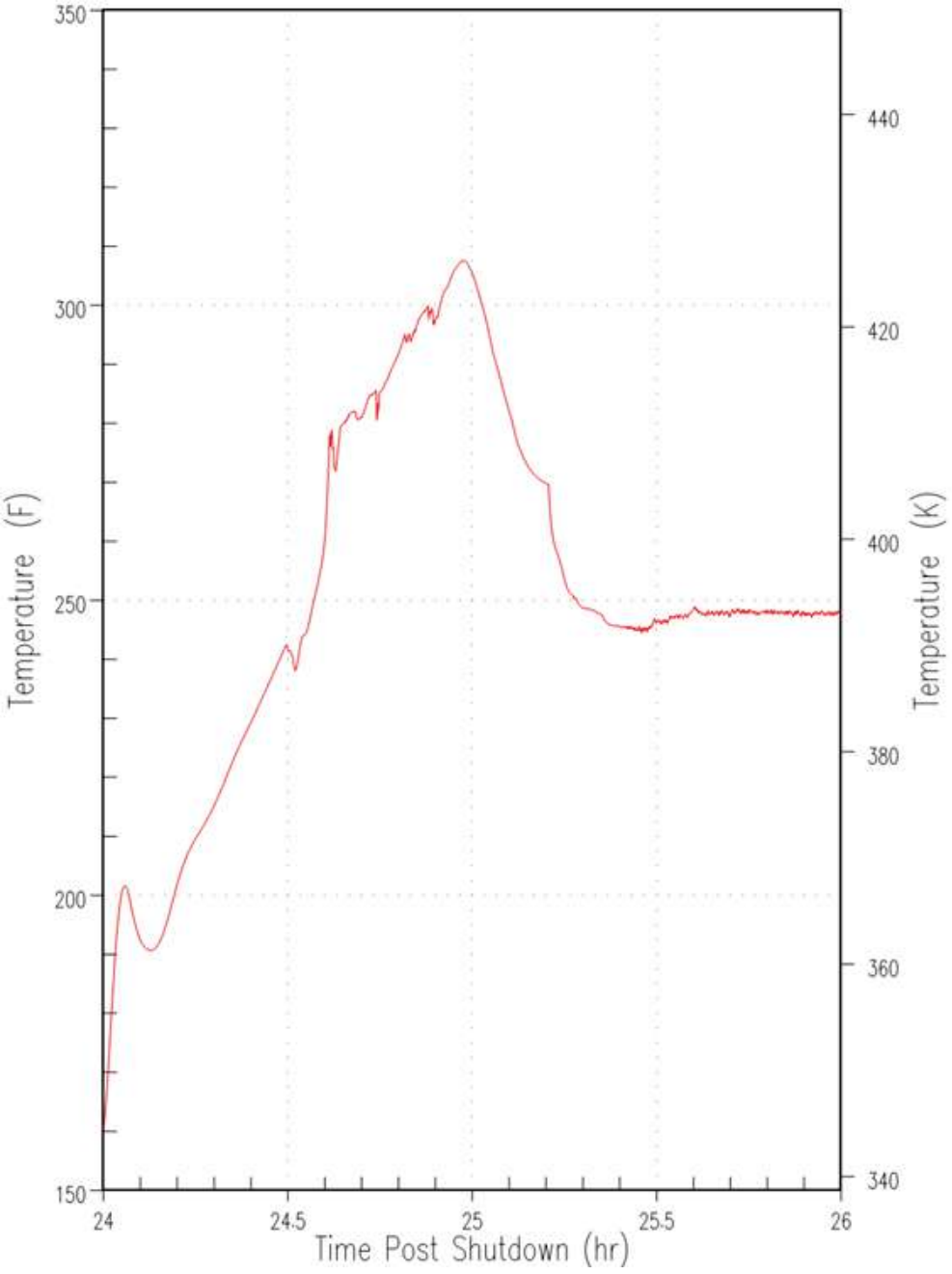


Figure 9.8.5-18. Core Outlet Fluid Temperature, Loss of RNS in Mode 5 with RCS Open

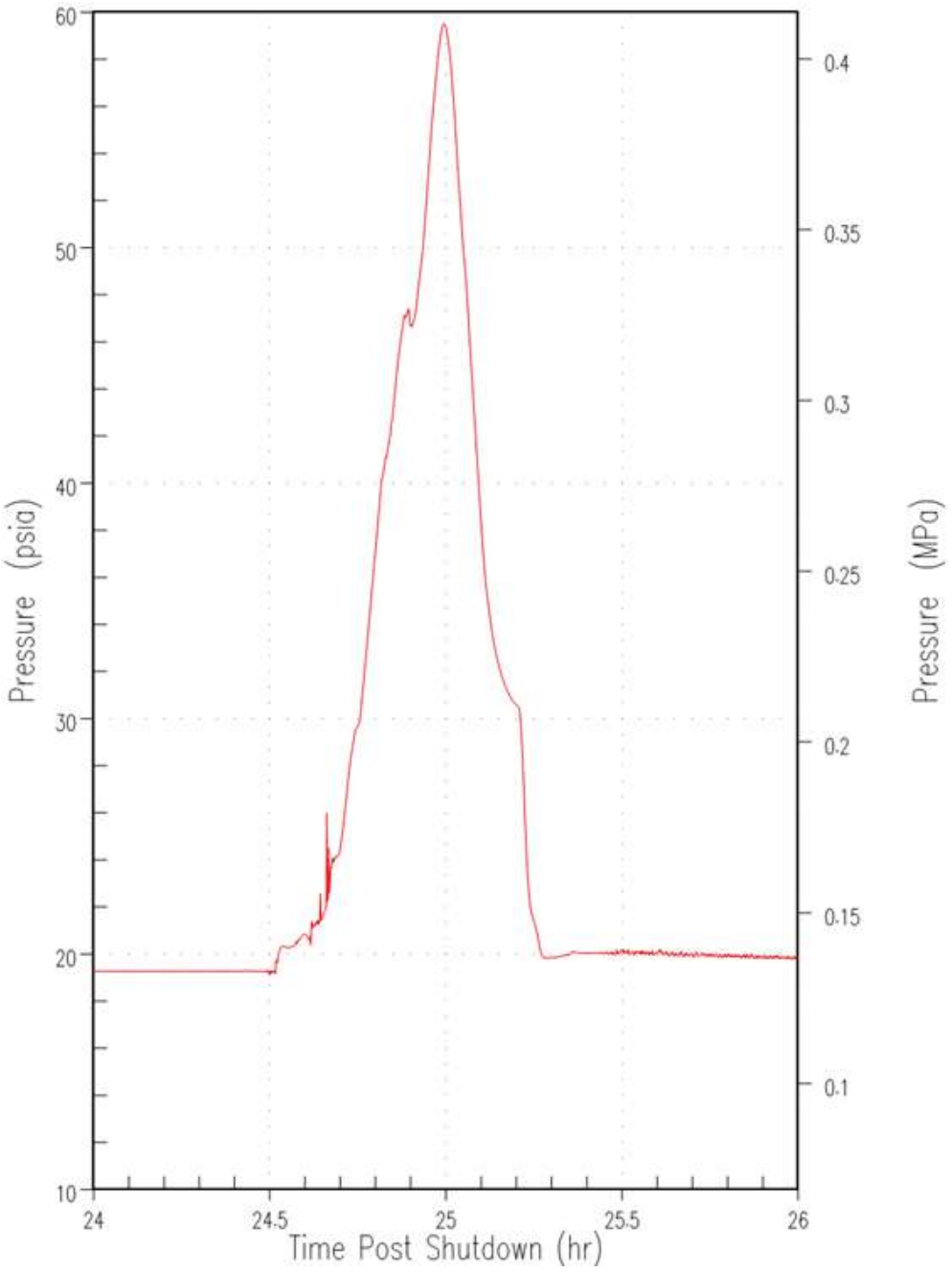


Figure 9.8.5-19. Pressuriser Pressure, Loss of RNS in Mode 5 with RCS Open

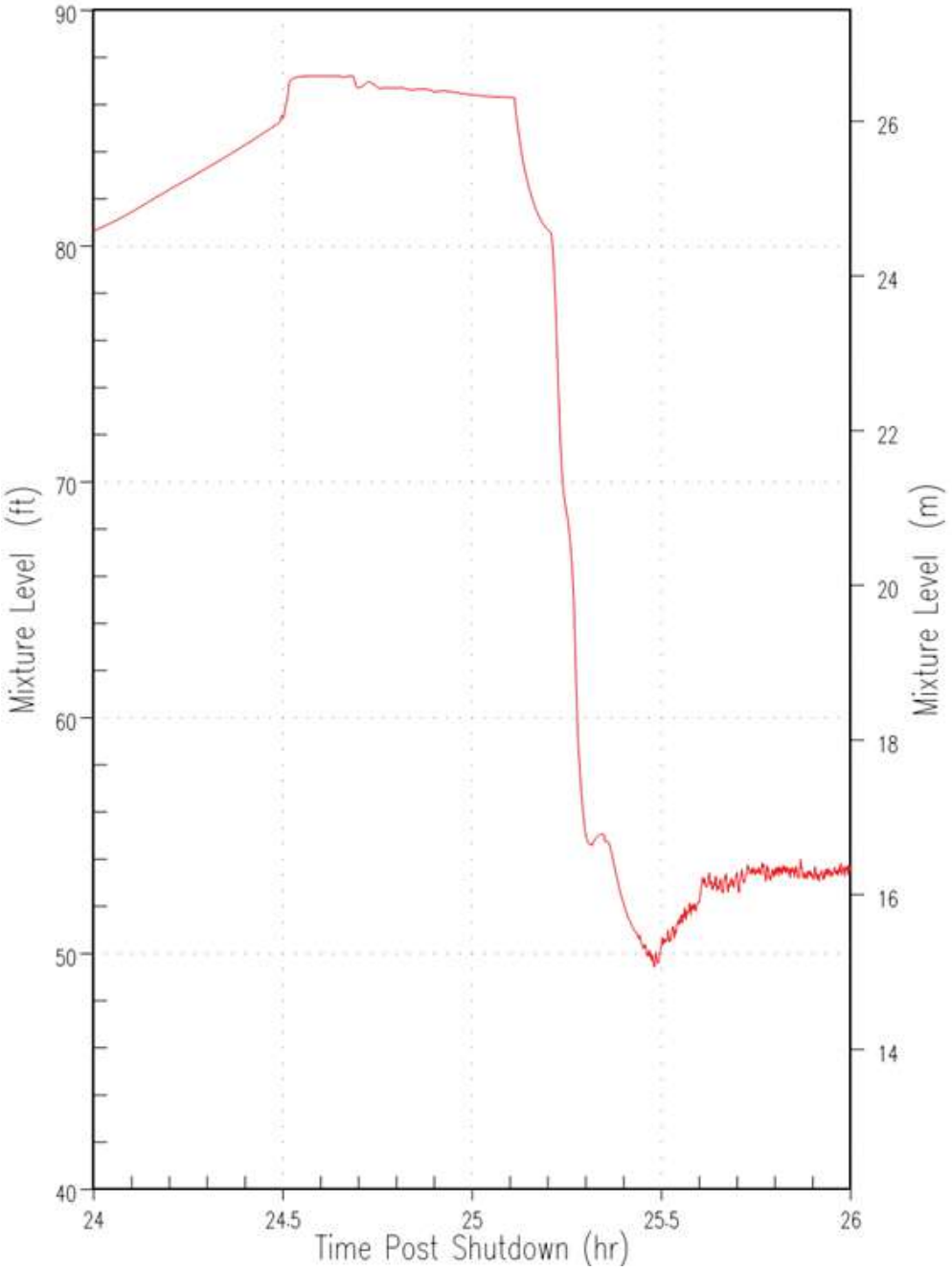


Figure 9.8.5-20. Pressuriser Mixture Level, Loss of RNS in Mode 5 with RCS Open

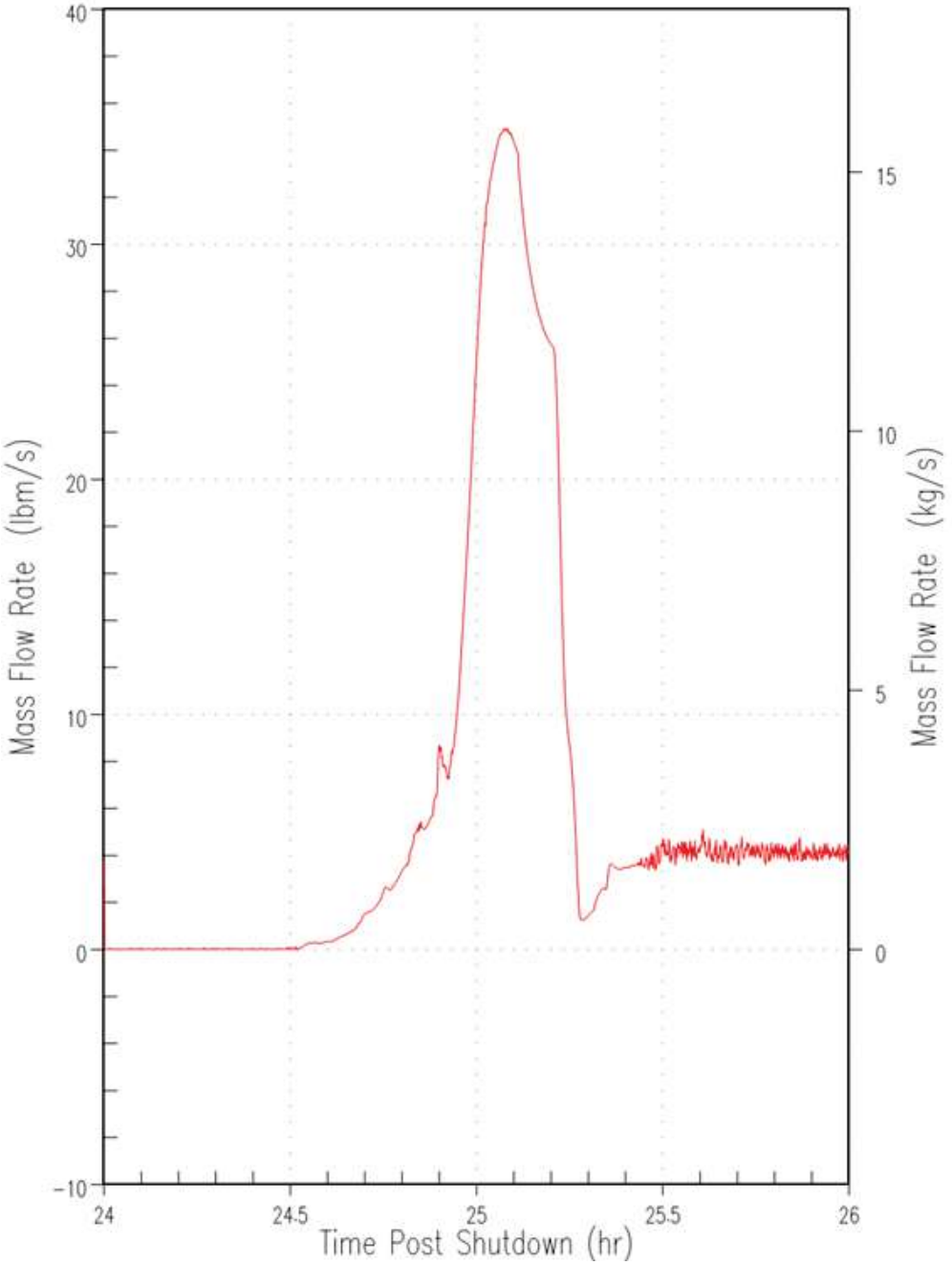


Figure 9.8.5-21. ADS Stages 1-3 Vapour Flow, Loss of RNS in Mode 5 with RCS Open

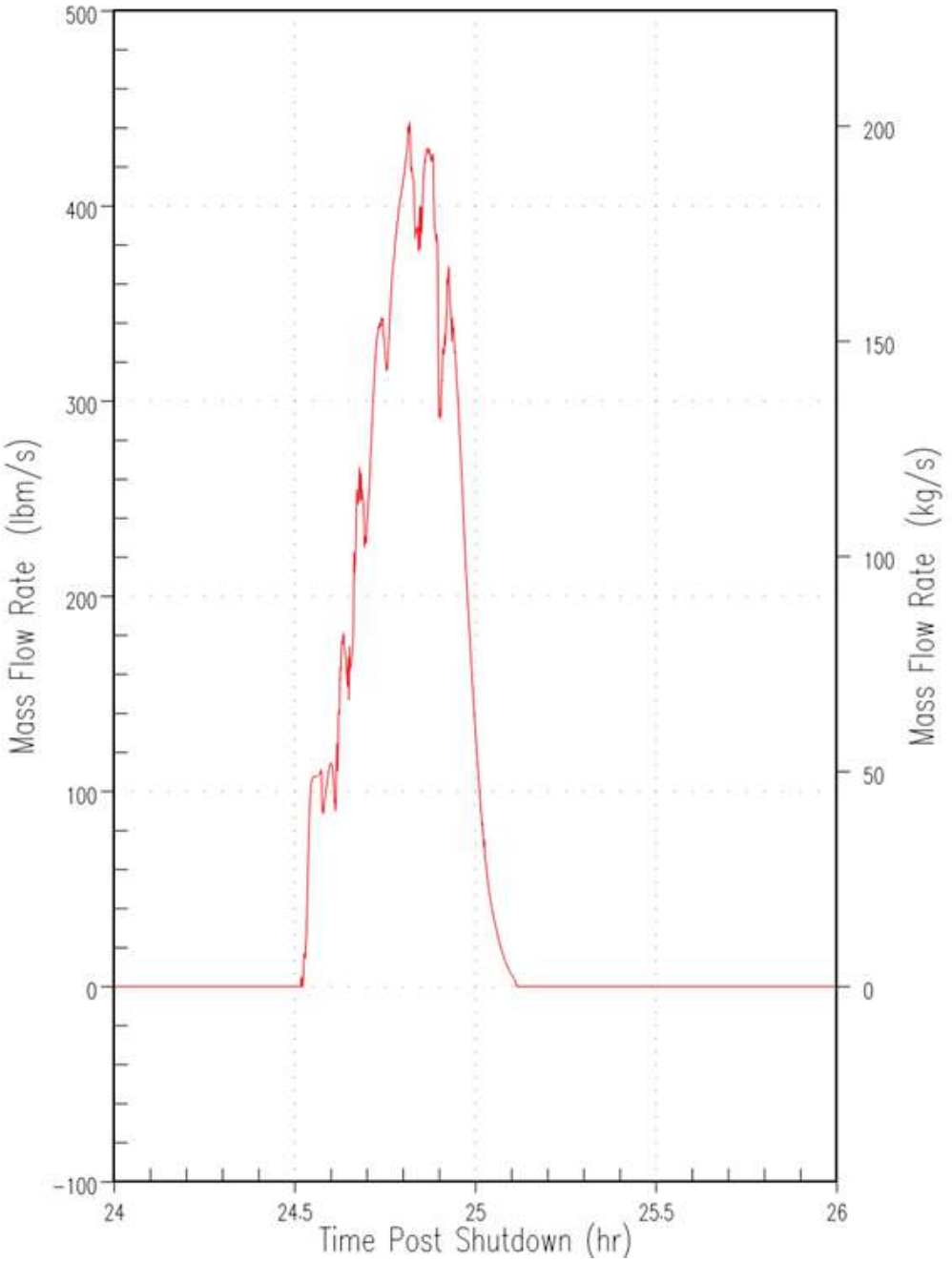


Figure 9.8.5-22. ADS Stages 1-3 Liquid Flow, Loss of RNS in Mode 5 with RCS Open

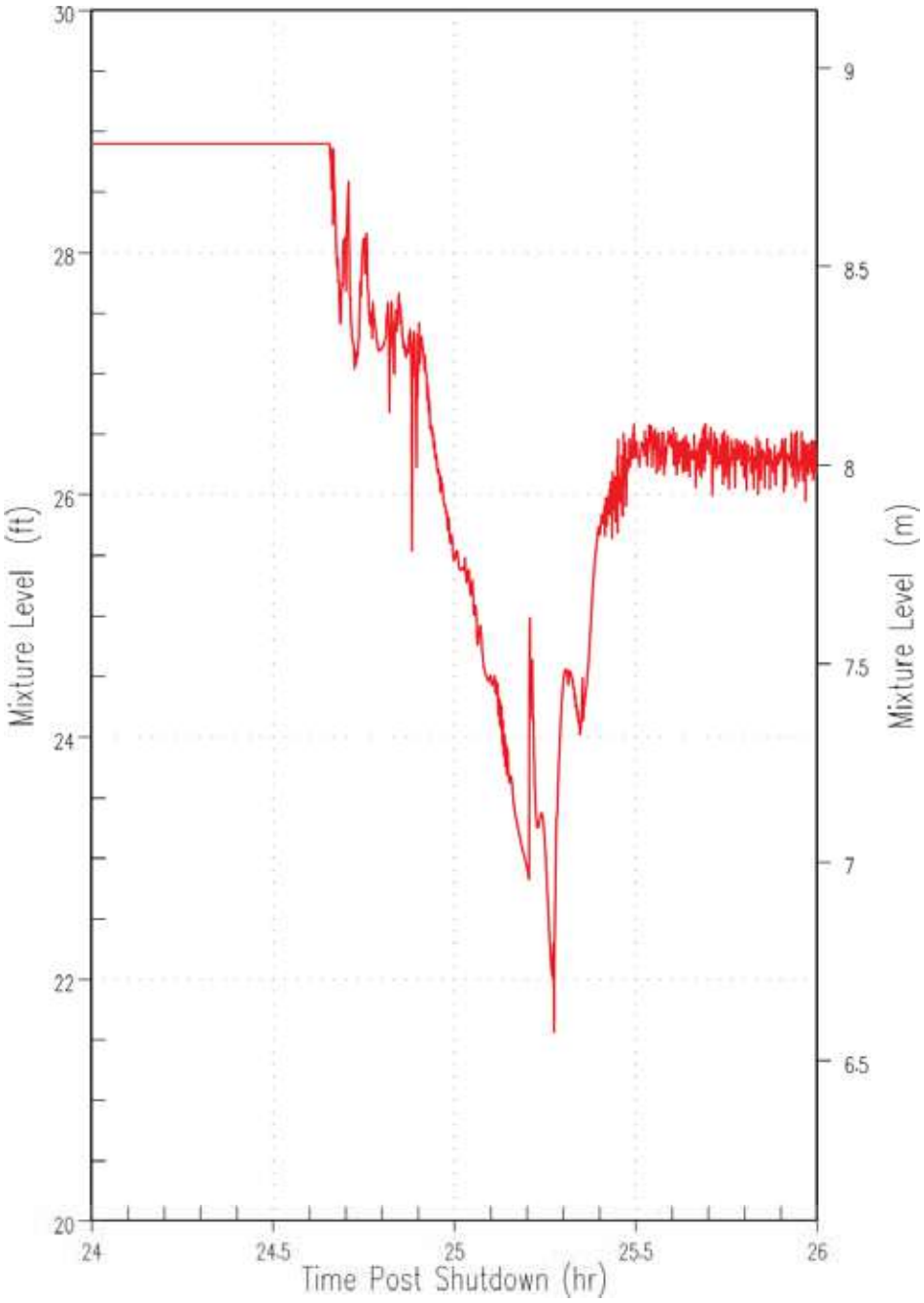


Figure 9.8.5-23. Core Stack Mixture Level, Loss of RNS in Mode 5 with RCS Open

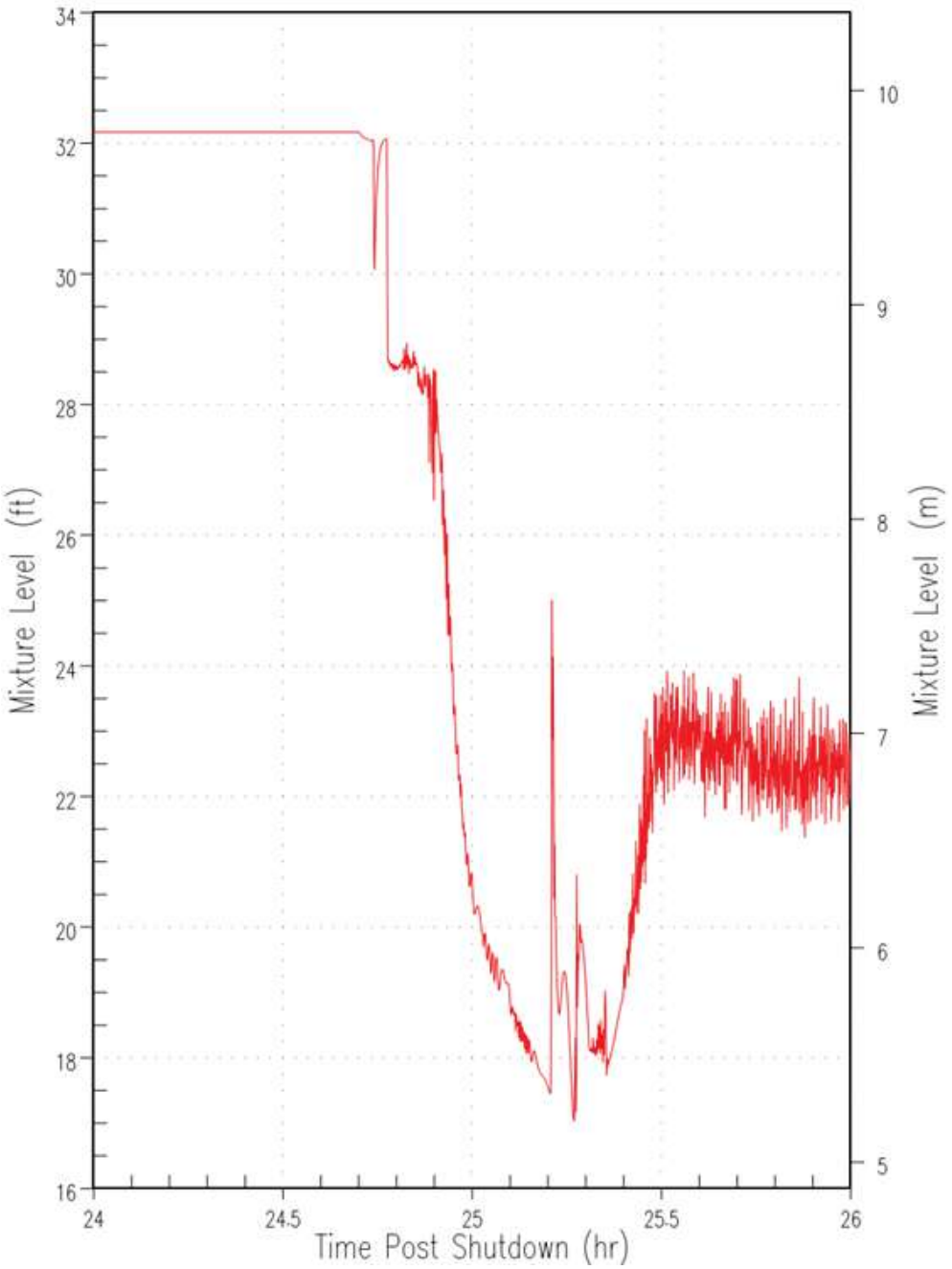


Figure 9.8.5-24. Downcomer Mixture Level, Loss of RNS in Mode 5 with RCS Open

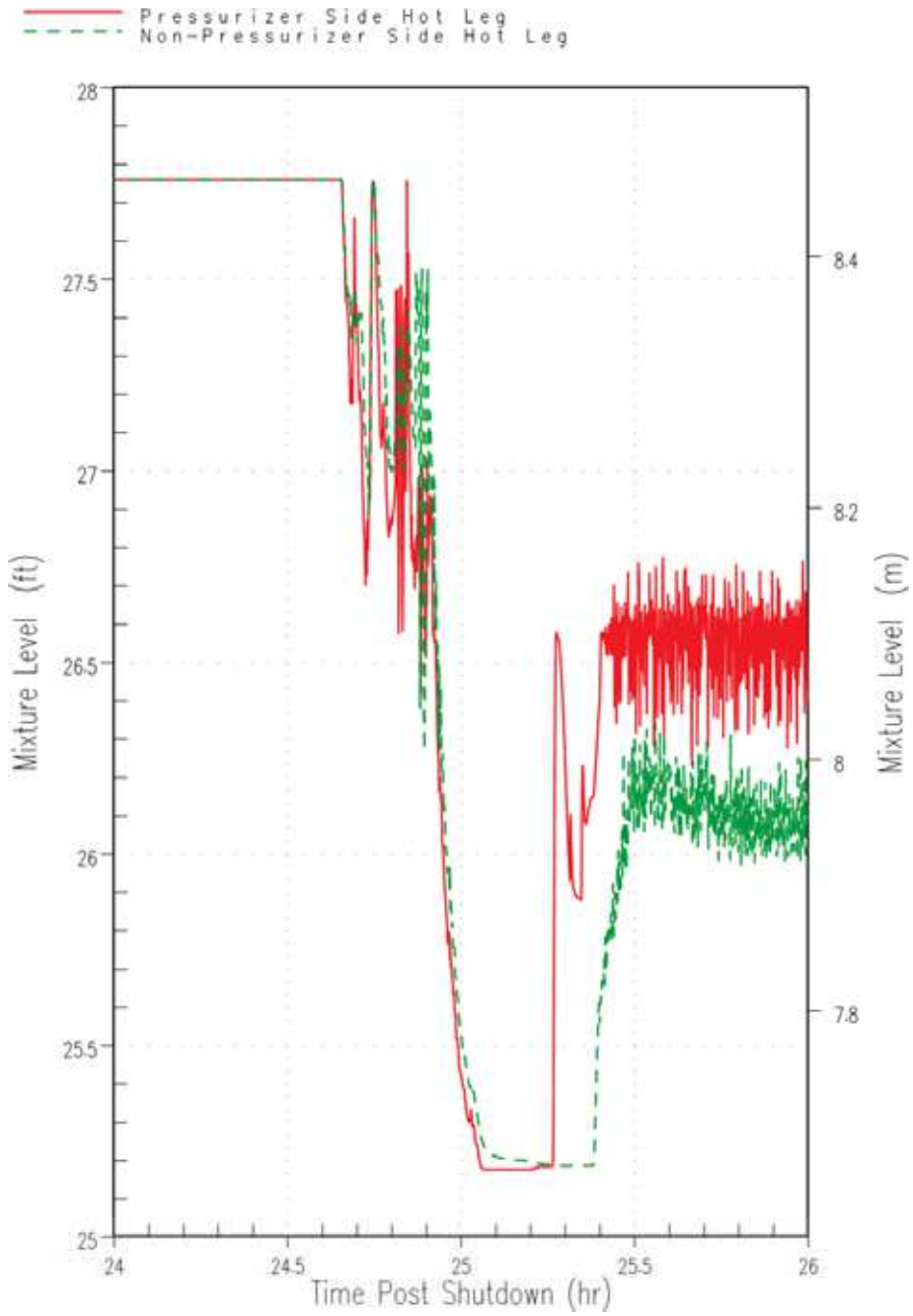


Figure 9.8.5-25. Loop 1 and Loop 2 Hot-Leg Mixture Levels, Loss of RNS in Mode 5 with RCS Open

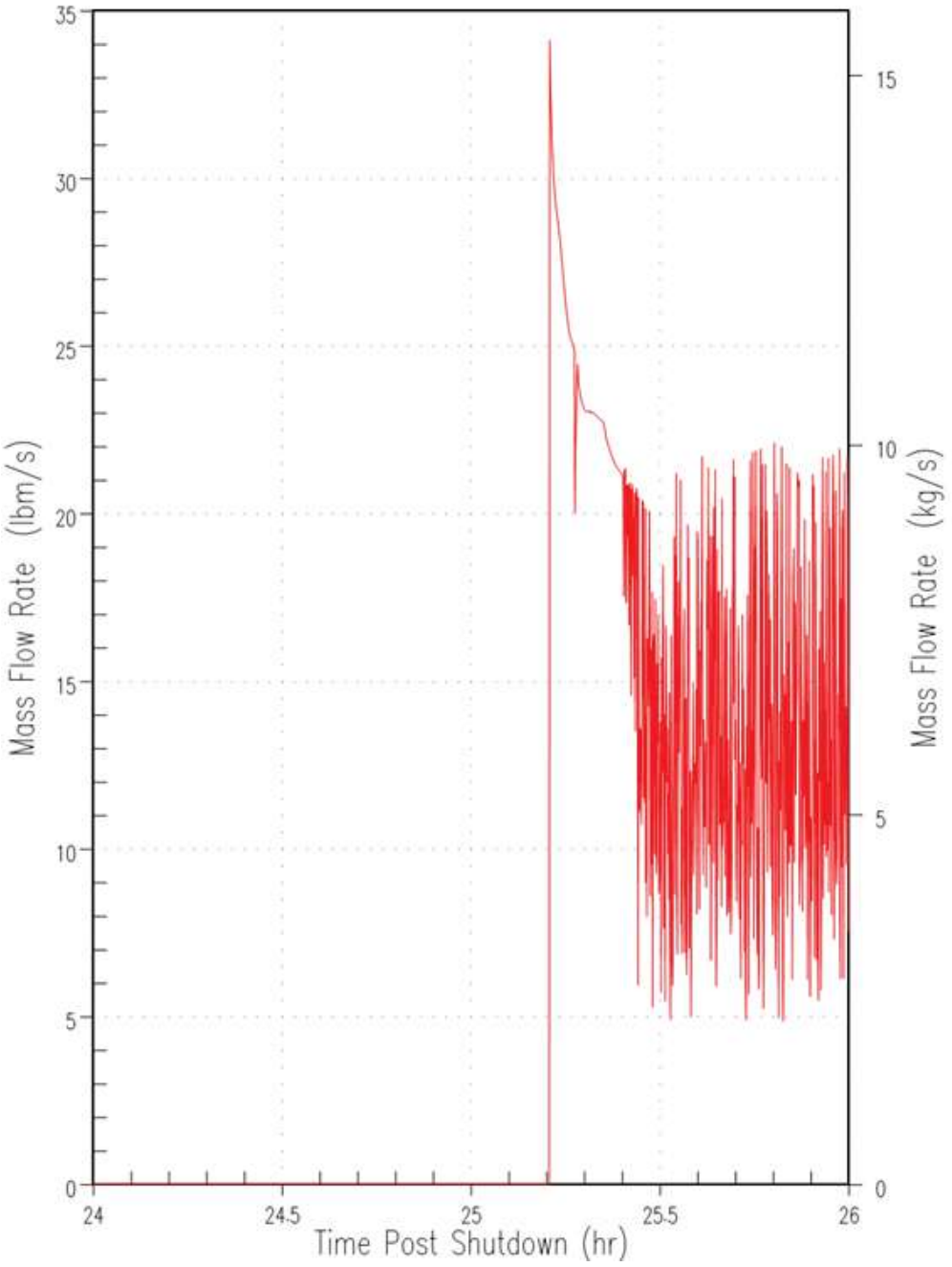


Figure 9.8.5-26. ADS Stage 4 Vapour Flow, Loss of RNS in Mode 5 with RCS Open

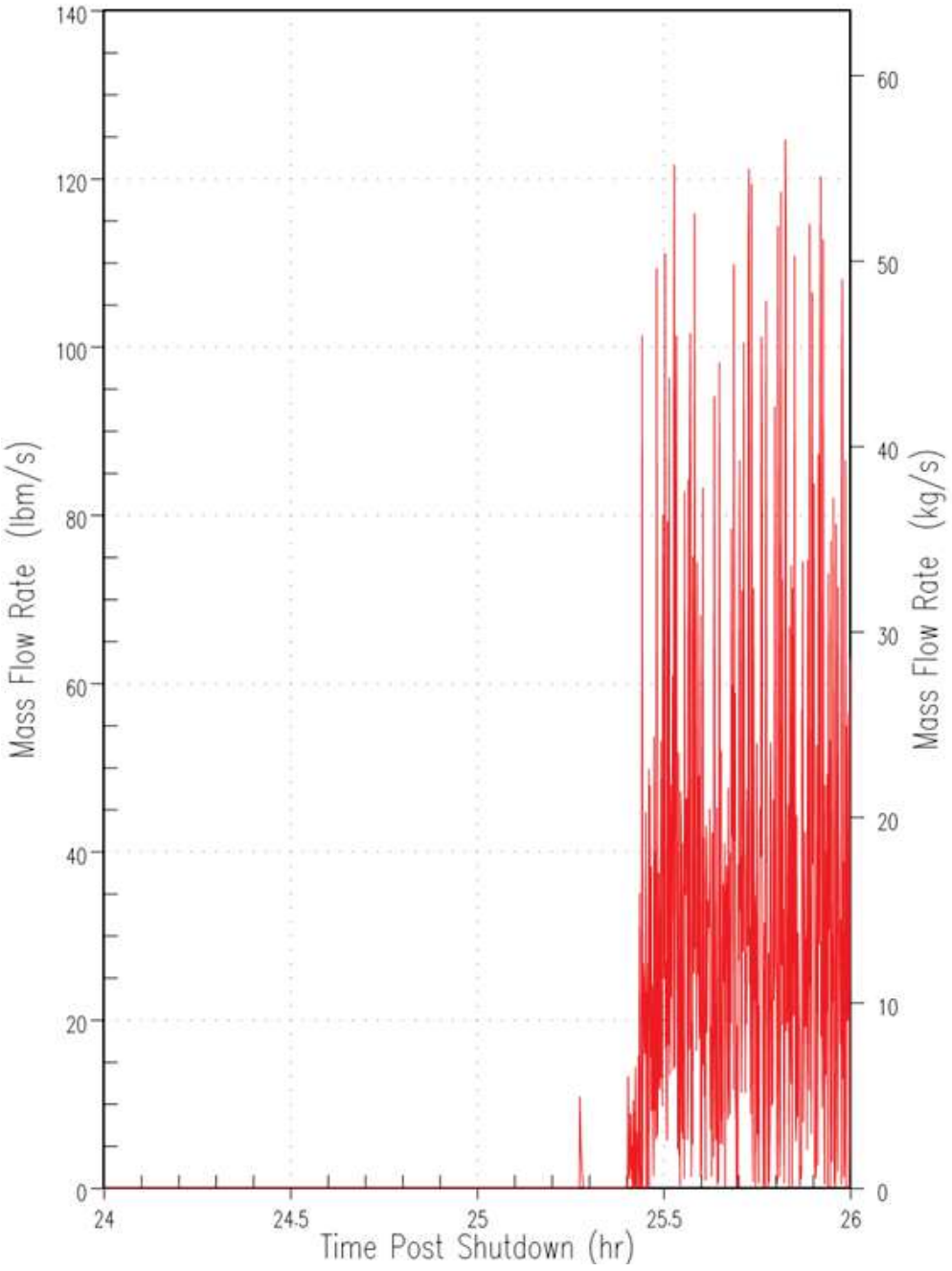


Figure 9.8.5-27. ADS Stage 4 Liquid Flow, Loss of RNS in Mode 5 with RCS Open

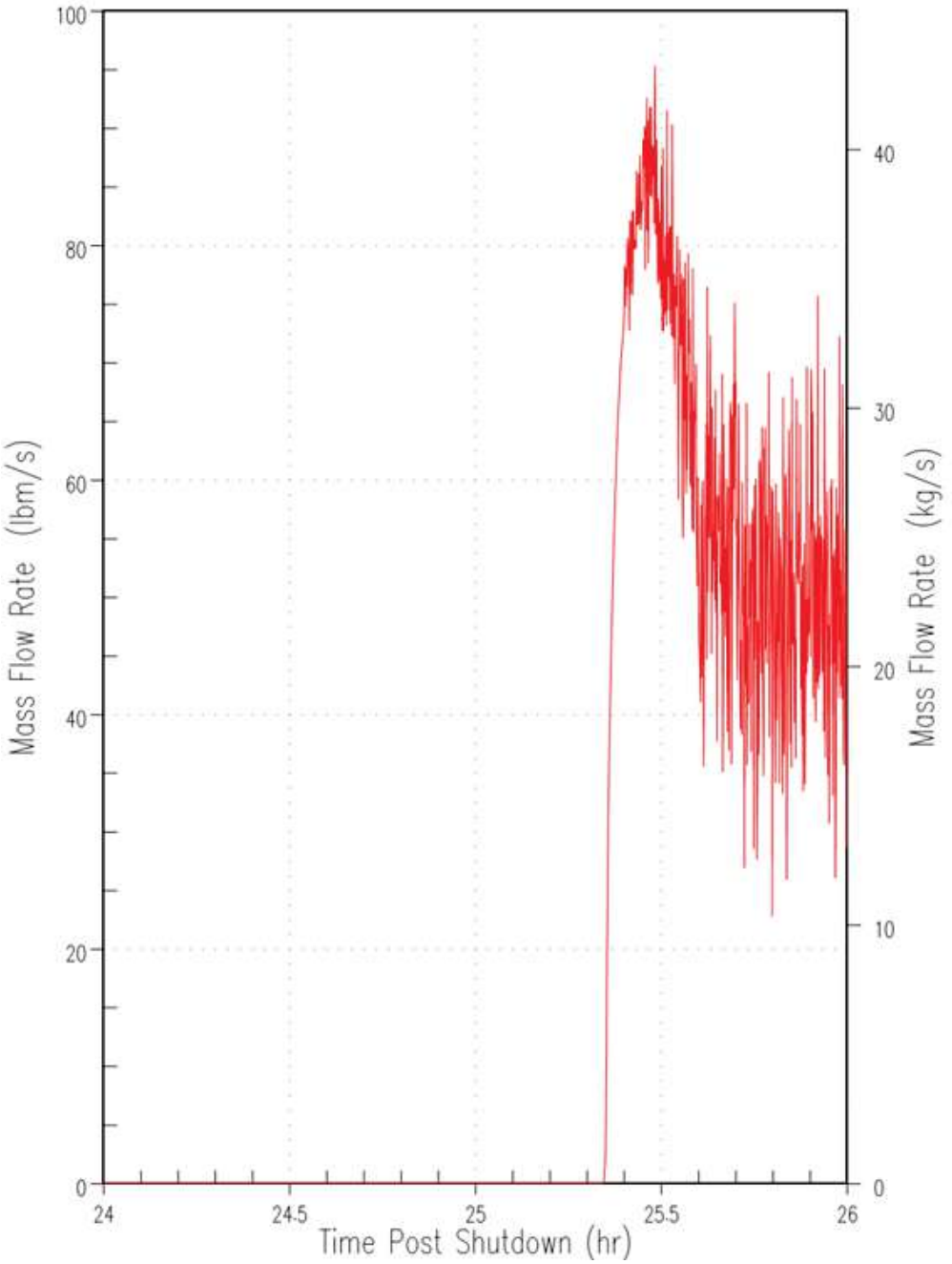


Figure 9.8.5-28. IRWST Injection Flow, Loss of RNS in Mode 5 with RCS Open

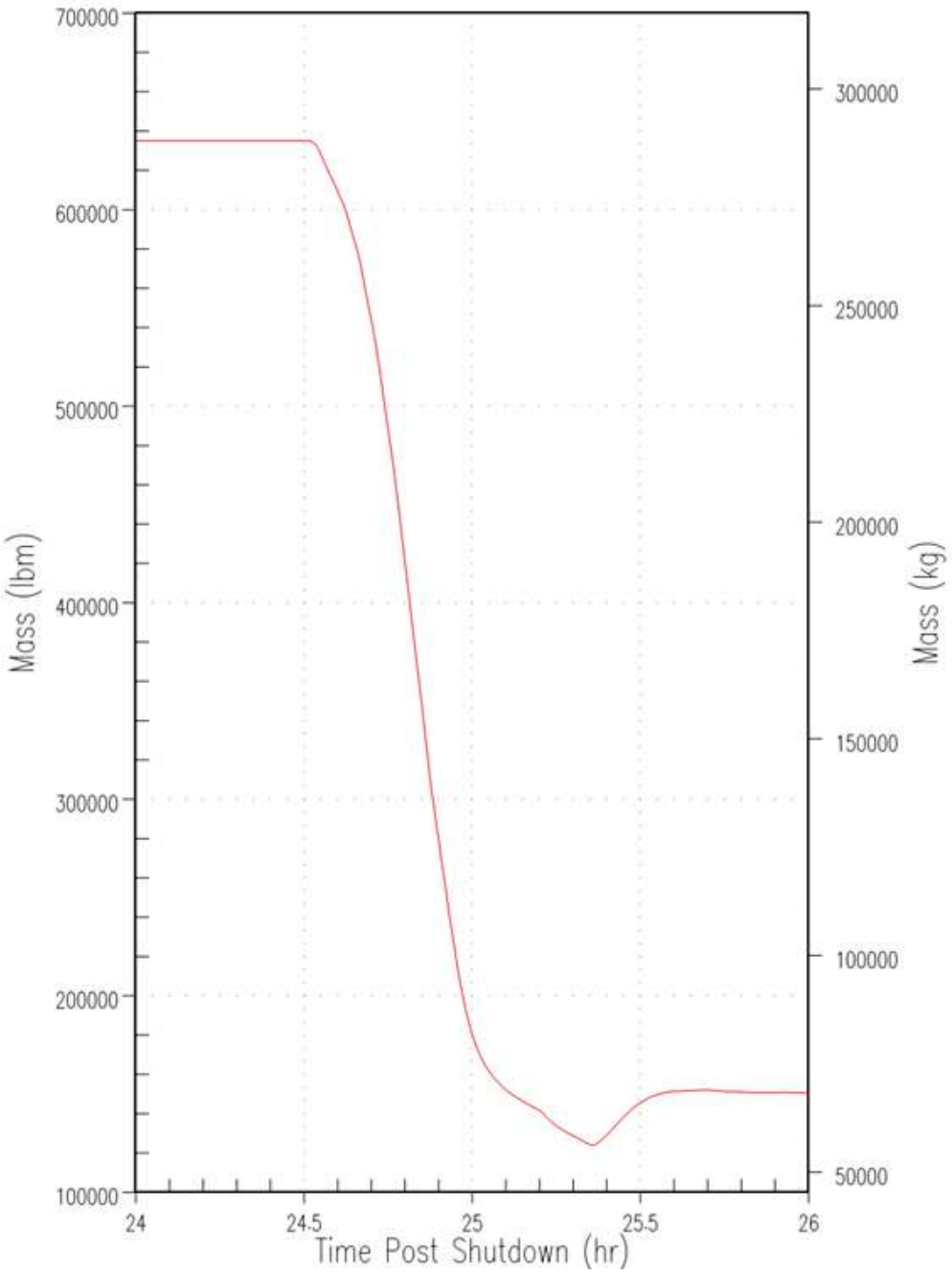


Figure 9.8.5-29. Primary Mass Inventory, Loss of RNS in Mode 5 with RCS Open

9.9 Dropped Loads

This section considers specific faults from dropped loads from lifting equipment such as cranes and hoists. The potential for dropped loads, both within the reactor containment and for other facilities on the site, is extensively considered in Chapter 11, Internal Hazards. A dropped load event is considered to be one that may directly cause harm or damage and consequently presents a threat to the fundamental safety functions. Chapter 11 discusses the safety aspects of the lifting equipment, load paths, and operation; and identifies any safety-significant items that could be damaged as a result of failure. This section considers specific fault sequences that require more detailed analysis, particularly with regard to radiological consequences.

Crane Faults Considered

The cranes used in the AP1000 plant facility are fixed as opposed to mobile cranes, which are commonly seen on construction sites. Therefore, because of the nature of cranes used in the AP1000 plant facility, faults associated with cranes and lifting equipment that are excluded from this study are: slewing (lateral movement of the crane's boom or jib), jibbing (moving the crane's lifting apparatus closer to/further from the working radius), swinging loads, and crane or hoist collapse.

9.9.0 Introduction and Overview of Faults

A number of faults were identified from the fault list. The faults fall into two groups:

- Drop of a fuel cask
  - Dropped fuel cask in loading bay (spent fuel). The loading bay is also known as the rail car bay in the auxiliary building
  - Dropped fuel cask in spent fuel storage pool (spent or new)
- Dropped fuel assembly onto other fuel
  - Damage to fuel assembly/core following drop of assembly on reactor core
  - Damage to fuel assembly (spent or new) resulting from drop in refuelling cavity
  - Dropped fuel assembly in spent fuel storage pool (spent or new)

A number of other faults were identified at hazard identification exercises (described in Chapter 8) but were screened out in the fault list (Appendix 8A). Additional fuel cask drops are examined in the dropped loads internal hazards section, see Section 11.8.

9.9.0.1 Drop of a Fuel Cask

Description

The identified faults can result in three potential outcomes: activity release, a threat to the structural integrity of the building fabric, and a threat to an SSC that could be damaged by a dropped load.

Fault 3.1.9 - dropped fuel cask in rail car bay, involves a fuel cask being dropped. If the containment of the fuel cask is damaged, a release of activity could result. This fault also has the potential to damage the building fabric or an SSC.

Fault 3.2.12 - dropped fuel cask in spent fuel storage pool (spent or new), is screened out because the cask handling crane is mechanically prevented from travelling over the SFP by use of a restricted length of crane rails (which support the crane). Therefore, the fault cannot occur.

Initiating Event Frequency[1]

The AP1000 design PSA does not give the IEF for the dropped fuel cask in rail car.

The dropped fuel cask in spent fuel storage pool cannot occur.

Design Basis Class

The event is in the DB0 class.

9.9.0.2 Dropped Fuel Assembly onto Other Fuel

Description

The identified faults can result in three potential outcomes: activity release, a threat to the structural integrity of the building fabric, and a threat to an SSC that could be damaged by a dropped load.

Fault 2.4.9 - damage to fuel assembly/core following drop of assembly on reactor core, involves a dropped load falling onto the reactor core, potentially causing a release of activity. This fault also has the potential to damage the building fabric or an SSC.

Faults 3.1.4 and 3.2.11 consider the movement of fuel under water. The fault scenario is that control of the movement of fuel underwater is lost and fuel is dropped and its cladding is damaged. This causes a release of activity into the water, some of which is then released into the air. This has the potential to give rise to an operator dose. Release of this activity through the facility's ventilation system could give rise to a public dose. All dropped loads are examined regarding the potential to damage the building fabric or an SSC from this fault scenario.

Initiating Event Frequency[1]

The AP1000 design PSA gives the IEF for the dropped fuel assembly faults as less than 1.0E-3/yr (Table 8A-2). Therefore this can be classified as an infrequent fault.

Design Basis Class

The unmitigated consequences of a dropped assembly are assumed to be less than the Target 4 BSL for frequent faults (1 mSv offsite and 20 mSv onsite). Given the IEF above, the event is in the DB0 class.

---

[1] As discussed in Chapter 8, the frequency for initiating events from the PSA is used in both Chapters 8 and 9 with the sole purpose of supporting the categorisation of the fault to a specific DB category. As noted in Chapter 8, these probabilities should not be considered to be representative of actual frequency of the events, and for several events they can be significantly conservative. Detailed PSA results and their basis are discussed in Chapter 10.

9.9.1 Dropped Fuel Cask in Rail Car Bay (Fault 3.1.9)

9.9.1.1 Identification of Causes and Accident Description

This fault considers the dropping of a fuel cask in the rail car bay in the auxiliary building. The fault could occur by a variety of initiators, such as operator error or failure of lifting equipment. It involves the movement of the cask both onto and from the train or a road vehicle.

The capacity of the cask handling crane (MHS-MH-02) is 136.1 tonnes (136 Mg).

The cask handling crane is designed to lower spent fuel casks through hatches at the 110.74 m (135'-3")[1] elevation down to a cask transporter located at the 100 m (100'-0") elevation. Therefore, the drop height is 10.74 m (35'-3"), excluding the clearance of the transporter base. No loss of spent fuel cask containment would take place for this drop, as the cask transport safety case (to be produced) will demonstrate the robustness of the cask to prevent a release of activity.

The device used to move fuel casks, the cask handling crane, is described as follows.

The cask handling crane lifts the spent fuel shipping cask from the cask transporter in the rail car bay, into the fuel handling area of the auxiliary building, places the cask in the cask washdown and cask loading pits, is used to remove and replace the cask lid, and lowers the loaded cask onto the cask transporter. The crane is designed to operate in the fuel handling area environmental conditions, and is typically used only when fuel movement activities associated with refuelling the reactor are not in progress.

Movements of the bridge, trolley, main, and auxiliary hoists can be controlled from a radio remote control or from a pendant suspended from the crane. Both the pendant and radio remote controls include a main power control switch. The crane is equipped with a keylock switch that inhibits control from the radio remote control and the pendant at the same time. Motion control push buttons on the radio remote control and on the pendant return to the OFF position when released.

9.9.1.2 Analysis of Effects and Consequences

A fuel cask can contain either new or spent fuel. The most onerous radiological consequences come from spent fuel, so this is considered as the bounding case for this fault.

There are two fault modes that may result from the dropping of a fuel cask: a release of activity from the loss of containment of the cask, and damage to the building fabric or to an SSC from the impact.

Loss of Cask Containment from a Dropped Fuel Cask

If a fuel cask is dropped, then it could become damaged and lose containment. However, there will be a transport safety case for the cask. This will need to consider the integrity of the cask when dropped from specific heights and orientations and onto appropriate surfaces. In short, the cask transport safety case will need to demonstrate that the cask can withstand such initiators when being transported on public roads and on the licencee's site. Therefore, it is assumed that the cask transport safety case is adequate to justify that the cask will not release

1. Note that the basis for all elevations is set to 100 feet in US design and 100 m in metric design.

its contents during reasonable fault conditions that may be experienced in the AP1000 plant facility. Consequently, this fault mode is not considered further.

Damage to the Building Fabric or to SSCs from the Impact of a Dropped Fuel Cask

This fault mode considers the damage that could be done by dropping a fuel cask onto the building fabric or onto an SSC. For the former, the building fabric will be designed to withstand a minimum dropped load, and it is assumed that the dropping of a fuel cask (with a known mass) from a known height in any orientation will not threaten the structural integrity of the building.

As the fuel cask is one of many objects that could be dropped, it is judged that evidence of substantiation of structural integrity will be attained by the normal design process. The AP1000 plant facility will be constructed to UK standards, and a designation is made as follows:

- **SSC** – Walls and floors
- **Safety function** – To maintain structural integrity following impact from a fuel cask when dropped from the cask handling crane

The latter consequence results in an SSC being damaged and failing to perform its function. Clearly, if the fuel cask fell onto a pump, then it is conceivable that the pump could be damaged. To provide confidence that no Categroy A or B safety function is interrupted by a dropped load, it is standard practice to analyse the load paths for any crane or lifting equipment. An evaluation of all SSCs under the hook coverage that could be affected by a dropped load is completed in Section 11.8.

9.9.1.3 Radiological Consequences

Dropping a fuel cask may jeopardise the operation of the train or road transport device used to move the casks into and out of the AP1000 plant facility, but this would cause operational difficulties rather than a radiological hazard.

The ability of the building structure to withstand a dropped fuel cask (as described above) is ensured by the engineering design (Chapter 16, Civil Engineering). Assuming that the building integrity is not damaged from a dropped fuel cask (as described above) and that no SSCs can be damaged by a dropped fuel cask, then there are no radiological consequences from this fault to operators or to members of the public.

9.9.1.4 As Low As Reasonably Practicable Assessment

Although the radiological consequences of this fault are deemed to be zero, it is still prudent to minimise the number of lifts of fuel casks. Elimination of dropped load hazards is highly challenging when using any lifting equipment. Human error may be a common initiating event, yet operators are needed to operate most lifting equipment, and the cranes and hoists in the AP1000 plant facility are no exception.

Substituting any of the proposed cranes or hoists for other engineered measures will not reduce risks involving human error, as operators are still required to operate the machinery.

Use of cranes and lifting equipment is subject to the Lifting Operations and Lifting Equipment Regulations 1998, Safe Use of Work Equipment Regulations 1998, and Provision and Use of Work Related Equipment Regulations 1998.

Other systems are also used by licencees to manage lifting hazards, such as permit to work and safe systems of work. These methods prompt operators to consider factors such as barriers and fencing involved with each lift. Lifting equipment is inspected, often daily, for crane and carrier systems. Maintenance will be carried out and equipment will be calibrated. Use of markings will be made on lifting equipment, such as the safe working load.

No further measures are practicable, and the risk is considered to be ALARP. As such, this fault is not considered further.

9.9.1.5 Conclusion

Damage to SSCs within the hook coverage of the cask crane has been evaluated in Section 11.8, and the risks have been reduced to be ALARP. The Category A safety functions of SSCs reviewed in Section 11.8 are maintained. Structural integrity of the building is also maintained. Radiological consequences of a dropped cask are evaluated by the site specific safety case for the chosen design of cask.

9.9.2 Dropped Fuel Assembly onto Other Fuel

9.9.2.1 Identification of Causes and Accident Description

This fault considers the dropping of fuel in water, either onto stored fuel or onto a reactor core. It considers three faults that were identified in the fault list (Appendix 8A): fault 2.4.9, damage to fuel assembly/core following drop of assembly on reactor core; fault 3.1.4, damage to fuel assembly (spent or new) resulting from drop in refuelling cavity; and fault 3.2.11, dropped fuel assembly in spent fuel storage pool.

9.9.2.1.1 Bounding Case

Of the three faults considered in this group, the highest radiological consequences are judged to involve the dropping of a fuel assembly onto fuel either in the reactor core (fault 2.4.9) or in the SFP (fault 3.2.11), as these locations contain the highest fuel inventory. Regarding fault 3.1.4, only a limited number of fuel assemblies are stored in the refuelling cavity at any one time, and they are afforded some protection by the storage racks.

Faults 2.4.9 and 3.2.11 are considered here to determine the appropriate bounding case.

- Fault 3.2.11, dropped fuel assembly in spent fuel storage pool

  The fuel handling machine is required to move new and irradiated fuel from the fuel storage racks in the auxiliary building fuel handling area to the fuel transfer system outside containment. The fuel handling machine is also designed so that during operation when handling irradiated fuel assemblies, there will always be an adequate depth of water to maintain sufficient shielding of personnel on the fuel handling machine gantry.

- Fault 2.4.9, damage to fuel assembly/core following drop of assembly on reactor core

  The function of the refuelling machine (RM) is to move new and spent fuel from the RV to the fuel transfer system in containment. It is also designed to maintain a minimum depth of water cover to act as shielding to protect operators on the RM gantry.

- Comparison of faults 3.2.11 and 2.4.9

Fuel movements involving the RM or the fuel handling machine are always carried out underwater in both cases. The following are considered in determining whether the radiological consequence of a fuel assembly dropped by the RM is bounded by a fuel assembly dropped by the fuel handling machine:

- The minimum depth of water cover when using the RM to move a fuel assembly is at least equal to that described when fuel assemblies are moved by the fuel handling machine.
- The maximum distance of a fuel assembly dropped by the RM is not greater than the maximum distance of a fuel assembly dropped by the fuel handling machine.
- The activity released by a fuel assembly dropped from the RM is not greater than the activity released from a fuel assembly dropped by the fuel handling machine.

The fuel assembly is lifted a predetermined height from the reactor core to still leave sufficient water covering the fuel assembly. The minimum depth of water cover required for normal fuel movement is 2.667 m (8.75 ft).

It is assumed that dropping any fuel assembly will not result in structural damage. Damage to SSCs within the load path is evaluated in Section 11.8 and is found to be within acceptable limits.

Fault 3.2.11 is considered to be the bounding case, and the assessment continues on this basis.

9.9.2.2 Analysis of Effects and Consequences

9.9.2.2.1 Fuel Handling Machine

Fuel assemblies are moved by the fuel handling machine.

The fuel handling machine is used to handle new fuel assemblies in the rail car bay, new fuel rack, and new fuel elevator. The capacity of the fuel handling machine, while over the new fuel storage rack, is limited to lifting a fuel assembly, control rod assembly, and handling tool. The new fuel storage rack is not accessed by the cask handling crane. This precludes the movement of loads greater than fuel components over stored new fuel assemblies.

The fuel handling machine traverses the spent fuel pool, the fuel transfer canal, the cask loading pit, the new fuel storage pit, and the rail car bay. It is used in the movement of both new and spent fuel assemblies. The fuel handling machine is used to transfer new fuel assemblies from the new fuel storage rack into the spent fuel pool. A new fuel elevator in the spent fuel pool lowers the new fuel to an elevation accessible by the fuel handling machine.

In the fuel handling area, fuel assemblies are moved about by the fuel handling machine. Initially, a short tool is used to handle new fuel assemblies and place them in the new fuel elevator. The new fuel elevator must be used to lower the assembly to a depth at which the fuel handling machine and a long handling tool can place the new fuel assemblies into or out of the new fuel elevator or the spent fuel storage racks.

The fuel handling machine performs fuel handling operations in the new and spent fuel handling area. It also provides a means of tool support and operator access for long tools used in various services and handling functions. The fuel handling machine is equipped with two 2-ton (2-Mg) hoists, one of which is single failure proof.

9.9.2.2.2 Structural Damage

Spent fuel is designed to be lifted a maximum height of 2.667 m (8.75 ft) above the fuel rack to maintain adequate water cover to shield operators.

The spent fuel hoist (one of two hoists on the fuel handling machine) is designed to prevent the lifting of fuel higher than 304.8 mm (12") above a fuel rack.

Reference 9.9-2, Section 2.8.5 examines three scenarios of a drop from a height of 914.4 mm (36 inches):

1. A drop of a fuel assembly with a control rod assembly plus a handling tool (conservatively modelled as a total mass of 1363.63 kg (3100 lb)) from 914.4 mm (36 inches) above the top of the spent fuel storage rack with subsequent impact on the edge of a cell

2. A drop of a fuel assembly with a control rod assembly plus a handling tool from 914.4 mm (36 inches) above the top of the rack down through an empty cell with impact on the rack baseplate away from the rack pedestal

3. A drop of a fuel assembly with a control rod assembly plus a handling tool from 914.4 mm (36 inches) above the top of the rack down through an empty cell with impact on the rack baseplate directly above the rack pedestal

For all three hypothetical drop scenarios, the results are, respectively:

1. The active fuel region remains surrounded by an undamaged cell wall.
2. Only the dropped fuel assembly is moved downward more than 51 mm (2 inches).
3. The postulated drop event will not breach the SFP floor liner.

Therefore, it is concluded that a dropped fuel assembly will not cause the spent fuel storage pool to lose containment. Therefore, this fault mode is not considered further.

9.9.2.2.3 Damage of Fuel Rod Cladding

This is discussed in “Radiological Consequences” below.

9.9.2.3 Radiological Consequences

A fuel assembly contains 264 fuel rods. If a fuel assembly is dropped, then it is pessimistic to assume that cladding on all the fuel rods are damaged enough to lose containment.

Operational evidence states that in fuel drop incidents from around the world, often no fuel rods are damaged (see Chapter 17 for details).

For the purposes of this fault assessment, it is assumed that two fuel rods have been damaged and that their cladding has released all the activity contained within the fuel gap (the space between the fuel matrix and the interior surface of the cladding).

Many factors are inputs into the dose assessment calculations (Reference 9.9-3), including the release fraction of material leaving the fuel matrix and entering the gap between the matrix and the internal surface of the cladding (the gap inventory) and the DF associated with the depth of water above the damaged fuel required by Technical Specifications.

One other pertinent factor is the decay period. The length of time used in this assessment could have been longer, which would have reduced the calculated doses. However, the period of 48 hours was used and is retained here as a practicable period of time to allow outage work to begin on the reactor without delaying operations.

The consequence assessment (Reference 9.9-3) states that the calculated doses are as follows:

Offsite dose: 0.26 mSv Worker dose: 1.21 mSv.

These doses are within the Target 4 BSL for frequent faults (1 mSv offsite and 20 mSv onsite).

9.9.2.3.1 Operator Dose Uptake

Fuel assemblies are generally moved during an outage (although fuel can be moved during all modes); each outage is expected to last approximately 2 to 3 weeks. In terms of whether a dropped fuel assembly is a revealed or unrevealed event, it is conceded that it is not as revealed as a drop of a fuel cask from a crane positioned at significant height. However, at least one operator involved with moving a fuel assembly will be expected to observe it while it is being moved (the person operating the lifting machinery or the banksman standing near the water's edge).

Outage tasks will involve suitable training and briefing of all relevant personnel. Regarding the movement of a fuel assembly, it is assumed that the person organising work (POW) will brief these relevant personnel at the beginning of each shift or day.

- **Operating instruction –** The POW will brief all personnel associated with tasks involving the movement of a fuel assembly at the beginning of each shift or day.

The POW will be the one individual who, if required, would communicate to the rest of the team when to instigate an evacuation procedure in the event of a dropped fuel assembly. This minimises confusion regarding who has responsibility for reporting the event, as the operator charged with moving the fuel assembly need only be concerned with telling the POW if the POW has not already noticed that the fuel assembly has dropped.

So, if a fuel assembly is dropped, it is assumed that the POW would realise it quickly and instruct operators to evacuate as follows:

- **Operating instruction –** In the event of a dropped or mishandled fuel assembly, personnel should evacuate immediately when told to do so by the POW.

In this event, activity has the potential to be released through the water of the spent fuel storage pool and into the operating area. Activity-in-air monitors and alarms will be in place to warn personnel to evacuate; these are described below.

Minimising Operator Dose Uptake from Airborne Activity

Activity-in-air monitors are designed to alert personnel in the event of airborne activity breaching a predetermined limit. Air exhausted from the auxiliary building, fuel handling area of the auxiliary building, and the annex building is monitored for high airborne activity. Means are provided to shut off supply air and divert exhaust air through high efficiency particulate air filters and charcoal adsorbers upon detection of high airborne activity. Alarms are provided in the main control room for these discharge flows.

The activity-in-air instrument (VAS-JE-RE001) can be used to alert operators of an abnormally high airborne concentration. The fuel handling area exhaust radiation monitor (VAS-JE-RE001) measures the concentration of radioactive materials in the exhaust air from the fuel handling area. This radiation monitor is located upstream of the exhaust air isolation damper. When a predetermined setpoint is exceeded, the fuel handling area exhaust radiation monitor provides signals to alarm in the main control room, to initiate closure of the fuel handling area supply and exhaust air isolation dampers, to open the fuel handling area exhaust air isolation damper to the containment air filtration exhaust units, and to start a containment air filtration exhaust unit. These actions provide a filtered air path from the fuel handling area to the plant vent. The fuel handling area exhaust radiation monitor is an inline monitor that uses a beta-sensitive scintillation detector. It is located with the sensitive volume inside the exhaust duct.

The activity-in-air instrument (fuel handling area exhaust radiation monitor VAS-JE-RE001) is able to alert operators to evacuate and reduce the risk of exposure from airborne contamination; on this basis, it is designated as follows:

- **SSC** – Fuel handling area exhaust radiation monitor (activity-in-air monitor VAS-JE-RE001)

- **Safety function** – To minimise operator exposure to airborne activity, Category B, Class 2

In order to ensure that the consequences of a dropped fuel assembly are <20 mSv to the operator (as detailed below), a safety instruction is raised to ensure that personnel start to evacuate within 1 minute:

- **Safety instruction** – In the event of a dropped or mishandled fuel assembly, personnel should evacuate the fuel handling area within 1 minute.

Table 9.9-4 summarises the SSCs from this fault assessment.

Table 9.9-5 provides the operator actions relevant to this fault assessment.

Table 9.9-6 provides the LCOs related to the dose assessment for this fault.

9.9.2.4 As Low As Reasonably Practicable Assessment

As the assessment of the consequences and frequency are in the DB0 category, there is no formal requirement to designate any safety measures. However, the requirement to carry out an ALARP assessment still holds.

First, the operator dose calculation assumes that the operator will begin to evacuate the area within 1 minute. It is expected that an operator would leave much more quickly than this, thereby reducing dose uptake. One minute has been used to determine the DB dose. Shorter times would be more appropriate in the probabilistic assessment.

Second, there are a number of features of the refuelling machine that have not been formally claimed in the above assessment. The following design intentions are provided, although these are not claimed in the above assessment:

- The RM can only place a fuel assembly in the core, in the in-containment storage rack, or in the fuel transfer system.

- When the RM gripper is engaged, the machine cannot traverse unless the fuel assembly bottom nozzle is clear of the lower core plate alignment pins.

- When the RM gripper is disengaged, the machine cannot traverse unless the gripper is withdrawn into the mast.

- Simultaneous traversing and hoisting operations are prevented.

- The fuel gripper is monitored by devices to confirm operation to the fully engaged or fully disengaged position. Alarms are actuated if both engage and disengage switches are actuated at the same time, or if neither is actuated.

- Lowering of the gripper is not permitted if slack cable exists in the hoist.

- The gripper tube is prevented from lowering completely out of the mast.

- Before the fuel gripper can release a fuel assembly, the fuel gripper must be in its down position in the core, in-containment storage rack, or fuel transfer system.

- The weight of the fuel assembly must be off the gripper before the fuel gripper can release a fuel assembly.

- The RM hoist is prevented from moving in the transfer machine zone unless the up-ender is vertical. An interlock is provided from the fuel transfer system to the RM to accomplish this.

As Low As Reasonably Practicable Discussion – Operator Dose

No further measures are practicable and the risk to operators is considered to be ALARP.

As Low As Reasonably Practicable Discussion – Public Dose

Technology is available to reduce the public dose from this fault mode by way of capturing the nuclides that enter the ventilation system. HEPA filters and charcoal adsorbers are capable of capturing nuclides to reduce activity released to the atmosphere.

The main contributor to dose uptake is I-131 (Reference 9.9-3). A charcoal filter can retain I-131 for approximately 6 weeks (Reference 9.9-1, Datasheet 5.2), by which time the activity will reduce to insignificant levels (Reference 9.9-1, Datasheet 5.2). (I-131 half-life is approximately 8 days (Reference 9.9-3).)

The subsystem of the VAS that serves the fuel handling area is equipped with HEPA filtration, which provides protection to members of the public; on this basis, the HEPA filters in the VAS are claimed in order to reduce risk to members of the public. A designation is made on this basis:

- **SSC** – HEPA filters and charcoal adsorbers in the VAS

- **Safety function** – To minimise dose uptake to members of the public. Category B, Class 2

A DF of 1E4 is possible with charcoal filters (Reference 9.9-1, Datasheet 5.2). Even if the charcoal filtration units were underperforming, a DF of 10 is still possible because of bypassing and leakage (Reference 9.9-1, datasheet 5.2).

No further measures are practicable and the risk to members of the public is considered to be ALARP. As such, this fault is not considered further.

9.9.2.5 Conclusion

Radiological consequences are within the Target 4 BSL for frequent faults (1 mSv offsite and 20 mSv onsite), and the risks have been reduced to be ALARP.

9.9.3 References

9.9-1 Sellafield Ltd. "Safety & Risk Management Technical Guide," Release Fraction Database v5.0, January 2010.

9.9-2 Westinghouse Report APP-GW-GLR-033, Rev. 5, "Spent Fuel Storage Racks Structural/Seismic Analysis," November 2014.

9.9-3 PGEN/E.004067/02/18/091, Rev. 2, "Calculation of Operator and Public Dose for Dropped Loads in the AP1000 PWR," July 2010.

Tables 9.9-1 through 9.9-3 Not Used.

Table 9.9-4. SSCs for 9.9.0.2 Dropped Fuel Assembly onto Other Fuel

Safety Function	Provision	SSCs	Classification
To minimise operator exposure to airborne activity.	Primary means	Fuel handling area exhaust radiation monitor (activity-in-air monitor VAS-JE-RE001).	2
To reduce dose uptake to members of the public.	Primary means	HEPA filters and charcoal adsorbers in the VAS.	2

Table 9.9-5. Operator Actions Related to Dropped Fuel Assembly onto Other Fuel

Operator Action	Class
The person organising work will brief all personnel associated with tasks involving the movement of a fuel assembly at the beginning of each shift or day.	2
In the event of a dropped or mishandled fuel assembly, personnel should evacuate immediately when told to do so by the person organising work.	2
In the event of a dropped or mishandled fuel assembly, personnel should evacuate the fuel handling area within one minute.	2

Table 9.9-6. LCOs for Dropped Fuel Assembly onto Other Fuel

Limit or Condition	Technical Specification Identification and Notes
Spent Fuel Pool Water Level	3.7.5 The spent fuel pool water level shall be ≥ 7.0 m (23 ft) above the top of irradiated fuel assemblies seated in the storage racks.
Refuelling Cavity Water Level	3.9.3 Refueling Cavity Water Level shall be maintained ≥ 7.0 m (23 ft) above the top of the reactor vessel flange.
Refuelling Machine	The minimum depth of water between the top of a fuel assembly and the surface of the water is not to be less than 2.667m (8.75 ft) when fuel assemblies are moved by the Refuelling Machine.

9.10 Operator Exposure Faults

A hazard identification exercise was undertaken as part of the development of the AP1000 design PCSR GDA step 4 (See Chapter 8). This process identified a number of hazards that have the potential to be a hazard to the operator and members of the public. The pre-construction safety case for the operation of the AP1000 reactor must address non-reactor faults (i.e., faults that are unrelated to the reactor but that may still occur within the facility). This section covers faults that result in operators being exposed to radiation during reactor startup, maintenance, refuelling, and spent fuel storage.

Faults Considered

Operators may be exposed to radiation from non-reactor faults in a variety of ways, from direct exposure to inhalation or ingestion of contamination. These faults are mainly associated with operations during refuelling within the fuel storage pool or flooded refuelling cavity, or from general use of sources of radiation within the controlled areas.

9.10.0 Introduction and Overview of Faults

A total of 13 faults were identified at hazard identification exercises (See Chapter 8); subsequently, nine of them (3.1.7, 3.2.15, 3.2.16, 3.3.1, 3.3.2, 3.4.9, 3.4.10, 3.6.4, and 3.6.5) were screened out in the fault list with the reasons presented in Table 9.10-1.

The remaining four faults, identified below, are grouped into two fault modes: dose uptake by the operator through falling into the pool or cavity water, and dose because of working in an area of increased activity.

Fault ID	Description
3.1.5	Operator falls into flooded refuelling cavity
3.1.6	Water level fall in refuelling cavity (shielding lost)
3.2.13	Operator falls into spent fuel storage pool
3.2.14	Water level fall in spent fuel storage pool (shielding lost)

For faults 3.1.5 and 3.2.13, the operator falls into the storage pool or refuelling cavity (when flooded), resulting in the operators receiving a direct dose from the fuel and any activity dissolved in the water plus an ingestion dose from swallowing pool water.

For faults 3.1.6 and 3.2.14, the water level falls in the storage pool or refuelling cavity, resulting in an increased direct dose to operators.

9.10.1 Operator Falls into Flooded Refuelling Cavity or Fuel Storage Pool (Faults 3.1.5 and 3.2.13)

9.10.1.1 Identification of Causes and Accident Description

Removal of spent fuel from the reactor and transfer operations to the fuel storage pool are performed under borated water to provide radiation protection and maintain subcriticality. During these operations, operators are required to work around and above the fuel storage pool and the flooded refuelling cavity. This fault considers the potential consequences of an operator falling into the pool or flooded cavity during refuelling operations.

The minimum allowable water depths above active fuel in a fuel assembly during fuel handling are 2.667 m (8.75 ft) in the reactor cavity and 2.667 m (8.75 ft) in the fuel transfer canal and spent fuel pool. This limits the dose to personnel on the spent fuel pool handling machine to less than 0.025 mSv/hr for an assembly in a vertical position. The minimum water depth above the stored assemblies is about 7.92 m (26 ft), and for this depth the dose rate at the pool surface is small.

The spent fuel pool cooling system clarification capability is sufficient to permit necessary operations that must be conducted in the spent fuel pool area. The spent fuel pool cooling system is designed to perform its purification function in accordance with the following additional criterion:

- The spent fuel pool cooling system is designed to limit exposure rates to personnel on the spent fuel pool fuel handling machine to less than 0.025 mSv/hr. This corresponds to an activity level in the water of approximately 185 Bq/g (0.005 μCi/g) for the dominant gamma-emitting isotopes at the time of refuelling.

The concentration of tritium in the SFP water is maintained at less than 18.5 kBq/g (0.57 μCi/g).

Initiating Event Frequency

An IEF is not assigned to this fault. The estimated dose is minimal, and hence a probabilistic assessment is not required (see Section 9.10.1.3).

Design Basis Class

The consequences of an operator falling into the flooded refuelling cavity or fuel storage pool are calculated to be 0.091 mSv worker dose and nothing to members of the public (see Section 9.10.1.3). These doses are less than the Target 4 basic safety objectives (BSOs) of 0.1 mSv for the workers and 0.01 mSv for the public.

There is no requirement for a DB0 fault assessment, but an ALARP assessment is provided in Section 9.10.1.4.

Bounding Case

An operator could fall into the pool when there are no fuel movements, for example, during maintenance activities of fuel handling equipment (i.e., when all spent fuel is stored with more than 7.9 m (26 ft) of water as a shield). This scenario is deemed to correspond to a situation where there is an insignificant dose rate at the pool surface, and therefore is not bounding.

The most onerous, and therefore bounding, radiological consequence is considered to occur if an operator falls into the pool during spent fuel movements, i.e., with a covering depth of water of approximately 2.667 m (8.75 ft) over a single raised high burnup fuel element.

9.10.1.2 Analysis of Effects and Consequences

Should an operator fall into the pool during fuel movements, it is assumed that the time spent under the water is minimal, but that the operator remains on the surface of the water for 5 minutes in close proximity to the fuel handling machine and swallows up to 50 ml (50 g) of pool water before being recovered. (Note that when the pool contains fuel, the water will be

acidic and borated, and therefore, unlike clean fresh water, it will be obvious to the operator that pool water has entered the mouth.)

9.10.1.3 Radiological Consequences

It is assumed that there is no newly failed fuel within the pool at the time of the accident and that the dominant isotope in the pool water is Co-60, as the other significant isotope, I-131, has a relatively short half-life of approximately 8 days. The dominant dose uptake will be from direct gamma radiation and ingestion of pool water.

The worst-case dose rate at the pool surface during spent fuel movement is 0.25 mSv/hr, which, for a 5-minute exposure at the surface, would equate to a whole body dose of 0.021 mSv.

It is assumed that approximately 50 ml (i.e., 50 g) of pool water is ingested containing 18.5 kBq/g (0.57 μCi/g) tritium (H-3) and 185 Bq/g (0.005 μCi/g) of the dominant gamma isotope, Co-60. Reference 9.10-2 shows that the committed effective dose equivalents (CEDEs) for ingestion are as follows:

- CEDE for Co-60 is 3.4E-9 Sv/Bq
- CEDE for H-3 is 4.2E-11 Sv/Bq

Therefore, for a 50-g ingestion, the Co-60 dose is 3.4E-9 Sv/Bq × 185 Bq/g × 50g = 0.000031 Sv or 0.031 mSv

For a 50-g ingestion, the H-3 dose is 4.2E-11 Sv/Bq × 1.85E4 Bq/g × 50 g = 0.000039 Sv or 0.039 mSv

Therefore, the total dose assuming the operator remains at the pool surface = (0.021+0.031+0.039) mSv = 0.091 mSv

9.10.1.4 As Low As Reasonably Practicable Assessment

Although the radiological consequences of this fault are deemed to be very low, it is still required that the potential for an operator to fall into the fuel storage pool or flooded refuelling cavity is minimised. This is especially the case for this particular scenario, as the most severe consequence for an operator from falling into water is a fatality as a result of drowning.

Therefore, where there is a requirement for operators to work near or over the storage pool or flooded cavity, the risks, where practicable, should be minimised. This will primarily be achieved by the adoption of standard building and industrial practices. For example, the edge of the pool and cavity is protected by walls and/or the use of handrails. Egress ladders should be provided at points around the pool and any requirement to work on access platforms (e.g., for fuel handling over the water), especially over water, will require suitable railings. If work is required outside these barriered areas, then the utility must provide harnesses, and operators must use them.

Within the area of the storage pool and flooded refuelling cavity, lifebuoys and equipment suitable for retrieving a person in the water, such as suitable egress ladders, shepherd's hooks, and poles, should be provided.

Therefore, considering the recommendations above, the radiological risks to an operator from falling into the storage pool or flooded refuelling cavity are ALARP.

9.10.1.5 Conclusion

Radiological consequences are within the Target 4 BSOs (0.01 mSv offsite and 0.1 mSv onsite), and the risks have been reduced to be ALARP.

Operator actions relevant to this fault assessment are provided in Table 9.10-2

LCOs related to the dose assessment for this fault are provided in Table 9.10-3

9.10.2 Water Level Fall in the Refuelling Cavity or Storage Pool (Faults 3.1.6 and 3.2.14)

9.10.2.1 Identification of Causes and Accident Description

Removal of spent fuel from the reactor and transfer operations to the fuel storage pool are performed under borated water to provide radiation protection and maintain subcriticality. During these operations, operators are required to work around and above the fuel storage pool and the flooded refuelling cavity. This fault considers the potential consequences of a significant fall in the water level in the flooded refuelling cavity or storage pool during these operations.

The minimum allowable water depths above active fuel in a fuel assembly during fuel handling are 2.667 m (8.75 ft) in the reactor cavity and 2.667 m (8.75 ft) in the fuel transfer canal and spent fuel pool. This limits the dose to personnel on the spent fuel pool handling machine to less than 0.025 mSv/hr for an assembly in a vertical position. The minimum water depth above the stored assemblies is about 7.92 m (26 ft), and for this depth the dose rate at the pool surface is small.

The connections from the spent fuel pool cooling system to the pool are such that leakage in the spent fuel pool cooling system will not result in the pool water level falling to unacceptable levels.

Connections to the spent fuel pool are made at an elevation to preclude the possibility of inadvertently draining the water in the pool to an unacceptable level.

The spent fuel pool cooling system is connected to the spent fuel pool at two locations. The two suction lines connect to the spent fuel pool at an elevation 6 feet (1.83 m) below the operating deck. Each line has a skimmer connection to take suction from the water surface of the spent fuel pool. This suction arrangement prevents the spent fuel pool from inadvertently being drained below a level that would prevent the water in the spent fuel pool from performing its safety related function.

The water level in the storage pool is maintained within strict limits above the top of the active fuel when stored correctly within the fuel racks:

- Maximum level (high alarm) – 8.14 m (26.7 ft)
- Minimum level (low alarm) – 7.97 m (26.1 ft)
- Lowest level (low-low alarm) – 7.33 m (24 ft)

In the unlikely event of an extended loss of normal spent fuel pool cooling, the water level will drop. Low spent fuel pool level alarms in the control room will indicate to the operator the need to initiate makeup water to the pool.

The minimum volume in the passive containment cooling water storage tank for spent fuel pool makeup is 2864.42 m^3 (756,700 US gallons).

Initiating Event Frequency

An IEF is not assigned to this fault. The estimated dose is negligible, and hence a probabilistic assessment is not required (see Section 9.10.2.3).

Design Basis Class

The direct radiological consequences of a fall in the water level in the refuelling cavity or storage pool to workers are minimal and to members of the public are negligible (see Section 9.10.2.3). These doses are significantly less than the Target 4 BSOs of 0.1 mSv for the workers and 0.01 mSv for the public.

There is no requirement for a DB0 fault assessment, but an ALARP assessment is provided in Section 9.10.2.4.

Bounding Case

The loss of pool water has much more significant consequences than local operator dose from, for example, loss of or reduced fuel cooling. However, there are two general ways in which the pool (or cavity) water level could reduce: over an extended period of time because of inadequate management of water levels as a result of low rate leaks or evaporation, or quickly as a result of a seismic event causing failure of pool cooling water pipework.

For the purpose of this assessment, it is considered that a reduction of water level over an extended period of time would be identified (level alarms, routine monitoring, and general observation by operators) and easily corrected by topping up the pool water. Therefore, the most significant fault would be the rapid loss of water from the pool while operators are working adjacent to or over the pool.

9.10.2.2 Analysis of Effects and Consequences

The rapid loss of pool water could occur as a result of a failure of pipework, such as the pool cooling circuit, resulting from, for example, a seismic event. However, even a significant event, such as failure of cooling system pipework, would not cause an instant lowering of the pool level, as this would occur over many minutes or even hours. Therefore, with the provision of seismically qualified level alarms to AP1000 plant Class C seismic Category I as well as operator awareness (especially for a seismic event,) and the large volume of pool makeup water available in the passive containment cooling water storage, it is unlikely that any DB event could lead to a significant direct radiation dose to the operators.

In the event of a sudden loss of pool water or a seismic event, the operators would be expected to place any raised spent fuel assembly in a safe location and leave the storage pool or containment area within a few minutes.

9.10.2.3 Radiological Consequences

During defueling and refuelling operations, operators could be located over the storage pool or cavity. However, it is considered that the radiological consequences will be insignificant, as the operators would place any raised spent fuel assembly in a safe location and leave the area within a few minutes of an uncontrolled lowering of the water level, and it is inconceivable that any fuel could become uncovered because connections to the SFP are made at an elevation to preclude the possibility of inadvertently draining the water in the pool to an unacceptable level.

Outside refuelling or fuel transfer operations, the fuel is stored in the pool with a normal minimum-covering depth of water of 7.92 m (26 ft) that corresponds to an insignificant dose at the pool surface. The loss of 1.83 m (6 ft) of water from the pool would not lead to a significant increase in dose rates from fuel stored in the racks and would certainly result in an alarm to the control room and action taken to top up the pool, exclude operators from the area, or a combination of these actions.

It is considered inconceivable that a member of the public would receive any dose from this fault.

9.10.2.4 As Low As Reasonably Practicable Assessment

Although the probability of significant radiological consequences of this fault are deemed to be very low and are within the BSO, it is still required that the potential for an operator to receive a dose from this potential accident is minimised.

The fuel storage pool has level alarms set at a minimum level of 7.92 m (26 ft) and at a lowest level (the low-low alarm) of 7.33 m (24 ft) above the top of the active fuel. Low SFP level alarms in the control room will indicate to the operator the need to initiate makeup water to the pool. These level instruments in the SFP are seismically qualified.

Therefore, the risks to an operator from direct radiation as a result of the water level falling in the storage pool or flooded refuelling cavity are ALARP.

9.10.2.5 Conclusions

Radiological consequences are within the Target 4 BSOs (0.01 mSv offsite and 0.1 mSv onsite), and the risks have been reduced to be ALARP.

Operator actions relevant to this fault assessment are provided in Table 9.10-4.

LCOs related to the dose assessment for this fault are provided in Table 9.10-5.

9.10.3 References

9.10-1 ICRP Publication 72, “Age-dependent Doses to Members of the Public from Intake of Radionuclides: Part 5 Compilation of Ingestion and Inhalation Dose Coefficients,” Annals of the ICRP, Volume 25, No. 3-4, 1996.

Table 9.10-1. Screened-out Faults

Fault No.	Fault Description	Description – Screened Out
3.1.7 and 3.2.15	Over-raising fuel in refuelling cavity; storage pool	The lift height of the RM mast and fuel handling machine hoist(s) is limited such that the minimum required depth of water shielding is maintained. The RM and fuel handling machine will be tested by attempting to raise a dummy fuel assembly with success if the bottom of the dummy fuel assembly cannot be raised to within 7.47 m (24.5 ft) of the operating deck.
3.2.16	Exposure in areas contaminated by pool water	Pool water is cleaned by the pool water cooling plant. Normal contamination levels are limited to 185 Bq/g (0.005 μCi/g) gamma emitting isotopes and 18.5 kBq/g (0.57 μCi/g) tritium. These levels of contamination in the form of a puddle of spilled water would give very low dose rates, and areas where spills could occur would be routinely monitored by health physics and be easily cleaned.
3.3.1 and 3.4.9	Unauthorised operator entry into active areas/areas of high dose	The Combined Licence applicant will address the administrative controls for use of the design features provided to control access to radiologically restricted areas, including potentially very high radiation areas, such as the fuel transfer tube during refuelling operations and the reactor cavity. Based on actual operating plant data, ingress or egress of plant operating personnel to radiologically restricted areas will be controlled and monitored.
3.3.2	Inappropriate handling or use of other sources	There are no significant neutron or radioactive sources outside the reactor fuel. All other radioactive sources required for use on the station, such as X-ray machines for radiography or test sources for radiation monitoring equipment, will be subject to controls as required by the ionising radiation regulations. All such radiation sources would be held and used only under the local control of health physics.
3.4.10	Failure to adequately control chemistry to manage dose rates (approach to be decided)	Management of water chemistry will be a routine task. Operators required to work in potentially active areas will be subject to monitoring and control access (see faults 3.22 and 3.32).
3.6.4	Operator exposure from stored waste because of inadequate shielding or waste consignment error	Shielding is provided as necessary for the waste storage areas in the radwaste building to meet the radiation zone and access requirements. Temporary partitions and shield walls will be provided, as required, to supplement the permanent shield walls surrounding the waste accumulation and packaged waste storage rooms inside the radwaste building. Health physics will control the monitoring of radwaste consignments.
3.6.5	Operator exposure from incorrect consignment of waste because of assessment, clerical, or sampling errors	All radwaste packaged and accumulated by an AP1000 reactor unit will be transferred for disposal. The AP1000 plant has no provisions for permanent storage of radwaste. Packaging will be done in accordance with local and national requirements. Health physics will control the monitoring of radwaste consignments.

Table 9.10-2. Operator Actions for Section 9.10.4

Operator Action	Class
(None)	N/A
ALARP recommendation	2
1. Consider providing safety harnesses for operators working outside barriered areas over deep water.	2
2. Consider providing lifebuoys and equipment suitable for retrieving a person from the water, e.g., egress ladders.	2

Table 9.10-3. LCOs for Section 9.10.4

Limit or Condition	Technical Specification Identification and Notes
Fuel storage pool water gamma activity	Maximum activity level in the water of 185 Bq/g (0.005 μCi/g) for the dominant gamma-emitting isotopes at the time of refuelling.
Fuel storage pool water tritium	Maximum concentration of tritium in the SFP water maintained at less than 18.5 kBq/g (0.57 μCi/g).
Fuel storage pool water levels	Maximum (high-level alarm) 8.14 m (26.7 ft); minimum (low-level alarm) 7.97 m (26.1 ft).

Table 9.10-4. Operator Actions for Section 9.10.5

Operator Action	Class
Maintain water level in the fuel pool between 7.97 m (26.1 ft) and 8.14 m (26.7 ft) and initiate makeup water to the pool if the SFP low-level alarm actuates in the control room.	2

Table 9.10-5. LCOs for Section 9.10.5

Limit or Condition	Technical Specification identification and Notes
Fuel handling	Minimum allowable water depths above active fuel in a fuel assembly during fuel handling are 2.667 m (8.75 ft) in the reactor cavity and 2.667 m (8.75 ft) in the fuel transfer canal and SFP. (This limits the dose to personnel on the SFP handling machine to less than 0.025 mSv/hr for an assembly in a vertical position.)

9.11 Safety Assessment of Heating, Ventilation, and Air Conditioning Faults

9.11.1 Introduction

The hazard identification exercise undertaken as part of the development of the AP1000 plant PCSR GDA step 4 (as discussed in Chapter 8 of this PCSR) identified a number of faults relating to the use of the HVAC systems that have the potential to present a hazard to the operator and members of the public.

9.11.2 Normal Operations

The systems that serve the various building and structures of the plant in terms of air conditioning, cooling and ventilation comprise the following:

- Nonradioactive ventilation system (VBS)
- Annex/auxiliary building nonradioactive HVAC system (VXS)
- Diesel generator building heating and ventilation system (VZS)
- Containment recirculation cooling system (VCS)
- Turbine building ventilation system (VTS)
- Health physics and hot machine shop HVAC system (VHS)
- Radiologically controlled ventilation system (VAS)
- Containment air filtration system (VFS)
- Radwaste building HVAC system (VRS)

Figure 9.11-1 is a schematic diagram illustrating aerial release vents from the AP1000 plant and their associated monitors.

The ventilation systems serving the following structures are considered to be potentially radioactive and hence are considered in this assessment:

- Containment building (served by the VFS)
- Annex / Auxiliary building (served by the VAS)
- Fuel handling area of auxiliary building (served by the VAS)
- Radwaste building (served by the VRS)
- Health physics and hot machine shop (served by the VHS)

The MCR is considered to be a nonradioactive area. Other structures contain insignificant sources of airborne radioactivity and are not addressed any further in this assessment.

9.11.2.1 Ventilation Subsystems

Health Physics and Hot Machine Shop Heating, Ventilation, and Air Conditioning System

The VHS supply air system serves one annex building stairwell, the personnel decontamination area, frisking and monitoring facilities, containment access corridor, and health physics facilities of the hot machine shop; and provides radiation monitoring of the exhaust prior to release to the environment.

In addition it also provides:

- Conditioned air to work areas to maintain acceptable temperatures for equipment and personnel working in those areas

- Air movement from clean to potentially contaminated areas to minimise the spread of airborne contamination
- An exhaust route from the welding booths, grinders, and other miscellaneous equipment in the hot machine shop
- Radiation monitoring of exhaust air prior to release to the environment
- HEPA filtration of the exhaust to prevent release of particulate activity or transport of contamination
- Negative pressure to the access control area and hot machine shop with respect to the outside environment and the clean areas of the annex building to prevent unmonitored releases of radioactive contaminants
- Humidity at a minimum of 35 percent

The hot machine shop provides a dedicated workshop/location within the controlled area for repair and refurbishment of items of equipment from within the controlled area (they may not actually be contaminated or activated). Operations in the hot machine shop are conventional hands-on work (i.e., there is no provision for remote handling).

The exhaust ducts have isolation dampers that close to protect the areas served by the VHS system from radiation inleakage when the VHS system is off.

In the event that a high amount of radiation is detected in the exhaust air flow, the VHS exhaust air is diverted to the VFS system.

A further description of the VHS is given in Chapter 23.

Radwaste Building Heating, Ventilation, and Air Conditioning System

The VRS serves the radwaste building and provides radiation monitoring of exhaust prior to release to the environment. The VRS also serves the clean electrical/mechanical equipment room and the potentially contaminated HVAC equipment room, the packaged waste storage room, the waste accumulation room, and the mobile system facility.

The VRS is a once-through ventilation system that consists of the radwaste building supply air system and the radwaste building exhaust system. The radwaste building exhaust system has HEPA-filtered exhaust to prevent release of activity or transport of contamination.

These subsystems operate in conjunction with each other to maintain temperatures in the areas served, while controlling airflow paths and building negative pressure. This system is discussed in more depth in Chapter 23.

Radiologically Controlled Area Ventilation System

The VAS serves the fuel handling area of the auxiliary building and the radiologically controlled portions of the auxiliary and annex buildings, with the exception of areas served by the VHS. It consists of two subsystems: the auxiliary/annex building ventilation system and the fuel handling area ventilation subsystem. These subsystems are discussed in more depth in Chapter 23.

The fuel handling area ventilation subsystem and exhaust ductwork is arranged to exhaust the SFP area separately from the auxiliary building. It provides directional airflow from the rail car/bay filter storage area into the spent resin equipment rooms. The exhaust fans discharge filtered air into the plant vent for monitoring of offsite airborne gaseous and other radiological releases. Routine releases for the fuel handling area are low. The potential for accidental release is low; however, if radiation monitors detect a high level of radiation, the fuel handling exhaust is diverted to the VFS, which contains HEPA and charcoal filters.

The auxiliary building and annex building exhaust air ductwork is routed to minimise the spread of airborne contamination. The supply airflow is directed from the low-radiation access areas into the radioactive equipment and piping rooms that have a greater potential for airborne contamination. The exhaust ducts have isolation dampers that close to isolate the auxiliary and annex building from the outside environment when high airborne activity is detected in the exhaust air duct. The dampers are also configured so that two building zones can be independently isolated. A radiation monitor is located in the duct for each zone.

Each subsystem functions to:

- Provide ventilation to maintain the occupied areas and access and equipment areas within design temperature range.
- Provide outside air for plant and personnel and prevent the unmonitored release of airborne radioactivity to the atmosphere or adjacent plant areas.
- Isolate automatically selected building areas by closing the supply and exhaust duct isolation dampers.
- Start the VFS when high airborne radioactivity in the exhaust air duct or high ambient pressure differential is detected.

The VAS overall airflow direction is from areas of lower potential airborne contamination to areas of higher potential contamination. The VAS operates at a slightly negative pressure to prevent the uncontrolled release of airborne radioactivity to the atmosphere or adjacent clean plant area.

The fuel handling area ventilation subsystem has passive HEPA-filtered exhaust to prevent release of activity or transport of contamination.

Containment Air Filtration System

The VFS provides intermittent flow of outdoor air to purge and filter the containment atmosphere of airborne radioactivity during normal plant operation, and continuous flow during hot or cold plant shutdown conditions to reduce airborne radioactivity levels for personnel access. The VFS also provides filtered exhaust for the VAS and VHS during abnormal conditions.

The VFS is controlled by the PLS except for the containment isolation valves, which are controlled by the PMS and DAS. It preserves the containment integrity (by isolation of the VFS lines penetrating containment); and provides the intermittent flow of outdoor air to purge the containment atmosphere during normal plant operations, and continuous flow during hot or cold plant shutdown conditions.

The VFS serves the containment, fuel handling area, and the other radiologically controlled areas of the auxiliary and annex buildings.

The VFS purges the containment by providing fresh air from outside and exhausting air to plant vents. The VFS exhausts areas served by the VAS and VHS after receipt of a high-radiation signal in the VAS or the VHS exhaust, respectively. The air exhausted by the VFS is filtered sequentially by high efficiency filters, charcoal filters, and post-filters.

The VFS comprises two parallel systems that may be operated individually or simultaneously as required by the operating regime, with or without associated inlet air handling units (AHUs). Each system is equipped with HEPA filtration and charcoal filters for the removal of particulate and iodine vapour, respectively. A high-efficiency filter is installed before the HEPA filter to increase operational life and reduce the quantity of low-level waste (LLW).

The exhaust air filtration units are located within the radiologically controlled area of the annex building. The units are connected to a ducted system (with isolation dampers) and provide HEPA filtration and charcoal adsorption of exhaust air from containment, the fuel handling area, and the radiological controlled areas of the auxiliary and annex buildings. A gaseous radiation monitor (located downstream of the exhaust air filtration units in the common ductwork) provides an alarm if abnormal gaseous releases are detected.

9.11.3 Overview of Faults

The safety case for operation of the AP1000 reactor includes non-reactor faults (i.e., faults that are unrelated to the reactor but that still occur within the facility). These non-reactor faults include HVAC faults.

9.11.4 Analysis of Faults

Nine faults were identified and are extracted from the fault list (Appendix 8A):

Fault No.	Fault
3.5.1	Failure of HVAC filter leading to a potential external release of radioactivity
3.5.2	Blockage of HVAC filter leading to an increase in air radioactivity level in the affected working area
3.5.3	Failure of HVAC fans leading to an increase in air radioactivity level in the affected working area
3.5.4	Failure of HVAC dampers leading to an increase in air radioactivity level in the affected working area
3.5.5	Leakage leading to an increase in air radioactivity level in the affected working area
3.5.6	Fire resulting in the release of trapped activity from filters involved in the fire leading to an increase in air radioactivity level in the affected working area and a potential external release of radioactivity
3.5.7	Dropped filters during handling (filter exchange, transfer to or processing in radwaste building) leading to an increase in air radioactivity level in the affected working area
3.5.8	Failure of gaseous radwaste system (WGS) beds, leading to a potential release of

radioactive gas

3.5.9 Failure of stack monitoring system, leading to an inability to monitor routine discharges

Fault 3.5.9 was identified at the hazard identification exercise (described in Appendix 8A), but was screened out during the exercise as an operability issue in the fault list that did not result in any abnormal discharges (Appendix 8A).

Fault 3.5.5 was identified at the hazard identification exercise (described in Appendix 8A) and was screened out. The HEPA filter banks are designed with replaceable cells that are clamped in place against compression seals. Normal operations dictate that when the filters are replaced, they are pressure-tested to ensure that they are seated in the housing correctly and can maintain pressure. The pressure differential across a filter bank is used as an indication of correct installation. Pressure indication and high differential pressure alarms are provided for filters in the AHUs and room coolers. These alarms will sound if the filters are incorrectly installed, and thus alert operators to a fault. In addition, the filter housing is designed and tested to be airtight with bulkhead-type doors that are closed against compression seals, and thus any leak would stay within the filter house.

9.11.5 Fault Groups

From analysis of the faults listed above, similar faults can be bounded into groups. For brevity, it has been decided to create three groups: the first will consider filter failures in the HVAC system (Faults 3.5.1, 3.5.6, and 3.5.8); the second will consider dropped HVAC filters during handling (Fault 3.5.7); and the third will consider reduced airflow in the HVAC system because of failure of the HVAC fans and dampers, and blockage of HVAC fans (Faults 3.5.2, 3.5.3, and 3.5.4).

Therefore, this assessment considers the following three groups:

1. Failure of filters in HVAC system
2. Dropped filters
3. Reduced airflow

9.11.6 Failure of Filters in the Heating, Ventilation, and Air Conditioning System (Faults 3.5.1, 3.5.6, and 3.5.8)

9.11.6.1 Fault Group Description

This fault considers the failure of a filter in the HVAC systems. The fault could occur by a variety of initiators, including operator error causing damage during installation or change procedures, or by a filter fire caused by a burning particle drawn into the exhaust system. The worse-case scenario would be if the filters in the VFS were to ignite as they were filtering all the unfiltered vents from several areas of the plant, and hence would be likely to contain the most activity.

This fault group also considers fires in the charcoal guard and delay beds. The radioactive gases removed from the RCS at the WLS vacuum degasifier are directed through the gas cooler, moisture separator, charcoal guard bed, and two charcoal delay beds. The effluent is then discharged via the plant vent. The radwaste assessment (Section 9.12) identifies the possibility of a fire in the radwaste system as being very low. Additionally, the inventory of

the charcoal guard and delay beds is purely noble gases and as such, there will be no inhalation dose if they catch fire. From further examination of a potential fire in the charcoal guard and delay beds, it is concluded that this fault is bounded by the filter fire fault and so it is not discussed any further.

9.11.6.2 Initiating Event Frequency

An IEF is not assigned to this fault. The estimated dose is minimal and hence a probabilistic assessment is not required (see Section 9.11.6.6).

9.11.6.3 Design Basis Class

The consequences from a release of the inventory from an HVAC filter resulting from a fire are calculated to be 2.05E-5 mSv for members of the public and 6.38E-4 mSv for worker dose (Reference 9.11-1), which is significantly less than the Target 4 BSOs of 0.01 mSv for the public and 0.1 mSv for the workers.

There are no requirements for a DB0 fault assessment, but an ALARP assessment should be considered.

9.11.6.4 Bounding Fault

For filter failure, the bounding fault would be a filter fire leading to the release of the inventory of the filters in the VFS.

9.11.6.5 Design Basis Fault Progression and Assessment

Filters could potentially be ignited by a burning particle drawn into the exhaust system. However, there is no mechanism for a fire to start spontaneously in a filter, so there has to be a fire somewhere else, either in the filter housing itself or somewhere else connected by ventilation ducting.

The potential for a fire in the filter housing is controlled by good housekeeping procedures, ensuring that there is a lack of combustible material stored in or near the filter housing. Normal good housekeeping procedures will ensure that any combustible waste is placed in robust containers (fire-resistant if appropriate) and the contents are emptied on a regular basis (see Section 11.2). In addition, early detection and warning of fire will be provided by the automatic fire detection and alarm system (AFD). The AFD is provided throughout the AP1000 plant and will be designed, installed, and commissioned in accordance with appropriate standards. The AFD provides audible and visual alarms, as well as system trouble annunciation in both the MCR and the security central alarm station, and thus will alert operators to a fire in a ventilation system. Operators will be able to investigate and control a fire in the filter housing in accordance with firefighting procedures (see Section 11.2).

The fire damper design used in the VFS does not require any external power source or actuation signals. Actuation is achieved by heat from the air in the duct melting the fusible link and a spring mechanism closing the damper. This provides a high degree of inherent safety and high reliability. There is extensive experience with operating these types of dampers to give confidence that, if they are adequately maintained, they will not seize or jam and will move to the closed position when the temperature rises above a specified point (see Section 23.3).

Differential pressure indication and high differential pressure alarms are provided for filters in the AHUs and room coolers. Pressure differential indication and alarms are provided via

instruments (VAS-030, VAS-032, VAS-033, and VAS-034) to control the negative pressure in the radiologically controlled areas of the auxiliary and annex buildings. A filter fire would result in a loss of pressure and hence the alarms would sound, thereby alerting operators to a potential problem with the filters. Assuming that activity is released during the fire, activity-in-air monitors would alert personnel in the event of airborne activity breaching a predetermined limit.

Therefore, either the filter will not be affected by a fire or any release will be mitigated by the operation of the fire dampers, differential pressure indication alarms, and activity-in-air alarms.

9.11.6.6 Radiological Consequences

A calculation has been performed to determine the doses to the public and to the workers (Reference 9.11-1). This calculation assumes the contact dose rate on a filter to be 1 mSv/hr. This is significantly greater than what would be expected for normal filter change operations: filters would normally be monitored to ensure that they do not exceed contact dose rates for LLW and may also be changed at a predetermined pressure drop or age, well before significant activity levels are reached.

A dose rate of 1 mSv/hr equates to an inventory of 1E8 Bq (2.70E3 μCi) Cs-134 and 4E7 Bq (1.08E3 μCi) Cs-137 based on the primary coolant nuclide activities. The consequences are calculated to be 2.05E-5 mSv for members of the public and 6.38E-4 mSv for worker dose (Reference 9.11-1), which is significantly less than the Target 4 BSOs of 0.01 mSv for the public and 0.1 mSv for the workers; therefore, no further discussion is required.

9.11.6.7 As Low As Reasonably Practicable Assessment

The general design of the ventilation system is to have enough duct length to ensure that a burning particle has extinguished before it reaches the filters. In addition, in-situ ventilation spark arresters will prevent a burning particle from reaching the filters. There will also be fire dampers at each fire barrier the duct crosses between the fire compartment and the filter. These are rated the same as the barrier (generally 2 or 3 hours); so as long as they operate, the filter will be protected.

Passive FPSs are used to protect ventilation ductwork from the effects of fire. A 3-hour fire-rated ventilation ductwork enclosure/shaft is used to segregate the VXS and VFS from one another as they enter and leave the Lower South Air Handling Equipment Room in the annex building.

The plant vent radiation monitor measures the concentration of radioactive airborne contamination being released through the plant vent. The plant vent is a post-accident monitor and is sampled continuously for the full range of concentrations between normal conditions and those postulated. Alarms are provided in the MCR if radioactivity concentrations exceed predetermined setpoints. The plant vent radiation monitor also provides data for plant effluent release reports.

No further measures are practicable and the risk is considered to be ALARP.

9.11.6.8 Conclusions

Radiological consequences are within the Target 4 BSOs (0.01 mSv offsite and 0.1 mSv onsite), and the risks have been reduced to be ALARP.

Operator actions relevant to this fault assessment are provided in Table 9.11-1.

LCOs related to the dose assessment for this fault are provided in Table 9.11-2.

9.11.7 Dropped Filters (Fault 3.5.7)

9.11.7.1 Fault Group Description

This fault considers the consequences of a dropped filter during an outage for maintenance purposes.

9.11.7.2 Initiating Event Frequency

An IEF is not assigned to this fault. The estimated dose is minimal and hence a probabilistic assessment is not required (see Section 9.11.7.5).

9.11.7.3 Design Basis Class

Reference 9.11-1 calculates the worker and public consequences from the release of the inventory of an HVAC filter to be 1.3E-4 mSv to the worker and 4.1E-6 mSv to members of the public, which is significantly less than the Target 4 BSOs of 0.01 mSv for the public and 0.1 mSv for the workers.

There are no further requirements for a DB0 fault assessment, but an ALARP assessment should be considered.

9.11.7.4 Design Basis Fault Progression and Assessment

If a filter is dropped, it could become damaged and release activity into the local area and potentially result in a public dose. The loading of the filters and adsorbers with radioactive material during normal plant operation is a slow process. In addition to monitoring for pressure drop, the filters are checked for radioactivity on a scheduled maintenance basis with portable equipment. The filter elements are replaced before the radioactivity level is of sufficient magnitude to create a personnel hazard. In the case of excessive radioactivity caused by a postulated accident, the filter is replaced before normal personnel access is resumed. It is not necessary for workers to handle filter units immediately after a DB accident, so exposure can be minimised by allowing the short-lived isotopes to decay before changing the filter.

Access to ventilation systems in potentially radioactive areas can result in operator exposure during maintenance, inspection, and testing. Equipment locations are selected to minimise personnel exposure. The outside air supply units and building exhaust system components are located on the roof of the Auxiliary Building. These areas are accessible to the operators. Work space is provided around each unit for anticipated maintenance, testing, and inspection.

Radioactive filters from ventilation exhaust filtration units are bagged and transported to the radwaste building, where they are temporarily stored. The filters may be compacted along with other dry radioactive wastes. It is noted that compaction is outside the scope of this assessment.

It is expected that mobile handling equipment will be used to move filters if the radioactivity readings make it ALARP to do so. It is also assumed that if a filter is dropped, the POW will instigate the evacuation procedure of all personnel in the affected area:

- **Operating Instruction -** In the event of a dropped filter, the POW must instigate the evacuation procedure.

The dropping of a filter under the circumstances described above is classified as a revealed event.

9.11.7.5 Radiological Consequences

A calculation of dose has been performed in Reference 9.11-1. This assumes an initial inventory of 1E8 Bq (2.70E3 μCi) Cs-134 and 4E7 (1.08E3 μCi) Bq Cs-137 based on a 1-mSv/hr contact dose rate and the primary coolant nuclide activities. The consequences are calculated to be 1.3E-4 mSv to a worker and 4.1E-6 mSv to a member of the public, which are significantly less than the Target 4 BSOs of 0.1 mSv for the public and 0.01 mSv for the workers.

9.11.7.6 As Low As Reasonably Practicable Assessment

Under normal operations, the HVAC filters are monitored to ensure that they do not exceed the allowable dose limits for contact handleable LLW.

It is assumed that a standard safe change bagging procedure is used to change the filters and that the filters will be changed at least once every 5 years.

It is assumed that operators performing filter change operations will be wearing appropriate personal protective equipment (PPE). Respirators are able to offer a minimum DF of 40 (Reference 9.11-2). The PPE requirements will be determined by the health physics team at the time of use and therefore are not designated here.

Other assumptions that will reduce the risk associated with this fault are that suitable training and briefing of infrequent procedures (such as moving filters) will be carried out.

No further measures are practicable and the risk is considered to be ALARP.

9.11.7.7 Conclusions

Radiological consequences are within the Target 4 BSOs (0.01 mSv offsite and 0.1 mSv onsite), and the risks have been reduced to be ALARP.

Operator actions relevant to this fault assessment are provided in Table 9.11-3.

LCOs related to the dose assessment for this fault are provided in Table 9.11-4.

9.11.8 Reduced Airflow (Faults 3.5.2, 3.5.3, and 3.5.4)

9.11.8.1 Fault Group Description

This fault considers a reduction in airflow in the HVAC system. The fault could occur by a variety of initiators, such as an operator error causing dampers to be closed, filters becoming blocked, or fans failing. These faults could potentially result in an increased operator dose.

9.11.8.2 Initiating Event Frequency

An IEF is not assigned to this fault. The estimated dose is minimal and hence a probabilistic assessment is not required (see Section 9.11.8.4).

9.11.8.3 Design Basis Fault Progression and Assessment

This fault considers the failure of dampers and fans and partial blockage of filters. Partial failure of a filter is bounded by a failure of the filters (as discussed in Section 9.11.6), and so a partial blockage in a filter will not be considered any further in this section, as it would only result in a reduced flow rate. This section will only consider the failure of dampers and fans. It is considered that failure of fans and dampers in the VFS would present the worst case.

Fan Failure

Operation of the supply and exhaust fans ensures that a suitable airflow can be achieved through the containment purge operations to reduce radiation levels in the containment environment. The exhaust fans provide a filtered exhaust route from the fuel handling area, auxiliary building, or annex building, maintaining a negative pressure differential relative to the surrounding areas. The supply and exhaust fans operate in response to signals from the PLS (see Section 23.3 of this PCSR). They are manually operated for containment purge functions, so a fault with the fans would be revealed during containment purge. The exhaust fans respond automatically to signals that include high/low pressure differential in the fuel handling area, auxiliary area, or annex building; and high radiation in these areas.

Conceivable failure modes for this type of fan include items such as failed bearings or a failed drive belt. These types of mechanical failures are avoidable with appropriate maintenance and can be readily detected and rectified. There is extensive experience in operating these types of fans (designed and constructed to similar standards) to give confidence that, if they are adequately maintained, they will have a good reliability in service and will be able to meet their safety requirements.

Failure of the exhaust fans when demanded to exhaust from the fuel handling area, auxiliary, or annex buildings may prevent the maintenance of a pressure differential in those areas and lead to an unmonitored release of air to the operational environment or surrounding areas. The exhaust fans also function to maintain a negative pressure differential in the fuel handling area, auxiliary or annex building areas served by the VAS following detection of high radiation. This prevents an unmonitored release of air to the environment and surrounding areas. In doing this, the fans control the level of radioactivity released to the working environment.

Two exhaust fans are installed; only one fan is required to meet the demand, however, and will start and operate to exhaust air from the fuel handling area, auxiliary, or annex building areas following detection of high radiation by the VAS (see Section 23.3).

The air exhausted by the VFS is filtered sequentially with high-efficiency filters, charcoal filters, and post filters. The VFS also exhausts areas served by the VAS and VHS after receipt of a high-radiation signal in the VAS or the VHS exhaust, respectively. Therefore, any dose to the public is bounded by failure of a filter as discussed in Section 9.11.6; as such, no further assessment is required.

Failure of Dampers

If high airborne activity is detected in the exhaust air from the auxiliary or annex buildings, the supply and exhaust duct isolation dampers automatically close to isolate the affected area from the outside environment. The VFS mitigates the resuspension of unfiltered airborne activity by maintaining the isolated zone at a slightly negative pressure with respect to the outside environment and adjacent unaffected plant areas.

If high airborne activity is detected in the exhaust air from the health physics and hot machine shop areas, the supply and exhaust duct shutoff dampers automatically close to isolate the affected areas from the outside environment. The VFS mitigates the resuspension of unfiltered airborne activity by maintaining the isolated zone at a slightly negative pressure with respect to the outside environment and adjacent unaffected plant areas.

The auxiliary/annex building subsystem remains in operation at a reduced capacity if either the auxiliary or annex building is not isolated. A disruption in the normal ventilation airflow rate that causes a high differential with respect to the outside environment causes the same automatic actuations. The VFS maintains negative pressure with respect to the outside environment until operation of the auxiliary building/annex building subsystem is restored.

If high airborne radioactivity is detected in the exhaust air from the fuel handling area, the supply and exhaust duct dampers automatically close to isolate the fuel handling area from the outside environment. The VFS mitigates resuspension of unfiltered airborne activity by maintaining the isolated zone at a slightly negative pressure differential with respect to the outside environment and adjacent unaffected plant areas. A disruption in the normal ventilation airflow rate that causes a high pressure differential with respect to the outside environment causes the same automatic actuations. The VFS maintains a slightly negative pressure differential with respect to the outside environment until operation of the fuel handling area ventilation subsystem is restored.

The isolation and shutoff dampers operate in response to signals from the PLS (Section 23.3).

The dampers are manufactured to appropriate industrial or nuclear standards to ensure a high reliability. Balancing dampers are set during commissioning and are not required to actuate during operation. In general, active dampers are located in redundant supply/exhaust lines such that failure of a damper will not prevent the VFS from performing its safety function. It is considered that the likelihood of coincidental failure of an isolation damper and the occurrence of an event leading to a release of activity in a working area is very low. As such, no further assessment is required.

9.11.8.4 Radiological Consequences

Section 9.11.6 calculates the failure of filters in the HVAC system. The consequences for the failure of fans will be bounded by this calculation, and hence will be significantly less than the Target 4 BSOs of 0.1 mSv for the public and 0.01 mSv for the workers. Therefore, no further discussion is required (see Section 9.11.6.6).

9.11.8.5 As Low As Reasonably Practicable Assessment

Redundant fans are provided in the design to further reduce the risk of a total failure of the VFS exhaust from the fuel handling area, auxiliary, or annex building areas (see Section 9.11.8.6).

Maintenance will be performed in line with the manufacturer's information. There is extensive experience in operating these types of fans (designed and constructed to similar standards) to give confidence that, if adequately maintained, they will have good reliability in service and be able to meet their safety requirements.

Radioactivity indication and alarms are provided to inform the MCR operators of gaseous radioactivity concentrations in the exhaust ducts from the fuel handling area and the radiologically controlled areas of the auxiliary and annex buildings. These local alarms would alert workers to increased activity in the area and prompt an evacuation.

Activity-in-air monitors are designed to alert personnel in the event of airborne activity breaching a predetermined limit.

Air exhausted from the auxiliary building, fuel handling area of the auxiliary building, and the annex building is monitored for high airborne activity. Means are provided to shut off supply air and divert exhaust air through high efficiency particulate air filters and charcoal adsorbers upon detection of high airborne activity. Alarms are provided in the main control room for these discharge flows.

The activity-in-air instrument (VAS-JE-RE001) can be used to alert operators of an abnormally high airborne concentration in the fuel handling area. This is an example of one of the activity-in-air instruments and additional airborne monitors are located in the auxiliary building and annex building (VAS-JE-RE002 and 003).

The fuel handling area exhaust radiation monitor (VAS-JE-RE001) measures the concentration of radioactive materials in the exhaust air from the fuel handling area. This radiation monitor is located upstream of the exhaust air isolation damper.

The fuel handling area exhaust radiation monitor is an inline monitor that uses a beta-sensitive scintillation detector. It is located with the sensitive volume inside the exhaust duct.

The activity-in-air instrument (fuel handling area exhaust radiation monitor (VAS-JE-RE001)) can alert operators to evacuate and reduce the risk of exposure from airborne activity; on this basis, it is designated as follows:

- **SSC** – fuel handling area exhaust radiation monitor (activity-in-air monitor VAS-JE-RE001)
- **Safety function** – to minimise operator exposure to airborne activity

No further measures are practicable and the risk is considered to be ALARP.

9.11.8.6 Summary of Safety Designations

Radiological consequences are within the Target 4 BSOs (0.01 mSv offsite and 0.1 mSv onsite), and the risks have been reduced to be ALARP.

Table 9.11-5 summarises the SSCs from this fault assessment.

Operator actions relevant to this fault assessment is provided in Table 9.11-6

LCOs related to the dose assessment for this fault is provided in Table 9.11-7.

9.11.9 References

9.11-1 Serco Report PGEN/E.004067/02/18/092, Rev. 2, Public and Worker Dose Calculation for Fire/Dropped HVAC Filter in the AP1000 PWR, March 2011.

9.11-2 ISBN 978 0 7176 2904 6 HSG53, 3rd Edition "Respiratory Protective Equipment at Work – A Practical Guide," HSE, 2005.

Table 9.11-1. Operator Actions Relevant for Section 9.11.6

Operator Action	Class
(None)	

Table 9.11-2. LCOs Related to the Dose Assessment for Section 9.11.6

Limit or Condition	Technical Specifications Identification and Notes
HVAC system	Filters are to be monitored to ensure that they do not exceed the allowable dose rate limits for contact handleable LLW.

Table 9.11-3. Operator Actions Relevant for Section 9.11.7

Operator Action	Class
In the event of a dropped HVAC filter, the POW must initiate the evacuation procedure.	2

Table 9.11-4. LCOs Related to the Dose Assessment for Section 9.11.7

Limit or Condition	Technical Specifications Identification and Notes
HVAC system	Filters are to be monitored to ensure that they do not exceed the allowable dose rate limits for contact handleable LLW.

Table 9.11-5. SSCs Used in Section 9.11.8

Safety Function	Provision	SSCs	Classification
To minimise operator exposure to airborne activity	Primary means	Fuel Handling Area Exhaust Radiation Monitor (activity-in-air monitor VAS-JE-RE001). Auxiliary Building Exhaust Radiation Monitor (VAS-JE-RE002) Annex Building Exhaust Radiation Monitor (VAS-JE-RE003)	2
To maintain negative pressure differential to control levels of radioactivity released to the environment	Primary means	Containment Exhaust Fan A VFS-MA-02A Containment Exhaust Fan B VFS-MA-02B	2
To monitor volume of airflow released to the environment	Primary means	Containment Exhaust Fan A Flow Sensor VFS-011A Containment Exhaust Fan B Flow Sensor VFS-011B	3

Table 9.11-6. Operator Actions Relevant to Section 9.11.8

Operator Action	Class
None	

Table 9.11-7. LCOs Related to the Dose Assessment for Section 9.11.8

Limit or Condition	Technical Specifications Identification and Notes
None	

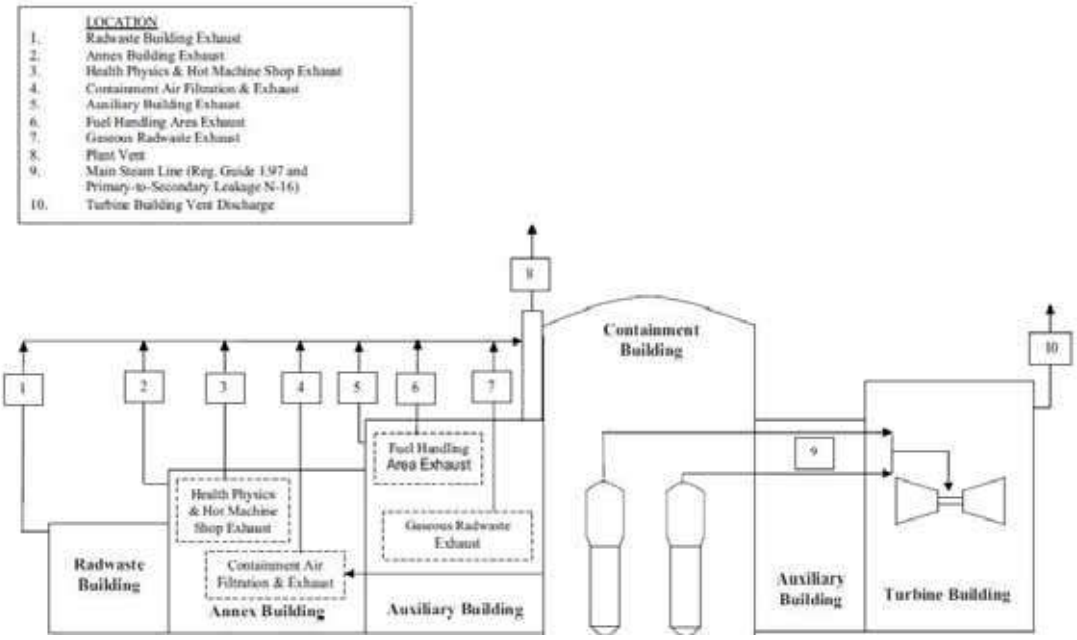


Figure 9.11-1. Schematic of Plant HVAC System

9.12 Radioactive Waste Handling

9.12.1 Introduction and Overview of Faults

The safety case for the operation of the AP1000 reactor includes non-reactor faults. These non-reactor faults include those associated with handling radioactive waste (radwaste).

9.12.2 Overview of the Solid, Liquid, and Gaseous Waste Management Systems

Chapter 26 provides an in-depth discussion of the AP1000 radioactive waste management systems. Chapter 26 also addresses the radioactive waste management strategy and discusses the WGS, the WLS, and the solid radwaste system (WSS). The chapter provides details on the sources of the various waste streams and provides details on the emissions to air; liquid discharges; and the minimisation, handling, and storage of solid waste.

A brief overview of the systems designed to manage solid, liquid, and gaseous radioactive wastes is presented below.

9.12.2.1 Solid Waste Management

The WSS is designed to collect and accumulate spent ion exchange resins, deep-bed filtration media, spent filter cartridges, dry radioactive wastes, and mixed wastes generated as a result of normal plant operation. The system is located in the auxiliary and radwaste buildings.

Processing and packaging of wastes are by mobile systems in the auxiliary building rail car bay and by mobile and fixed systems in the mobile systems facility in the radwaste building. The packaged waste may be accumulated in the auxiliary and radwaste buildings until it is moved to longer-term storage or disposal.

This system does not handle large, radioactive waste materials such as core components or radioactive process wastes from the plant's secondary cycle.

9.12.2.2 Liquid Waste Management

The systems that process liquid radwaste include the following:

- WLS
- Radioactive waste drain system (WRS)

The WLS is designed to control, collect, process, handle, store, and dispose of liquid radioactive waste in a controlled manner. Liquid waste is produced on both the primary side (primarily from adjustment of reactor coolant boron concentration and from reactor coolant leakage) and the secondary side (primarily from SG blowdown processing when there is secondary-side leakage). The AP1000 plant does not recycle primary-side effluents for re-use (except for RCS degasification in anticipation of shutdown). Primary effluents are discharged to the environment after processing. Liquids collected by drains in the WRS are also treated by the WLS.

Radioactive inputs to the WLS include fission and activation products produced in the core and reactor coolant system.

Ion Exchange Media Replacement

When ion exchange media are spent and ready to be transferred to the WSS, the vessel containing the media is isolated from the process flow. The flush water line is opened to the sluice piping, and demineralised water (DMW) is pumped into the vessel through the normal process outlet connection upward through the media retention screen. When the bed has been fluidised, the sluice connection is opened and the bed is sluiced to the spent resin tanks in the WSS. DMW flow continues until the bed has been removed and the sluice lines are clean of spent resin.

9.12.2.3 Gaseous Management

The WGS is a once-through, ambient temperature, activated-carbon delay system. The system includes a gas cooler, a moisture separator, an activated-carbon-filled guard bed, and two activated-carbon-filled delay beds. Also included in the system are an oxygen analyser subsystem and a gas sampling subsystem.

The radioactive fission gases entering the system are carried by hydrogen and nitrogen and are cooled to about 4°C (39°F). Radioactive decay of the fission gases during the delay period significantly reduces the radioactivity of the gas flow leaving the system.

9.12.3 Assumptions – Radwaste Generation

The expected radwaste generation rate is based upon the following:

- All ion exchange resin beds are disposed of and replaced every refuelling cycle.
- The WGS activated-carbon guard bed is replaced every refuelling cycle.
- The WGS delay beds are replaced every 10 years.
- All wet filters are replaced every refuelling cycle.

The maximum radwaste generation rate is based upon the following assumptions:

- The maximum expected rates of compactable and noncompactable radwaste, chemical waste, and mixed wastes are about 50 percent greater than the expected volumes to be generated.

- The ion exchange resin beds are replaced based upon operation with 0.25-percent fuel defects.

- The WGS activated-carbon guard bed is replaced twice every refuelling cycle.

- The WGS delay beds are replaced every 5 years.

- All wet filters are replaced based upon operation with 0.25-percent fuel defects.

- Primary-to-secondary system leakage contaminates the condensate polishing system and steam generator blowdown system (BDS) resins and membranes, which are designed to be replaced.

9.12.4 Analysis of Faults

The potential for a radioactive release from AP1000 plant subsystems events include, but are not limited to, the following:

- Gas waste management system leak or failure
- Liquid waste management system leak or failure (atmospheric release)
- Releases of radioactivity to the environment via liquid pathways

No analysis is provided of a gas waste management system leak or failure, as it would result in an insignificant release. Therefore, this event was not considered at the hazard identification exercise as a credible fault and so is not discussed any further in this chapter. However, the hazard identification exercise did identify a potential issue with wet activated carbon; which is discussed later.

Similarly, no analysis is provided for an atmospheric release in the liquid waste management system because of a leak or failure, as the effluent is routed via the WLS vacuum degasifier before being stored in the effluent holdup tanks. Therefore, the liquid radwaste tanks will not contain significant gaseous activity. This fault is not discussed any further in this section of the PCSR.

Releases of radioactivity to the environment were considered as part of the hazard identification exercise, as discussed below:

A total of 15 faults were identified at hazard identification exercises; the following six faults were screened out in the fault list (Appendix 8A) for the reasons presented below:

- Fault 3.6.3, setting fire to solid waste (WSS)

  The potential for a fire is controlled by good housekeeping procedures, ensuring a lack of combustible material stored in or near potential sources of ignition. Electrical ignition sources, such as those from machinery and electrical items, are minimised because of a number of factors. Items will be tested and maintained in accordance with statutory legislation and approved codes of practice. Further details can be found in Chapters 17 and 18. Normal good housekeeping procedures will ensure that any combustible waste is placed in robust containers (fire-resistant if appropriate) and the contents emptied on a regular basis (Section 11.4). In addition, early detection and warning of fire will be provided by the AFD. The AFD is provided throughout the AP1000 plant and will be designed, installed, and commissioned in accordance with appropriate standards. The AFD provides audible and visual alarms, as well as system trouble annunciation, in both the MCR and the security central alarm station, and thus will alert operators to a solid waste fire. Operators will be able to control and extinguish the fire. The fire loads at any point in time of the life of the AP1000 plant facility will be low when compared with older existing nuclear licensed sites because of it being built to modern standards. This basis will minimise the risk that fires will spread within the facility; the number of locations of fire is expected to be comparatively small.

  Section 9.11 considers filter fires and fires in the charcoal and delay beds.

  From an examination of a potential fire in the charcoal guard and delay beds, it is concluded that this fault is bounded by the filter fire fault (see Section 9.11), and so it is not discussed any further in this section.

- Fault 3.6.6, spills of liquid waste (leak to ground from vessel or pipework) (WLS)

  Normally nonradioactive liquid waste sumps and tanks are sampled for radioactivity to determine whether the liquid wastes have been inadvertently contaminated.

The design process has considered leaks that have been identified in this fault schedule as initiators; therefore, it is proposed to screen out faults 3.6.6 and 3.6.7 and not consider them further in the PCSR.

- Fault 3.6.7, spills of liquid waste (leak to drain) (WLS)

  As for fault 3.6.6, all streams of nonradioactive liquid waste, chemical, detergent, and oily waste are collected in the appropriate tanks and sumps. Radwaste is collected in the radwaste system. All nonradioactive tanks and sumps are routinely monitored. Therefore, active spills into any normally nonactive system would be detected prior to disposal.

- Fault 3.6.8, unauthorised discharge of gaseous waste (WGS)

  The WGS is designed to receive hydrogen-bearing and radioactive gases generated during process operation. The WGS is designed to reduce the controlled activity releases in support of the overall AP1000 plant release goals. To prevent an unauthorised gaseous discharge, however, each licencee's management systems will need to be robust enough to prevent an act of noncompliance.

- Fault 3.6.9, unauthorised discharge of liquid (WLS)

  The liquid radwaste system provides the capability to reduce the amounts of radioactive nuclides released in the liquid wastes through the use of demineralization and time delay for decay of short-lived nuclides.

  Before radioactive liquid waste is discharged, it is pumped to a monitor tank. A sample of the monitor tank contents is analysed, and the results are recorded. In this way, a record is kept of planned releases of radioactive liquid waste.

  The liquid waste is discharged from the monitor tank in a batch operation, and the discharge flow rate is restricted as necessary to maintain an acceptable concentration when diluted by the circulating water discharge flow. These provisions preclude uncontrolled releases of radioactivity.

  In addition, the discharge line contains a radiation monitor with diverse methods of stopping the discharge. The first method closes an isolation valve in the discharge line, which prevents any further discharge from the liquid radwaste system. The valve automatically closes and an alarm is actuated if the activity in the discharge stream reaches the monitor setpoint. The second method stops the monitor tank pumps.

  To minimize leakage from the liquid radwaste system, the system is of welded construction except where flanged connections are required to facilitate component maintenance or to allow connection of temporary or mobile equipment. Air-operated diaphragm pumps or pumps having mechanical seals are used. These pumps minimize system leakage thereby minimizing the release of radioactive gas that might be entrained in the leaking fluid to the building atmosphere.

  Provisions are made to control spills of radioactive liquids due to tank overflows. In addition, the radioactive waste collection tanks (i.e., the effluent holdup tanks, waste holdup tanks, and chemical tank) are located within the auxiliary building, which is well sealed and equipped with an extensive floor drain system. The radwaste monitor tanks are located in the auxiliary building and in the radwaste building, which has a well sealed, contiguous basemat with integral curbing and a floor drain system. Routing of both of the auxiliary building and radwaste building floor drain systems are to the liquid radwaste

system. This eliminates the potential for undetected tank leakage to the environment.

The monitored radwaste discharge pipeline is engineered to preclude leakage to the environment. This pipe is routed from the auxiliary building to the radwaste building (the short section of pipe between the two buildings is fully available for visual inspection as noted above) and then out of the radwaste building to the licensed release point for dilution and discharge. The discharge radiation monitor and isolation valve are located inside the radiologically controlled area. The exterior piping is designed to preclude inadvertent or unidentified releases to the environment; it is either enclosed within a guard pipe and monitored for leakage, or accessible for visual inspection. No valves or vacuum breakers are incorporated outside of monitored structures. This greatly reduces the potential for undetected leakage from this discharge to the environment at a non-licensed release point.

To prevent an unauthorised gaseous discharge, however, each licencee's management systems will need to be robust enough to prevent an act of noncompliance.

- Fault 3.6.10, mispackaging of waste for offsite disposal (WSS)

  Each licencee will have its own management systems to control the sentencing of waste consignments. All radwaste that is packaged and accumulated by an AP1000 reactor unit will be transferred for disposal. The standard AP1000 plant has no provisions for permanent storage of radwaste, but licensees may construct facilities for radwaste storage. Packaging will be done in accordance with local and national requirements. Health physics will control the monitoring of radwaste consignments.

  The consequences realised in this fault would require a failure of these systems, which incorporate health physics checks. Even if intermediate-level waste (ILW) was erroneously consigned instead of LLW by the site, it may not yield a significant public dose if the recipient has its own checks to determine that the waste meets its acceptance criteria.

The remaining nine faults, identified below, are assessed within this section unless as noted below:

Fault ID	Description
3.4.2	Fault in handling spent resins (ILW); leakage during transfer to collection tank, tank overfill, or tank rupture/leakage (WSS)
3.4.3	Fault in handling spent resins (LLW and WSS)
3.4.4	Fault in handling wet activated carbon (WGS)
3.4.5	Fault in handling SG blowdown material (resins) (WLS)
3.4.6	Fault in handling SG blowdown material (membranes) (WLS)
3.4.7 and 3.4.8	Fault in handling spent filters (higher activity)
3.6.1	Drop/impact of solid waste (LLW and WSS)
3.6.2	Drop/impact of solid waste (ILW and WSS)

Fault ID	Description
3.5.7	Dropped filters during handling (filter exchange, transfer to, or processing in radwaste building) (WSS) (Addressed in Section 9.11.7)

A number of other faults were identified during hazard identification exercises (described in Chapter 8) but were screened out in the fault list (Appendix 8A).

The initiators of the nine identified faults can result in two fault modes: loss of containment of spent resin, and dropping of radioactive exchangeable items (filters and charcoal adsorbers).

- Fault 3.4.2 involves the movement of spent resin from ion exchangers positioned around the plant. DMW is used to flush the spent resin into spent resin collection tank. The fault also considers the dropping of spent resin during the preparation of a shipping container for permanent storage offsite.

  Numerous initiators could result in the loss of containment of spent resin. The fault would result in a dose to an operator. As the movement of spent resin is contained entirely within the AP1000 plant facility where ventilation systems use filtration technology, the public consequences from this fault are deemed to be insignificant.

- Fault 3.4.3 considers the same scenario as that described in fault 3.4.2, except that it is assumed that the activity of the resin is less onerous (LLW as opposed to ILW).

- Fault 3.4.4 is involved with the handling of wet activated carbon. This carbon arises from the charcoal adsorbers, which are expected to be exchanged once every refuelling cycle (every 18 months); the maximum exchange rate is twice every 18 months.

- Faults 3.4.5 and 3.4.6 discuss the resin and membranes, respectively, involved with SG blowdown. Although there are many steps involved with this task, the fault here analyses a drop of resin and of a membrane from the filter used with the blowdown process.

- Faults 3.4.7, 3.4.8, and 3.5.7 describe the dropping of a filter.

9.12.5 Fault Groups

From analysis of the faults listed above, similar faults can be linked into fault groups. For brevity, it has been decided to create two groups.

1. Loss of containment of spent resin
2. Dropping of radioactive exchangeable items (filters and charcoal adsorbers)

9.12.5.1 Bounding Faults

Each of the above groups contains a bounding fault used as the basis of study.

The bounding fault for the loss of containment of spent resin group is considered to be the loss of containment of the spent resin collection tanks. This is because the volume of spent

resin considered here (15.6 m^3 (550 ft^3)) is greater than the volume of a container used for shipping the spent resin.

For the dropping of radioactive exchangeable items group, many items can be dropped. However, in comparing the annual production of spent resin to that of filters, it was determined that there is more activity associated with resin than with a filter. Therefore, the bounding fault is the dropping of spent resin.

9.12.6 Loss of Containment of Spent Resin (Faults 3.4.2 and 3.4.3)

9.12.6.1 Fault Group Description

This group considers two scenarios: mechanical failure (from a ruptured tank or failed valve, for example) and the dropping of a shipping flask containing spent resin destined for permanent offsite storage. Both scenarios result in a loss of containment of spent resin.

The resin change operation is described below. This illustrates the plant and equipment used to move the spent resin from the ion exchangers situated throughout the plant to the two spent resin collection tanks (MV01A/B) situated in the southwest corner of the auxiliary building.

Resin Change Operation

Spent resin is stored in tanks and a basis of a minimum of 30-day storage prior to interim storage on site or permanent storage offsite is assumed. This allows activity to fall prior to shipment.

The resin transfer lines from the ion exchangers are routed to the spent resin collection tanks on the 100-m level in the southwest corner of the auxiliary building. The spent resin system pumps, valves, and piping are located in shielded rooms near the spent resin collection tanks.

DMW is used to pump spent resins from the various ion exchangers to the spent resin tanks. The resin mixing pump is aligned to discharge excess transfer water through the resin fines filter to the liquid waste processing system. During the transfer operation, the tank level is monitored and the resin mixing pump is operated, if required, to limit tank water level. The operator stops the transfer when the closed-circuit television camera viewing the sight glass indicates on a control panel monitor that the sluice water is clear and the transfer line is, therefore, flushed of resins.

The radwaste building houses the mobile systems facility. It also includes the waste accumulation room and the packaged waste storage room. These rooms are serviced by the mobile systems facility crane.

Fault Mechanism

<u>Loss of Containment from Plant and Equipment of the Resin Change System</u>

The fault considers the release of spent resin through the loss of containment of plant and equipment involved with the movement of the spent resin from the ion exchangers to the spent resin collection tanks (MV01A/B).

The two spent resin collection tanks are effectively joined by common feed pipework. Failure of a valve could result in spent resin accumulating beneath these tanks.

The fault pessimistically considers an inventory of the maximum amount of resin produced by the plant in 1 year (15.6 m^3 (550 ft^3)), which is twice that of the normal amount expected to be produced each year.

Each of the two tanks has a maximum volume of 7.8 m^3 (275 ft^3)[2] of spent resin. In the event of valve failure, the maximum spilled volume is 2×7.8 m^3 (275 ft^3) = 15.6 m^3 (500 ft^3) and the fault is considered on this basis.

The failure of a valve in a room not normally occupied, behind significantly thick concrete shielding, would mean that this fault is likely to be unrevealed.

Dropping of a Shipping Container

Other initiators can result in the release of spilled, spent resin. For example, a shipping container could be filled with spent resin and then be dropped. The volume of a shipping container, however, is expected to be significantly less than 15.6 m^3 (500 ft^3). It is also noted that the dropping of a shipping container is more likely to be a revealed event.

9.12.6.2 Bounding Fault

The bounding fault for this group considers the loss of containment from plant and equipment of the resin change system of a volume 15.6 m^3 (500 ft^3) of spent resin.

9.12.6.3 Initiating Event Frequency[1]

The IEF is calculated on the volumetric basis, mentioned above, that the maximum volume of spent resin produced in 1 year is the volume of two spent resin collection tanks (15.6 m^3 (500 ft^3)). Also mentioned above is that the expected volume of spent resin to be produced each year is actually half this figure (7.8 m^3 (275 ft^3)). Therefore, it is reasonable to assume that the spent resin collection tanks will be required to be emptied less than once per year.

Many initiators could cause the spent resin collection tanks to fail (as identified in Appendix 8A). Although mechanical failure of valves or welds would have a low IEF, human error may be involved in a scenario where a valve has been left in the wrong orientation when the spent resin collection tanks are being emptied. This would cause unplanned emptying of the tanks' contents, possibly unrevealed for some time. The volume of spent resin would only reach 15.6 m^3 (500 ft^3) if the fault occurred in the latter part of a rolling 12-month period. On this basis, a human error value of 1E-03/yr^{-1} is assumed for the probability of failure on demand (pfd) using the same methodology as in Chapter 13. The IEF is calculated as the pfd multiplied by the number of demands per year. As the frequency of moving the spent resin from a spent resin collection tank is <1/yr^{-1}, the IEF is <1E-03/yr^{-1}.

1. As discussed in Chapter 8, the frequency for initiating events from the PSA is used in both Chapters 8 and 9 with the sole purpose of supporting the categorisation of the fault to a specific DB category. As noted in Chapter 8, these probabilities should not be considered to be representative of actual frequency of the events, and for several events they can be significantly conservative. Detailed PSA results and their basis are discussed in Chapter 10.
2. Note that actual usable volume of the tank is 7.0 m^3 (247 ft^3) and thus assuming a higher maximum volume of spent resin is conservative.

9.12.6.4 Design Basis Class

Using the above-mentioned IEF and the calculation used to support this FSG (Reference 9.12-2), it can be seen that the operator and public doses from this fault are categorised as DB0.

9.12.6.5 Design Basis Fault Progression and Assessment

The failure of a valve near the spent resin collection tanks would cause a spillage onto the area below the tanks. As this area is not normally manned, it would only give rise to an operator dose if an operator were in the vicinity. This fault could not give anything more than a trivial dose to a member of the public. Airborne contamination is assumed to be released in trace amounts because of the filtration technology (HEPA filters and charcoal adsorbers) in the ventilation system.

As mentioned above, the spent resin collection tanks are connected, so it is assumed that the entire volume of 15.6 m^3 (500 ft^3) is released in this fault.

Access to the solid waste storage areas is controlled. Therefore, it is expected that health physics monitors carrying detection instrumentation will accompany an operator entering the spent resin collection tanks area (the WSS valve and piping area on the 7.62-m (25 ft) level above grade) to allow access to the ladder down toward the tanks.

In the event of a spillage, it is assumed that operators discovering it would be trained to evacuate the area and report the spillage to a superior. The superior member of personnel would then be assumed to organise the recovery and cleanup process.

The dose to an operator is below 20 mSv (see the "Radiological Consequences" section below). This leads to the following operating instruction:

Operating instruction – A spillage of spent resin is to be reported to a team leader, who will then instigate evacuation procedures.

9.12.6.6 Radiological Consequences

The supporting calculation (Reference 9.12-2) contains many assumptions. First, as spent resin is classified as ILW, no operator is expected to be within 6 m (19.7 ft) of the spent resin collection tanks under normal circumstances:

Operating instruction – Unless instructed to do so by a team leader, no personnel are to be within 6 m (19.7 ft) of the spent resin collection tanks.

This is not thought to be too restrictive, as there is approximately 6 m (19.7 ft) from the midpoint between the spent resin collection tanks to the back of the rail car bay. There is also over 10 m (32.8 ft) of vertical distance between the removable cover on the operating deck (situated 10.7 m (35.1 ft) above ground, allowing access to the spent resin collection tanks) and the base of the tanks.

Concerning the spillage of spent resin from a dropped shipping container, the crane operator will be positioned up to 15.4 m (50.5 ft) from the waste disposal containers used to ship the spent resin from the AP1000 plant facility. The exposure time used in the calculation (Reference 9.12-2) was 5 minutes, as it is assumed that if a crane operator were required to evacuate, sufficient time would be required to exit the crane control cab. However, for most

personnel needing to evacuate because of a spillage of resin, it is assumed that evacuation time would be significantly less than 5 minutes.

The calculation (Reference 9.12-2) states that the dose to an operator is 10.4 mSv. A calculation for dose to members of the public shows that the highest dose is to a 1-year-old child and is 0.45 mSv (Reference 9.12-3).

Respirators are able to offer a DF of 40 (Reference 9.12-5). It is considered that the donning of a respirator could be designated here; however, it may be restrictive (e.g., it may restrict vision). The PPE requirements will be determined by the health physics team at the time of use and are therefore not designated here.

In summary, the doses to the operator and to members of the public for this FSG are below the Target 4 BSL for frequent faults (1 mSv offsite and 20 mSv onsite).

9.12.6.7 As Low As Reasonably Practicable Assessment

Instrumentation such as activity-in-air monitors and level detectors near spent resin collection tanks could be designated but the areas are not normally manned. Health physics teams would be expected to accompany personnel routinely upon entry into such unmanned areas. In the event of an operator attending a normally unmanned area in response to an instrument alarm, it would also be expected that health physics monitors would need to be present to determine that it is safe for the operator to enter. Such a regime would preclude the need for instrumentation to be situated permanently in such rooms, so no designation is made here.

Other factors that have the potential to reduce the risk associated with this fault are that suitable training and briefing of infrequent procedures will be performed on tasks associated with the emptying of the spent resin collection tanks. It is also assumed that those operators will be donning appropriate PPE.

No further measures are practicable and the risk is considered to be ALARP.

9.12.6.8 Conclusion

Radiological consequences are within the Target 4 BSLs for frequent faults (1 mSv offsite and 20 mSv onsite), and the risks have been reduced to be ALARP.

Operator actions relevant to this fault assessment are provided in Table 9.12-1.

LCOs related to the dose assessment for this fault are provided in Table 9.12-2.

9.12.7 Dropping of Radioactive Exchangeable Items (Filters and Charcoal Adsorbers) (Faults 3.4.4 through 3.4.8 and Faults 3.6.1 to 3.6.2)

9.12.7.1 Fault Group Description

This fault considers the dropping or mishandling of a number of potentially radioactive objects, each of which is considered below.

Dropped Filter

A filter transfer cask is used to change the higher-activity filters of the CVS and spent fuel cooling system. The filter vessel is drained and the filter cover is opened remotely. The shield plug of the port over the filter is removed and the transfer cask, without its bottom shield cover, is lifted and positioned on the port directly over the cartridge in the filter vessel.

A grapple inside the transfer cask is remotely lowered and connected to the filter cartridge. The cartridge is lifted into the transfer cask, and the cask is transferred over plastic sheeting to the bottom shield cover. The dose rate of the cartridge is measured with a long probe, and the cask is lowered onto and connected to the bottom shield cover. The transfer cask is then moved to the auxiliary building rail car bay.

Radioactive filters from ventilation exhaust filtration units are bagged and transported to the radwaste building, where they are temporarily stored. The filters may be compacted along with other dry radioactive wastes. It is noted that compaction is outside the scope of this assessment.

A cartridge unit is described as stainless-steel housing and pleated polypropylene cartridge with stainless-steel screen outer jacket. A filter cartridge is a metallic cylinder, where the maximum volume produced is 0.4 m^3/yr (14 ft^3/yr).

Wet Activated Carbon

No inventory information appears to exist for activated carbon, but it is classified as ILW.

Steam Generator Blowdown Material: Resins and Membranes

No inventory information appears to exist for resins and membranes associated with SG blowdown, but it is classed as LLW.

9.12.7.2 Bounding Fault

From inspection of the above, the most onerous scenario is a dropped filter.

9.12.7.3 Initiating Event Frequency[1]

The IEF for dropping a filter is assumed to comprise human error and error associated with remote handling.

Reference is made to a study analysing 34 years of crane operating experience of US reactors (Reference 9.12-1). This report (page B-15) gives a failure rate (including failures of the crane itself and human errors) of 6.7E-06 per demand.

It is not clear how often a filter will require to be replaced. However, it is assumed that it will be significantly less than 100 times per year.

1. As discussed in Chapter 8, the frequency for initiating events from the PSA is used in both Chapters 8 and 9 with the sole purpose of supporting the categorisation of the fault to a specific DB category. As noted in Chapter 8, these probabilities should not be considered to be representative of actual frequency of the events, and for several events they can be significantly conservative. Detailed PSA results and their basis are discussed in Chapter 10 of this PCSR.

Even assuming 100 filter replacements per year, this would give an IEF of 6.66E-04/yr^{-1}.

Reference 9.12-1 states that the mean annual failure rate is to be used in connection with a distribution curve and more accurate values are calculated when using the mean failure rate and percentiles. The mean failure rate of 6.7E-06 per demand corresponds to a percentile value of approximately 71; in other words, there is 71-percent likelihood that the failure rate is less than 6.7E-04/yr^{-1}.

9.12.7.4 Design Basis Class

The consequences have been calculated below as being 0.29 mSv. Using the IEF value calculated above and considering that the consequences to the operator are less than 2 mSv which is less then the Target 4 BSL for frequent faults of 20 mSv to workers, this puts the fault into the DB0 category. The dose to a member of the public has not been calculated, as it is assumed to be significantly less than the Target 4 BSL for frequent faults of 1 mSv to the public.

9.12.7.5 Design Basis Fault Progression and Assessment

The transfer cask bottom cover is disconnected. The transfer cask is lifted by the crane and transferred to a position over a waste container via a port in the top of a portable processing and storage cask. Plastic coverings are removed; and the container is capped, smear-surveyed, and decontaminated as required, using reach-rod tools through a cask port. The dose rate survey is also made through a cask port.

Transfer of the filled waste container to the transfer cask, including cask cover handling, is then performed using remote control. Radioactive filters from ventilation exhaust filtration units are bagged and transported to the radwaste building, where they are temporarily stored.

As the items listed above contain a potentially significant amount of activity, it is prudent to designate an operating instruction to ensure that a minimum distance is maintained between the operator and the unshielded source:

- **Operating instruction –** No personnel are to be positioned within 4 m (13.1 ft) of an unshielded cartridge, filter, or charcoal adsorber while it is being moved or replaced.

This requirement is not considered to be too restrictive, as it is expected that mobile handling equipment will be used to move filters if the radioactivity readings make it ALARP to do so. It is also assumed that if a filter is dropped, then the POW instigates the evacuation procedure of all personnel in the affected area:

- **Operating instruction –** In the event of a dropped filter, the POW must instigate the evacuation procedure.

The dropping of a filter under the circumstances described above is classified as a revealed event.

9.12.7.6 Radiological Consequences

A calculation has been performed on the radiological consequences to an operator (Reference 9.12-4). It is assumed that the evacuation time is 5 minutes to allow personnel such as crane operators time to leave the crane cab. For most operators, however, this is pessimistic, as evacuation would be expected to be carried out well within 5 minutes for such a revealed event.

Respirators are able to offer a DF of 40 (Reference 9.12-5). It is considered that the donning of a respirator could be stated as a requirement here; however, it may be restrictive (e.g., it may restrict vision). The PPE requirements will be determined by the health physics team at the time of use and therefore are not designated here.

Assuming that the operator is positioned at least 3.63 m (11.9 ft) away from the dropped filter, the dose to the operator is 0.29 mSv.

A calculation of dose to members of the public has not been prepared, as it is assumed to be significantly less than the Target 4 BSL for frequent faults of 1 mSv because of the DF afforded by the HEPA filter and charcoal adsorbers.

9.12.7.7 As Low As Reasonably Practicable Assessment

Assumptions that will reduce the risk associated with this fault are that suitable training and briefing of infrequent procedures (such as moving filters) will be performed. It is also assumed that those operators will be donning appropriate PPE.

No further measures are practicable and the risk is considered to be ALARP.

9.12.7.8 Conclusions

Radiological consequences are within the Target 4 BSLs for frequent faults (1 mSv offsite and 20 mSv onsite), and the risks have been reduced to be ALARP.

Operator actions relevant to this fault assessment are provided in Table 9.12-3.

LCOs related to the dose assessment for this fault are provided in Table 9.12-4.

9.12.8 References

9.12-1 NUREG-1774, "A Survey of Crane Operating Experience at U.S. Nuclear Power Plants from 1968 through 2002," U.S. Nuclear Regulatory Commission, July 2003.

9.12-2 Serco Report PGEN/E.004067/02/18/089, "Calculation of Operator Dose from Spilt Resins in the AP1000 PWR," August 2010.

9.12-3 Serco Report PGEN/E.004067/02/18/088, "Calculation of Public Dose from Spilt Resins in the AP1000 PWR," August 2010.

9.12-4 Serco Report PGEN/E.004067/02/18/090, "Calculation of Operator Dose from Dropped Filters in the AP1000 PWR," August 2010.

9.12-5 ISBN 978 0 7176 2904 6 HSG53, 3rd Edition "Respiratory Protective Equipment at Work – A Practical Guide," HSE, 2005.

Table 9.12-1. Operator Actions Relevant to Section 9.12.6

Operator Action	Class
A spillage of spent resin is to be reported to a team leader who will then instigate evacuation procedures.	2
Unless instructed to do so by the responsible operator under the supervision of health physics, no personnel are to be within 6 metres of the spent resin collection tanks.	2

Table 9.12-2. LCOs Related to the Dose Assessment for Section 9.12.6

Limit or Condition	Technical Specification Identification and Notes
(None)	

Table 9.12-3. Operator Actions Relevant to Section 9.12.7

Operator Action	Class
No personnel are to be positioned within 4 metres (13.1 ft) of an unshielded cartridge, filter, or charcoal adsorber whilst it is being moved or replaced.	2
In the event of a dropped filter, the person organising work must instigate the evacuation procedure.	2

Table 9.12-4. LCOs Related to the Dose Assessment for Section 9.12.7

Limit or Condition	Technical Specification Identification and Notes
Radwaste generation :	All ion exchange resin beds are disposed and replaced every refuelling cycle or with >0.25% fuel defects
Radwaste generation :	The WGS activated carbon guard bed is to be replaced every refuelling cycle
Radwaste generation :	The WGS delay beds are to be replaced every 10 years.
Radwaste generation :	All wet filters are to be replaced every refuelling cycle.

9.13 Conclusions

This chapter has presented a description and/or analysis of each design basis fault listed in Table 8A-2. The DB response of the system and of the corresponding SSCs to mitigate each fault has been analysed to demonstrate that the dose targets given in the ONR SAPs, specifically Target 4, are met. The set of SSCs required to ensure that the targets are met have been assigned the appropriate classification and the corresponding safety function(s) to the appropriate category, using the scheme described in Chapter 5.

Where the fault falls into the category of frequent faults (i.e., IEF > 1E-03 events/year), a diverse means of providing the necessary safety functions has also been identified to comply with the SAPs requirement that frequent faults should have diverse means of providing the necessary safety functions.

Also as part of this process, as required under site licence condition (SLC) 23, limits and conditions have been identified that may be candidates for Operating Rules or that may have Operating Rules associated with them. Similarly, required operating instructions (applicable, for example, to manually initiated safety systems) have been identified. These operating instructions are considered in Chapter 13. Finally, other SSCs have been identified that may provide defence in depth and contribute to reducing risks ALARP.

Chapter 9 demonstrates that DB dose targets are met when the identified SSCs are operating and the identified limits and conditions are met. Furthermore, for all the faults, the risks from all modes of normal operation and fault conditions are shown to be ALARP.

9A Evaluation Models and Parameters for Analysis of Radiological Consequences of Accidents

This appendix contains the parameters and models that form the basis of the radiological consequences analyses for the various postulated accidents.

9A.1 Offsite Dose Calculation Models

Radiological consequences analyses are performed to determine the total effective dose equivalent (TEDE) doses associated with the postulated accident. The determination of TEDE doses takes into account the CEDE dose resulting from the inhalation of airborne activity (that is, the long-term dose accumulation in the various organs) as well as the effective dose equivalent (EDE) dose resulting from immersion in the cloud of activity and dose resulting from deposition on the ground.

Credit is taken for the decay of radionuclides until release to the environment. After release to the environment, no credit is taken for radioactive decay or cloud depletion by ground deposition during transport offsite.

9A.1.1 Immersion Dose (Effective Dose Equivalent)

Assuming a semi-infinite cloud, the immersion doses are calculated using the equation:

$$D_{im} = \sum_i DCF_i \sum_j R_{ij} (\chi/Q)_j$$

where:

D_{im} = Immersion (EDE) dose (Sv)

DCF_i = EDE dose conversion factor for isotope i (Sv-m^3/Bq-s)

R_{ij} = Amount of isotope i released during time period j (Bq)

$(\chi/Q)_j$ = Atmospheric dispersion factor during time period j (s/m^3)

9A.1.2 Inhalation Dose (Committed Effective Dose Equivalent)

The CEDE doses are calculated using the equation:

$$D_{CEDE} = \sum_i DCF_i \sum_j R_{ij} (BR)_j (\chi/Q)_j$$

where:

D_{CEDE} = CEDE dose (Sv)

DCF_i = CEDE dose conversion factor (Sv per Bq inhaled) for isotope i

R_{ij} = Amount of isotope i released during time period j (Bq)

$(BR)_j$ = Breathing rate during time period j, 6.02E-5 m^3/s (1-2 year child), 3.10E-4 m^3/s (adult) (m^3/s)

$(\chi/Q)_j$ = Atmospheric dispersion factor during time period j (s/m^3)

9A.1.3 Ground Deposition Dose (Effective Dose Equivalent)

Assuming a semi-infinite cloud, the ground deposition doses are calculated using the equation:

$$D_{gd} = (S_{gd}) \sum_i DCF_i \sum_j (IAR)_{ij}$$

where:

D_{gd} = Ground deposition (EDE) dose (Sv)

S_{gd} = Shielding factor for dose from ground deposition dose (unitless)

DCF_i = EDE dose conversion factor for isotope i (Sv-m^3/Bq-s)

$(IAR)_{ij}$ = Integrated activity for isotope i deposited on ground during time period j (Bq-s/m^3)

The assumed deposition velocities of 0.01 m/sec for iodine or 0.002 m/sec for other nongaseous nuclides (the noble gases do not deposit in the soil).

9A.1.4 Total Dose (Total Effective Dose Equivalent)

The TEDE doses are the sum of the EDE and the CEDE doses.

9A.2 Main Control Room Dose Models

Radiological consequences analyses are performed to determine the TEDE doses associated with the postulated accident. The determination of TEDE doses takes into account the CEDE dose resulting from the inhalation of airborne activity (that is, the long-term dose accumulation in the various organs) as well as the EDE dose resulting from immersion in the cloud of activity.

There are two approaches used for modelling the activity entering the main control room. If power is available, the HVAC system will switch over to a supplemental filtration mode.

Alternatively, if the normal HVAC is inoperable or, if operable, the supplemental filtration train does not function properly resulting in increasing levels of airborne iodine in the main control room, the emergency habitability system would be actuated when High-2 iodine or particulate radioactivity is detected. The emergency habitability system provides passive pressurisation of the main control room from a bottled air supply to prevent inleakage of contaminated air to the main control room. The bottled air also induces flow through the passive air filtration system which filters contaminated air in the main control room. There is a 72-hour supply of air in the emergency habitability system. After this time, the main control room is assumed to be opened and unfiltered air is drawn into the main control room by way of an ancillary fan. After 7 days, offsite support is assumed to be available to re-establish operability of the control room habitability system by replenishing the compressed air supply.

The main control room is accessed by a vestibule entrance, which restricts the volume of contaminated air that can enter the main control room from ingress and egress. The design of the

VES provides clean air to the control room and maintains it in a pressurised state. The path for the purge flow out of the main control room is through the vestibule entrance and this should result in a dilution of the activity in the vestibule and a reduction in the amount of activity that might enter the main control room. However, no additional credit is taken for dilution of the vestibule via the purge. The dose analyses allow for a limited amount of outside air infiltration.

Control room model input is provided in Table 9A-8.

9A.2.1 Immersion Dose Models

Due to the finite volume of air contained in the main control room, the immersion dose for an operator occupying the main control room is substantially less than it is for the case in which a semi-infinite cloud is assumed. The finite cloud doses are calculated using the geometry correction factor from Murphy and Campe (Reference 9A-1).

The equation is:

$$D_{im} = \frac{1}{GF} \sum_i DCF_i \sum_j (IAR)_{ij} O_j$$

where:

D_{im} = Immersion (EDE) dose (Sv)

GF = Main control room geometry factor
= $352/V^{0.338}$

V = Volume of the main control room (m^3)

DCF_i = EDE dose conversion factor for isotope i (Sv-m^3/Bq-s)

$(IAR)_{ij}$ = Integrated activity for isotope i in the main control room during time period j (Bq-s/m^3)

O_j = Fraction of time period j that the operator is assumed to be present

9A.2.2 Inhalation Dose

The CEDE doses are calculated using the equation:

$$D_{CEDE} = \sum_i DCF_i \sum_j (IAR)_{ij} (BR)_j O_j$$

where:

D_{CEDE} = CEDE dose (Sv)

DCF_i = CEDE dose conversion factor (Sv per Bq inhaled) for isotope i

$(IAR)_{ij}$ = Integrated activity for isotope i in the main control room during time period j (Bq-s/m^3)

$(BR)_j$ = Breathing rate during time period j, 3.10E-4 m^3/s (adult) (m^3/s)

O_j = Fraction of time period j that the operator is assumed to be present

9A.2.3 Total Dose (Total Effective Dose Equivalent)

The TEDE doses are the sum of the EDE and the CEDE doses.

9A.3 General Analysis Parameters

9A.3.1 Source Terms

The sources of radioactivity for release are dependent on the specific accident. Activity may be released from the primary coolant, from the secondary coolant, and from the core if the accident involves fuel failures. The radiological consequences analyses use conservative design basis source terms.

9A.3.1.1 Primary Coolant Source Term

The accident dose analyses apply primary coolant source terms for iodines and noble gases consistent with the technical specification limits of 9.25E6 Bq/kg (0.25 μCi/g) dose equivalent I-131 for the iodines and 2.6E9 Bq/kg (70 μCi/g) dose equivalent Xe-133 for the noble gases. The alkali metals are based on continuous plant operation with 0.25-percent fuel defects. Table 9A-1 lists the concentrations of isotopes considered in the analyses.

The radiological consequences analyses for certain accidents also take into account the phenomenon of iodine spiking, which causes the concentration of radioactive iodines in the primary coolant to increase significantly. This is an iodine spike that occurs prior to the accident and for which the peak primary coolant activity is reached at the time the accident is assumed to occur. These isotopic concentrations are defined as 5.55E8 Bq/kg (15 μCi/g) dose equivalent I-131 (60 times the values listed in Table 9A-1). This corresponds to the short term abnormal operation technical specification limit. The probability of this adverse timing of the iodine spike and accident is small.

Although it is unlikely for an accident to occur at the same time that an iodine spike is at its maximum reactor coolant concentration, for many accidents it is expected that an iodine spike would be initiated by the accident or by the reactor trip associated with the accident. Table 9A-2 lists the iodine appearance rates (rates at which the various iodine isotopes are transferred from the core to the primary coolant by way of the assumed cladding defects) for normal operation. The iodine spike appearance rates are assumed to be as much as 500 times the normal appearance rates.

9A.3.1.2 Secondary Coolant Source Term

The secondary coolant source term used in the radiological consequences analyses is conservatively assumed to be 10 percent of the primary coolant equilibrium source term, consistent with the ratio of the primary and secondary technical specification limits for equilibrium iodine concentrations.

Because the iodine spiking phenomenon is short-lived and there is a high level of conservatism for the assumed secondary coolant iodine concentrations, the effect of iodine spiking on the secondary coolant iodine source terms is not modelled.

There is assumed to be no secondary coolant noble gas source term because the noble gases entering the secondary side due to primary-to-secondary leakage enter the steam phase and are discharged via the condenser air removal system.

9A.3.1.3 Core Source Term

Table 9A-3 lists the core source terms at shutdown for an assumed three-region equilibrium cycle at end of life after continuous operation at 1 percent above full core thermal power. The main feedwater flow measurement supports a 1-percent power uncertainty. In addition to iodines and noble gases, the source terms listed include nuclides that are identified as potentially significant dose contributors in the event of a degraded core accident. The design basis loss-of-coolant accident analysis is not expected to result in significant core damage, but the radiological consequences analysis assumes severe core degradation.

9A.3.2 Nuclide Parameters

The radiological consequence analyses consider radioactive decay of the subject nuclides prior to their release, but no additional decay is assumed after the activity is released to the environment. Table 9A-4 lists the half-lives for the nuclides of concern.

Table 9A-4 also lists the dose conversion factors for calculation of the doses.

The CEDE dose conversion factors (DCFs) model the dose due to inhalation of activity and the values are taken from Annex III of the 96/29/Euratom document (Reference 9A-2). Bounding values were selected.

The combined effect of the age-related dose conversion factors and breathing rates were evaluated and it was determined that the limiting child age range is the 1-2 year old child. Doses for other age ranges are not calculated.

The EDE DCFs model the dose due to submersion in a cloud of activity and the values are taken from the electronic supplement to U.S. Federal Guidance Report 13 (Reference 9A-3). Note that the EDE value listed for Cs-137 is that provided in Reference 9A-3 for Ba-137m. The Ba-137m value is much higher than that for Cs-137. Since Ba-137m is produced by the decay of Cs-137 and has a short half-life, the dose associated with its decay is included as being from Cs-137.

The DCFs for activity deposited on the ground are obtained from the electronic supplement to U.S. Federal Guidance Report 13 (Reference 9A-3). Note that, as with the EDE DCF, the value listed for Cs-137 is that provided for Ba-137m.

9A.3.3 Atmospheric Dispersion Factors

Table 9A-5 lists the off-site short-term atmospheric dispersion factors (χ/Q) for the reference site. The atmospheric dispersion factors (χ/Q) to be applied to air entering the main control room following a design basis accident are specified at the HVAC intake and at the annex building entrance (which would be the air pathway to the main control room due to ingress/egress). A set of reference AP1000 χ/Q values is identified for each potential activity release location that has been identified and the two control room receptor locations. These reference AP1000 χ/Q values are listed in Table 9A-6 and are provided in Table 2-1 (Sheet 3 of 3).

The site-specific control room χ/Q values shall be bounded by the values in Table 9A-6. For a site selected that has χ/Q values that exceed the values in Table 9A-6, how the radiological consequences associated with the controlling design basis accident continue to meet the control

room operator dose limits using site-specific χ/Q values should be addressed. Topographical characteristics in the vicinity of the site for restrictions of horizontal and/or vertical plume spread, channelling or other changes in airflow trajectories, and other unusual conditions affecting atmospheric transport and diffusion between the source and the receptors should be considered. No further action is required for sites within the bounds of the site parameters for atmospheric dispersion.

Table 9A-7 identifies the AP1000 source and receptor data to be used when determining the site-specific control room χ/Q values.

The main control room reference AP1000 χ/Q values do not incorporate occupancy factors.

The locations of the potential release points and their relationship to the main control room air intake and the annex building access door are shown in Figure 9A-1.

9A.4 Moisture Carryover

The moisture carryover is used to define the particulate (non-volatile) iodine and alkali metal releases from the steam generators. Moisture carryover at lower powers is much lower than the typical full power design value. Low power moisture carryover ranges from 10E-5 to 10E-4, depending on whether recirculating conditions are maintained. Recirculating conditions are assumed to be maintained when the water level is greater than 65% of the tube bundle height. From Reference 9A-4, the moisture carryover under non-recirculating conditions may be taken to be 10E-4 or 0.01%. However, it is also noted that moisture carryover increases when secondary relief valves are opened and that the maximum expected moisture carryover when the water level is below the dryer inlet is 0.05% and 0.4% when the water level is above the dryer inlet. To determine the moisture carryover fraction(s) modelled in each dose analysis, an assessment of the water level relative to the dryer inlet is made.

Thus, the moisture carryover is modelled as 0.05% unless the water level reaches the dryer inlet. If the water level reaches the dryer inlet the moisture carryover changes to 0.4%.

9A.5 Iodine Chemical Forms

The chemical form of iodine present is determined by whether or not reducing (i.e., excess hydrogen) conditions are maintained and whether oxygen is present. In the RCS, a reducing environment is maintained to limit corrosion. Under normal operating conditions the RCS H_2 concentration is maintained at >25 cc H_2 (STP)/kg H_2O, with STP defined as 0°C (32 °F) and 101.3 kPa (14.7 psia). The reducing environment, combined with the high electronegativity of iodine, will favour the formation of ionic iodine (I^-). Ionic iodine is the anionic component of iodine salts, such as CsI, which are particulates.

The design of the AP1000 significantly limits the introduction of oxygen to the RCS post-accident. In the AP1000 design, the CMT, which provides passive boration, is filled with heavily-borated primary reactor coolant at a pressure on the order of RCS operating pressure; as such, it is not open to the atmosphere and would not be a source of oxygen.

However, operation of the CVS is conservatively assumed to provide make up flow. The CVS makeup flow originates from the Boric Acid Storage Tank, which communicates with the atmosphere. Thus, the CVS is assumed to be a source of oxygen. Although the H_2 injection subsystem would be expected to be online when the H_2 concentration approaches 25 cc H_2 (STP)/kg H_2O, credit for the hydrogen injection system is not taken post-accident.

Consistent with Reference 9A-4, Section 4.4.4, the oxygen introduced via CVS is assumed to react stoichiometrically with Hydrogen (H_2) according to the equation:

$$H_2 + 0.5*O_2 = H_2O$$

Thus, the oxygen would act to decrease the hydrogen concentration with time. From Section 4.4.5 of Reference 9A-4, reducing conditions with respect to iodine are assumed to be lost when

$$[H_2]/[I] > 3.65E5$$

To conservatively estimate when reducing conditions are lost, the change in RCS H_2 and iodine concentrations are needed. After reducing conditions are lost, some of the oxygen entering the RCS is assumed to react with iodine, forming volatile iodine species.

Section 9A.5.1 presents the calculations of the RCS iodine concentration. Section 9A.5.2 presents the hydrogen concentration in the RCS. Section 9A.5.3 determines the assumptions to be applied with respect to iodine chemical forms modelled in the analysis.

9A.5.1 RCS Iodine Concentration

The concentration of RCS iodine vs. time can be calculated from the initial concentrations in t from Table 9A-1 and assumed spike rates and durations. Table 9A-1 considers I-130 though I-135, which are the iodine nuclides with the most significant dose impact. Additionally, more stable iodine nuclides (I-127 and I-129) must also be considered because the stable iodines dominate the mass of iodine in the primary coolant. Coolant concentrations of 4.55E-01 Bq/kg (1.23E-08 µCi/g) for I-129 and 1.32E-11 kg/kg for I-127 are used in the calculation of the RCS iodine concentration. The mass of iodine is calculated from the specific activities and half-lives as applicable. A total RCS iodine mass of 1.52E-02 g (3.351E-05 lbm) is calculated, dominated by I-129. Thus, 129 g/mol is taken as a representative molar mass for iodine, resulting in a calculated 1.18E-04 mol of iodine in the RCS.

An RCS mass of 1.684E5 kg (371,258 lbm) is used, consistent with the dose analysis assumptions. A density of 0.725 kg/L (45.26 lbm ft^{-3}) (reflecting expected operating condition) is used to calculate an RCS volume of 2.323E5 L (8204 ft^3).

With an RCS volume of 2.323E5 L, the molar concentration of iodine is 5.08E-10 mol/L.

9A.5.2 RCS Hydrogen Concentration

Under normal operating conditions, the RCS H_2 concentration is maintained at >25 cc H_2 (STP)/kg H_2O, with STP defined as 0°C (273 K) and 101.3 kPa. To calculate the molar concentration in the RCS (mol/L), the number of moles is needed as is the RCS volume.

H_2 is assumed to behave as an ideal gas, and the number of moles in 25 cc at the defined STP is calculated:

$n=PV/RT$

Where

P = 101.3 kPa

V = 25 cc (25 cm^3)

T = 273 K

R = 8.314E3 kPa*cm^3/mol*K

n is calculated to be 1.116E-03 mol, which is per kg H_2O in the RCS.

The RCS mass modelled is 1.684E5 kg, thus the total H_2 in the RCS is 1.879E2 mol.

The RCS volume was calculated to be 2.323E5 L.

The initial RCS H_2 concentration is calculated 1.879E2 mol / 2.323E5 L = 8.09E-04 mol/L.

9A.5.3 RCS Iodine Chemical Fractions

From Section 4.4.5 of Reference 9A-4, reducing conditions with respect to iodine are assumed to be lost when

$[H_2]/[I] > 3.65E5$

The initial H2 concentration was calculated as 8.09E-04 mol/L. Thus, reducing conditions are assumed to be lost when:

[I] > (8.09E-04 mol/L)/3.65E5

or

[I] > 2.22E-09 mol/L.

The calculated initial iodine concentration for the analysis was calculated as 5.08E-10 mol/L. It is apparent that any significant perturbation in iodine concentration (e.g. iodine spike or release from failed fuel) would cause the iodine concentration to increase above 2.22E-09 mol/L. Thus, it is conservatively assumed that reducing conditions are lost at the start of the event.

From the discussion in Section 4.4.5 and Figure 11 of Reference 9A-4, the maximum percentage of oxidized iodine is 0.07% at temperatures above 140 °C.

The RCS temperatures during the period of interest are well above 140°C, and thus, the maximum degree of oxidation expected is 0.07%. For conservatism, 0.1% of the iodine in the RCS is modelled as being in an oxidized (i.e., volatile) form. The volatile iodines will be assumed to be 97% elemental and 3% organic.

Note that, for additional conservatism, during periods where flashing of primary to secondary leakage is assumed, the amount of iodine assumed to be volatile is arbitrarily doubled to 0.2%.

9A.5.4 SG Iodine Chemical Fractions

Under normal operating conditions, reducing conditions are maintained in the SGs to limit corrosion. Unless SFW is running, the SGs are not fed post-trip, and thus there is no introduction of oxygen into the SGs. With SFW available, further oxidation of the iodide to convert it to the volatile form is possible with the added oxygen in the feedwater. However, this is insignificant owing to the rapid stripping of dissolved oxygen into the steam and low rate of thermal oxidation of iodide, as stated on page 35 in Reference 9A-4. Therefore, the iodine in the SGs is assumed to remain in a reduced (i.e., non-volatile particulate) form.

9A.6 References

9A-1 Murphy, K. G., Campe, K. M., “Nuclear Power Plant Control Room Ventilation System Design for Meeting General Criterion 19,” paper presented at the 13th AEC Air Cleaning Conference.

9A-2 96/29/Euratom, "Council Directive 96/29/EURATOM of 13 May 1996 laying down basic safety standards for the protection of the health of workers and the general public against the dangers arising from ionizing radiation," 5/1996.

9A-3 U.S. Federal Guidance Report 13, "Cancer Risk Coefficients for Environmental Exposure to Radionuclides: CD Supplement," EPA 402-C-99-001, Rev. 1, 2002.

9A-4 European Commission Report EUR 15615 EN, "Realistic Methods for Calculating the Release of Radioactivity following Steam Generator Tube Rupture Faults (A Consensus Document)," L.C.M. Dutton, et al, 1994.

Table 9A-1. Reactor Coolant Concentrations For Accident Analyses

Nuclide	Bq/kg (μCi/g)
Kr-85m	8.10E+06 (2.19E-01)
Kr-85	2.85E+07 (7.70E-01)
Kr-87	4.66E+06 (1.26E-01)
Kr-88	1.41E+07 (3.81E-01)
Xe-131m	1.21E+07 (3.27E-01)
Xe-133m	1.40E+07 (3.78E-01)
Xe-133	1.15E+09 (3.11E+01)
Xe-135m	1.61E+06 (4.35E-02)
Xe-135	2.89E+07 (7.81E-01)
Xe-138	2.44E+06 (6.59E-02)
Kr-85m	8.10E+06 (2.19E-01)
I-130	5.85E+04 (1.58E-03)
I-131	6.59E+06 (1.78E-01)
I-132	9.51E+06 (2.57E-01)
I-133	1.25E+07 (3.38E-01)
I-134	2.42E+06 (6.54E-02)
I-135	7.99E+06 (2.16E-01)
Cs-134	1.68E+07 (4.54E-01)
Cs-136	2.46E+07 (6.65E-01)
Cs-137	1.37E+07 (3.70E-01)
Cs-138	1.18E+07 (3.19E-01)
Rb-86	1.94E+05 (5.24E-03)

Table 9A-2. Iodine Appearance Rates In The Reactor Coolant

Nuclide	Equilibrium Appearance Rate Bq/min (Ci/min)
I-130	3.74E+07 (1.01E-03)
I-131	3.09E+09 (8.35E-02)
I-132	1.39E+10 (3.76E-01)
I-133	7.14E+09 (1.93E-01)
I-134	7.47E+09 (2.02E-01)
I-135	6.44E+09 (1.74E-01)

Table 9A-3. Reactor Core Source Term(1)

Nuclide	Bq (Ci)
Kr-85m	9.32E+17 (2.52E+07)
Kr-85	3.96E+16 (1.07E+06)
Kr-87	1.84E+18 (4.97E+07)
Kr-88	2.46E+18 (6.65E+07)
Xe-131m	3.81E+16 (1.03E+06)
Xe-133m	2.25E+17 (6.08E+06)
Xe-133	7.10E+18 (1.92E+08)
Xe-135m	1.51E+18 (4.08E+07)
Xe-135	1.43E+18 (3.86E+07)
Xe-138	6.14E+18 (1.66E+08)
I-130	6.92E+16 (1.87E+06)
I-131	3.51E+18 (9.49E+07)
I-132	5.11E+18 (1.38E+08)
I-133	7.22E+18 (1.95E+08)
I-134	8.10E+18 (2.19E+08)
I-135	6.85E+18 (1.85E+08)
Cs-134	6.11E+17 (1.65E+07)
Cs-136	1.43E+17 (3.86E+06)
Cs-137	4.03E+17 (1.09E+07)
Cs-138	6.73E+18 (1.82E+08)
Rb-86	6.66E+15 (1.80E+05)

Note:

1. The following assumptions apply:
   - Core thermal power of 3434 MWt (1 percent above the design core power of 3400 MWt). The main feedwater flow measurement supports a 1-percent power uncertainty.
   - Three-region equilibrium cycle core at end of life.

Table 9A-4. Nuclide Parameters

Nuclide	Half Life (sec)	EDE DCF ($Sv•m^3/Bq•sec$)	Adult CEDE DCF (Sv/Bq)	Child CEDE DCF (Sv/Bq)	Ground DCF ($Sv•m^2/Bq•sec$)
Kr-85m	1.61E+04	6.88E-15	0.00E+00	0.00E+00	0.00E+00
Kr-85	3.38E+08	2.40E-16	0.00E+00	0.00E+00	0.00E+00
Kr-87	4.58E+03	3.98E-14	0.00E+00	0.00E+00	0.00E+00
Kr-88	1.02E+04	9.72E-14	0.00E+00	0.00E+00	0.00E+00
Xe-131m	1.03E+06	3.50E-16	0.00E+00	0.00E+00	0.00E+00
Xe-133m	1.89E+05	1.29E-15	0.00E+00	0.00E+00	0.00E+00
Xe-133	4.53E+05	1.34E-15	0.00E+00	0.00E+00	0.00E+00
Xe-135m	9.17E+02	1.90E-14	0.00E+00	0.00E+00	0.00E+00
Xe-135	3.27E+04	1.11E-14	0.00E+00	0.00E+00	0.00E+00
Xe-138	8.50E+02	5.48E-14	0.00E+00	0.00E+00	0.00E+00
I-130	4.45E+04	9.68E-14	1.90E-09	7.40E-09	2.05E-15
I-131	6.95E+05	1.69E-14	2.00E-08	7.20E-08	3.64E-16
I-132	8.28E+03	1.05E-13	3.10E-10	9.60E-10	2.20E-15
I-133	7.49E+04	2.76E-14	4.00E-09	1.80E-08	6.16E-16
I-134	3.16E+03	1.22E-13	1.50E-10	3.70E-10	2.52E-15
I-135	2.38E+04	7.54E-14	9.20E-10	3.70E-09	1.47E-15
Cs-134	6.50E+07	7.07E-14	2.00E-08	6.30E-08	1.48E-15
Cs-136	1.13E+06	9.94E-14	2.80E-09	1.10E-08	2.03E-15
Cs-137	9.46E+08	2.69E-14	3.90E-08	1.00E-07	5.78E-16
Cs-138	1.93E+03	1.15E-13	4.60E-11	2.80E-10	2.26E-15
Rb-86	1.61E+06	4.95E-15	1.30E-09	7.70E-09	1.67E-16

Table 9A-5. Offsite And Onsite Atmospheric Dispersion Factors (X/Q) For Accident Dose Analysis(1)

Offsite χ/Q (s/m^3)	
Containment	1.93×10^{-4}
Building	3.30×10^{-4}
Onsite χ/Q (s/m^3)	
Containment	2.80×10^{-4}
Building	4.65×10^{-4}

Note:

1. LOCA and Rod Ejection assume releases from the containment. All other accidents assume releases from the building.

Table 9A-6. Control Room Atmospheric Dispersion Factors (X/Q) For Accident Dose Analysis

χ/Q (s/m^3) at HVAC Intake for the Identified Release Points[1]						
	Plant Vent or PCS Air Diffuser[3]	Ground Level Containment Release Points[4]	PORV and Safety Valve Releases[5]	Steam Line Break Releases	Fuel Handling Area[6]	Condenser Air Removal Stack[7]
0 – 2 hours	3.0E-3	6.0E-3	2.0E-2	2.4E-2	6.0E-3	6.0E-3
2 – 8 hours	2.5E-3	3.6E-3	1.8E-2	2.0E-2	4.0E-3	4.0E-3
8 – 24 hours	1.0E-3	1.4E-3	7.0E-3	7.5E-3	2.0E-3	2.0E-3
1 – 4 days	8.0E-4	1.8E-3	5.0E-3	5.5E-3	1.5E-3	1.5E-3
4 – 30 days	6.0E-4	1.5E-3	4.5E-3	5.0E-3	1.0E-3	1.0E-3
χ/Q (s/m^3) at Annex Building Door for the Identified Release Points[2]						
	Plant Vent or PCS Air Diffuser[3]	Ground Level Containment Release Points[4]	PORV and Safety Valve Releases[5]	Steam Line Break Releases	Fuel Handling Area[6]	Condenser Air Removal Stack[7]
0 – 2 hours	1.0E-3	1.0E-3	4.0E-3	4.0E-3	6.0E-3	2.0E-2
2 – 8 hours	7.5E-4	7.5E-4	3.2E-3	3.2E-3	4.0E-3	1.8E-2
8 – 24 hours	3.5E-4	3.5E-4	1.2E-3	1.2E-3	2.0E-3	7.0E-3
1 – 4 days	2.8E-4	2.8E-4	1.0E-3	1.0E-3	1.5E-3	5.0E-3
4 – 30 days	2.5E-4	2.5E-4	8.0E-4	8.0E-4	1.0E-3	4.5E-3

1. These dispersion factors are to be used 1) for the time period preceding the isolation of the main control room and actuation of the emergency habitability system, 2) for the time after 72 hours when the compressed air supply in the emergency habitability system would be exhausted and outside air would be drawn into the main control room, and 3) for the determination of control room doses when the non-safety ventilation system is assumed to remain operable such that the emergency habitability system is not actuated.
2. These dispersion factors are to be used when the emergency habitability system is in operation and the only path for outside air to enter the main control room is that due to ingress/egress.
3. These dispersion factors are used for analysis of the doses due to a postulated small line break outside of containment. The plant vent and PCS air diffuser are potential release paths for other postulated events (loss-of-coolant accident, rod ejection accident, and fuel handling accident inside the containment); however, the values are bounded by the dispersion factors for ground level releases.
4. The listed values represent modelling the containment shell as a diffuse area source, and are used for evaluating the doses in the main control room for a loss-of-coolant accident, for the containment leakage of activity following a rod ejection accident, and for a fuel handling accident occurring inside the containment.
5. The listed values bound the dispersion factors for releases from the steam line safety & power-operated relief valves. These dispersion factors would be used for evaluating the doses in the main control room for a steam generator tube rupture, a main steam line break, a locked reactor coolant pump rotor, and for the secondary side release from a rod ejection accident.
6. The listed values bound the dispersion factors for releases from the fuel storage and handling area. The listed values also bound the dispersion factors for releases from the fuel storage area in the event that spent fuel boiling occurs and the fuel building relief panel opens on high temperature. These dispersion factors are used for the fuel handling accident occurring outside containment and for evaluating the impact of releases associated with spent fuel pool boiling.
7. This release point is included for information only as a potential activity release point. None of the design basis accident radiological consequences analyses model release from this point.

Table 9A-7. Control Room Source/Receptor Data For Determination Of Atmospheric Dispersion Factors

Source Description	Release Elevation(1) m (ft)	Horizontal Straight-Line Distance To Receptor		
		Control Room HVAC Intake (Elevation 19.9 m [65.3 ft]) (Δ1)	Annex Building Access (Elevation 1.5 m [4.9 ft]) (Δ2)	Comment
Plant Vent (⬡1)	55.7 (182.8)	44.9 m (147.2 ft)	115.6 m (379.3 ft)	
PCS Air Diffuser (⬡2)	69.8 (229.0)	36.0 m (118.1 ft)	104.6 m (343.2 ft)	
Fuel Building Blowout Panel (⬡3)	17.4 (57.1)	61.9 m (203.2 ft)	130.3 m (427.4 ft)	Note 3
Radwaste Building Truck Staging Area Door (⬡4)	1.5 (4.9)	218.5 ft (66.6 m)	433.5 ft (132.1 m)	Note 3
Steam Vent (⬡5)	17.1 (56.1)	18.8 m (61.5 ft)	79.7 m (261.6 ft)	
PORV/Safety Valves (⬡6)	19.2 (63.0)	20.4 m (66.9 ft)	77.8 m (255.4 ft)	
Condenser Air Removal Stack (⬡7)	47.9 (157.2)	97.5 m (319.9 ft)	36.6 m (120.0 ft)	Note 3
Containment Shell (Diffuse Area Source) (⬡8)	Same as Receptor Elevation (19.9 m [65.3 ft] or 1.5 m [4.9 ft])	12.8 m (42.0 ft)	83.0 m (272.3 ft)	Note 2

Notes:
1. All elevations relative to grade at 0.0 m.
2. For calculating distance, the source is defined as the point on the containment shell closest to receptor.
3. Vertical distance travelled is conservatively neglected.
4. ⬡ – Refer to Symbols on Figure 9A-1.
5. Δ – Refer to Symbols on Figure 9A-1.

Table 9A-8 (Sheet 1 of 2). Assumptions And Parameters Used In Calculating Control Room Doses

– Main control room volume, m^3 (ft^3)	1.011E3 (3.57E4)
– Volume of HVAC, including main control room and control support area, m^3 (ft^3)	2.987E3 (1.055E5)
– Atmospheric dispersion factors (sec/m^3)	See Table 9A-6
– Occupancy	
• 0 - 24 hr	1.0
• 24 - 96 hr	0.6
• 96 - 720 hr	0.4
– Breathing rate (m^3/sec)	3.1E-04
Normal HVAC operation	
• Air intake flow, m^3/sec (ft^3/min)	9.085E-01 (1.925E3)
• Filter efficiency	Not applicable
Control room with emergency habitability system credited (VES Credited)	
– Main control room activity level at which the emergency habitability system actuation is actuated, Bq/m^3 (Ci/m^3)of dose equivalent I-131)	7.4E4 (2.0E-6)
– Response time to actuate VES based on radiation monitor response time and VBS isolation (sec)	180
– Interval with operation of the emergency habitability system	
• Flow from compressed air bottles of the emergency habitability system, m^3/sec (ft^3/min)	2.832E-02 (60)
• Unfiltered inleakage via ingress/egress & from other sources, m^3/sec (ft^3/min)	7.079E-03 (15)
• Recirculation flow through filters, m^3/sec (ft^3/min)	2.832E-01 (600)
• Filter efficiency (%)	
–Elemental iodine	90
–Organic iodine	30
–Particulates	99
– Time at which the compressed air supply of the emergency habitability system is depleted (hr)	72
– After depletion of emergency habitability system bottled air supply (>72 hr)	
• Air intake flow, m^3/sec (ft^3/min)	8.023E-01 (1700)
• Intake flow filter efficiency (%)	Not applicable
• Recirculation flow, m^3/sec (ft^3/min)	Not applicable
– Time at which the compressed air supply is restored and emergency habitability system returns to operation (hr)	168

Table 9A-8 (Sheet 2 of 2). Assumptions And Parameters Used In Calculating Control Room Doses

Control room with credit for continued operation of HVAC (VBS Supplemental Filtration Mode Credited)	
– Time delay to switch from normal operation to the supplemental air filtration mode (sec)	60
– Unfiltered air inleakage, m^3/sec (ft^3/min)	1.180E-02 (25)
– Filtered air intake flow, m^3/sec (ft^3/min)	4.059E-01 (860)
– Filtered air recirculation flow, m^3/sec (ft^3/min)	1.293E0 (2740)
– Filter efficiency (%)	
• Elemental iodine	90
• Organic iodine	90
• Particulates	99

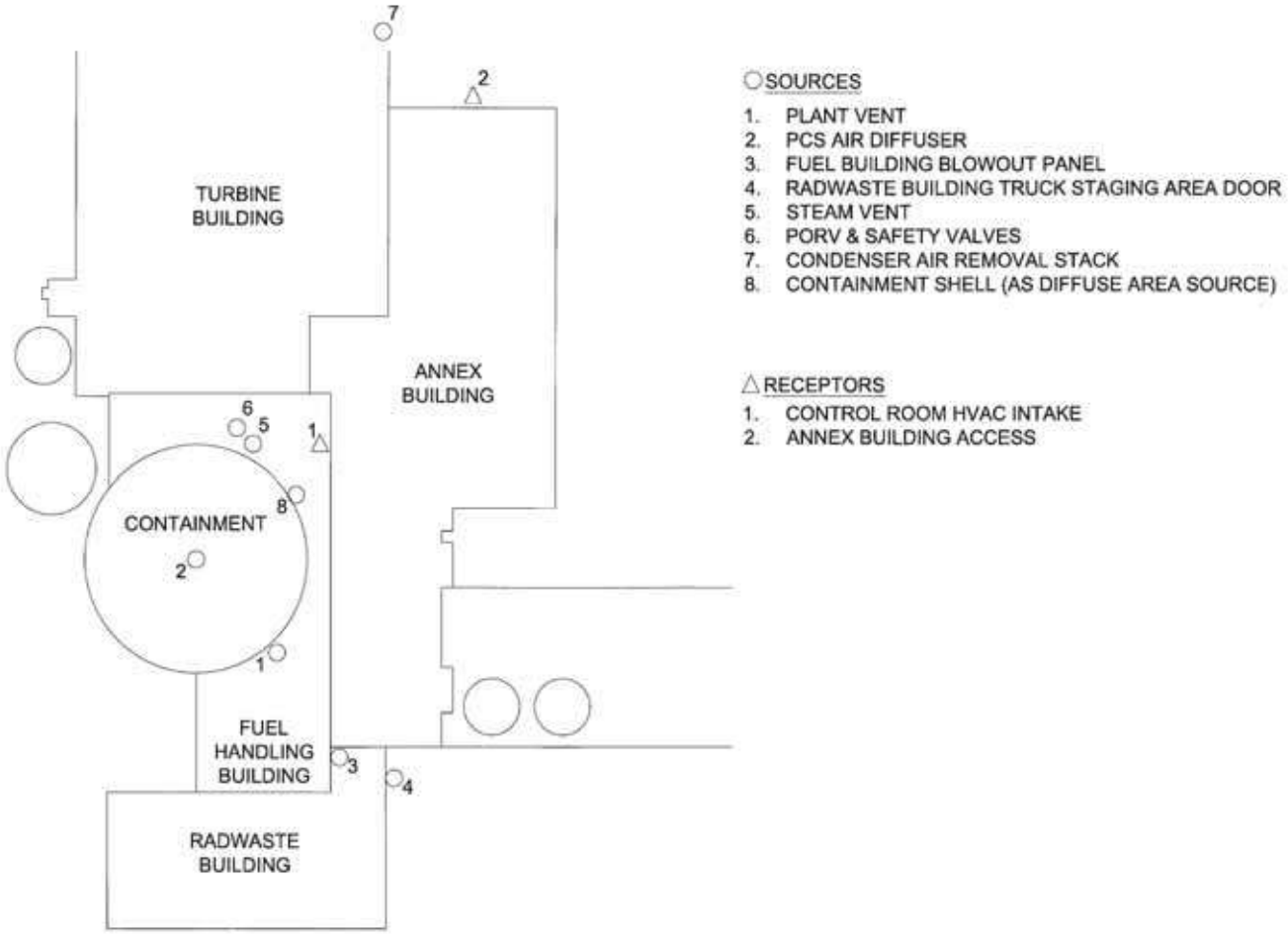


Figure 9A-1. Site Plan with Release and Intake Locations

9B Code Verification and Validation

9B.1 Introduction

The description of the design basis analysis of bounding faults presented in the main body of Chapter 9 shows that the analyses utilise computer codes extensively to demonstrate compliance with AP1000 plant design criteria. Assurance of the validity of such analyses relies on systematic and thorough verification and validation of the computer codes employed. The HSE nuclear division (ND) technical assessment guide T/AST/042 (Reference 9B-1) defines verification and validation as follows:

- **Verification** is the process of ensuring that the controlling physical equations have been correctly translated into computer code or, in the case of hand calculations, correctly incorporated into the calculational procedures.

- **Validation** is the testing and evaluation of the whole system at the completion of its development to ensure compliance with the requirements specified. In fault analysis, validation can be defined as the evidence which demonstrates that the computer code or calculational method is correct by comparison of models with experimental or other available data.

The term evaluation model (EM) is used for the calculational framework for evaluating the behaviour of the reactor system during a postulated transient or design-basis accident. As such, the EM may include one or more computer programmes, special models, and all other information needed to apply the calculation methodology to a specific event. Most EMs used to analyse transient events rely on a systems codes that describe the transport of fluid mass, momentum, and energy throughout the reactor coolant systems. The extent and complexity of the physical models needed in the systems code are strongly dependent on the reactor design and the transient being analysed. Often a general purpose systems code may be developed to address similar phenomenological aspects of several diverse classes of transients. This presents unique challenges in the definition, development, assessment, and review of those codes as they apply to a particular transient EM. The NRC refers to the latter activities under the acronym EMDAP (Evaluation Model Development and Review Process) and has issued guidelines as to how this should be conducted and due process demonstrated. EMDAP comprises four sequential elements, which enable a decision to be made concerning the adequacy of the EM (see Figure 9B-1).

The development of a phenomena identification and ranking table (PIRT) is a significant component of element 1 of the EMDAP process. The PIRT provides a means to identify and classify, in terms of importance, the thermal-hydraulic phenomena expected to occur in transients and accidents that must be included in the analytical models, and for which data must, therefore, be available to evaluate those analytical models. Section 2 of WCAP-15613 (Reference 9B-2) contains separate PIRTs for LBLOCAs, SBLOCAs, and non-LOCA transients for the AP1000 plant design, as well as those for the AP600 plant design.

Element 2 of EMDAP requires the establishment of an adequate experimental database for the EM assessment and development process. In particular, separate effects experiments are needed to develop and assess empirical correlations and other closure models used within the EM. Also, integral systems tests are undertaken to assess system interactions and global code capability. It needs to be demonstrated that the experimental facilities used to obtain relevant data are scaled appropriately to minimise any distortions introduced by the reduction in geometrical size.

For PWR systems in general, few full scale (geometrical) primary circuit transient experiments have been performed (largely on grounds of rig construction and operating costs) and consequently the majority of the pertinent integral experimental data has been obtained at smaller scales. Even where, in some cases, the experimental rig has been engineered to replicate the scale of the full size plant in one dimension (e.g., by retaining full height to faithfully replicate gravitational effects), design constraints dictate a reduction in scale in the other two dimensions. The effect of scaling is therefore an important issue and the objectives of scaling analysis are to identify:

(a) Design parameters for reduced-size test facilities;

(b) Conditions for operating experiments, such that at least the dominant phenomena taking place in the full-size plant are reproduced in the experimental facility, over the range of plant conditions;

(c) Non-dimensional parameters which facilitate the efficient and compact presentation and correlation of experimental results which, by virtue of similarity and the parameter selection, apply to many systems, including both the test facility and the full-size plant;

(d) The extent of scale distortion and the uncertainty that this may introduce in assessments made using the EM.

A number of methodologies which aim to meet the objectives (a) to (d) above have been described in the literature. The approach used initially for AP600 and latterly for AP1000, has followed Zuber's H2TS system. H2TS is the scaling method expounded by Zuber (References 9B-3 and 9B-4), originally for severe accident type scenarios, but it has a very general applicability to complex systems. Zuber's presentation of the methodology (References 9B-3 and 9B-4) is generalised and consequently is not easy to follow in terms of its direct applicability to PWR analysis. The application of the principles however, was placed on a firmer foundation by Reyes (Reference 9B-5) in the context of the scaling analysis of the OSU AP600 test facility APEX. Further work extended the scaling analysis to AP1000 (Reference 9B-6).

The development of the EM model, which includes aspects such as the model representation of the plant or individual components and nodalisation scheme, are included within element 3.

Element 4 of EMDAP covers the appropriate comparisons between experiment and calculation that establish the extent of the applicability, fidelity, accuracy, and scalability of the EM for its intended purpose.

It is considered that EMDAP fully addresses the following principles relating to the assurance of validity of data and models as identified in the ONR SAPs (Reference 9B-7).

AV.1 Theoretical models should adequately represent the facility and site.

AV.2 Calculational methods used for the analyses should adequately represent the physical and chemical processes taking place.

AV.3 The data used in the analysis of performance with safety significance should be shown to be valid for the circumstances by reference to established physical data, experiment or other appropriate means

AV.6 Studies should be carried out to determine the sensitivity of the analysis (and the conclusions drawn from it) to the assumptions made, the data used and the methods of calculation.

The following sections of this appendix provide a brief summary of the codes used to perform design basis fault transient analysis and provide the link to external documented evidence (as required by SAP AV.5) that should facilitate independent review of the adequacy of the EM models and data. Quality assurance procedures implemented by Westinghouse for computer models and datasets used to support the analysis (as required by SAP AV.4) are outlined. Provision for data collection throughout the operational life of a facility (SAP AV.7) and update and review of the fault analysis (SAP AV.8) is also mentioned.

9B.2 Brief Description of Codes Used in Fault Studies Analysis

9B.2.1 LOFTRAN

The LOFTRAN (Reference 9B-8) programme is used for studies of transient response of a pressurised water reactor system to specified perturbations in process parameters. LOFTRAN simulates a multi-loop system by a model containing reactor vessel, hot and cold leg piping, steam generator (tube and shell sides), and pressuriser. The pressuriser heaters, spray, and safety valves are also considered in the programme. Point model neutron kinetics, and reactivity effects of the moderator, fuel, boron, and rods are included. The secondary side of the steam generator uses a homogeneous, saturated mixture for the thermal transients and a water level correlation for indication and control. The protection and safety monitoring system is simulated to include reactor trips on high neutron flux, over temperature ΔT, high and low pressure, low reactor coolant flow, and high pressuriser level. Control systems are also simulated, including rod control, turbine bypass, feedwater control, and pressuriser level and pressure control. The emergency core cooling system, including the accumulators, is also modelled. LOFTRAN is a versatile programme, suited to accident evaluation and control studies, as well as parameter sizing. LOFTRAN also has the capability of calculating the transient value of DNBR based on the input from the core limits. The core limits represent the minimum value of DNBR as calculated for typical or thimble cell. The LOFTRAN code is modified to allow the simulation of the PRHR heat exchanger, CMTs, and associated protection and safety monitoring system actuation logic.

A discussion of these models and additional validation is presented in WCAP-14234 (Reference 9B-9).

9B.2.2 FACTRAN

FACTRAN (Reference 9B-10) calculates the transient temperature distribution in a cross section of a metal-clad UO2 fuel rod and the transient heat flux at the surface of the cladding using as input the nuclear power and the time-dependent coolant parameters (pressure, flow, temperature, and density). The code uses a fuel model which simultaneously exhibits the following features:

- A sufficiently large number of radial space increments to handle fast transients such as rod ejection accidents

- The necessary calculations to handle post-DNB transients: film boiling heat transfer correlations, zircaloy-water reaction, and partial melting of the materials

FACTRAN is further discussed in WCAP-7908-A (Reference 9B-10).

9B.2.3 NOTRUMP

NOTRUMP (References 9B-18 and 9B-19) is a general one-dimensional nodal network code. NOTRUMP is used in the analysis of DBA small and medium break LOCAs in the reactor coolant system. A detailed description of the code as it relates to these analyses is presented in Section 9.6.5.2.1.

In ATWT analyses, NOTRUMP is used to calculate steam generator tube bundle heat transfer degradation as inventory is depleted in the secondary-side of the steam generator and to correlate steam generator inventory with actual and measured secondary-side level.

Important phenomena for calculating steam generator transients are addressed in NOTRUMP and include single and two-phase flow, heat transfer through the steam generator tube bundle, critical flow, and special steam generator separator models for mechanical separation of fluid phases. The code-modelling concept is one of using multiple independent fluid control volumes (nodes) interconnected by appropriate flow paths (flow links) to allow mass and energy exchange. NOTRUMP uses a control volume model that has options to simulate either a single homogeneous region within a control volume or two separate regions (upper and lower regions) within a control volume including a distinct mixture level. The volume of each of the regions within a control volume can vary with time and the regions can be in thermal non-equilibrium with each other. Flows and pressure drops associated with the flow paths are applied one-dimensionally between the control volumes. The flow path model includes options for calculating the pressure drop for cross flow and parallel flow in a steam generator tube bundle. The NOTRUMP code includes many slip and drift flux correlations which are used to calculate the flow quality in the flow paths.

In the ATWT NOTRUMP model, the primary side of the steam generator tube bundle, the heat transfer through the tube walls, and the secondary side of the steam generator is simulated. Heat transfer from the tube bundle into control volumes is determined from the local primary and secondary-side control volume fluid conditions and tube wall characteristics. The code includes heat transfer correlations appropriate for single-phase convection heat transfer and pool-boiling heat transfer. Boundary conditions to the NOTRUMP steam generator model are supplied by the system code LOFTRAN. The boundary conditions consist of the reactor coolant flow, temperature and pressure entering the primary side of the steam generator tubes. On the secondary side of the NOTRUMP steam generator model, feedwater flow and steam system flow are supplied as boundary conditions.

9B.2.4 VIPRE-01

The VIPRE-01 core model as approved by the NRC (Reference 9B-11) is used with the applicable DNB correlations to determine DNBR distributions along the hot channels of the reactor core under all expected operating conditions. The VIPRE-01 modelling method is described in Reference 9B-11, including empirical models and correlations used. The effect of crud on the flow and enthalpy distribution in the core is not directly accounted for in the VIPRE-01 evaluations. However, conservative treatment by the Westinghouse VIPRE-01 modelling method has been demonstrated to bound this effect in DNBR calculations (Reference 9B-11).

Extensive additional experimental verification of VIPRE-01 is presented in Reference 9B-12. The VIPRE-01 analysis is based on a knowledge and understanding of the heat transfer and hydrodynamic behaviour of the coolant flow and the mechanical characteristics of the fuel elements. The use of the VIPRE-01 analysis provides a realistic evaluation of the core performance.

VIPRE-01 is capable of transient DNB analysis. The conservation equations in the VIPRE-01 code contain the necessary accumulation terms for transient calculations. The input description can include one or more of the following time dependent arrays:

1. Inlet flow variation
2. Core heat flux variation
3. Core pressure variation
4. Inlet temperature or enthalpy variation

At the beginning of the transient, the calculation procedure is carried out as in the steady state analysis. The time is incremented by an amount determined either by the user or by the time step control options in the code itself. At each new time step the calculations are carried out with the addition of the accumulation terms which are evaluated using the information from the previous time step. This procedure is continued until a pre-set maximum time is reached. At time intervals selected by the user, a complete description of the coolant parameter distributions, as well as DNBR, is printed out. In this manner the variation of any parameter with time can be readily determined.

The VIPRE-01 code is described in detail in Reference 9B-12, including discussions on code validation with experimental data.

9B.2.5 WGOTHIC

WGOTHIC is used for the licensing basis analyses of LOCA and secondary side high energy line breaks to predict containment temperatures and pressures. WGOTHIC is also used to predict containment temperature and pressure increases due to mass and energy releases to the containment during other non-LOCA and ATWT events. During non-LOCA and ATWT events, heat transfer through the PRHR heat exchanger into the IRWST can cause steaming from the IRWST into containment. Fluid releases through the pressuriser safety valves into the containment may occur during ATWT events.

The Westinghouse GOTHIC (WGOTHIC) computer code (Reference 9B-13) is a computer programme for modelling multiphase flow in a containment transient analysis. It solves the conservation equations in integral form for mass, energy, and momentum for multi-component flow. The momentum conservation equations are written separately for each phase in the flow field (drops, liquid pools, and atmosphere vapour). The following terms are included in the momentum equation: storage, convection, surface stress, body force, boundary source, phase interface source, and equipment source.

To model the passive cooling features of the AP1000, several assumptions are made in creating the plant input. The external cooling water does not completely wet the containment shell; therefore, both wet and dry sections of the shell are modelled in the WGOTHIC analyses. The analyses use conservative coverage fractions to determine evaporative cooling. Heat conduction from the dry to wet section is considered in the analysis. The combination of passive containment cooling system coverage area and heat conduction from the dry to wet sections is explained in Chapter 7 of Reference 9B-13. The effects of water flowing down the shell from gravitational forces are explicitly considered in the analysis. The passive internal containment heat sink data used in the WGOTHIC analyses is presented in Reference 9B-13, Chapter 13. Data for both metallic and concrete heat sinks are presented.

9B.2.6 RELAP

The RELAP family of codes was developed to perform analyses of postulated accidents in nuclear power plants. The RELAP5 (Reference 9B-14) computer code performs calculations

to simulate multi-dimensional thermal-hydraulics, heat transfer, and control systems. The thermal hydraulics behaviour under single phase and two phase conditions is simulated. The hydrodynamics models track the flow of liquid, vapour and non-condensable gases. RELAP5 includes component models of valves, separators, dryers, pumps, electric heaters, turbines, and accumulators. The control system models include functions for trip logic and arithmetic functions for simulation of system filters.

Some of the non-LOCA events, such as loss of reactor coolant flow, have a small amount of steam voids generated in the core. The LOFTRAN model assumes homogeneous flow in the RCS outside the reactor vessel. The validity of the LOFTRAN model for these cases has been verified by analysis with RELAP or a LOCA code such as NOTRUMP.

For RCS depressurisation, a LOCA code such as RELAP is used when void formation in the RCS goes beyond the point where LOFTRAN is useful.

9B.2.7 TWINKLE

This multidimensional spatial neutronics code uses an implicit finite-difference method to solve the two-group transient neutronics equations in one, two, and three dimensions. TWINKLE (Reference 9B-15) can be used to calculate the kinetic response of a reactor for transients, such as the RCCA bank withdrawal from subcritical conditions and RCCA ejection events, which cause a major perturbation in the spatial neutron flux distribution. As documented in Reference 9B-15 the NRC has approved this code for operating Westinghouse plants. Since the AP1000 fuel design is similar to that of operating Westinghouse plants (i.e., falls within the NRC-approved applicable range of the code), the application of the TWINKLE code to the AP1000 for analysis of kinetic responses is acceptable.

9B.2.8 WCOBRA/TRAC

WCOBRA/TRAC is a thermal-hydraulic computer code that calculates realistic fluid conditions in a PWR during the blowdown and reflood of a postulated large-break LOCA. The methodology used for the AP1000 analysis is documented in WCAP-12945-P-A, WCAP-14171, Revision 2, WCAP-16009-P-A (References 9B-20, 9B-21 and 9B-22), and Reference 9B-23.

WCOBRA/TRAC is used in the analysis of Large Break LOCAs and a description of the code is presented in Section 9.6.4.1.1.

9B.2.9 Data Transfer Between Codes

See Figure 9B-2.

9B.3 Code Validation and Verification

Reference 9B-17 documents an assessment performed by Westinghouse of the safety analysis codes that were developed and approved for the AP600 plant to determine their applicability and use for the AP1000 plant. The analysis codes that were approved for the purpose of performing safety analyses of the AP600 passive plant are:

- LOFTRAN – transient analyses
- NOTRUMP – small-break LOCA analyses
- WCOBRA/TRAC – large-break LOCA and long-term cooling analyses
- WGOTHIC – containment analyses

9B.4 Quality Assurance Arrangements

The Westinghouse Quality Management System and Westinghouse Level 2 Policies and Procedures provide the governing procedures, including those for software control. The Level 2 software control procedures include processes for development, validation, configuration control, software error reporting, and maintenance. These procedures are utilised for all safety-related software applications, such as the safety analysis codes.

9B.5 Ongoing Data Collection Throughout Facility Life

A database of inputs to the safety analyses has been created for the standard plant and can be maintained on a plant-specific basis. Changes to the safety analysis data can be evaluated via the safety evaluation process.

9B.6 Update and Periodic Review of Safety Analysis

Safety analyses can be reviewed periodically, typically on a reload basis, for important reload parameter changes and for errors that have been identified.

9B.7 References

9B-1 HSE ND Technical Assessment Guide T/AST/042, "Containment: Validation of Computer Codes and Calculational Methods," Issue 001, 10 July 2000.

9B-2 Westinghouse Document WCAP-15613, Rev. 0, "AP1000 PIRT and Scaling Assessment Report," March 2001.

9B-3 NUREG/CR-5809, "A Hierarchical, Two-Tiered Scaling Analysis," Appendix D, U.S. Nuclear Regulatory Commission, November 1991.

9B-4 Zuber N., et al., "An Integrated Structure and Scaling Methodology for Severe Accident Technical Issue Resolution: Development of Methodology," *Nuclear Engineering and Design*, 186, pp. 1-21, 1998.

9B-5 Reyes J. N., Hochreiter L. "Scaling Analysis for the OSU AP600 Test Facility (APEX)," *Nuclear Engineering and Design*, 186, pp. 53–109, 1998.

9B-6 NUREG-1826, "APEX-AP1000 Confirmatory Testing To Support AP1000 Design Certification (Non-Proprietary)," U.S. Nuclear Regulatory Commission, August 2005.

9B-7 ONR "Safety Assessment Principles for Nuclear Facilities," Rev. 0, Office of Nuclear Regulation, 2014.

9B-8 Westinghouse Documents WCAP-7907-P-A, Rev. 0 (Proprietary) and WCAP-7907-A, Rev. 0 (Non-Proprietary), "LOFTRAN Code Description," April 1984.

9B-9 Westinghouse Documents WCAP-14234, Rev. 1 (Proprietary) and WCAP-14235, Rev. 1 (Non-Proprietary), "LOFTRAN and LOFTTR2 AP600 Code Applicability Document," August 1997.

9B-10 Westinghouse Document WCAP-7908-A, Rev. 0 (Non-Proprietary), "FACTRAN A FORTRAN-IV Code for Thermal Transients in a UO_2 Fuel Rod," December 1989.

9B-11 Westinghouse Document WCAP-14565-P-A, Rev. 0 (Proprietary), and WCAP-15306-NP-A, Rev. 0 (Non-Proprietary), "VIPRE-01 Modeling and Qualification for Pressurized Water Reactor Non-LOCA Thermal-Hydraulic Safety Analysis," October 1999.

9B-12 NP-2511-CCM-A, "VIPRE-01: A Thermal-Hydraulic Code for Reactor Core," Volume 1-3 (Revision 3, August 1989), Volume 4 (April 1987), Electric Power Research Institute, Stewart, C. W., et al.

9B-13 Westinghouse Documents WCAP-15846, Rev. 5 (Proprietary) and WCAP-15862, Rev. 5 (Non-Proprietary), "WGOTHIC Application to AP600 and AP1000," September 2016.

9B-14 NUREG/CR-5535, EGG-2596, "RELAP5/MOD3 Code Manual," EG&G Idaho, Inc, June 1990.

9B-15 Westinghouse Documents WCAP-7979-P-A, Rev. 0 (Proprietary) and WCAP-8028-NP-A, Rev. 0 (Non-Proprietary), "TWINKLE – A Multi-Dimensional Neutron Kinetics Computer Code," January 1975.

9B-16 Not Used.

9B-17 Westinghouse Documents WCAP-15644-P, Rev. 2 (Proprietary) and WCAP-15644-NP, Rev. 2, (Non-Proprietary), "AP1000 Code Applicability Report," March 2004.

9B-18 Westinghouse Documents WCAP-10079-P-A, Rev. 0 (Proprietary) and WCAP-10080-A (Non-Proprietary), "NOTRUMP A Nodal Transient Small Break and General Network Code," August 1985.

9B-19 Westinghouse Documents WCAP-10054-P-A, Rev. 0 (Proprietary) and WCAP-10081-A, (Proprietary), "Westinghouse Small Break ECCS Evaluation Model Using the NOTRUMP Code," August 1985.

9B-20 Westinghouse Documents WCAP-12945-P-A (Proprietary) (Volume 1 - Revision 2; Volumes 2 through 5 - Revision 1) and WCAP-14747 (Non-Proprietary), "Code Qualification Document for Best Estimate LOCA Analysis," 1998.

9B-21 Westinghouse Documents WCAP-14171, Rev. 2 (Proprietary) and WCAP-14172, Rev. 2 (Non-Proprietary), "WCOBRA/TRAC Applicability to AP600 Large-Break Loss-of-Coolant Accident," March 1998.

9B-22 Westinghouse Documents WCAP-16009-P-A, Rev. 0 (Proprietary) and WCAP-16009-NP-A, Rev. 0 (Non-Proprietary), "Realistic Large-Break LOCA Evaluation Methodology Using the Automated Statistical Treatment Of Uncertainty Method (ASTRUM)," January 2005.

9B-23 Westinghouse Letter LTR-NRC-12-86, "Westinghouse Response to NRC RAIs on WCAP-17524, 'AP1000 Core Reference Report' (Proprietary/Non-Proprietary)," January 2, 2013.

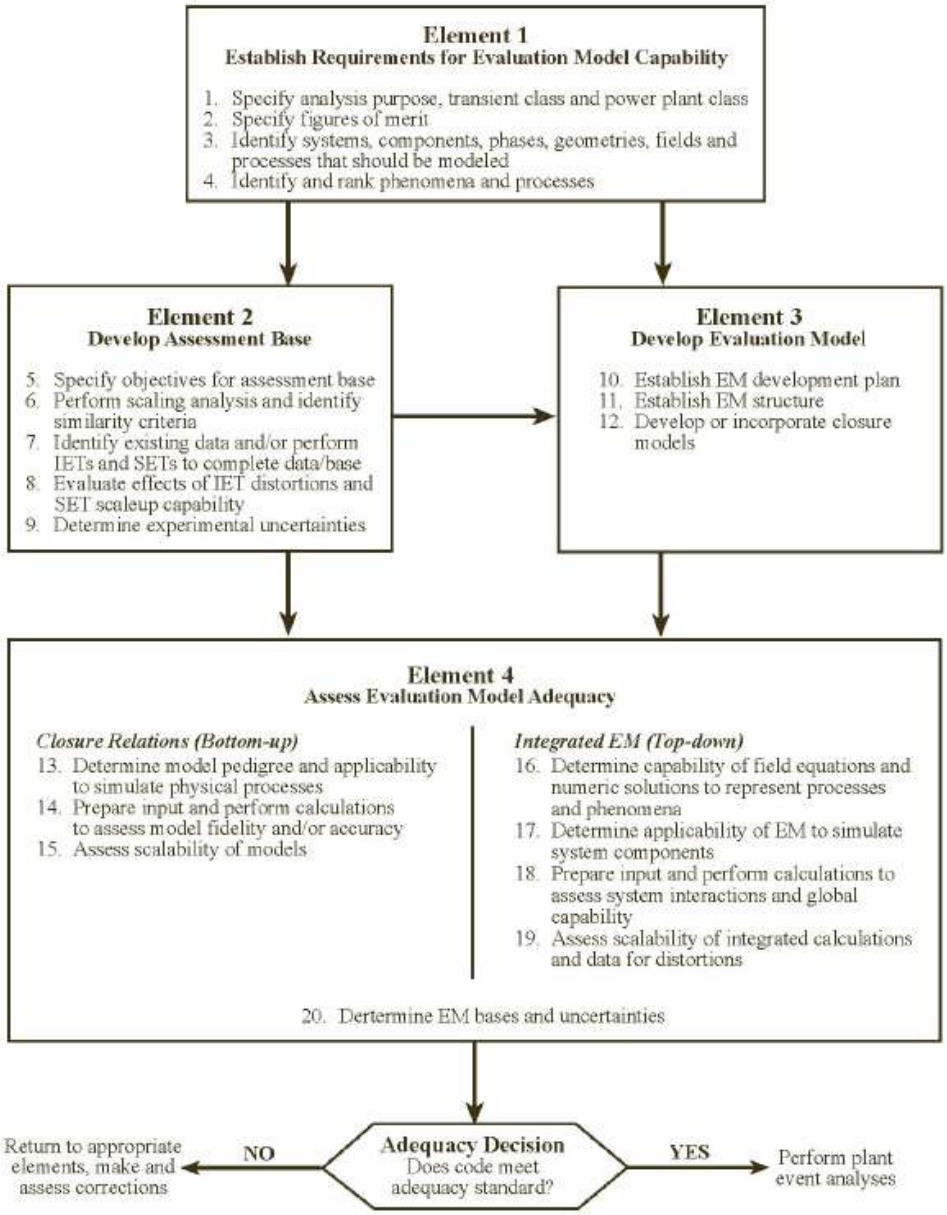


Figure 9B-1. Flowchart Outlining the EMDAP Process

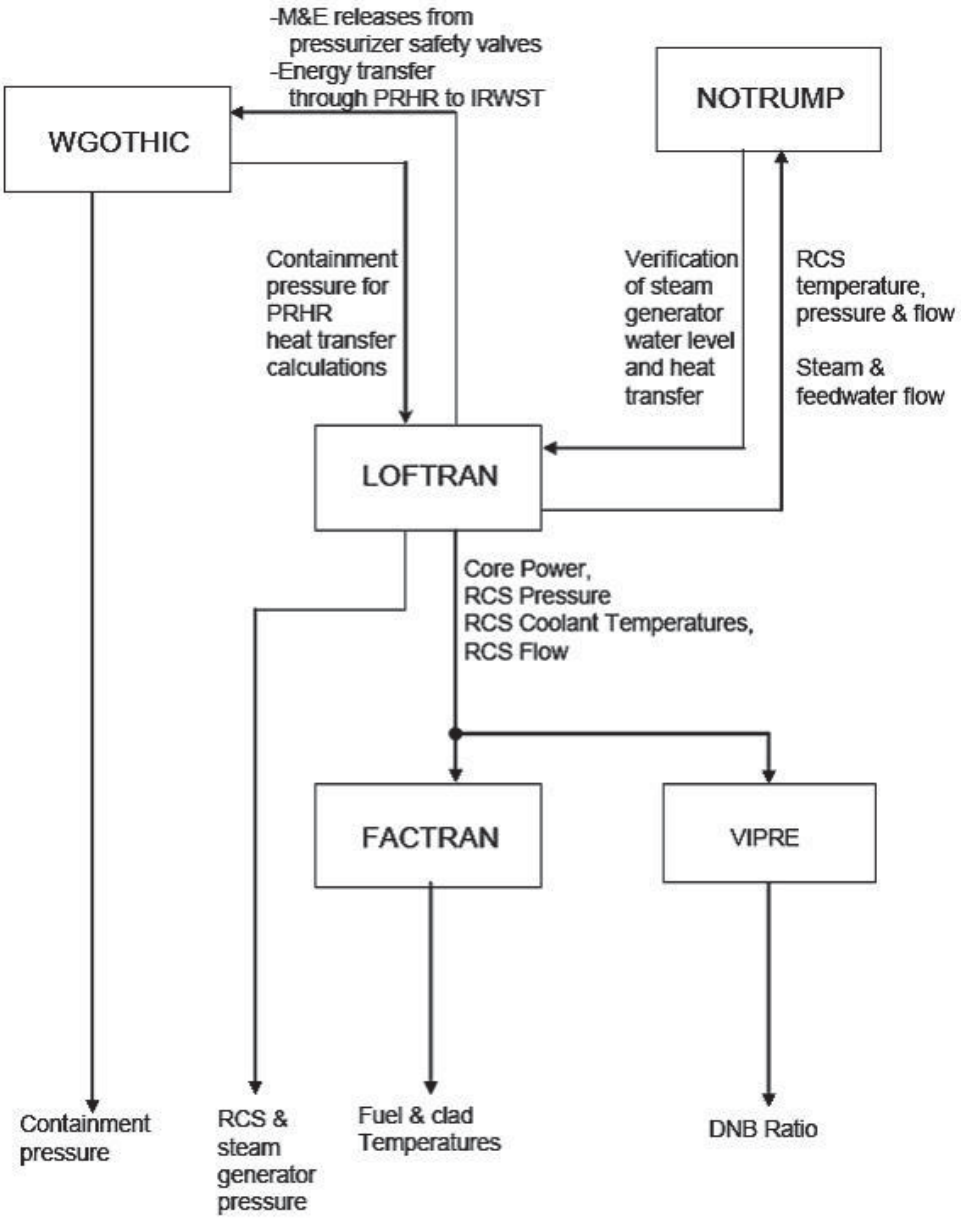


Figure 9B-2. Data Transfer Between Codes

9C Assessment of Safe Shutdown for Design Basis Faults

9C.1 Introduction

This appendix demonstrates the ability of the AP1000 plant to achieve a safe shutdown state following design basis faults. The short term mitigation of design basis faults is presented in the various detailed accident analyses contained within Chapter 9. This appendix shows that the plant can transition from the conditions after short term mitigation to a safe shutdown state.

Table 8A-2 lists all of the AP1000 design basis faults. For these faults, the plant will eventually reach one of two different end states, considering the type of initiating event and the Class 1 passive systems used to mitigate the event. Those two end states are:

1. The RCS pressure boundary is intact with closed loop cooling provided by the PRHR HX

2. The RCS pressure boundary is not intact with open loop cooling provided by ADS and PXS injection

End state 1 usually occurs after intact circuit (i.e., non-LOCA) faults, such as loss of main feedwater. However, it also occurs after a SGTR; this fault generally behaves like an intact circuit fault because the PRHR HX operation automatically terminates the RCS leak into the SG.

End state 2 usually occurs after open circuit faults such as LOCAs. However, it is also the credited diverse means of core cooling for frequent fault intact circuit faults. This diverse means of core cooling for intact circuit faults uses the same SSCs that are used for the non-intact circuit faults except for the C&I functionality, where DAS is used instead of PMS. Because of the design of DAS, some actuations are manual. There is a variation in end state 2 that applies to frequent fault small-break LOCAs, which relies on the use of the Class 2 RNS for injection and diverse portions of the Class 1 passive features.

Section 9C.2 describes the operation of different systems and components used in achieving safe shutdown for these faults. This section includes discussion on the primary Class 1 passive SSCs as well as the limited use of Class 2 SSCs to support claims for diverse mitigation of frequent faults.

Limiting faults have been analysed in order to bound all other design basis faults. Section 9C.3 describes the behaviour and analysis results of the AP1000 plant during mitigation of faults on the path to reaching safe shutdown. UKP-PXS-GLR-001 (Reference 9C-1) summarizes the basis supporting the condensate return analysis including relevant documentation regarding identification of important phenomena, design changes, and analyses demonstrating long term PRHR HX operation.

Note that the AP1000 plant has a list of operating modes that are used in the Technical Specifications (see Table 8A-1). One of those modes is called “Safe Shutdown”. This mode only applies to normal operation and does not apply to post faults conditions; as a result, it does not apply to the safe shutdown discussion in this appendix.

9C.1.1 Safe Shutdown Considerations

Acceptance Criteria

Chapter 9 presents the accident analyses for design basis faults that challenge the reactor from a thermal hydraulic perspective. At the end of each of these analyses the plant has achieved a safe, stable state with the reactor subcritical and all applicable safety criteria limits met. These short-term acceptance criteria vary based on the initiating event, and are summarised in Table 9.0-3; additionally, they are clarified as part of each individual analysis discussion throughout Chapter 9.

Following the end of these accident analyses, it is required to demonstrate that the plant transitions to the safe shutdown condition. This transition involves reducing the RCS temperature to less than 216ºC (420ºF) while maintaining the reactor subcritical and continuing to satisfy all other applicable safety criteria, as noted above. Regardless of initiating event, once the plant reaches an open loop cooling state, core cooling is maintained for an indefinite time.

As intact circuit faults may eventually require open loop cooling in the event that offsite power is not restored after an extended duration, the acceptance criteria for these faults (Table 9C.3-4) also includes the ADS actuation criteria. This progression from intact RCS conditions with the PRHR HX removing decay heat to open loop cooling with operation of ADS and passive injection is always available. The emergency procedures direct the operators to initiate open loop cooling in the longer term based on specific plant parameters, primarily high RCS temperature or pressure (Reference 9C-4).

Transition Time to Safe Shutdown

The duration of the cooldown for the plant to transition from this safe, stable state in the short-term to the final safe shutdown condition varies based on the initiating event. Some transition times include:

1. Infrequent fault LOCAs (breaks greater than 5.1 cm [2 inch]) – Less than 1 hour
2. Frequent fault small-break LOCAs (and RCS leaks) - Several hours to several days
3. Intact circuit faults – More than 72 hours

All of these transition times are demonstrated to be safe and are considered adequate.

Consequential Faults While At Safe Shutdown Conditions

There is a potential concern with long transition times in that there may be a risk of an independent event occurring during that time. However, most initiating events are not applicable once the reactor is shutdown and passive Class 1 SSCs are in use. Examples of such faults include:

- Loss of offsite power
    - The reactor and the RCPs are shutdown and AC power is not used to support passive system operation
- Loss of non-Class 1 systems required for normal plant operation such as main feedwater, condenser cooling, auxiliary cooling water systems, HVAC, instrument air, etc.

  - None of these non-Class 1 systems are used to support passive system operation

- Reactivity faults such as RCCA withdrawal, boron dilution, etc.
  - The RCCAs are inserted and boron dilution sources are isolated.

The remaining fault of concern is a LOCA occurring following an intact circuit fault with extended loss of ac power. Smaller LOCAs, the most likely fault based on event frequency, have an initiating event frequency in the range of 1E-03 to 1E-04 per year (Table 8A-2). If the RCS remained near normal operating pressures and temperatures for an extended time following an intact circuit fault, a small LOCA might occur. However, the risk of a small LOCA occurring following an intact circuit fault is acceptably low based on the following:

- Assuming conservative, bounding intact circuit operation (including high decay heat and minimum PRHR performance) the RCS temperature will be near normal hot standby temperatures and the RCS pressure will drop to about saturation, less than 11.0 MPa (1600 psia) (Reference 9C-1). However, the plant will eventually see an increase in the RCS pressure and temperature due to a decrease in the IRWST level and uncovery of the PRHR tubes; Supporting analyses discussed in Reference 9C-1 indicate this could occur in approximately 7 days or longer. The plant operators would then manually initiate passive feed and bleed operation based on their emergency procedures.
- Assuming realistic intact circuit operation (including expected decay heat and PRHR performance) the RCS temperature and pressure would reduce to a significantly lower value (less than the safe shutdown temperature of 216ºC [420ºF]) within 36 hours. This condition can be maintained for greater than 14 days, and supporting analyses discussed in Reference 9C-1 indicate approximately 30 days or longer. Eventually, the RCS pressure and temperature will increase due to a decrease in the IRWST level and uncovery of the PRHR tubes.

It should also be recognized that operation of the PRHR during intact circuit faults is considered a success path in Chapter 8 and in the PSA. In both Chapter 8 frequent fault sequences and in the PSA, the PRHR is claimed as a success path and open loop passive feed and bleed is a diverse backup. In both of these situations the use of realistic analysis assumptions is appropriate. Also note that Reference 9C-1 shows that the probability of the PRHR operation duration being limited by conservative bounding assumption is very low and need not be considered in either of these situations.

9C.2 Required SSCs to Achieve Safe Shutdown

This section describes the different SSCs that are used to establish safe shutdown conditions for the plant following different types of initiating events. Generally, these SSCs are actuated automatically and no operator actions are required. The Class 1 SSCs relied upon for safe shutdown are listed in Table 9C.1-1. The limited Class 2 SSCs relied upon for diverse safe shutdown capabilities are included in Tables 9C.3-1 and 9C.3-2. Additionally, the AP1000 plant design also has defence in depth features that can support safe shutdown; however, they are not credited in the deterministic UK safety case and are provided as a demonstration of additional means of protection.

9C.2.1 Safe Shutdown Using Primary and Diverse Means

Class 1 passive systems provide the primary means to achieve safe shutdown. For frequent faults, which require a diverse means, different SSCs are required. For the AP1000 plant

design, these different SSCs are generally other Class 1 SSCs. There are a few exceptions where a few Class 2 SSCs are credited with different Class 1 SSCs in the diverse means to achieve safe shutdown.

When only Class 1 safety systems are credited, offsite electrical power sources are not essential and are assumed to be lost during the event. This results in a loss of the reactor coolant pumps. With loss of the reactor coolant pumps, reactor coolant system natural circulation flow initiates and transfers core heat to the steam generators. Although feedwater flow is lost, the existing steam generator water inventory provides initial decay heat removal capability. With the loss of main ac power, the Class 1 dc batteries are relied upon to supply power to the Class 1 dc power distribution network and the four Class 1 ac instrumentation divisions via the inverters.

The following sections describe the use of Class 1 safety systems to provide the primary and diverse means of achieving and maintaining safe shutdown.

9C.2.1.1 Safe Shutdown for Intact Circuit Faults with Class 1 SSCs, Primary Means

Note that power from the four Class 1 batteries is not required for this intact circuit fault since all of the passive means associated with the primary Class 1 systems fail to their safe conditions on loss of dc power. This includes the PRHR HX, CMTs, and PCS.

If the Class 1 dc power is not lost, the PRHR HX is actuated by the PMS due to low steam generator water level. The PRHR HX removes decay heat from the core by transferring this heat to the IRWST. Initially, the PRHR HX does not completely match the decay heat and as a result some heat is removed by steaming of the initial SG inventory through the SG safety valves. Once the decay heat level drops below the PRHR HX capacity, steaming from the SG will stop and the RCS temperature will begin to decrease.

As the RCS cooldown continues, the RCS pressure decreases due to contraction of the RCS inventory since the pressuriser heaters are de-energised. An engineered safety system actuation signal occurs when pressuriser pressure decreases below a setpoint. This actuates the CMTs, if they had not been previously actuated due to a low pressuriser level. The CMTs provide borated water injection to the RCS. The injection of boron supplements the control rods, RCS cooldown compensates for decay of xenon and other poisons.

The engineered safety function actuation signal generated on low pressuriser pressure also actuates containment isolation. Note that the containment isolation valves that are connected directly to the RCS or to the containment atmosphere are also fail safe (closed) valves. This prevents loss of water inventory and any release of radioactive materials from containment and permits long-term operation of the PRHR HX.

The IRWST starts to boil approximately four hours after PRHR HX operation is initiated. Once boiling occurs, the IRWST begins steaming to containment which transfers heat to the containment atmosphere and also to the containment shell. This steaming causes the containment pressure to increase and automatically actuates the PCS on a high containment pressure signal. When the setpoint is reached, this signal opens the valves that allow water to drain from the PCCWST onto the outside of the containment shell which provides heat removal from the containment through evaporative cooling to the outside air. Note that the challenge to the passive containment cooling capability for this sequence is much less than for the limiting challenge to the containment, which comes from a large LOCA that releases a higher amount of mass and energy in containment. The performance of the PCS during the

limiting faults is demonstrated in Appendix 9D. Since the challenge to the PCS is much less during intact circuit faults, additional discussion is not necessary.

The PCCWST is sized for 72 hours. After 72 hours, more water will be transferred to the PCCWST by small pumps (either installed or brought in from offsite).

Gutters located at several elevations in the containment (operating deck, stiffener and polar crane girder) collect condensate from the inside of the containment shell. Pipes connected to those gutters normally drain the condensate to the containment waste sump. A PRHR HX actuation signal closes redundant fail safe valves in this line to divert the condensate back to the IRWST. The return of condensate to the IRWST provides for long-term operation of the PRHR HX.

Once the RCS and the safety systems are in this configuration, the plant is in a safe, stable shutdown condition. Section 9C.3.1.1 shows that with conservative design basis assumptions, the PRHR HX can maintain the plant in a safe stable state for at least 72 hours. In addition, as discussed in Section 9C.1.1, the RCS temperatures and pressures are expected to slowly decrease, reaching 216°C (420°F) within 36 hours based on realistic assumptions (Reference 9C-1). This reduced temperature condition is expected to be maintained for greater than 14 days. Note that the duration of operation in this condition can be limited by RCS leakage (see 9C.3.2) or by the fraction of IRWST steam condensate returned to the IRWST.

Four 24 hour Class 1 dc batteries provide power to actuate the ADS, IRWST injection and containment recirculation valves for at least 24 hours. There is a timer that measures the time that ac power sources are unavailable. This timer provides for automatic actuation of these valves before the 24 hour Class 1 dc batteries are discharged. The emergency response guidelines direct the operator to assess the need for ADS before the timer completes its count (approximately 22 hours). The operator assessment considers CMT level, and RCS hot leg level, temperature, and pressure. If ADS is not needed, the operator is directed to de-energise all loads on the 24 hour Class 1 dc batteries. This action preserves the capability for the operator to initiate ADS at a later time based on assessment of the same parameters.

Note that the CMTs can only supply a limited amount of makeup in the event there is RCS leakage. Eventually the volume of the water in the CMTs will decrease to the first stage ADS setpoint. With normal RCS leak rates it is expected that the CMTs can make up for the leakage for many weeks. However, if there was an abnormally high RCS leak the operators could conclude (at 22 hours) that there will be a need for ADS in the near future and not take action to de-energise the battery loads.

Some of the IRWST steam condensate will not return to the IRWST. Over time, these losses will reduce the IRWST water level and the PRHR HX heat transfer. Reference 9C-1 provides an evaluation of how this loss affects IRWST water level and as a result the PRHR HX and resultant plant performance. This evaluation shows that the PRHR HX is expected to be able to operate for greater than 14 days before the PRHR HX heat removal would fall behind decay heat and ADS might be needed.

When the four actuation battery loads are de-energised, the operators would monitor the RCS conditions using power from two Class 1 batteries which are sized for 72 hours. After 72 hours, if normal ac power (offsite or onsite) was not recovered, power would be provided by two, small diesel generators (either the installed Ancillary DGs or DGs brought in from offsite).

If the RCS conditions degraded sufficiently (i.e. RCS temperature or pressure increased above values specified in the procedures) the operators would re-connect the four Class 1 batteries and allow the PMS cabinets to actuate ADS, IRWST injection and containment recirculation. These actuations would maintain the plant in safe shutdown using an open loop cooling process. The discussion that follows on non-intact circuit faults provides more detail on this mode of operation.

The ADS can be manually initiated by the operator at any time, but no operator action is needed to provide safe shutdown conditions. Once the ADS sequence initiates, the plant automatically transitions to lower pressure and temperature conditions that establish and maintain long term safe shutdown of the plant.

9C.2.1.2 Safe Shutdown for Intact Circuit Faults with Class 1 SSCs, Diverse Means

The above discussion also applies to the primary mitigation of a frequent intact circuit fault. In addition, frequent faults also require another, diverse means of mitigation. This section describes a situation where following an intact circuit frequent fault, there has been a low probability CCF affecting the primary means (Class 1 passive systems) of achieving safe shutdown. Such CCFs need only be considered for frequent faults. If such a low probability CCF occurred, different Class 1 passive systems can be used to bring the plant to a safe shutdown. Table 9C.3-1 lists these systems. Note that Table 9C.3-1 treats the systems used to provide the primary and the diverse means as two separate groups. This is a conservative approach and is not necessary since there is no single CCF could cause all of the primary systems to fail. For example, a CCF could cause the PMS to fail but that CCF would not affect the mechanical parts of the passive fluid systems; in this case the DAS would automatically actuate the same systems that PMS would have actuated for an intact circuit fault (PRHR, CMT, and PCS).

The diverse means to achieve safe shutdown following an intact circuit fault uses a passive feed-and-bleed approach. The bleed, release of RCS energy, is performed by manual actuation of the ADS. The feed, RCS inventory makeup, is performed by the accumulators and IRWST gravity injection. In the long term, when the IRWST reaches a low level, recirculation from the containment will be started. These features provide core cooling, long-term reactivity control, and RCS inventory control sufficient to bring the plant to safe shutdown conditions.

As indicated above, diversity is required in the safety functions credited in mitigating frequent faults. Table 8A-4 lists the features that provide this diversity. Note that for the AP1000 plant, the ultimate heat sink is provided by the PCS for both the primary and the backup diverse cases. This is acceptable because there is no CCF that can cause the PCS to fail to meet its diverse cooling requirements. Section 8A.1 provides a more detailed discussion of the diverse aspects of the PCS design and operation.

9C.2.1.3 Safe Shutdown for Non-Intact Circuit Faults with Class 1 SSCs, Primary Means

The Class 1 passive safety systems identified in Table 9C.3-2 bring the plant to a controlled state following a LOCA. These same systems also bring the plant to a safe shutdown state. This discussion bounds the system operation for different size and location LOCAs.

In the event of a LOCA, operation of the PRHR HX will be limited; once ADS is actuated the PRHR HX becomes in-effective. In such a fault, open loop reactor cooling and inventory control is provided by the ADS and PXS water injection tanks. Note that this mode is also applicable to excessive RCS leak situations, where the CMT inventory drops to the ADS

stage 1, 2, and 3 setpoint at a later time than for a LOCA; depending on the leak rate ADS could be actuated anywhere between a half of a day out to several weeks.

The CMTs provide RCS injection at high pressures. For small LOCAs, they start injecting in recirculation mode without draining. If the CLs void, the CMTs will start to drain with a higher flow rate. When the CMT level decreases to a low level setpoint, level sensors in the tanks actuate ADS stages 1, 2, and 3. This signal automatically actuates the first stage depressurisation valves, which initiates the RCS depressurisation sequence. The second and third stage depressurisation valves open in turn, based on automatic timers that are started upon the actuation of the first stage depressurisation valves. The water and steam vented from the RCS flows into the IRWST and the steam is initially condensed. As this operation continues, water will overflow into the refuelling canal and then into the containment. This overflow initiates the floodup of containment.

The RCS pressure decreases due to ADS operation and the LOCA break, which allows for the accumulators to inject borated water into the RCS. The accumulators inject for a limited duration (several minutes). When the volume of the water in the CMTs decrease to the fourth stage automatic depressurisation system setpoint, the fourth stage depressurisation valves and the IRWST injection valves are opened. The fourth stage ADS valves reduce RCS pressure sufficiently so that IRWST injection can begin as the CMTs empty. The CMT drain down injection duration lasts for about [ ].

The drain down of the IRWST is relatively slow, taking several hours. As the IRWST continues to inject, the floodup level in the containment rises and eventually reaches a level that can provide for natural circulation flow from the containment into the RCS. When the IRWST level drops to nearly empty, the containment recirculation valves automatically open to allow for containment recirculation.

The final long term safe shutdown plant conditions are maintained with the RCS depressurised to about [ ] at saturated conditions, venting steam through the ADS valves to containment, with heat transferred to the outside atmosphere via the PCS. Note that by the time IRWST injection begins, the RCS pressure has been reduced to about [ ] and since the RCS coolant will be saturated, its temperature will be at approximately [ ]. As a result, the plant will be in safe shutdown conditions. Containment isolation maintains the water inventory inside containment and provides for an indefinite cooling water supply for core decay heat removal.

In this mode of operation (with the RCS open and containment recirculation by Class 1 passive core cooling means), the only change that can occur is a slight reduction in the containment water level caused by water leaking into a couple of rooms that don't initially flood. Section 9.6.6 describes this reduction in water level and its timing.

9C.2.1.4 Safe Shutdown for Non-Intact Circuit Faults with Class 1 SSCs, Diverse Means

There are three different non-intact circuit frequent faults. Because of their high frequency they are classified as DB2 faults and as a result require diverse mitigation.

- Small LOCAs (<5.1 cm [2"])
- RCS leaks with failure of CVS makeup
- SGTRs

The RCS leak fault is not discussed further since it is bounded by the small LOCA case. The SGTR systems operation is not discussed further since it is identical to intact circuit faults; note that the concern over back flow from the SG diluting the RCS boron concentration is addressed separately in the results section (See Section 9C.3.3).

For small LOCA frequent faults, three different sets of SSCs have been defined to provide diverse core cooling considering a single common cause failure. Two of the sets of SSCs are considered primary cases (#1 and #2) and use the PMS, passive IRWST injection and passive containment recirculation. The diverse case uses DAS and RNS. The PRHR HX, CMTs, accumulators, and the ADS stages are divided up in these three cases. Table 9C.3-2 lists the SSCs credited in each case.

In the primary 1 case, the ADS stages 1-3 and accumulators are not credited so that they can be used in other cases. The PRHR HX provides the initial decay heat removal and functions to reduce RCS pressure (together with the break) to a low enough pressure that ADS stage 4 can be successfully actuated. In a low probability sequence such as this, the RCS pressure could be as high as 4.1 MPa gauge (600 psig) for ADS stage 4 actuation. The CMTs provide RCS injection, long-term boration, and automatic control of ADS stage 4. Passive IRWST injection and containment recirculation are credited.

In the primary case 2, the PRHR HX and accumulators are not credited so that they can be used in other cases. In this case, manual actuation of ADS stages 1-3 provides the RCS pressure reduction to allow successful ADS stage 4 actuation. Passive IRWST injection and containment recirculation are credited.

In the diverse case, the CMTs and the IRWST passive injection and passive containment recirculation are not credited so that they can be used in other cases. The PRHR HX provides the initial decay heat removal. Manual actuation of ADS stages 1-3 is credited so that PRHR HX operation need not be credited after the accumulators empty and nitrogen gas enters the RCS, potentially degrading the PRHR HX performance. The accumulators provide RCS injection during the transition to lower pressure conditions. Manual actuation of RNS injection provides low pressure injection and later containment recirculation, without the need for ADS stage 4 and the passive IRWST injection and recirculation valves.

Additional diversity cases for the small-break LOCA fault are evaluated for ATWT considerations, as discussed in 9.6.5.3

9C.2.2 Safe Shutdown Using Defence in Depth Means

Use of these Class 2 systems is not credited in the deterministic UK safety case other than as discussed in Section 9C.2.1.

9C.2.2.1 Safe Shutdown Using Class 1 and 2 SSCs

As discussed in Section 9C.1.1, the plant can be placed in a safe shutdown condition and maintained there using Class 1 systems and no operator actions. This section describes situations where Class 2 safety features of the plant are used together with Class 1 systems to establish safe shutdown conditions.

Following PRHR HX actuation the IRWST heats up and starts to boil after about four hours of operation. If normal steam generator heat removal is re-established, then PRHR HX operation may be terminated. If SG heat removal is not re-established, then the operators can align the RNS to cool the IRWST. This operation prevents significant steaming to the containment.

In case the ADS is actuated, the operators are instructed to align the RNS pumps to provide injection to the RCS. This action causes the CMT level to remain above the fourth stage ADS valve actuation setpoint and prevents significant steaming to and flooding of the containment.

Use of these Class 2 systems is not credited in the deterministic UK safety case other than as discussed in Section 9C.2.1.

9C.2.2.2 Safe Shutdown Using Class 2 Systems

This section describes the process to establish and maintain safe shutdown conditions using the Class 2 safety systems. The Class 2 safety systems normally used to support plant shutdown operations are expected to be available. These Class 2 systems would be powered by onsite diesel generators in case offsite power was unavailable. The use of these Class 2 systems is not credited in the deterministic UK safety case, with the exception for a frequent fault small break LOCA where the RNS is credited to support the backup diverse capability.

For the purposes of this discussion, the Class 2 safety system operation following a reactor trip is described. As assumed in the discussion in Section 9C.1.1 on safe shutdown using Class 1 systems, the RCS is assumed to be intact during plant safe shutdown operations.

The Class 2 safety systems and equipment used to establish and maintain safe shutdown conditions are the same systems and equipment that are operated during normal plant startup and shutdown evolutions. The safe shutdown capability using the Class 1 safety systems, described in Section 9C.1.1, is only expected to be used in the event that the Class 2 safety systems are not available.

The Class 2 safety systems actuate automatically to establish and maintain the safe shutdown conditions within the time limits discussed in Section 9C.1.1. The operational philosophy following any event is to maintain appropriate safe shutdown conditions based on the duration of the shutdown, until the plant is able to re-start.

Cold shutdown conditions would only be established if it is necessary for equipment repair or due to limitations of the Class 2 safety systems in maintaining safe shutdown conditions (such as feedwater system water inventory). This philosophy reduces unnecessary challenges to plant safety due to the transition from operating systems to infrequently operated standby systems.

If offsite electrical power is available, the normal Class 3 systems would automatically maintain short-term safe shutdown conditions. This operation would involve the RCS forcing flow through the steam generators, feedwater from the main feedwater pumps, steam from the steam generators directed to the main condenser using turbine bypass valves, condenser heat removal provided by the main circulating water system, RCS inventory and boration control by the CVS and RCS pressure control using pressuriser heaters and normal spray.

If offsite power is not available, the reactor coolant pumps, main feedwater pumps, and main circulating water pumps will not be operating. However, Class 2 safety systems would automatically maintain safe shutdown conditions without offsite electrical power as follows:

- Electrical power provided to the required Class 2 safety systems by the diesel-generators of the onsite standby power system
- Heat removal by the steam generators directly to the atmosphere through the power-operated relief valves

- Feedwater from the startup feedwater system
- RCS flow to the steam generators via natural circulation
- RCS inventory and boration control by the CVS
- RCS pressure control using pressuriser heaters and auxiliary spray.

Operation of the Class 2 safety systems in this mode maintains safe shutdown conditions and RCS temperature and pressure remain near no-load conditions. If it becomes necessary to perform a plant cooldown and depressurisation, the Class 2 safety systems are used, following the normal plant cooldown procedures. Manual boration to the cold shutdown boron concentration is provided by the CVS by initiating RCS letdown in combination with makeup pump operation. After the boration is completed and letdown is secured, the makeup pumps automatically maintain RCS inventory throughout the remainder of the cooldown process.

When offsite electrical power is unavailable, reactor coolant temperature is automatically maintained by the steam generator atmospheric power-operated relief valves instead of the turbine bypass valves. The steam generator power-operated relief valves maintain a pre-set steam generator pressure by throttling the steam discharged directly from the steam generators to the atmosphere. Automatic operation of the startup feedwater subsystem maintains steam generator inventory with the pumps powered from the diesel-generators. The direct discharge of steam to the atmosphere prevents condensate recovery, which limits the water inventory for the startup feedwater system.

Without offsite electrical power, the pressuriser heaters are manually energised after the diesel-generators start. Without reactor coolant pump operation, normal pressuriser spray is unavailable to counteract system pressure increases. Therefore, auxiliary spray provided by the CVS makeup pumps is manually initiated to decrease RCS pressure, if necessary. The operation of the CVS makeup pumps to maintain RCS inventory is similar to their operation when offsite power is available, except that the pumps are manually controlled and powered from the diesel-generators.

When the RCS temperature and pressure are reduced to within the capabilities of the RNS, at approximately 177°C (350°F) and 2.76 MPa gauge (400 psig), the system is manually aligned to the RCS and started to continue the cooldown process. The final shutdown conditions established would be dependent upon the specific maintenance required.

The use of the Class 2 safety systems and equipment for safe shutdown also requires the operation of associated support systems. These normally operating support systems include component cooling water, service water, chilled water, compressed air, area ventilation, and Class 2 safety instrumentation and control power. These systems are started as required following a loss of offsite power, once the Class 2 safety diesel-generators are started.

9C.3 Results for Safe Shutdown for Design Basis Faults

The list of design basis faults is shown in Appendix 8A; this table includes internal faults and internal/external hazards.

As described in 9C.1 there are two basic safe shutdown sequences. The limiting initiating fault for each is described:

- Intact circuit faults using closed loop cooling by the PRHR HX. The limiting initiating fault is a loss of main feedwater (Reference 9C-1). The operation of the plant for this fault is described in Section 9C.3.1.

- Non-intact circuit faults using open loop cooling by ADS and PXS injection. The bounding initiating fault is a DVI LOCA. This LOCA is limiting because containment recirculation is reached the fastest (resulting in higher decay heat) and the initial containment water level is lowest (due to flooding of a PXS compartment, which is normally avoided in a normal floodup scenario). The operation of the plant for this fault is described in Section 9C.3.2.

The frequent fault diversity cases are not limiting for safe shutdown because:

- Frequent intact circuit faults use open loop cooling as do LOCAs, however containment recirculation occurs several hours later (resulting in lower decay heat) and the initial containment water level is higher (neither PXS room floods).

- Frequent small break LOCA faults use open loop cooling crediting different combinations of the SSCs credited in infrequent LOCAs as well as the RNS. Three different combinations of SSCs are considered to allow for a common cause failure and provide the necessary shutdown functions as described in Section 9C.2.1.4.

The following sections describe the plant behaviour for the different initiating events that need to be considered for the safe shutdown of the plant. These include:

- Intact Circuit Safe Shutdown (Section 9C.3.1),

- Post-LOCA Long-Term Cooling (Section 9C.3.2), and

- SGTR Safe Shutdown (Section 9C.3.3).

The sections describe the response of the plant and the systems required to achieve safe shutdown under each scenario.

9C.3.1 Results for Safe Shutdown for Intact Circuit Faults

The primary means that are relied upon to achieve safe shutdown following a design basis intact circuit fault are the Class 1 passive safety systems (PRHR HX, CMTs, and PCS). For intact circuit frequent faults, the diverse means of achieving safe shutdown are different Class 1 passive systems (passive feed and bleed). The design also provides Class 2 active DiD systems that provide a third way of achieving safe shutdown of the plant (Section 9C.2.2), although they are not required to meet UK relevant good practice. The specific systems used in these three different means are listed in Table 9C.3-1.

Section 9C.3.1.1 discusses the "Primary" means (Class 1 passive systems) that are relied upon to achieve safe shutdown. Section 9C.3.1.2 discusses the "Diverse" means (alternative Class 1 passive systems) that are relied upon for intact circuit frequent faults to achieve safe shutdown.

9C.3.1.1 Results for Safe Shutdown for Intact Circuit Faults, Primary Means

The primary means of achieving safe shutdown for intact circuit faults in described in Section 9C.2.1.1. As discussed in Section 9C.1.1, the plant is considered to have reached long term safe shutdown if all applicable acceptance criteria are met, and the reactor is kept in a safe, stable state for at least 72 hours. Additionally, realistic analyses support that the plant meets the applicable acceptance criteria core average temperature is reduced to less than 216ºC (420ºF) within 36 hours, and these conditions can be maintained for greater than 14 days. The conservative design basis case is discussed below. The expected cooldown performance is discussed in Reference 9C-1.

As discussed in Section 9C.1.1 and Reference 9C-1, the PRHR HX operates to remove decay heat and then transition to, and maintain the plant in a safe stable state for at least 72 hours. An analysis of the loss of main feedwater with a loss of ac power event demonstrates that the passive systems can transition the plant to a safe stable state following postulated transients. A conservative bounding analysis is represented in Figures 9C.3-1 through 9C.3-5. The progression of this event is outlined in Table 9C.3-3.

The performance of the PRHR HX is affected by the containment pressure. Containment pressure determines the PRHR HX heat sink (the IRWST water) temperature. The WGOTHIC containment response model described in Appendix 9D was used to determine the containment pressure response to this transient, which was used as an input to the plant cooldown analysis performed with LOFTRAN.

The PRHR HX performance is also affected by the IRWST water level when the level drops below the top of the PRHR HX tubes. The IRWST water level is affected by the heat input from the PRHR HX and by the amount of steam that leaves the IRWST and does not return to the IRWST through the IRWST gutter arrangement. The principal steam condensate losses include steam that stays in the containment atmosphere, steam that condenses on heat sinks inside containment other than the containment vessel, and dripping or splashing losses from obstructions on the inner containment vessel wall. The WGOTHIC analysis inputs (including the mass of the heat sinks and heat transfer rates) were biased to increase steam condensate losses to maximize condensate losses. The WGOTHIC model provides the time-dependent condensate return rate, which was incorporated into the LOFTRAN computer code described in Appendix 9B to demonstrate that the RCS would be maintained in a safe stable state for at least 72 hours.

Summarizing this transient, the loss of normal ac power occurs (offsite and onsite), followed by the reactor trip. The PRHR HX is actuated on the low steam generator narrow range level coincident with low startup feed water flow rate signal. Eventually a safeguards actuation signal is generated on low cold leg temperature and the CMTs are actuated.

Once actuated, the CMTs operate in recirculation mode, injecting cold borated water into the RCS. The CMTs operate in conjunction with the PRHR HX to effectively reduce RCS temperature. However, when the CMT cooling effect decreases the RCS starts to heat up. The RCS temperature increases until the PRHR HX matches decay heat. The PRHR HX maintains safe, stable conditions for at least 72 hours as shown in Figures 9C.3-1 through 9C.3-5. The safety criteria applicable to this event are presented in Table 9C.3-4.

The AP1000 plant design meets all of the intact circuit fault safety criteria for the bounding safe shutdown state described in Section 9C.1.1, and presented in Table 9C.3-4, for 72 hours. Figure 9C.3-1 is the plot for the DNBR which remains above the minimum allowable value throughout the event. Figure 9C.3-2 is the plot for the RCS loop temperatures remain below the no-load temperature after PRHR HX actuation. Figure 9C.3-3 is the plot for RCS pressure which remains below the maximum allowable RCS pressure throughout the event. Figure 9C.3-4 is the plot for pressuriser water volume which remains below the maximum allowable pressuriser water volume throughout the event. Figure 9C.3-5 is the plot for the SG pressures which remains below the maximum allowable SG pressure throughout the event.

In addition to the above analysis discussion, Reference 9C-1 shows that with reasonable assumptions that the PRHR HX is capable of reducing the RCS temperature to below 216°C (420°F) within 36 hours and to maintain this temperature for greater than 14 days. As described in Section 9C.1.1, should power not be restored, the PRHR HX performance will degrade and ADS actuation would eventually be required to enter open loop passive feed and bleed cooling.

9C.3.1.2 Results for Safe Shutdown for Intact Circuit Faults with Class 1 SSCs, Diverse Means

This section describes a situation where following an intact circuit frequent fault, there has been a low probability CCF affecting the Class 1 primary means of achieving safe shutdown as described in Section 9C.2.1.2.

The diverse means of mitigating a frequent intact circuit fault utilizes passive feed and bleed cooling. The short term results are described in Section 9.2.7.3.2. In the long term, these same SSCs will continue to operate. As discussed in Section 9C.3.2.1, the only change that occurs in the long term is a slight reduction in the containment water level. The impact of this reduction in water level (discussed in Section 9.6.6) bounds this diverse case since it uses the same mode of passive system operation and this diverse case uses nominal conditions and assumptions appropriate for a diverse case, which will increase margins.

9C.3.2 Results for Safe Shutdown for Non-Intact Circuit Faults

For infrequent LOCA faults, the means of providing safe shutdown are discussed in Section 9C.3.2.1. For cliff edge frequent fault LOCAs, the primary and the diverse means of achieving safe shutdown are discussed in subsequent sections. Note that most LOCAs are infrequent faults and only small-break LOCAs and RCS leaks with failure of CVS makeup are considered cliff edge frequent faults. The small-break LOCA discussed in the following sections bounds an RCS leak fault.

9C.3.2.1 Results for Safe Shutdown for Infrequent Non-Intact Circuit Faults

Since this event is an infrequent fault, a CCF need not be considered and only one means of mitigation is required. Note that this category includes all LOCAs except for small-break LOCAs and RCS leaks with failure of the CVS makeup; these LOCAs are cliff edge frequent faults.

For these infrequent LOCAs, the passive features (PRHR HX, CMTs, accumulators, ADS stages 1-4) provide the initial response and bring the plant to a safe stable state. The specific timing and sequence of the initial actions vary somewhat based on the LOCA size and location. Refer to Sections 9.6.4 and 9.6.5 for discussion of the initial response of the plant for different sizes and locations of LOCAs. During all LOCAs, the plant will transition to the same end condition, with the RCS pressure reduced to low values by the ADS and with

IRWST providing gravity injection. At this time, the plant will be in a safe shutdown state because the RCS temperature is less than 215ºC (420ºF), and all other applicable acceptance criteria are met. Section 9.6.6 describes what happens after IRWST injection begins out through long term safe shutdown operations.

This description addresses the bounding LOCA case (DVI LOCA) since that results in the earliest initiation of containment recirculation (higher decay heat) and lowest initial recirculation water level (due to the DVI break causing flooding of one PXS valve room). In addition, this description also addresses a longer term situation where the two rooms that do not initially flood in this case, eventually do flood.

9C.3.2.2 Results for Safe Shutdown for Frequent Fault Non-Intact Circuit Faults, Primary and Diverse Cases

Three different sets of SSCs are described in Section 9C.2.1.4, to provide diverse core cooling mitigation of the frequent fault small LOCA. Table 9C.3-2 lists these SSCs.

Refer to Section 9.6.5.3 for a discussion of the results for these three cases (additional cases are also presented for ATWT considerations). During these three frequent fault LOCA cases, the plant will transition to essentially the same condition, with the RCS pressure reduced to low values by the ADS and with IRWST providing injection either by gravity injection or by RNS pump head. At this time, the plant will be in a safe shutdown state because the RCS temperature is less than 216ºC (420ºF), and all other applicable acceptance criteria are met.

This analysis shows that adequate core cooling is provided in each case. These cases confirm that:

Primary Case 1 – shows that the PRHR HX together with the LOCA bring the RCS pressure down to below the maximum allowable ADS stage 4 actuation pressure of 4.1 MPa gauge (600 psig). This case also shows that sufficient IRWST injection is achieved.

Primary Case 2 – Shows that sufficient IRWST injection is achieved when manual actuation of ADS stages 1-3 provides the RCS pressure reduction to allow successful ADS stage 4 actuation.

Diverse Case - Shows that operators have enough time to manually actuate ADS 1-4 and RNS. Also shows that no accumulator nitrogen is injected to the RCS before ADS is manually actuated which prevents the possibility of the nitrogen degrading the performance of the PRHR HX.

The same SSCs that provide short-term core cooling continue to operate and provide long term safe shutdown operation. As discussed in Section 9C.3.2.1, the only change that occurs in the long term is a slight reduction in the containment water level. The impact of this reduction in water level (discussed in Section 9.6.6) bounds the two primary cases since they are both based on passive system operation and with the use of nominal conditions and assumptions appropriate for these diverse cases the margins would increase. The diverse case uses the RNS pumps to provide long-term recirculation. In this case, the containment water level provides NPSH to the pumps. As the water level slowly decreases, the operators can reduce the RNS pump flow if needed to ensure that sufficient NPSH is available.

9C.3.3 Safe Shutdown for Steam Generator Tube Rupture Faults

As discussed in 9C.2.1.4, SGTR faults are considered cliff edge frequent faults and as such diverse means of achieving safe shutdown needs to be demonstrated. The SSCs used to provide primary and diverse mitigation of a SGTR are the same used to mitigate intact circuit faults and in the long-term these same SSCs continue to operate. The primary SSCs are the Class 1 PMS, PRHR HX, CMTs, containment isolation, and PCS. The diverse SSCs are those used for passive feed and bleed (ADS 1-4, accumulators, IRWST injection and containment recirculation, containment isolation and PCS). These specific systems are listed in Table 9C.3-1.

The unique capability of the primary passive SSCs is their ability to terminate the SG tube rupture leak automatically. Following break flow termination, the primary means of bringing the plant to a safe shutdown state is the continued operation of the same Class 1 passive systems that provided the initial fault mitigation.

The short term plant response using the primary and diverse SSCs is described in Section 9.6.3. Sections 9C.3.3.1 and 9C.3.3.2 provide discussion of the long term response using these two different sets of SSCs. These sections also discuss the claims made on operator actions and management of criticality challenges. Note that an SGTR does not present a challenge to containment and thus containment threats are not discussed further.

9C.3.3.1 Results for Safe Shutdown for SGTR Faults, Primary Means

The SGTR is analysed to demonstrate margin to ruptured SG overfill and to generate mass releases for the dose calculation. The limiting assumption for the margin to overfill is the failure of the start-up feedwater system (SFW, Class 2) to throttle when the setpoint is reached. The SFW is subsequently isolated automatically on a high SG water level signal in the ruptured SG. The limiting single failure for the mass release for dose analysis is the failure of the power operated relief valve (PORV, Class 2) on the ruptured SG in the open position. This is assumed to occur coincident with the actuation of the PRHR and CMT. The MSIV and PORV block valve associated with the SG with the ruptured tube automatically close on a low SG pressure signal.

The following describes how the plant is brought to a safe shutdown state using these same passive systems. Basically, in this case the operators do nothing and the PRHR HX operation automatically brings the plants to a safe shutdown. With the conservative bounding analysis assumptions the RCS remains in a safe stable state for at least 72 hours. The RCS temperature does not cool down very much although it is sufficient to reduce the RCS pressure and terminate the leak. With this analysis, there is no challenge to core shutdown margin since there is little if any back flow from the ruptured SG to the RCS.

However, the more likely situation is for the PRHR HX to cool the RCS down to 216ºC (420ºF) within 36 hours; this is similar to the intact circuit conclusions presented in Section 9C.3.1.1. In this situation, the RCS pressure will decrease further and some back flow will occur from the ruptured SG. The potential for this back flow to bring less borated SG secondary side water into the RCS and reduce the core shutdown margin has been analysed in Reference 9C-11. Note that this long-term mode of operation has two advantages:

1. It requires no operator actions

2. It minimises offsite radiological releases

3. It minimises the contamination, cleanup of the secondary side, impact to turbine island SSCs

Adequate core shutdown margin has been demonstrated using conservative assumptions including maximum SFW additions, maximum initial RCS boron concentration, and minimum CMT boron concentration, stuck rod, and no xenon. The RCS boron concentration remains well above the safe shutdown boron concentration.

The conservative hand calculation method used in Reference 9C-11 assumes that the RCS volume remains well mixed as water from the ruptured SG flows back into the RCS during the RCS cooldown caused by long term PRHR HX operation. This assumption is readily supported if there is forced circulation. Natural circulation conditions also support this assumption. Figure 3.2-4 of Reference 9C-3 provides evidence for crediting adequate mixing under natural circulation conditions. With natural circulation cooldown, during the post-SGTR recovery, the RCS cooldown rate is limited by the PRHR HX and the primary-to-secondary pressure differential and resultant reverse break flow rate would be low. With a low reverse break flow rate, the potentially unborated water entering into the RCS volume would mix with the circulating RCS coolant, and significant mixing would occur.

9C.3.3.2 Results for Safe Shutdown for SGTR Faults, Diverse Means

The diverse means to achieve safe shutdown uses a passive feed-and-bleed approach using DAS for the C&I. The bleed is performed by manual actuation of the ADS. The feed is performed by the accumulators and IRWST gravity injection. In the longer term, when the IRWST reaches a low level, recirculation from the containment will be actuated. These features provide core cooling, long-term reactivity control, and RCS inventory control sufficient to bring the plant to safe shutdown conditions.

This diverse safe shutdown uses passive containment cooling; refer to Section 9C.2.1.2 for discussion of the diversity within the PCS.

Reactivity concerns are avoided during the ADS operation because of the large, rapid injection of borated water from the accumulators and the IRWST as well as by a void that occurs in the core.

9C.4 Summary and Conclusions

The assessment of plant progression to a safe shutdown controlled state for all design basis faults is documented herein.

Chapter 8 contains a comprehensive list of all design basis faults. Section 9C.1 describes that these faults only result in two different reactor conditions at the end of the short-term mitigation.

The operation of the SSCs credited in providing safe shutdown for the plant is described in Section 9C.2. This description includes the primary Class 1 SSCs as well as the diverse SSCs (for frequent faults). Intact circuit faults as well as non-intact circuit faults (LOCAs and SGTRs) are included.

The resulting plant thermal hydraulic behaviour for each type of fault and mitigating SSCs is described in Section 9C.3. The analysis described shows that these SSCs allow the plant to reach and maintain the specified safe shutdown condition for the specified durations.

9C.5 References

9C-1 Westinghouse Report UKP-PXS-GLR-001, Rev. 0, "Condensate Return Analysis Summary Report," August 2016.

9C-2 Westinghouse Report UKP-SSAR-F5-001, Rev. 0 "AP1000 Safety Analysis Checklist (SAC) & Future Limits," July 2016.

9C-3 Westinghouse Report APP-PXS-GSR-001, Rev. 1, "Extended Closed Loop PRHR HX Performance Under Saturation Conditions," January 2016.

9C-4 Westinghouse Report APP-GW-GJP-323, Rev. 1, "Loss of AC Power," July 2014.

9C-5 Westinghouse Report UKP-GW-GL-067, Rev. 1, "AP1000 Assessment of Diverse Mitigation of Frequent Faults for the UK," December 2011.

9C-6 Westinghouse Report APP-GW-GJP-204, Rev. 8, "Steam Generator Tube Rupture," September 2014.

9C-7 Westinghouse Report APP-GW-GJR-204, Rev. 8, "Background Information for E-3, Steam Generator Tube Rupture," September 2014.

9C-8 Westinghouse Report APP-GW-GJP-237, Rev. 4, "Steam Dump to Condenser," July 2014.

9C-9 Westinghouse Report APP-GW-GJP-238, Rev. 4, "Steam Dump to Atmosphere," July 2014.

9C-10 Westinghouse Report APP-GW-GJP-207, Rev. 7, "Natural Circulation Cooldown," July 2014.

9C-11 Westinghouse Report UKP-GW-GL-079, Rev. 1, "AP1000 Assessment of Safe Shutdown for all Design Basis Faults," February 2011.

Table 9C.1-1. Class 1 SSCs Required for Safe Shutdown

Protection and Safety Monitoring System (PMS)
Passive Core Cooling System (PXS) Passive Residual Heat Removal Heat Exchanger Core Makeup Tanks Accumulators(1) In-Containment Refuelling Water Storage Tank Containment Recirculation(1) Automatic Depressurisation Valves(1)
Passive Containment Cooling System (PCS)
Class 1 dc and UPS System (IDS)
Containment Isolation Valves
Reactor System Control Rods

Notes: (1) These features are only required in LOCA faults or for intact circuit faults where in the long term it becomes necessary to transition from closed loop RCS cooling using the PRHR HX to open loop cooling using ADS.

Table 9C.3-1. Safe Shutdown SSCs for Intact Circuit Faults[1]

Function	Primary (Class 1 Passive)	Diverse Core Cooling (Class 1 and 2)	Diverse ATWT (Class 1 and 2)
Reactivity Control, Short-Term	Control rods	Control rods	Note 3
Reactivity Control, Long-Term	CMTs	Accumulators, IRWST injection	CMTs
Heat Removal, Short-Term (RCS to Ultimate Heat Sink)	PRHR HX, PCS	ADS, Accumulators, IRWST injection, PCS[5]	PRHR HX, PCS[5]
Heat Removal, Long-Term (RCS to Ultimate Heat Sink)	PRHR HX, PCS	ADS, Containment recirculation (gravity), PCS[5]	PRHR HX, PCS[5]
RCS Inventory	CMTs	Accumulators, IRWST	CMTs
Electrical Power	None (all fail safe on loss of power)	IDS, EDS[4]	EDS[4]
C&I	PMS	DAS[4]	DAS[4]

Notes:

1. Note that not all intact circuit faults are frequent faults. Note that these same cases also apply to SGTR.
2. Not used.
3. Short-term reactivity is provided for this case by a combination of core reactivity characteristics and core voiding. See Chapter 9 for descriptions of the different frequent intact circuit faults and a discussion of diverse means used to provide short-term reactor shutdown for ATWT sequences.
4. The DAS is a Class 2 system that has its own dedicated batteries.
5. The PCS incorporates diversity such that a CCF cannot cause its failure. Refer to Section 9C.2.1.2 for additional discussion.

Table 9C.3-2. Safe Shutdown SSCs For LOCA Faults

Function	Infrequent LOCAs (Class 1 Passive)[1]	Primary 1 for FF LOCAs (Class 1 Passive)	Primary 2 for FF LOCA (Class 1 Passive)	Diverse for FF LOCAs (Class 1 and 2)[2]
Reactivity Control, Short-Term	Control rods or RCS voiding	Control rods	Control rods	Control rods[6]
Reactivity Control, Long-Term	CMTs, accumulators, IRWST injection (gravity)	CMTs, IRWST injection (gravity)	CMTs, IRWST injection (gravity)	Accumulators, IRWST injection (RNS)[3]
Heat Removal Short-Term (RCS to Ultimate Heat Sink)	CMTs, Accumulators, ADS 1-3, IRWST injection (gravity), PCS	PRHR, CMTs, ADS 4, IRWST injection (gravity), PCS AOVs	CMTs, ADS 1-4, IRWST injection (gravity), PCS AOVs	PRHR, ADS 1-3, Accumulators, IRWST injection (RNS)[3], PCS[5]
Heat Removal Long-Term (RCS to Ultimate Heat Sink)	ADS 1-4, Containment recirculation (gravity), PCS	ADS 4, Containment recirculation (gravity), PCS AOVs[5]	ADS 1-4, Containment recirculation (gravity), PCS AOVs[5]	ADS 1-3, Containment recirculation (RNS)[3], PCS MOVs[5]
RCS Inventory	CMTs, Accumulators, IRWST injection (gravity)	CMTs, IRWST injection (gravity)	CMTs, IRWST injection (gravity)	Accumulators, IRWST injection (RNS)[3]
Electrical Power	Class 1 dc power (IDS)	Class 1 dc power (IDS)	Class 1 dc power (IDS)	Class 2 dc power (EDS), Class 2 ac power (ECS)
C&I	PMS	PMS	PMS	DAS[4], PLS

Notes:

1. Most LOCA faults are infrequent faults; the only exceptions are small-break LOCAs and RCS leaks (with failure of CVS) which are “cliff edge” frequent faults.
2. The “diverse” means of providing the AP1000 plant safe shutdown uses both Class 1 and Class 2 components.
3. The containment recirculation includes four paths. Two of the paths use valves that are diverse from the other two paths so that one CCF cannot cause all four paths to fail.
4. The DAS is a Class 2 system that has its own dedicated batteries.
5. The PCS incorporates diversity such that a CCF cannot cause its failure. Refer to Section 9C.2.1.2 for additional discussion.
6. An alternate ATWT case (without rod insertion) is discussed in Section 9.6.5.

Table 9C.3-3. Safe Shutdown Sequence of Events Following a Loss of AC Power (Bounding Case for 72 Hours)

Event	Time (seconds)
Feedwater is Lost	10.0
Low-2 Steam Generator Water Level (Narrow-Range) Reactor Trip Setpoint Reached	60.2
Rods Begin to Drop	62.2
RCPs Trip due to Loss of ac Power	70.2
Low Steam Generator Water Level (Wide-Range) Reached	214.5
PRHR HX Actuation on Low-2 Steam Generator Water Level (Narrow-Range Coincident with Low Startup Feedwater Flow)	214.5
Low-2 T_{cold} Setpoint Reached	8,319.7
Steam Line Isolation on Low-2 T_{cold} Signal	8,331.7
CMTs Actuated on Low-2 T_{cold} Signal	8,336.7
IRWST Reaches Saturation Temperature	15,900
Heat Extracted by PRHR HX Initially Matches Core Decay Heat	~30,000

Table 9C.3-4. Safe Shutdown Acceptance Criteria

Criterion	Safety Limit
After PRHR HX matches decay heat, RCS T_{avg} < ADS actuation temperature	296°C (565°F)
RCS pressure less than limit(1)	18.9 MPa (2749 psia)
Pressuriser water volume less than full	62.3 m^3 (2200 ft^3)
SG pressure less than limit(1)	9.1 MPa (1319 psia)
DNB Ratio greater than limit	Safety Analysis Limit(2)

Notes: (1) Pressure limit is ASME upset pressure limit of 110% of design pressure
(2) Specific limit maintained in Reference 9C-2

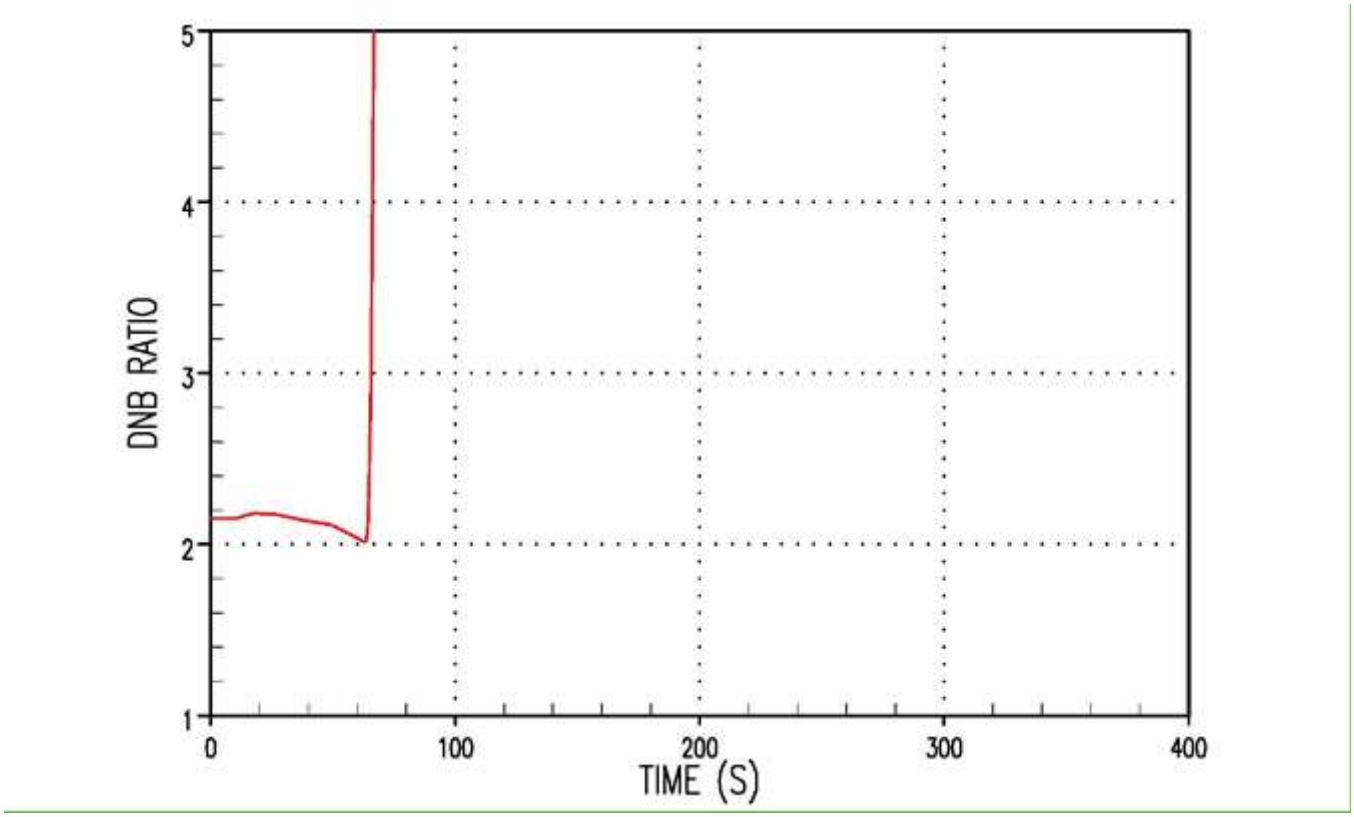


Figure 9C.3-1. Safe Shutdown Evaluation, DNB Ratio

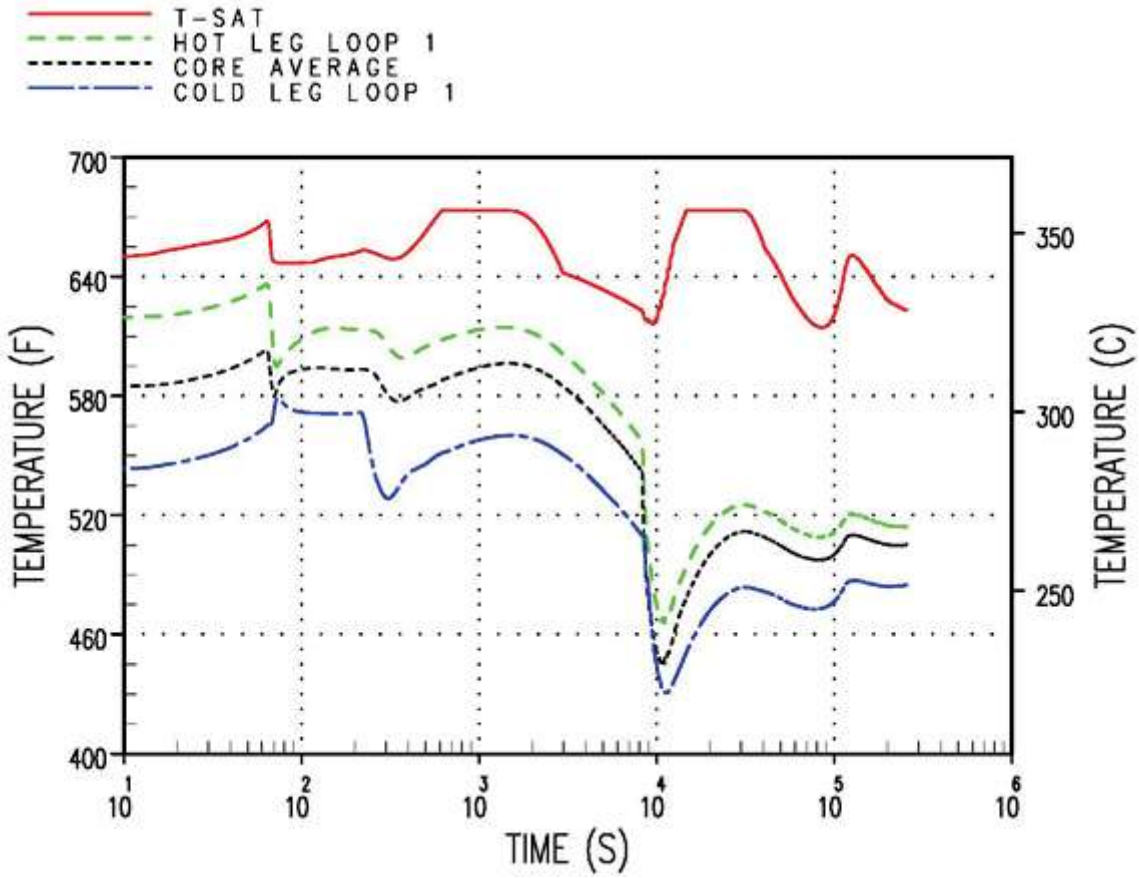


Figure 9C.3-2. Safe Shutdown Evaluation, RCS Temperature

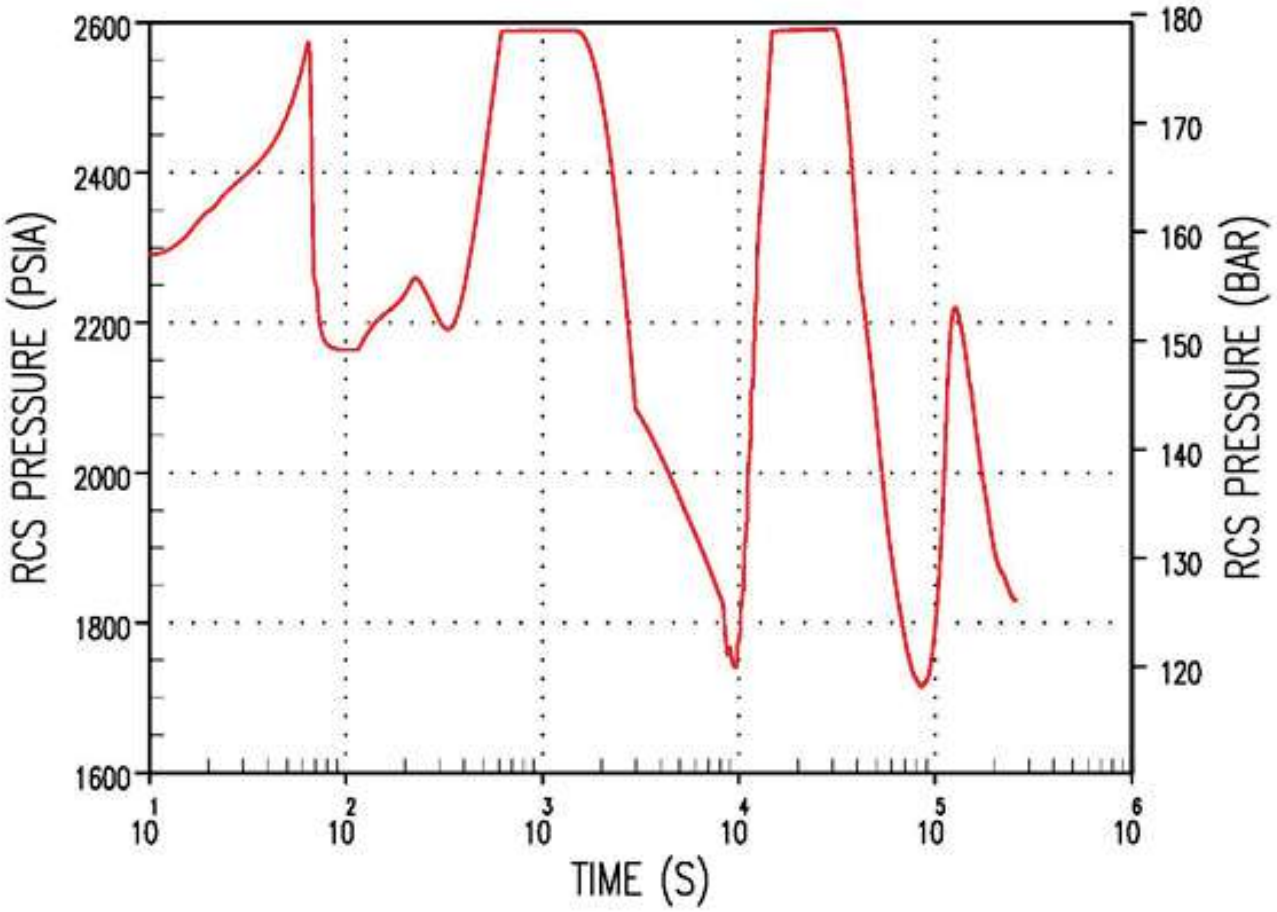


Figure 9C.3-3. Safe Shutdown Evaluation, RCS Pressure

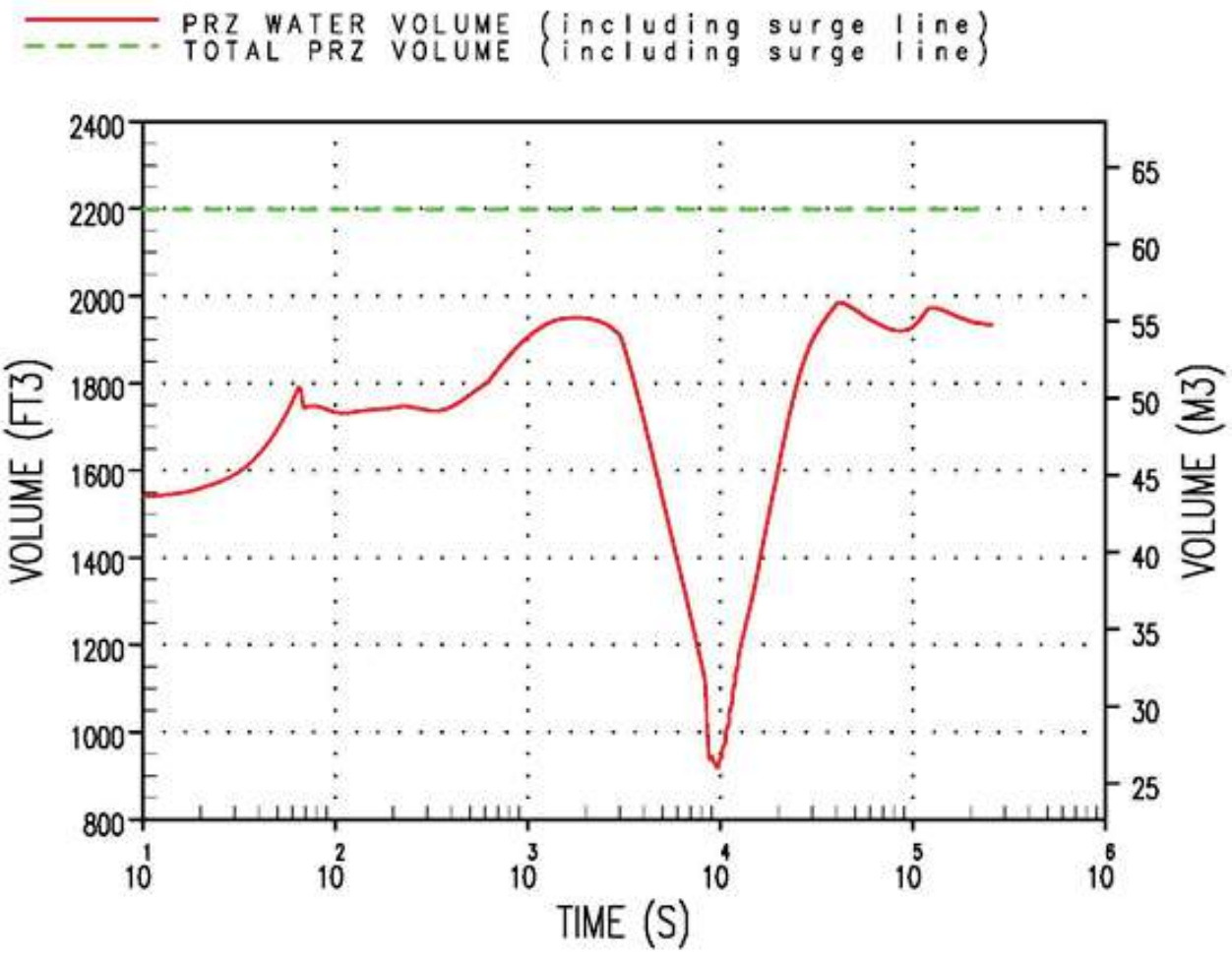


Figure 9C.3-4. Safe Shutdown Evaluation, Pressuriser Water Volume

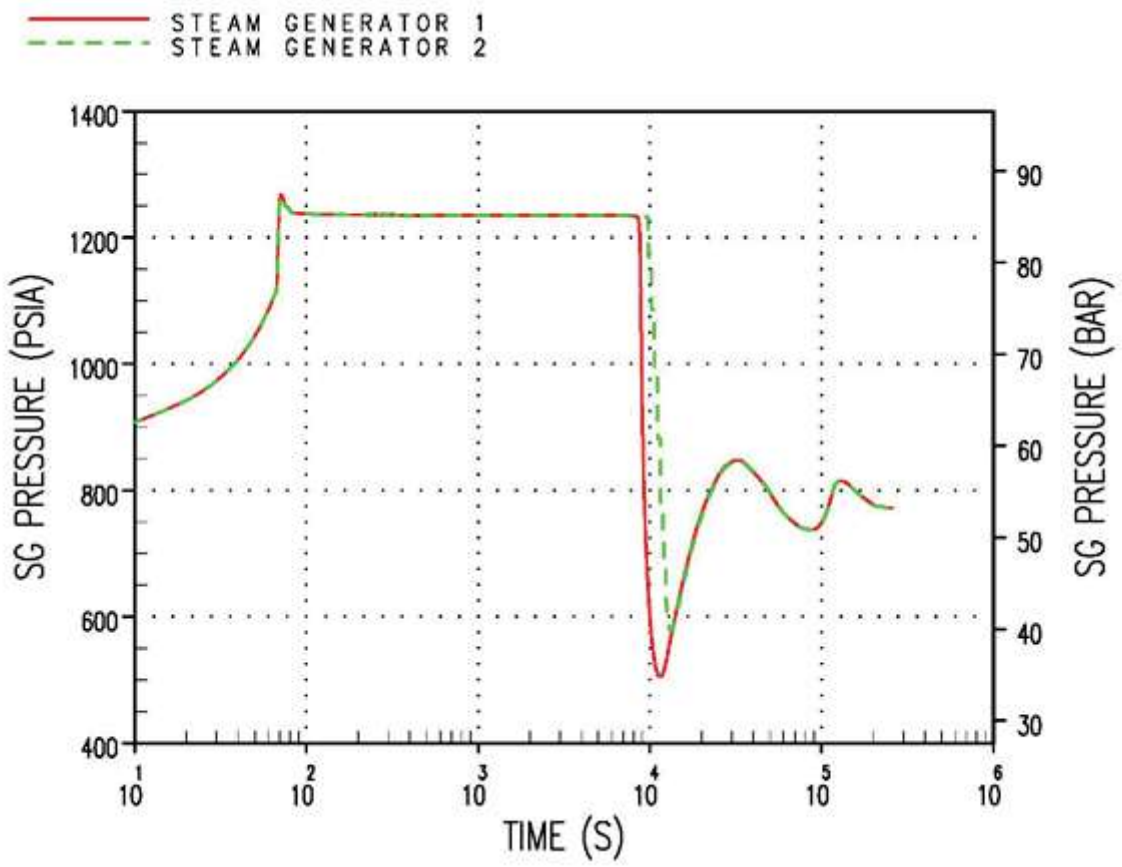


Figure 9C.3-5. Safe Shutdown Evaluation, Secondary Side Pressure

9D Containment Analyses

9D.1 Containment Structure

9D.1.1 Design Basis

The containment system is designed such that for all break sizes, up to and including the double-ended severance of a reactor coolant pipe or secondary side pipe, the containment peak pressure is below the design pressure. A summary of the results is presented in Table 9D.1-1.

This capability is maintained by the containment system assuming the worst single failure affecting the operation of the PCS. For primary system breaks, LOOP is assumed. For secondary system breaks, offsite power is assumed to be available when it maximises the mass and energy released from the break. Additional discussion of the assumptions made for secondary side pipe breaks may be found in subsection 9D.3.

The single failure postulated for the containment pressure/temperature calculations is the failure of one of the valves controlling the cooling water flow for the PCS. Failure of one of these valves would lead to cooling water flow being delivered to the containment vessel through two of three delivery headers. This results in reduced cooling flow for PCS operation. However, only one flowpath is necessary to meet containment cooling requirements and only one flowpath is assumed in the containment integrity analyses.

The containment integrity analyses for the AP1000 employ a multivolume lumped parameter model to study the long-term containment response to postulated LOCA and MSLB accidents.

The analyses presented in this section are based on assumptions that are conservative with respect to the containment and its heat removal systems, such as minimum heat removal, and maximum initial containment pressure.

The minimum containment backpressure used in the PXS analysis is discussed in Section 9D.4.

9D.1.2 Design Features

The reactor coolant loop is surrounded by structural walls of the containment internal structures. These structural walls are a minimum of 0.76 meter (2-feet - 6-inches) thick and enclose the reactor vessel, steam generators, reactor coolant pumps, and the pressuriser.

The containment vessel is designed and constructed in accordance with the ASME Code, Section III, Subsection NE, Metal Containment, as described in Appendix 10K.

Containment and subcompartment atmospheres are maintained during normal operation within prescribed pressure, temperature, and humidity limits by means of the VCS, and the central chilled water system (VWS). The recirculation system cooling coils are provided with chilled water for temperature control. The filtration supply and exhaust subsystem can be utilised periodically to purge the containment air for pressure control. Periodic inspection and maintenance verify functional capability.

9D.1.3 Design Evaluation

The WGOTHIC computer code (Reference 9D-6) is a computer programme for modelling multiphase flow in a containment transient analysis. It solves the conservation equations in integral form for mass, energy, and momentum for multicomponent flow. The momentum

conservation equations are written separately for each phase in the flow field (drops, liquid pools, and atmosphere vapour). The following terms are included in the momentum equation: storage, convection, surface stress, body force, boundary source, phase interface source, and equipment source.

To model the passive cooling features of the AP1000, several assumptions are made in creating the plant decks. The external cooling water does not completely wet the containment shell; therefore, both wet and dry sections of the shell are modelled in the WGOTHIC analyses. The analyses use conservative coverage fractions to determine evaporative cooling as explained in Chapter 7 of Reference 9D-6. The analyses conservatively assume that the external cooling water is not initiated until 400 seconds into the transient, allowing time to initiate the signal and to fill the headers and weirs and to develop the flow down the containment side walls. The effects of water flowing down the shell from gravitational forces are explicitly considered in the analysis.

The containment initial conditions of pressure, temperature, and humidity are provided in Table 9D.1-2. The WGOTHIC containment evaluation model is presented in Reference 9D-9.

For the LOCA events, two double-ended guillotine reactor coolant system pipe breaks are analysed. The breaks are postulated to occur in either a hot or a cold leg of the reactor coolant system. The hot leg break is limiting during the blowdown phase of the accident, and is only analysed for this time period. The cold leg break is the most limiting scenario after the blowdown, and is analysed for the long term containment response. The cold leg break analysis includes the long term contribution to containment pressure from the sources of stored energy, such as the steam generators. The LOCA mass and energy releases described in subsection 9D.2 are used for these calculations.

For the MSLB event, a double-ended pipe rupture is analysed at several initial power levels with the WGOTHIC code. The MSLB mass and energy releases described in subsection 9D.3 are used for these calculations.

Table 9D.1-4 summarises the required volume of steel inside containment to validate the heat sink input and methodology for the WGOTHIC containment analyses. It includes requirements for analyses that minimise heat sinks (the peak containment pressure analyses) and ones that maximise heat sinks (the minimum containment pressure analyses).

The methodology for calculating the internal containment heat sink data used in the WGOTHIC analyses is presented in Reference 9D-6, Section 13. Heat sinks include both metallic and concrete structures. Table 9D.1-5 lists the heat sinks that are credited for heat transfer in the containment evaluation model for peak containment pressure analyses. The physical properties of the heat sink materials are presented in Table 9D.1-3. These properties are inputs to the containment peak pressure evaluation, consistent with the methodology specified in Reference 9D-6, Section 13, including:

- The thermal conductivity and volumetric heat capacity of all steel materials are reduced by 10% per the ASME standard to account for variability of alloy content
- The thermal conductivity of inorganic zinc is reduced by a factor of two relative to the minimum test requirement
- Emissivity is reduced by 10%

All carbon steel and concrete heat sinks inside containment are modelled with a coating of epoxy on the exposed surface. The containment vessel is modelled with an inorganic zinc coating inside and outside containment. The containment vessel below the operating deck has both an inorganic zinc coating and an epoxy top coating.

The peak containment pressure and temperature results of the LOCA and MSLB postulated accidents are provided in Table 9D.1-1. The peak value is the maximum of any location within the multi-node WGOTHIC model.

The containment pressure response for the peak pressure steam line break case is provided in Figure 9D.1-1. The containment temperature response for the peak temperature steam line break case is provided in Figure 9D.1-2.

The containment pressure and temperature responses to a double-ended cold leg guillotine are presented in Figures 9D.1-3 and 9D.1-4 for the first 5000 seconds which shows the peak portion of the containment transients and Figures 9D.1-5 and 9D.1-6 for the 3 day transients. The containment pressure and temperature response to a double-ended hot leg guillotine break are presented in Figures 9D.1-7 and 9D.1-8. The plotted parameters are the total pressure and vapour temperature at the location of the break.

A separate analysis for the double-ended cold leg guillotine LOCA event, without considering heat conduction from the dry to wet section, results in somewhat higher containment pressure in the long term, but still below 50 percent of design pressure at 24 hours. This separate analysis confirms the assumption in subsection 9.6.4.2.2 of reducing the containment leakage to half its design value at 24 hours.

The instrumentation provided outside containment to monitor and record the containment pressure and the instrumentation provided inside containment to monitor and record temperature are found in Chapter 19.

9D.2 Mass and Energy Release Analyses for Postulated Pipe Ruptures

The section describes the methodology used to determine the mass and energy releases for the containment pressure and temperature calculations using the WGOTHIC code (Reference 9D-6) (referred to as the long term analysis). These releases are used for the containment integrity analysis in subsection 9D.1.

The containment system receives mass and energy releases following a postulated rupture of the reactor coolant system or a postulated rupture of the main steam line within containment.

9D.2.1 LOCA Long Term Mass and Energy Release Data

The LOCA release rates are calculated for pipe failure at two locations: the hot leg and the cold leg. These break locations are analysed for long-term transients. Because the initial operating pressure of the reactor coolant system is approximately 15.51 MPa (2250 psi), the mass and energy are released extremely rapidly when the break occurs. As the water exits from the broken pipe, a portion of it flashes to steam because of the differences in pressure and temperature between the reactor coolant system and containment. The reactor coolant system depressurises rapidly since break flow exits from both sides of the pipe in a DEG severance.

A long term LOCA analysis calculation model is typically divided into four phases: blowdown, which includes the period from the accident initiation (when the reactor is in a steady-state full power operation condition) to the time that the broken loop pressure equalises to the containment pressure; refill, which is the time from the end of the blowdown to the time when the PXS refills the vessel lower plenum; reflood, which begins when the water starts to flood the core and continues until the core is completely quenched; and post-reflood, which is the period after the core has been quenched and energy is released to the reactor coolant system primary system by the reactor coolant system metal, core decay heat, and the steam generators.

The long-term analysis considers the blowdown, reflood, and post-reflood phases of the transient. The refill period is conservatively neglected so that the releases to the containment are conservatively maximised.

The AP1000 long-term LOCA mass and energy releases are predicted for the blowdown phase for postulated double ended cold leg guillotine (DECLG) and double ended hot leg guillotine (DEHLG) breaks. The blowdown phase mass and energy releases are calculated using the NRC approved SATAN-VI computer code (Reference 9D-1). The post blowdown phase mass and energy releases for the postulated DECLG break are calculated considering the energy released from the available energy sources described below. The energy release rates are conservatively modelled so that the energy is released quickly. The higher release rates result in a conservative containment pressure calculation.

The LOCA mass and energy releases to calculate a peak containment pressure are documented in Reference 9D-10.

9D.2.1.1 Mass and Energy Sources

The following are accounted for in the long-term LOCA mass and energy calculation:

- Decay heat
- Core stored energy
- Reactor coolant system fluid and metal energy
- Steam Generator fluid and metal energy
- Accumulators, CMTs,, and the IRWST fluid energy
- Zirconium-water reaction.

The methods and assumptions used to release the various energy sources during the blowdown phase are given in Reference 9D-1.

The following parameters are used to conservatively analyse the energy release for maximum containment pressure:

- Maximum expected operating temperature
- Allowance in temperature for instrument error and dead band
- Margin in volume (+1.4 percent)
- Allowance in volume for thermal expansion (+1.6 percent)
- 100 percent full power operation
- Allowance for calorimetric error (+1.0 percent of full power)
- Conservatively modified coefficients of heat transfer
- Allowance in core stored energy for effect of fuel densification
- Margin in core stored energy (+15.0 percent)
- Allowance in pressure for instrument error and dead band
- Margin in steam generator mass inventory (+10.0 percent)
- One percent of the Zirconium surrounding the fuel is assumed to react.

9D.2.1.2 Description of Blowdown Model

A description of the SATAN-VI model that is used to determine the mass and energy released from the reactor coolant system during the blowdown phase of a postulated LOCA is provided in Reference 9D-1. Significant correlations are discussed in this reference.

9D.2.1.3 Description of Post-Blowdown Model

The remaining reactor coolant system and SG mass and energy inventories at the end of blowdown are used to define the initial conditions for the beginning of the reflood portion of the transient. The broken and unbroken loop SG inventories are kept separate to account for potential differences in the cooldown rate between the loops. In addition, the mass added to the reactor coolant system from the IRWST is returned to containment as break flow so that no net change in system mass occurs.

Energy addition due to decay heat is computed using the 1979 ANS standard (plus 2 sigma) decay heat table from Reference 9D-1. The energy release rates from the reactor coolant system metal and steam generators are modelled using exponential decay rates. This modelling is consistent with analyses for current generation design analyses that are performed with the models described in Reference 9D-1.

The accumulator, CMT, and IRWST mass flow rates are computed from the end of blowdown to the time the tanks empty. The rate of reactor coolant system mass accumulation is assumed to decrease exponentially during the reflood phase. More CMT and accumulator flow is spilled from the break as the system refills. The break flow rate is determined by subtracting the reactor coolant system mass addition rate from the sum of the accumulator, CMT and IRWST flow rates.

Mass which is added to, and which remains in, the vessel is assumed to be raised to saturation. Therefore, the actual amount of energy available for release to the containment for a given time period is determined from the difference between the energy required to raise the temperature of the incoming flow to saturation and the sum of the decay heat, core stored energy, reactor coolant system metal energy and SG mass and metal energy release rates. The energy release rate for the available break flow is determined from a comparison of the total energy available release rate and the energy release rate assuming that the break flow is 100-percent saturated steam following IRWST draindown. Saturated steam releases maximise the calculated containment pressurisation.

9D.2.1.4 Single Failure Analysis

The assumptions for the containment mass and energy release analysis are intended to maximise the calculated release. A single failure could reduce the flow rate of water to the RCS, but would not disable the passive core cooling function. The effects of a single failure are taken into account in the containment analysis of subsection 9D.1.

9D.2.1.5 Metal-Water Reaction

Consistent with 10 CFR 50, Appendix K criteria, the energy release associated with the zirconium-water exothermic reaction has been considered. The LOCA peak cladding temperature analysis, presented in Chapter 9, demonstrates compliance with the Appendix K criteria demonstrates that no appreciable level of zirconium oxidation occurs. This level of reaction has been bounded in the containment mass and energy release analysis by incorporating the heat of reaction from 1 percent of the zirconium surrounding the fuel. This exceeds the level predicted by the LOCA analysis and results in additional conservatism in the mass and energy release calculations.

9D.2.1.6 Additional Information Required for Confirmatory Analysis

System parameters and hydraulic characteristics needed to perform confirmatory analysis are provided in Table 9D.2-1 and Figures 9D.2-1 through 9D.2-4.

9D.3 Mass and Energy Release Analysis for Postulated Secondary-System Pipe Rupture Inside Containment

Steam line ruptures occurring inside a reactor containment structure may result in significant releases of high-energy fluid to the containment environment, possibly resulting in high containment temperatures and pressures. The quantitative nature of the releases following a steam line rupture is dependent upon the configuration of the plant steam system, the containment design as well as the plant operating conditions and the size of the rupture. This section describes the methods used in determining the containment responses to a variety of postulated pipe breaks encompassing variations in plant operation.

The steam line break mass and energy releases to calculate a peak containment pressure are documented in Reference 9D-11.

9D.3.1 Significant Parameters Affecting Steam Line Break Mass and Energy Releases

Four major factors influence the release of mass and energy following a steam line break: steam generator fluid inventory, primary-to-secondary heat transfer, protective system operation and the state of the secondary fluid blowdown. The following is a list of those plant variables which have significant influence on the mass and energy releases:

- Plant power level
- Main feedwater system design
- Startup feedwater system design
- Postulated break type, size, and location
- Availability of offsite power
- Safety system failures
- Steam generator reverse heat transfer and reactor coolant system metal heat capacity.

The following is a discussion of each of these variables.

9D.3.1.1 Plant Power Level

Steam line breaks are postulated to occur with the plant in any operating condition ranging from hot shutdown to full power. Since steam generator mass decreases with increasing power level, breaks occurring at lower power generally result in a greater total mass release to the containment. Because of increased energy storage in the primary plant, increased heat transfer in the steam generators and additional energy generation in the nuclear fuel, the energy released to the containment from breaks postulated to occur during power operation may be greater than for breaks occurring with the plant in a hot shutdown condition. Additionally, steam pressure and the dynamic conditions in the steam generators change with increasing power. They have significant influence on the rate of blowdown from the break following a steam break event.

Because of the opposing effects of changing power level on steam line break releases, no single power level can be pre-defined as a worst case initial condition for a steam line break event.

Therefore, several different power levels (101%, 70%, 30%, 0%) spanning the operating range as well as the hot shutdown condition are analysed.

9D.3.1.2 Main Feedwater System Design

The rapid depressurisation that occurs following a rupture may result in large amounts of water being added to the steam generators through the main feedwater system. Rapid closing isolation valves are provided in the main feedwater lines to limit this effect. The piping layout downstream of the isolation valves determines the volume in the feedwater lines that cannot be isolated from the steam generators. As the steam generator pressure decreases, some of the fluid in this volume will flash into the steam generator, providing additional secondary fluid that may exit out the rupture. This unisolated feedwater mass between the steam generator and isolation valve is accounted for within the results in subsection 9D.3.3.2. The assumed unisolable volume bounds the volume to either the feedwater control valve or the feedwater isolation valve on the faulted loop, so that no additional feedwater mass could be postulated due to a single failure of one of the valves.

The feedwater addition that occurs prior to closing of the feedwater line isolation valves is conservatively calculated based on the depressurisation of the faulted steam generator, and assuming that the feedwater control valve is fully open in response to the increased steam flow rate.

9D.3.1.3 Startup Feedwater System Design

Within the first minute following a steam line break, the startup feedwater system may be initiated on a low steam generator water level signal in combination with low main feedwater flow. The addition of startup feedwater to the steam generators would increase the secondary mass available for release to the containment through the steam line break. If the actuation signal occurs, maximum startup feedwater flow to the faulted steam generator is conservatively assumed until automatically terminated on a low RCS T_{cold} signal.

9D.3.1.4 Postulated Break Type, Size and Location

The steam line break is postulated as a full double-ended pipe rupture immediately downstream of the integral flow restrictor on the faulted steam generator. The forward break flow from the faulted steam generator is limited by the flow restrictor area (0.13 m^2 (1.4 ft^2)). The faulted steam generator is unisolable from the break location, and the forward break flow continues until the steam generator is empty. The reverse break flow consists of the initial steam within the steamline piping and steam that comes from the intact steam generator. The reverse break flow continues until MSIV closure. The modelling of the reverse break flow does not differentiate the location of the MSIVs, and all steam that has exited the intact steam generator prior to MSIV closure is assumed to be released out the break. This bounds the possible effects of an MSIV failed open.

No liquid entrainment is credited in the break effluent from the double-ended pipe rupture. The release of dry saturated steam from the largest possible break size maximises the mass and energy release to the containment.

9D.3.1.5 Availability of Offsite Power

The effects of the assumption of the availability of offsite power are enveloped in the analysis.

Offsite power is assumed to be available where it maximises the mass and energy released from the break because of the following:

- The continued operation of the reactor coolant pumps until automatically tripped as a result of CMT actuation. This maximises the energy transferred from the reactor coolant system to the steam generator.

- The continued operation of the feedwater pumps and actuation of the startup feedwater system until they are automatically terminated. This maximises the steam generator inventories available for release.

- The AP1000 is equipped with the passive safeguards system including the CMT and the PRHR heat exchanger. Following a steam line rupture, these passive systems are actuated when their setpoints are reached. This decreases the primary coolant temperatures. The actuation and operation of these passive safeguards systems do not require the availability of offsite power.

  When the PRHR is in operation, the core-generated heat is dissipated to the IRWST via the PRHR heat exchanger. This causes a reduction of the heat transfer from the primary system to the steam generator secondary system and causes a reduction of mass and energy releases via the break.

Thus, the availability of ac power maximises the mass and energy releases via the break. Therefore, blowdown occurring with the availability of offsite power is more limiting than cases where offsite power is not available.

9D.3.1.6 Safety System Failures

The calculation of the mass and energy release following a steam line rupture is done to conservatively bound the possible increase of mass release due to safety system failures. Two failures, which are bounded are:

- Failure of one main steam isolation valve, as discussed in subsection 9D.3.1.4
- Failure of one main feedwater isolation valve, as discussed in subsection 9D.3.1.2

9D.3.1.7 Steam Generator Reverse Heat Transfer and Reactor Coolant System Metal Heat Capacity

Once steam line isolation is complete, the steam generator in the intact steam loop becomes a source of energy that can be transferred to the steam generator with the broken line. This energy transfer occurs through the primary coolant. As the primary plant cools, the temperature of the coolant flowing in the steam generator tubes drops below the temperature of the secondary fluid in the intact unit, resulting in energy being returned to the primary coolant. This energy is then available to be transferred to the steam generator with the broken steam line.

Similarly, the heat stored in the metal of the reactor coolant piping, the reactor vessel, and the reactor coolant pumps is transferred to the primary coolant as the plant cooldown progresses. This energy also is available to be transferred to the steam generator with the broken line. Energy from the metal of the faulted steam generator is also transferred to the fluid in the faulted steam generator as the fluid temperature drops below the metal temperature.

The effects of the reactor coolant system metal, the steam generator metal, and the energy in the fluid from the intact steam generator are included in the results presented.

9D.3.2 Description of Blowdown Model

The steam line blowdown is calculated with the LOFTRAN code (Reference 9D-3) which has been modified to include simulation of the AP1000 passive residual heat removal heat exchanger, core makeup tanks, and associated protection and safety monitoring system actuation logic. Documentation of the code changes for the passive models is provided in Reference 9D-7. The methodology for the steam line break analysis is based on Reference 9D-2. The applicability of the LOFTRAN code to AP1000, and the applicability of the methodology used to analyse the steam line break blowdown are discussed in Reference 9D-8.

9D.3.3 Containment Response Analysis

The WGOTHIC Computer Code (Reference 9D-6) is used to determine the containment responses following the steam line break, which is described in subsection 9D.1.

9D.3.3.1 Initial Conditions

The initial containment conditions are discussed in subsection 9D.1.3.

9D.3.3.2 Mass and Energy Release Data

Using References 9D-2, 9D-3, 9D-7 and 9D-8 as a basis, mass and energy release data are developed to determine the containment pressure-temperature response for the spectrum of cases analysed. Table 9D.3-1 provides nominal plant data used in the steamline break mass and energy releases determination.

9D.3.3.3 Containment Pressure-Temperature Results

The results of the containment pressure-temperature analyses for the postulated secondary system pipe ruptures that produce the highest peak containment pressure and temperature are presented in subsection 9D.1.3.

9D.4 Minimum Containment Pressure Analysis for Performance Capability Studies of Emergency Core Cooling System (PWR)

An analysis is performed to establish a minimum containment pressure boundary condition applied to the WCOBRA/TRAC code for the cold leg guillotine break for the ECCS analysis presented in subsection 9.6.4. A single-node containment model is used with the WGOTHIC computer code to assess the containment pressure response. The calculated containment backpressure is provided in Figure 9D.4-1.

Minimum containment pressure analyses are also performed to provide the containment backpressure boundary condition for small-break LOCA (See Section 9.6.5) and post-LOCA long-term cooling analyses (see Section 9.6.6). A multi-node WGOTHIC containment model described in Section 13.8 of WCAP-15846 (Reference 9D-6) is used.

9D.4.1 Mass and Energy Release Data

The mathematical models which calculate the mass and energy releases to the containment are described in subsections 9.6.4 and 9.6.5. A break spectrum analysis is performed (see references in subsections 9.6.5 and 9.6.5) that considers various break sizes and Moody discharge coefficients for the double-ended cold leg guillotines and splits. Mixing of steam and accumulator

water injected into the vessel reduces the available energy released to the containment vapour space, thereby minimising calculated containment pressure.

9D.4.2 Initial Containment Internal Conditions

Initial containment conditions were biased for the emergency core cooling system backpressure analysis to predict a conservatively low containment backpressure. Initial containment conditions include an initial pressure of 0.100 MPa (14.5 psia), initial containment temperature of 32.2°C (90°F), and a relative humidity of 100 percent. An air annulus temperature of -17.8°C (0°F) is assumed. The initial through-thickness metal temperature of the containment shell is assumed to also be -17.8°C (0°F).

9D.4.3 Other Parameters

Containment parameters, such as containment volume and passive heat sinks, are biased to predict a conservative low containment backpressure. The containment volume used in the calculation is conservatively set to 1.05 times the free volume of the AP1000 containment Evaluation Model. Containment internal heat sinks used heat transfer correlations of 4 times Tagami (Reference 9D-4) during the blowdown phase followed by 1.2 times Uchida (Reference 9D-5) for the post-blowdown phase. Passive heat sink surface areas were increased by a factor of 1.35 relative to the heat sinks developed for the peak containment evaluation model as described in Section 13 of Reference 9D-6. Material properties were biased high (density, conductivity, and heat capacity). No air gap was modelled between the steel liner and base concrete of jacketed concrete heat sinks. The outside surface of the containment shell was maintained at -17.8°C (0°F) throughout the calculation. To further minimise containment pressure, containment purge was assumed to be in operation at time zero and air is vented through both the containment purge supply and exhaust lines until the isolation valves have fully closed. These valves were modelled to close after the high-2 containment pressure setpoint was reached.

9D.5 References

9D-1 Westinghouse Documents WCAP-10325-P-A (Proprietary) and WCAP-10326-A (Non-Proprietary), “Westinghouse LOCA Mass and Energy Release Model for Containment Design March 1979 Version,” May 1983.

9D-2 Westinghouse Documents WCAP-8822 (Proprietary) and WCAP-8860 (Non-Proprietary), “Mass and Energy Releases Following a Steam Line Rupture,”, September 1976; “Supplement 1 - Calculations of Steam Superheat in Mass/Energy Releases Following a Steamline Rupture,” WCAP-8822-P-S1 (Proprietary), January 1985; “Supplement 2 - Impact of Steam Superheat in Mass/Energy Releases Following a Steamline Rupture for Dry and Subatmospheric Containment Designs,” WCAP-8822-S2-P-A (Proprietary), September 1986.

9D-3 Westinghouse Documents WCAP-7907-P-A, Rev.0 (Proprietary) and WCAP-7907-A, Rev. 0 (Non-Proprietary), “LOFTRAN Code Description,” April 1984.

9D-4 T. Tagami, “Interim Report on Safety Assessment and Facilities Establishment Project in Japan for Period Ending June 1965 (No. 1),” prepared for the National Reactor Testing Station, February 28, 1966 (unpublished work).

9D-5 H. Uchida, A. Oyama, and Y. Toga, "Evaluation of Post-Incident Cooling Systems of Light-Water Power Reactors," Proc. Third International Conference on the Peaceful Uses of Atomic Energy, Volume 13, Session 3.9, United Nations, Geneva (1964).

9D-6 Westinghouse Documents WCAP-15846, Rev. 5 (Proprietary) and WCAP-15862 (Non-Proprietary), "WGOTHIC Application to AP600 and AP1000," September 2016.

9D-7 Westinghouse Documents WCAP-14234, Rev. 1 (Proprietary) and WCAP-14235, Rev. 1 (Non-Proprietary), "LOFTRAN & LOFTTR2 AP600 Code Applicability Document," August 1997.

9D-8 Westinghouse Documents WCAP-15644-P, Rev. 2 (Proprietary) and WCAP-15644-NP, Rev. 2 (Non-Proprietary), "AP1000 Code Applicability Report," March 2004.

9D-9 Westinghouse Document APP-SSAR-GSC-768, Rev. 0, "AP1000 WGOTHIC Evaluation Model for Peak Containment Pressure Analyses," July 2014.

9D-10 Westinghouse Document APP-SSAR-GSC-191, Rev. 1, "AP1000 LOCA Mass/Energy Releases with SATAN78 and Long Term LOCA Mass/Energy Release Spreadsheet Methodology," September 2016.

9D-11 Westinghouse Document APP-SSAR-GSC-172, Rev. 1, "AP1000 Steamline Break Mass and Energy Release Inside Containment Analysis," August 2014.

Table 9D.1-1. Summary Of Calculated Peak Containment Pressures And Vapour Temperatures

Break	Peak Pressure (MPaG/psig)	Available[(1)] Margin (MPa/psi)	Peak Temperature (°C/°F)
Double-ended hot leg guillotine	0.344/49.9	0.063/9.1	196.6/385.9
Double-ended cold leg guillotine	0.394/57.2	0.012/1.8	181.5/358.7
Full main steam line DER, 30% power, MSIV failure	0.396/57.4	0.011/1.6	196.6/385.9
Full main steam line DER, 101% power, MSIV failure	0.378/54.8	0.029/4.2	197.5/387.5

Note:
1. Design Pressure is 0.41 MPag (59 psig)

Table 9D.1-2. Containment Integrity Analysis Initial Conditions

Internal Temperature (°C/°F)	48.9/120
Pressure (MPa/psia)	0.108/15.7
Internal Relative Humidity (%)	0
Net Free Volume (m^3/ft^3)	5.83E+04/2.06E+06
External Temperature (°C/°F)	46.1/115 dry bulb 30.1/86.1 wet bulb

Table 9D.1-3 (Sheet 1 of 2). Material Properties Used in the WGOTHIC Containment Evaluation Model

Material		Thermal Conductivity [(W/m-°C)/ (BTU/hr-ft-°F)]	Volumetric Heat Capacity [(MJ/m^3-°C)/ (BTU/ft^3-°F)]	Emissivity
Epoxy		0.3245/0.1875	17.60/26.25	N/A
Inorganic zinc		0.523/0.302	15.308/22.825	0.54 (1)
Baffle aluminium		23.2/13.4	19.076/28.443	0.81 (1)
Concrete		1.4/0.83	17.8/26.6	0.81 (1)
Air	-17.8°C/0°F	0.0226/0.0131	0.013907/0.020736	N/A
	121°C/250°F	0.0332/0.0192	0.014076/0.020988	N/A
	260°C/500°F	0.0426/0.0246	0.014371/0.021427	N/A
Group A Carbon Steel	21°C/70°F	54.3/31.4	30.1/44.9	N/A
	37.8°C/100°F	54.0/31.2	31.0/46.2	N/A
	65.6°C/150°F	53.3/30.8	32.2/48.0	N/A
	93.3°C/200°F	52.4/30.3	33.3/49.6	N/A
	121°C/250°F	51.4/29.7	34.1/50.8	N/A
	149°C/300°F	50.4/29.1	34.8/51.9	N/A
Group B Carbon Steel	21°C/70°F	42.6/24.6	31.1/46.4	N/A
	37.8°C/100°F	42.9/24.8	32.1/47.8	N/A
	65.6°C/150°F	43.3/25.0	33.3/49.6	N/A
	93.3°C/200°F	43.3/25.0	34.5/51.4	N/A
	121°C/250°F	42.9/24.8	35.3/52.7	N/A
	149°C/300°F	42.6/24.6	36.2/54.0	N/A
Group C Carbon Steel	21°C/70°F	36.9/21.3	31.2/46.5	N/A
	37.8°C/100°F	36.7/21.2	31.6/47.1	N/A
	65.6°C/150°F	36.7/21.2	32.5/48.4	N/A
	93.3°C/200°F	36.7/21.2	33.5/49.9	N/A
	121°C/250°F	36.5/21.1	34.3/51.1	N/A
	149°C/300°F	36.5/21.1	35.2/52.5	N/A
Group D Carbon Steel	21°C/70°F	32.718.9	31.1/46.3	N/A
	37.8°C/100°F	32.7/18.9	31.6/47.1	N/A
	65.6°C/150°F	33.1/19.1	32.7/48.7	N/A
	93.3°C/200°F	33.2/19.2	33.5/49.9	N/A
	121°C/250°F	33.4/19.3	34.3/51.1	N/A
	149°C/300°F	33.6/19.4	35.0/52.2	N/A
Group J Stainless Steel	21°C/70°F	13.3/7.7	34.4/51.3	N/A
	37.8°C/100°F	13.5/7.8	34.5/51.5	N/A
	65.6°C/150°F	14.0/8.1	35.3/52.6	N/A
	93.3°C/200°F	14.5/8.4	36.0/53.7	N/A
	121°C/250°F	14.9/8.6	36.7/54.7	N/A
	149°C/300°F	15.2/8.8	37.0/55.1	N/A

Table 9D.1-3 (Sheet 2 of 2). Material Properties Used in the WGOTHIC Containment Evaluation Model

Material		Thermal Conductivity [(W/m-°C)/ (BTU/hr-ft-°F)]	Volumetric Heat Capacity [(MJ/m^3-°C)/ (BTU/ft^3-°F)]	Emissivity
Group K Stainless Steel	21°C/70°F	12.8/7.4	35.6/53.1	N/A
	37.8°C/100°F	13.0/7.5	35.8/53.4	N/A
	65.6°C/150°F	13.3/7.7	36.6/54.5	N/A
	93.3°C/200°F	13.7/7.9	36.6/54.6	N/A
	121°C/250°F	14.2/8.2	37.4/55.7	N/A
	149°C/300°F	14.5/8.4	37.4/55.8	N/A

Notes:

1. Emissivity is only credited outside containment

Table 9D.1-4. Plant Requirements for Metal Heat Sinks Inside Containment

Region	Metal Volume [m^3 (ft^3)] (minimum – maximum)
Above the operating deck	133.9 – 205.7 (4,730 – 7,264)
Inside SG/Pressuriser compartments	28.37 – 47.46 (1,002 – 1,676)
Below the operating deck	148.2 – 234.9 (5,232 – 8,296)
Total	326.81 – 488.07 (11,541 (3) - 17,236)

Notes:

1. Does not include the containment vessel.
2. Only includes structures and equipment that are typically less than or equal to containment ambient temperature.
3. The total minimum volume includes an additional 16.3 m^3 (577 ft^3) of metal inside containment.

Table 9D.1-5 (Sheet 1 of 3). Heat Sinks Credited in the Peak Containment Pressure Analyses

Description	Material	Surface Area [(m^2)/(ft^2)]	Metal Volume [(m^3)/(ft^3)]	Metal Effective Thickness [(cm)/(in)]
Above the Operating Deck				
Containment vessel above the operating deck	Carbon Steel A	5,851.8/62,988	254.5/8,986	4.128/1.625 and 4.445/1.750
Polar crane bridge and trolley	Carbon Steel B	836.1/9,000	54.82/1,936	6.556/2.581
Crane girder	Carbon Steel A	1,069.2/11,509	33.70/1,190	3.152/1.241
Circular walkway at 49.4m (162')	Carbon Steel B	1,095.9/11,796	9.77/345	0.892/0.351
Upper manway platforms at 50.6m (166') above SG rooms and ADS platform at 50.6m (166') and 53.913m (176.88') over pressuriser compartment	Carbon Steel B	1,213.3/13,060	6.74/238	0.556/0.219
Internal stiffener	Carbon Steel A	215.5/2,320	6.57/232	3.043/1.198
Integrated head stands	Carbon Steel B	64.3/692	4.81/170	7.468/2.940
Recirculation unit platforms at 46.6m (153') (CH53, CH57)	Carbon Steel B	758.5/8,164	4.67/165	0.615/0.242
Outer SG compartment walls (loop B)	Carbon Steel B, Concrete	168.0/1,808	3.94/139	2.34/0.922
Outer SG compartment walls (loop A)	Carbon Steel B, Concrete	146.0/1,572	2.97/105	2.03/0.800
Outer pressuriser walls	Carbon Steel B, Concrete	103.8/1,117	2.2/77	2.11/0.832
Stairs outside SG compartments	Carbon Steel B	408.2/4,394	2.1/74	0.511/0.201
Attachment plates above the operating deck	Carbon Steel A	63.0/678	1.8/62	2.769/1.090
Inside SG Compartments and Pressuriser Compartment				
Inner SG room walls (loop B)	Carbon Steel B, Concrete	635.3/6,838	10.3/364	1.62/0.639
Inner SG room walls (loop A)	Carbon Steel B, Concrete	533.1/5,738	8.89/314	1.67/0.656
Inner pressuriser compartment walls	Carbon Steel B, Concrete	274.8/2,958	4.25/150	1.54/0.608

Table 9D.1-5 (Sheet 2 of 3). Heat Sinks Credited in the Peak Containment Pressure Analyses

Description	Material	Surface Area [(m^2)/(ft^2)]	Metal Volume [(m^3)/(ft^3)]	Metal Effective Thickness [(cm)/(in)]
Lower manway platforms at 31.88m (104'-7") in SG compartments	Carbon Steel B	337.3/3,631	3.20/113	0.953/0.375
Tubesheet platforms at 35.51m (116'-6") in SG compartments	Carbon Steel B	369.7/3,979	0.93/33	0.254/0.100
Steel plate at 29.1m (95'-6") in SG compartment (loop B)	Stainless Steel K	22.2/239	0.76/27	3.480/1.370
Flow-Through Compartments Below the Operating Deck				
Containment vessel below operating deck	Carbon Steel A	964.43/10,381	42.87/1,514	4.445/1.750
CMTs	Carbon Steel C	195.9/2,109	33.61/1,187	17.16/6.754
Floor framing below operating deck	Carbon Steel A	858.1/9,236	14.0/495	1.63/0.643
Platform at 36.12m (118'-6") between maintenance floor and maintenance floor mezzanine	Carbon Steel B	2,573.7/27,703	12.4/439	0.483/0.190
Columns in maintenance floor room	Carbon Steel B	209.5/2,255	9.34/330	4.455/1.754
Curved IRWST wall	Stainless Steel K	381.8/4,110	6.20/219	1.62/0.639
Walls in maintenance floor and maintenance floor mezzanine	Carbon Steel B, Concrete	838.8/9,029	10.5/371	1.25/0.493
Walls in reactor coolant drain tank (RCDT) room and vertical access (VA) room	Carbon Steel B, Concrete	275.6/2,966	3.77/133	1.37/0.538
Platforms at 25m (83') and 32.6m (107'), and stairs in VA room	Carbon Steel B	290.9/3,131	1.1/37	0.356/0.140
Ceiling of maintenance floor mezzanine, Q-deck	Carbon Steel B, Concrete	515.8/5,552	0.79/28	0.15/0.060
Ceiling of maintenance floor mezzanine, steel plate (south)	Carbon Steel A, Concrete	47.8/514	0.37/13	0.744/0.293
Ceiling of pressuriser spray valve room	Carbon Steel B, Concrete	18.5/199	0.2/8	1.27/0.500

Table 9D.1-5 (Sheet 3 of 3). Heat Sinks Credited in the Peak Containment Pressure Analyses

Dead-end Compartments Below the Operating Deck				
Description	**Material**	**Surface Area [(m^2)/(ft^2)]**	**Metal Volume [(m^3)/(ft^3)]**	**Metal Effective Thickness [(cm)/(in)]**
Accumulators	Carbon Steel C	150.1/1,616	7.48/264	4.976/1.959
PXS compartments walls	Carbon Steel B, Concrete	510.2/5,492	7.39/261	1.45/0.569
Upper refuelling room walls	Stainless Steel K, Concrete	482.3/5,191	6.17/218	1.28/0.503
Platforms in PXS compartments	Carbon Steel B	595.0/6,404	4.47/158	0.752/0.296
CVS compartment walls	Carbon Steel B, Concrete	266.5/2,869	3.40/120	1.27/0.500
Demineralisers, reactor coolant filters in CVS compartment	Stainless Steel J	33.8/364	3.09/109	9.14/3.599
IRWST ceiling	Stainless Steel K, Concrete	202.0/2,174	2.5/87	1.22/0.479
PXS compartments ceiling	Carbon Steel A, Concrete	155.0/1,668	2.0/70	1.27/0.500
Lower refuelling room walls	Stainless Steel K, Concrete	108.1/1,164	1.9/66	1.73/0.681
CVS compartment ceiling	Carbon Steel A, Concrete	63.1/679	0.79/28	1.27/0.500
Hatches over PXS, CVS Rooms	Carbon Steel D	5.8/62	0.48/17	8.367/3.294

Table 9D.2-1. Parameters For LOCA Long-Term Containment Analysis

Number of Loops	2
Active Core Length (m/ft)	4.27/14.0
Core Power, license application (MWt)	3400
Nominal Vessel Inlet Temperature (°C/°F)	279.7/535.5
Nominal Vessel Outlet Temperature (°C/°F)	322.3/612.2
Steam Pressure (MPa/psia)	5.998/870.0
Rod Array	17 x 17
Accumulator Temperature (°C/°F)	48.89/120.0
Containment Design Pressure (MPa/psia)	0.508/73.7

Table 9D.3-1. Parameters For Steamline Break Mass And Energy Releases Inside Containment Analysis

Plant data for all cases:	
Power, Nominal Rating (MWt)	3415
Nominal RCS Flow [(m^3/hr)/GPM)]	68,108.7/299,880
Nominal Full Load T_{avg} (°C/°F)	300.9/573.6
Nominal RCS Pressure (MPa/psia)	15.51/2250
Nominal Steam Temperature (°C/°F)	274.2/525.5
Nominal Feedwater Enthalpy [(J/kg)/(BTU/lbm)]	9.755E+05/419.4

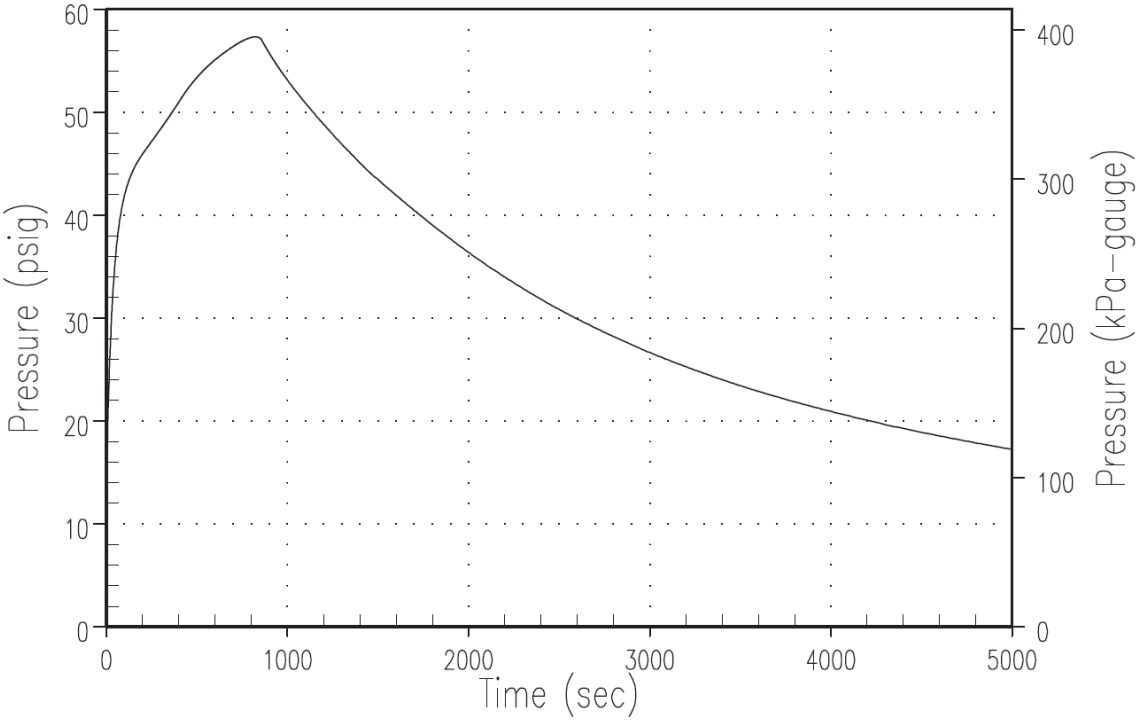


Figure 9D.1-1. AP1000 Containment Pressure Response for Full DER MSLB – 30% Power

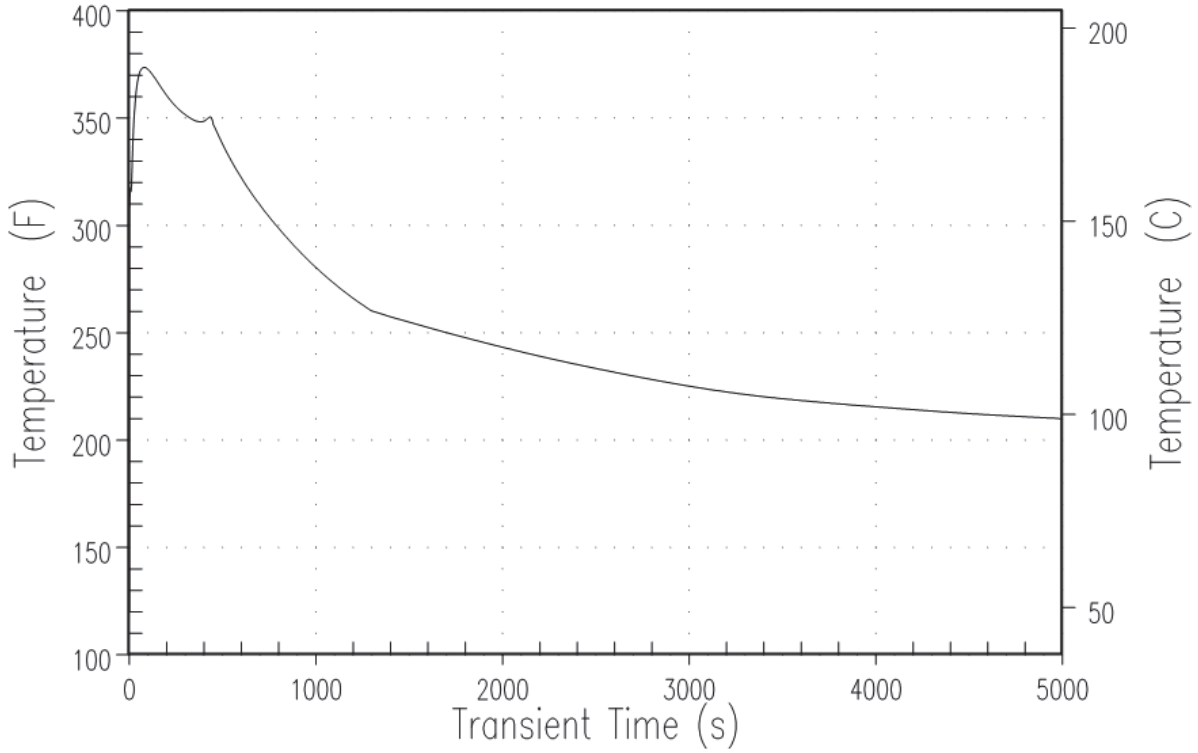


Figure 9D.1-2. AP1000 Containment Temperature Response for Full DER MSLB – 101% Power

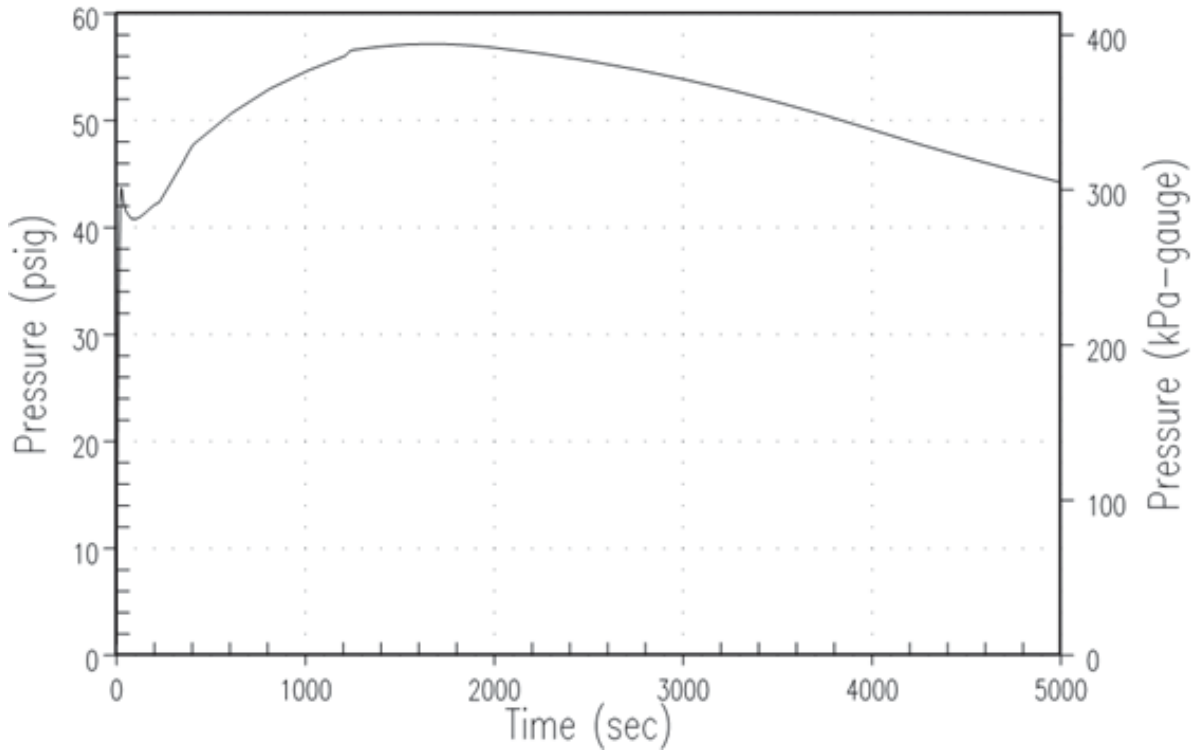


Figure 9D.1-3. AP1000 Containment Pressure Response for DECLG LOCA – 5000 sec

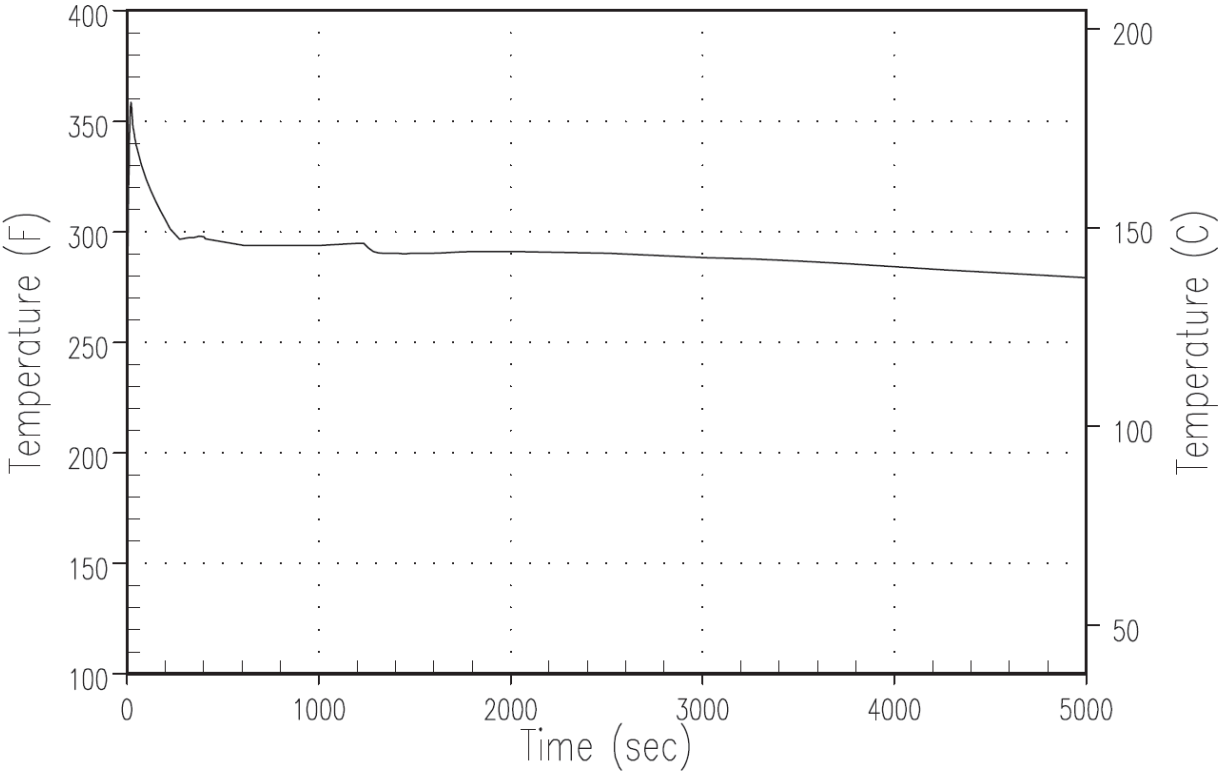


Figure 9D.1-4. AP1000 Containment Temperature Response for DECLG LOCA – 5000 sec

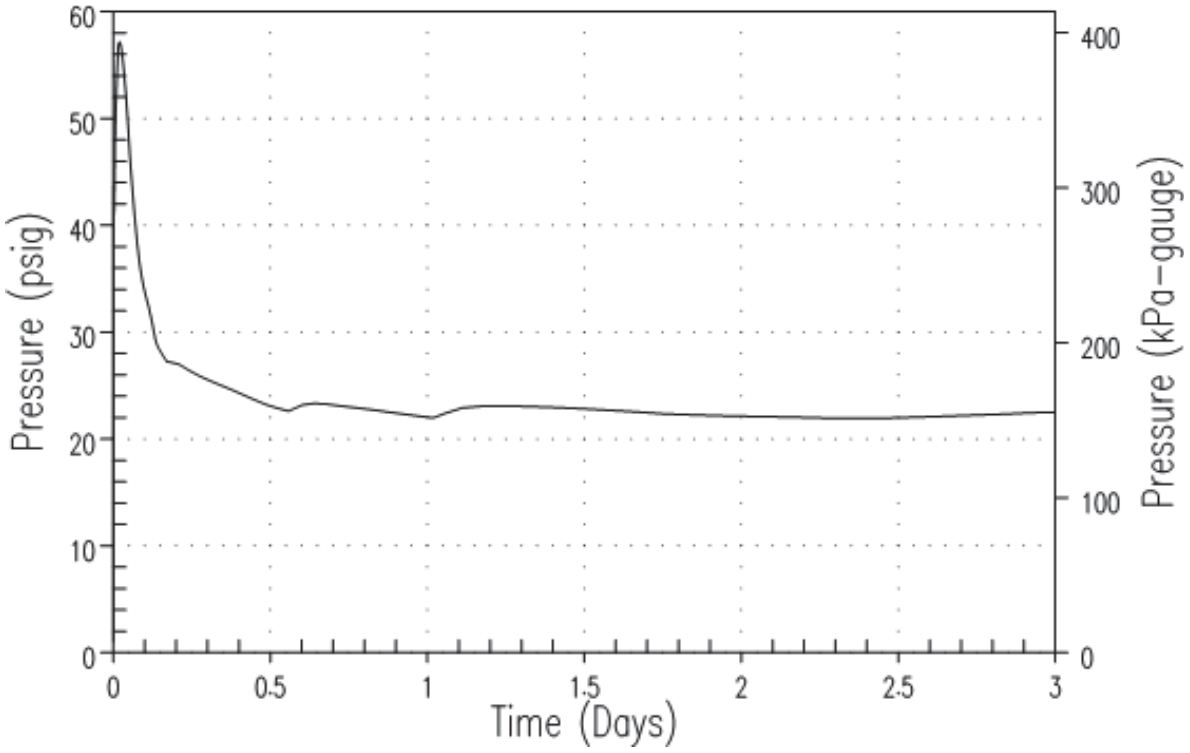


Figure 9D.1-5. AP1000 Containment Pressure Response for DECLG LOCA – 3 Days

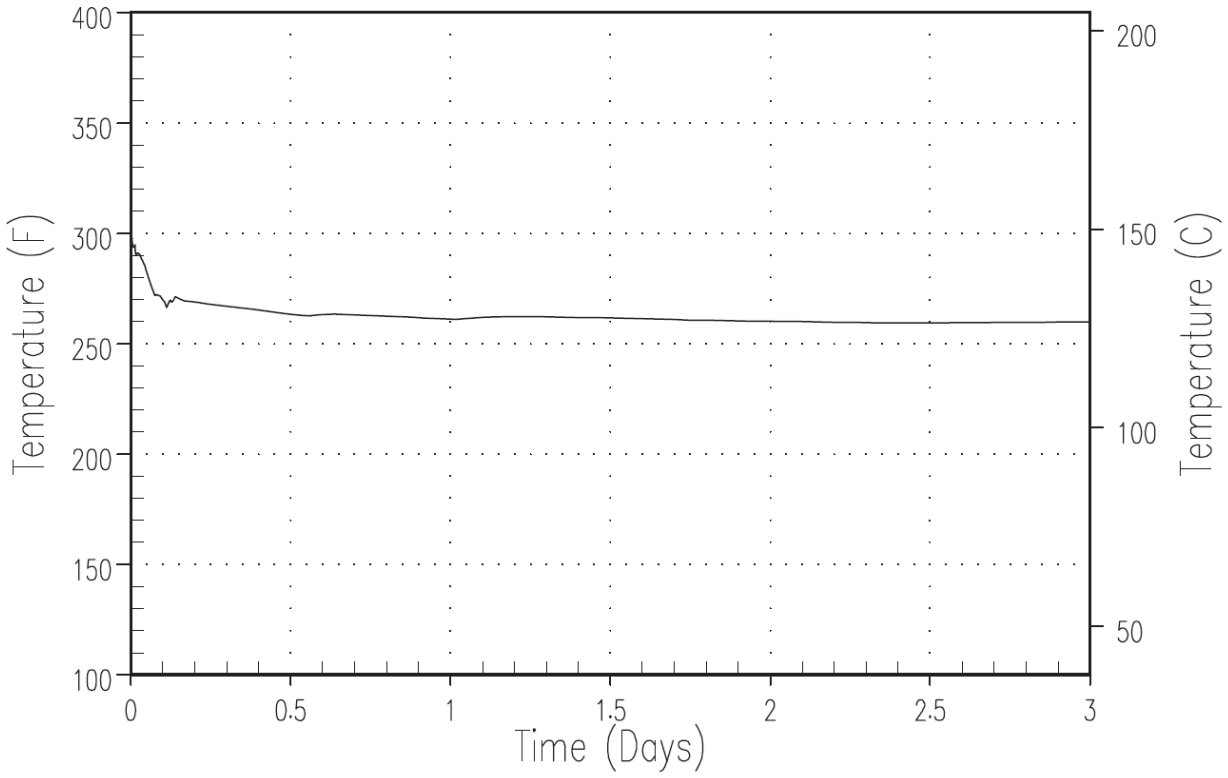


Figure 9D.1-6. AP1000 Containment Temperature Response for DECLG LOCA – 3 Days

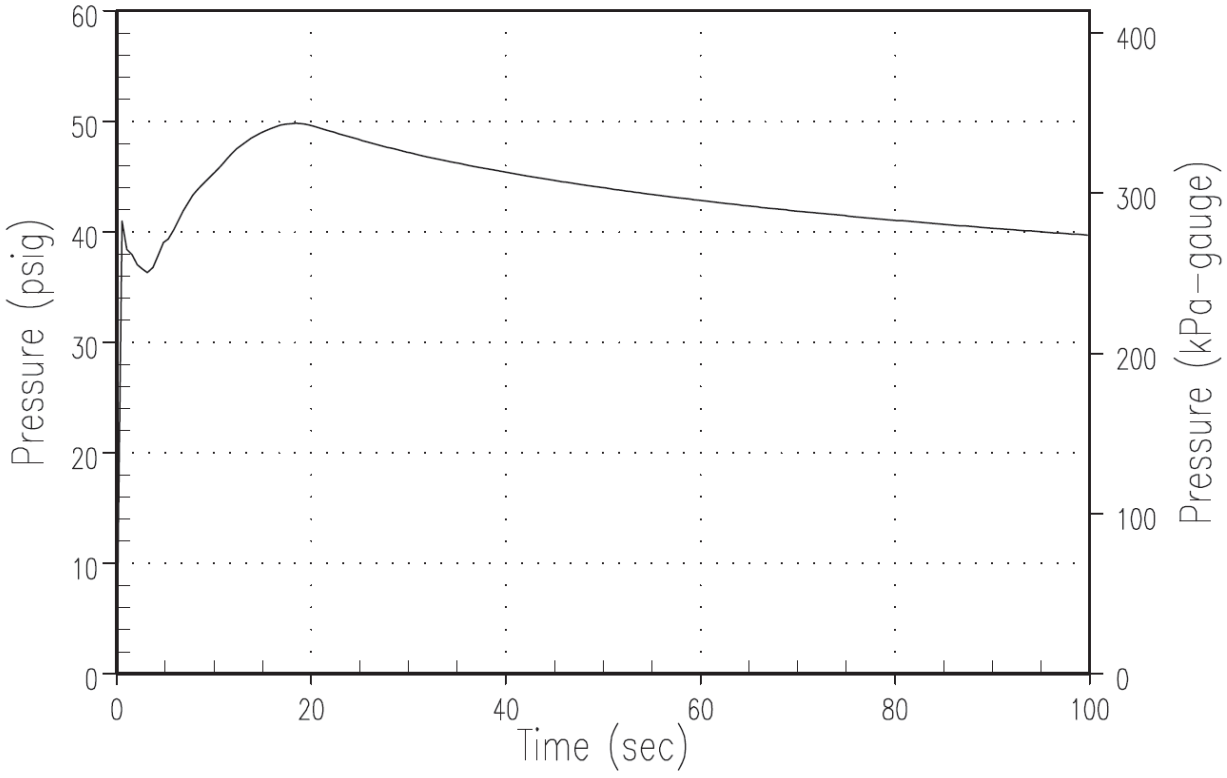


Figure 9D.1-7. AP1000 Containment Pressure Response – DEHLG LOCA

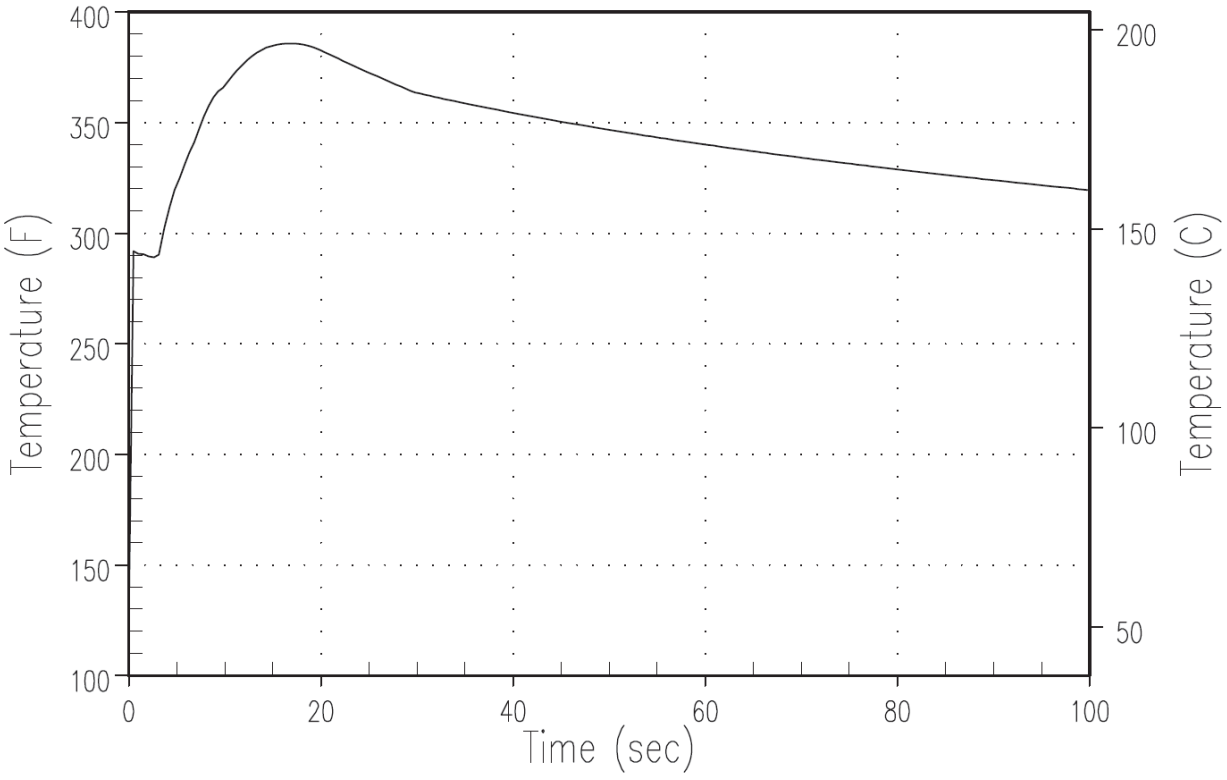


Figure 9D.1-8. AP1000 Containment Temperature Response for DEHLG LOCA

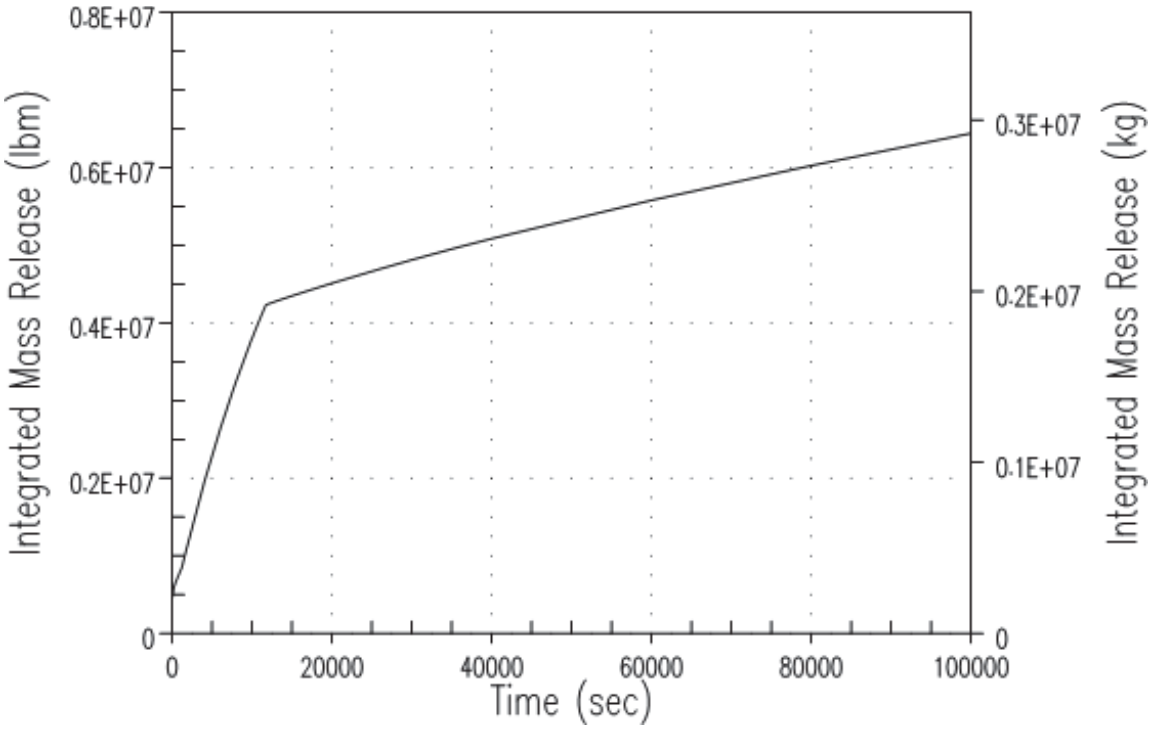


Figure 9D.2-1. AP1000 DECLG Integrated Break Flow

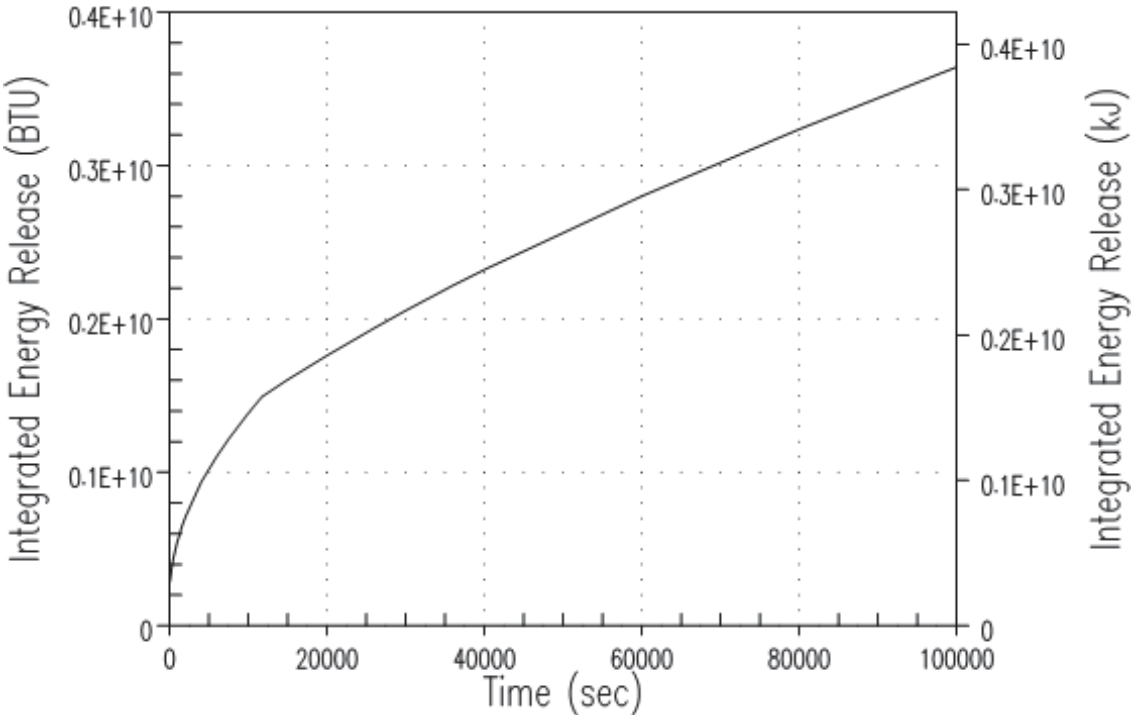


Figure 9D.2-2. AP1000 DECLG LOCA Integrated Energy Released

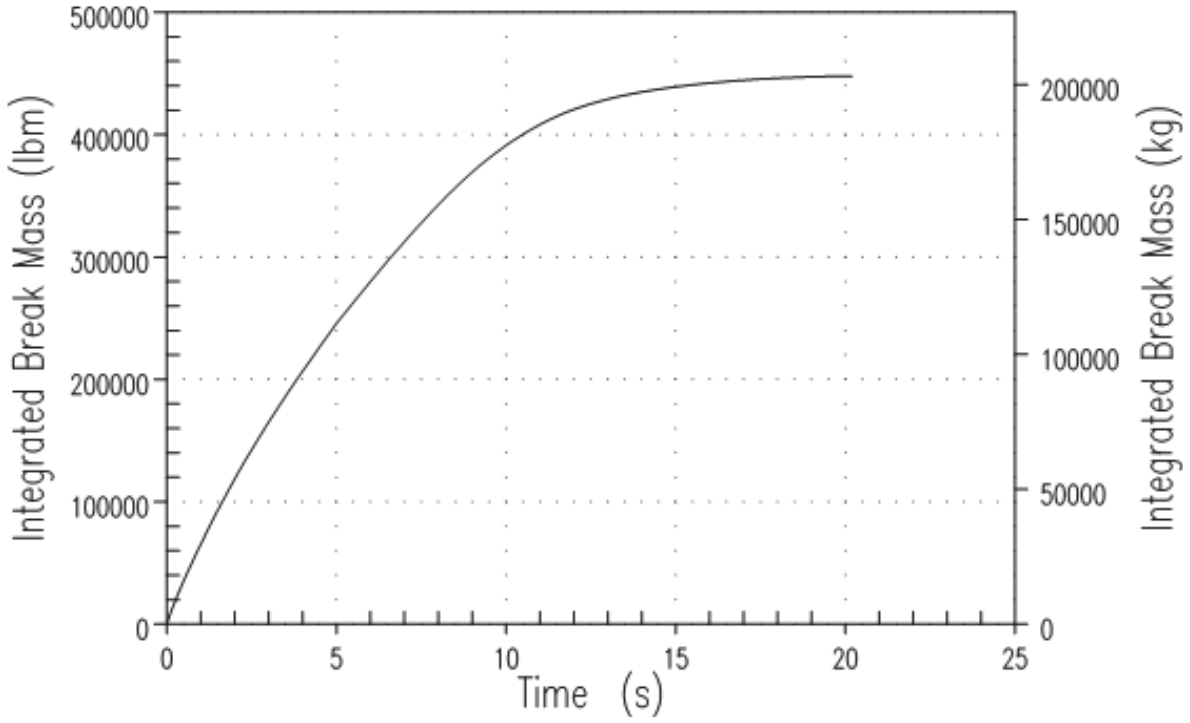


Figure 9D.2-3. AP1000 DEHLG Integrated Break Flow

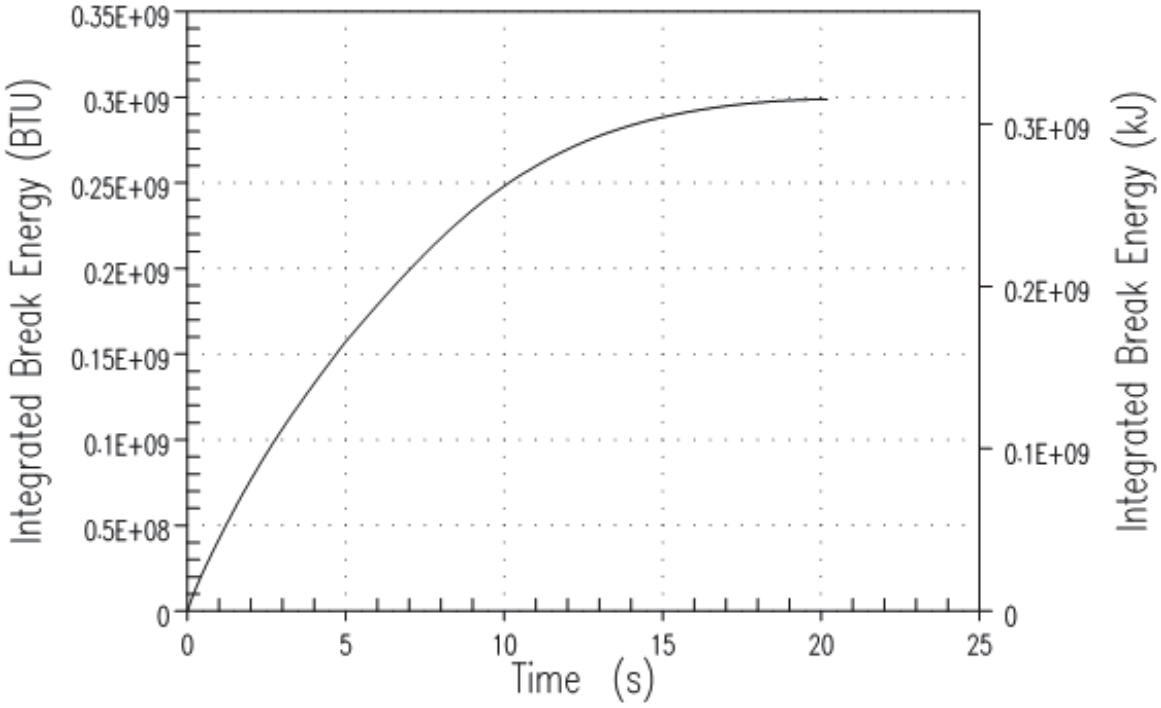


Figure 9D.2-4. AP1000 DEHLG LOCA Integrated Energy Released

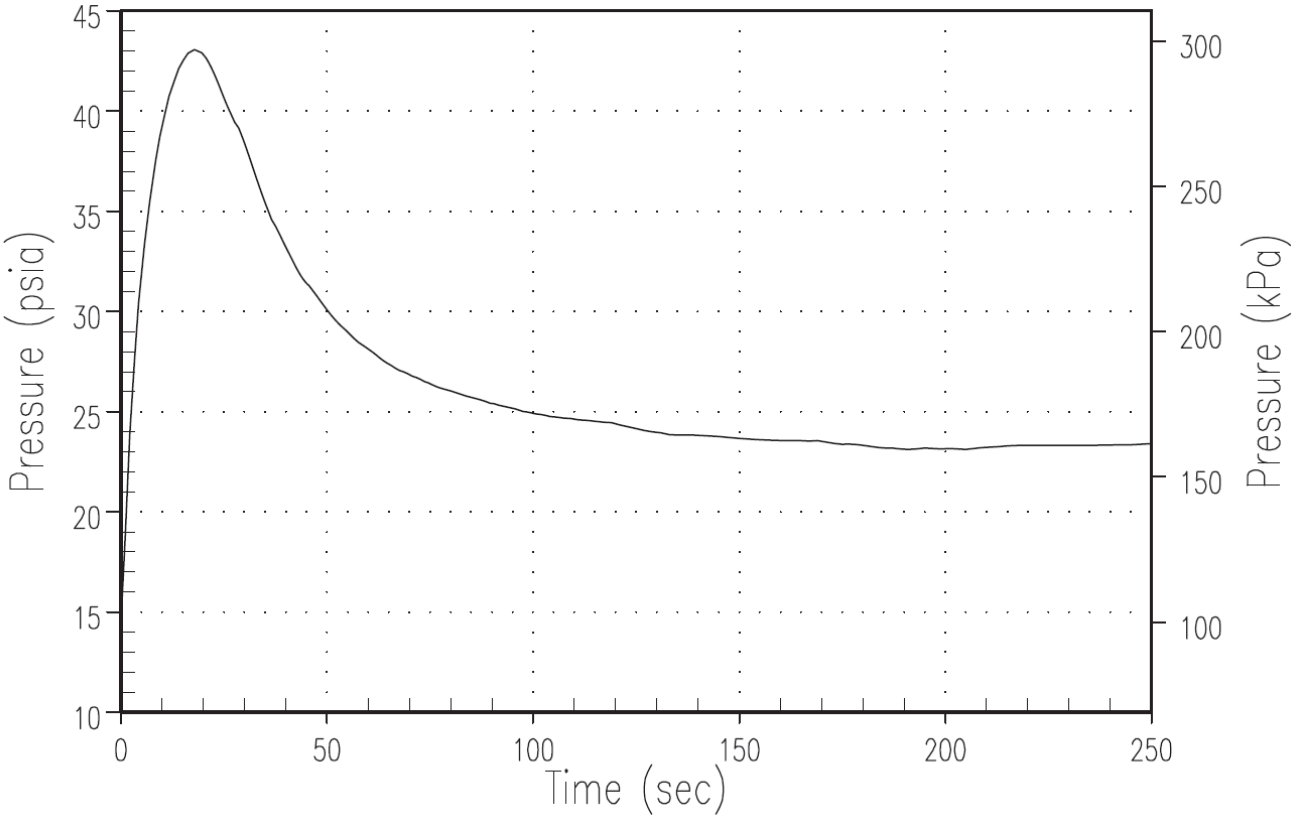


Figure 9D.4-1. AP1000 Minimum Containment Pressure for DECLG LOCA

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS AND ACRONYMS

ac	alternating current
ADS	automatic depressurisation system
ALARP	as low as reasonably practicable
ALWR	advanced light water reactor
ANS	American Nuclear Society
ANSI	American National Standards Institute
AOP	abnormal operating procedures
AOV	air-operated valve
ASME	American Society of Mechanical Engineers
ATWT (ATWS)	anticipated transient without trip (scram in US terminology)
BAST	boric acid storage tank
BE	basic event
BMMT	base mat melt through
BP	containment bypass
BPL	bistable processor logic
BSL	basic safety level
BSO	basic safety objective
CAFTA	comprehensive automated fault tree analysis software
CAS	compressed and instrument air system
CCDP	conditional core damage probability
CCCG	component common cause group
CCI	core concrete interaction
CDS	condensate system
CIV	containment isolation valve
C&I	control and instrumentation
CCF	common-cause failure
CCS	component cooling water system
CDF	core damage frequency
CET	containment event tree
CFE	containment failure early
CFI	containment failure intermediate
CFL	containment failure late
CHF	critical heat flux
CI	containment isolation
CLP	cask loading pit
CMT	core makeup tank
CNS	containment system
CST	condensate storage tank
CVS	chemical and volume control system
CWS	circulating water system
DAS	diverse actuation system
DBA	design basis accident
dc	direct current
DCH	direct containment heating
DEG	double-ended guillotine
DDS	data display and processing system
DDT	deflagration to detonation transition
DG	diesel generator
D-RAP	design reliability assurance programme
DRP	design reference point
DVI	direct vessel injection

LIST OF ABBREVIATIONS AND ACRONYMS (cont.)

ECS	main ac power system
EDE	effective dose equivalent
EDS	DC and uninterruptible power supply system
EOP	emergency operating procedures
EPRI	Electric Power Research Institute
EPS	electric power distribution systems
ESF	engineering safety features
FAI	Fauske and Associates, Inc.
FDF	fuel damage frequency
FPS	fire protection system
FWIV	feedwater isolation valve
FWLB	feedwater line break
FWS	main and startup feedwater system
GDA	generic design assessment
GPAB	global plant analysis boundary
HCLPF	high confidence of low probability of failure
HCS	central chilled water high capacity system
HELB	high-energy line break
HEP	human error probability
HF	human factors
HFE	human failure events
HPME	high-pressure melt ejection
HRA	human reliability analysis
HX	heat exchanger
HVAC	heating, ventilation, and air conditioning
IAEA	International Atomic Energy Agency
IC	intact containment
ICRP	International Commission on Radiological ProtectionIE initiating event
IDS	essential electrical supply system
IF-PSA	internal flooding probabilistic safety assessment
ILP	integrated logic processors
IRWST	in-containment refuelling water storage tank
IS	interfacing system
ISLOCA	interfacing-system loss-of-coolant accident
IV	isolation valve
IVR	in-vessel retention
kPa	kilopascal
LCF	late containment failure (CET end state)
LCL	local coincidence logic
LERF	large early release frequency
LIRF	large intermediate release frequency
LLOCA	large loss-of-coolant accident
LOCA	loss-of-coolant accident
LOOP	loss of offsite power
LP	low pressure
LPME	low-pressure melt ejection
LPSD	low power and shutdown
LRF	large release frequency
LTCA	long term cooling analysis
LVRF	large venting release frequency
LWR	light water reactor

LIST OF ABBREVIATIONS AND ACRONYMS (cont.)

MAAP	Modular Accident Analysis Programme
MCCI	molten core concrete interaction
MCR	main control room
MFCV	main feedwater control valve
MFW	main feedwater
MLOCA	medium loss-of-coolant accident
MG	motor-generator
MOV	motor-operated valve
MSIV	main steam isolation valve
MSLB	main steam line break
MSSV	main steam safety valve
NPP	nuclear power plant
NPSH	net positive suction head
NRC	Nuclear Regulatory Commission
NSSS	nuclear steam supply system
ONR	Office for Nuclear Regulation
OTDT	over temperature delta T
PAF	plant availability factor
PAM	post-accident monitoring
PAR	passive autocatalytic recombiner
PCCWST	passive containment cooling water storage tank
PCCAWST	passive containment cooling ancillary water storage tank
PCS	passive containment cooling system
PCSR	Pre-Construction Safety Report
PDS	plant damage state
pga	peak ground acceleration
PGS	plant gas system
PLS	plant control system
PMS	protection and safety monitoring system
PORV	power-operated relief valve
POS	plant operating state
PWROG	Pressurized Water Reactor Owners Group
PRA	probabilistic risk assessment (US terminology for PSA)
PRHR	passive residual heat removal
PSA	probabilistic safety assessment
PWR	pressurised water reactor
PXS	passive core cooling system
RAW	risk achievement worth
RC	release category
RCP	reactor coolant pump
RCS	reactor coolant system
RNS	normal residual heat removal system
ROAAM	risk-oriented accident analysis methodology
RPV	reactor pressure vessel
RRW	risk reduction worth
RWS	raw water system
RV	reactor vessel
SAA	severe accident analysis
SAMDA	severe accident mitigation design alternative
SAMG	severe accident management guidance

LIST OF ABBREVIATIONS AND ACRONYMS (cont.)

SAP	safety assessment principle
SBO	station blackout
SFCV	startup feedwater control valve
SFP	spent fuel pool
SFS	spent fuel pool cooling system
SFW	startup feedwater
SG	steam generator
SGS	steam generator system
SGTR	steam generator tube rupture
SI	safety injection
SLB	steam line break
SLOCA	small loss-of-coolant accident
SMA	seismic margin assessment
SOAR	state-of-the-art
SORV	stuck open relief valve
SOV	solenoid operated valve
SSC	system, structure, or component
SSIE	support system initiating event
SSE	safe shutdown earthquake
SSS	secondary sampling system
SVC	squib valve controller
SV	safety valve
SWS	service water system
TC	components and type codes
TEDE	total effective dose equivalent
THERP	technique for human error rate prediction
T-H	thermal-hydraulic
T&M	test and maintenance
TLFW	total loss of feedwater
TOPS	over pressure protection
UCSB	University of California at Santa Barbara
UET	unfavourable exposure time
UK	United Kingdom
URD	Utility Requirements Document
US	United States
VAS	radiologically controlled area ventilation system
VBS	nonradioactive ventilation system
VCS	containment recirculation cooling system
VES	main control room emergency habitability system
VHS	hot machine shop HVAC system
VRS	radwaste building HVAC system
VWS	central chilled water system
VXS	annex/auxiliary building nonradioactive ventilation system
WGS	gaseous radwaste system
WLS	liquid radwaste system
ZAS	main generator system
ZOS	onsite standby power system

10 REACTOR FAULTS PROBABILISTIC SAFETY ASSESSMENT AND SEVERE ACCIDENT ANALYSIS

10.1 Introduction

This chapter summarises the results of the AP1000 reactor probabilistic safety assessment (PSA) that are needed within the Pre-Construction Safety Report (PCSR). In addition, it supports and justifies the uses made of those results within the PCSR by doing the following:

- Stating the key assumptions on which the PSA is based.
- Describing the sources of information used in producing the PSA.
- Discussing the uncertainties in the results arising from scope limitation, methodology, assumptions, and other causes, and showing that they do not affect the conclusions being drawn from the results.
- Describing the forward programme for development of the PSA to the level needed for licensing and operation of individual units.

This chapter lists the areas of severe accident analysis that were performed for AP1000 plant and summarises the treatment in the PSA of severe accident phenomena. Severe accidents are defined as those fault sequences involving significant core damage and/or the potential for dose release in excess of design basis limits ((100 mSv (10 rem) offsite or 500 mSv (50 rem) onsite (Reference 10.1)).

10.1.1 Background and Overview

The AP1000 PSA was developed to support the application for United States (US) Design Certification of the AP1000 nuclear plant. The AP1000 design is based extensively on the AP600 standard nuclear plant that received US Design Certification in December 1999. The AP600 PSA, which was reviewed by the US Nuclear Regulatory Commission (NRC) in detail during the seven-year review of the AP600, is used as the starting point for the AP1000 PSA. Since the configuration of the AP1000 reactor and Class-1 systems is the same as the AP600, the AP600 PSA is used as the basis of the AP1000 PSA with relevant changes implemented in the model to reflect the AP1000 design changes. Additional AP1000 plant specific thermal-hydraulic (T-H) analyses are performed in order to determine the system success criteria. The core damage frequency (CDF) and large release frequency (LRF) are calculated for internal events. Selected internal hazard events and shutdown models are also quantitatively assessed to derive plant insights and plant risk conclusions. Seismic events are assessed using a margin approach to derive plant insights and plant risk conclusions. Other external hazards are evaluated with a qualitative approach.

The purpose of the PSA is to demonstrate that the risk goals are met and to provide inputs to the optimisation of the AP1000 design. As in the AP600, the PSA is being performed interactively with the design, analysis and operating procedures. The historical use of PSA and severe accident analysis to inform the AP1000 design is provided in APPENDIX 10A, Section 10A.1. Section 10A.2.2 shows that there were numerous design improvements made to the AP600 based on PSA insights. Section 10A.2.3 also shows that there were fewer, less significant, plant improvements made to the AP1000 plant based on PSA insights. Note that the very low risk of the AP600 plant has been maintained in the AP1000 plant. Insights from the analysis are provided discussing the effect on the PSA of differences between the AP600 and the AP1000 nuclear power plant (NPP) designs.

10.1.2 How the Reactor Probabilistic Safety Assessment Results Are Used Within the Pre-Construction Safety Report

The PSA is part of the fault and accident assessment for the AP1000 design. An overview of the entire assessment process is given in Chapter 8. The PSA results have been used in the PCSR to demonstrate the compliance with the Office for Nuclear Regulations (ONR) numerical targets and in the demonstration that the overall risks from planned operation of the reactor are as low as reasonably practicable (ALARP). Compliance with the quantitative targets is demonstrated in Chapter 14, where the risks and the frequencies of reactor accidents in different dose bands, as calculated in the PSA, are added to the corresponding quantities for non-reactor faults calculated in Chapter 9, and the totals compared with the targets.

The ALARP arguments made in Chapter 14 make use of the PSA results and analysis, both through the identification of design alternatives based on PSA insights (Section 14.6.3) and through the evaluation of alternatives on the basis of risk. The design alternatives considered include not only Level 1 measures to reduce CDF, but also the severe accident mitigation design alternatives (SAMDAs) aimed at reducing the size and frequency of releases following core damage (Section 14.7.3).

In addition, the estimated frequencies of different reactor initiating events (IEs) are included in the Fault Schedule (Appendix 8A), and are used in Chapter 9 in combination with design basis dose assessments to demonstrate compliance with the quantitative dose-frequency target for design basis accidents (DBAs) (Target 4).Finally, the spread of risk across the different types of reactor accidents is used in this chapter to demonstrate the well-balanced nature of the reactor design, with no particular accident providing a disproportionate share of the overall risk.

10.1.3 Documentation

The at-power internal events model has been updated since APP-GW-GL-022 (Reference 10.1). The updated at-power internal events model is summarized in this chapter. Results given in this chapter reflect these updates.

In addition, the fuel damage frequency from fuel pool faults was determined in UKP-GW-GL-743 (Reference 10.2). The fuel pool risk assessment is presented in Section10.19.

10.1.4 Scope and Exclusions

The updated PSA consists of a Level 1 and Level 2 analysis. The Design Reference Point (DRP) for the updated at-power Internal Events PSA corresponds with Revision 17 of the DCD.

The Level 1 analysis includes:

- Internal IEs evaluation
- Event tree and success criteria analyses
- Plant systems analysis using fault tree models
- Common cause failure and human reliability analyses
- Data analysis
- Fault tree and event tree quantification to calculate the core damage frequency

The Level 2 analysis includes:

- An evaluation of severe accident phenomena and fission product source terms
- Modelling of the containment event tree and associated success criteria
- Analysis of hydrogen burning and mixing

The Level 3 analysis for offsite dose evaluation was determined in APP-GW-GL-022 (Reference 10.1). This assessment has not been updated based on the updated at-power internal events PSA.

The low power and shutdown (LPSD) PSA was determined in APP-GW-GL-022 (Reference 10.1). This assessment has not been updated based on the updated at-power internal events PSA.

Area events and external events analyses, which have been updated based on the updated at-power internal events PSA, include:

- Internal fire assessment
- Internal flooding assessment
- External hazards qualitative screening assessment

The seismic margin assessment was determined in APP-PRA-GSC-027 (Reference 10.78). This assessment has not been updated based on the updated at-power internal events PSA.

The PSA does not address faults involving fuel-handling or other sources of radioactivity outside the reactor core.

The fuel damage frequency from fuel pool faults was determined in UKP-GW-GL-743 (Reference 10.2). This reference has not been updated based on the updated at-power internal events PSA.

10.2 Internal Initiating Events

10.2.1 Overview of IE Analysis Methodology

An IE is defined as an event which perturbs the steady state operation of the plant by challenging plant control and Class-1 systems whose failure could potentially lead to core damage or release of airborne fission products. The IEs described in this section are limited to the internal IEs that occur either as a result of equipment failures or operator action errors while performing tests, maintenance, or other task requirements. These internal IEs may cause a sequence of accident events during plant power operation that may lead to a core damage state. Initiating events are categorized into two different types: Loss of Coolant Accident (LOCA) and Transients.

LOCAs are accidents involving the rupture or failure of the Reactor Coolant System (RCS) boundary including piping, valves, pressure vessel, and interconnecting systems. The LOCAs consider loss of primary coolant inventory inside and outside the containment structure. LOCAs in the containment building are grouped into categories based on the rate of primary coolant loss that can be expressed as the size of the break. Large LOCA, medium LOCA, small LOCA, RCS leakage, safety injection line break, core makeup tank (CMT) line break, and passive residual heat removal (PRHR) tube rupture are considered as events where

equipment can mitigate core damage. Vessel ruptures beyond the core cooling system capability are considered as non-coolable events. Inadvertent valve opening events, such as spurious actuation of the Automatic Depressurization System (ADS) valves, are treated explicitly as inside containment LOCAs. LOCAs that may divert RCS coolant outside containment are segregated into steam generator tube rupture (SGTR) and interfacing system LOCA (ISLOCA) categories. Each of these initiators affects the plant and the event sequence differently and, therefore, is addressed separately.

Transient events disrupt normal plant operation sufficiently to cause a reactor trip and require decay heat removal, but do not directly result in a LOCA. NUREG/CR-3862 (Reference 10.21) classifies the abnormal events leading to pressurized water reactor (PWR) plant challenges into categories. These categories presented along with categories from NUREG/CR-5750 (Reference 10.22) and NUREG/CR-6928 (Reference 10.15) are generally applicable to existing PWR plants. The secondary side breaks upstream and downstream of the main steam line isolation valves and the main steam line stuck-open safety valve are considered as transients because the primary circuit remains intact during these events.

Events that only may occur during hot standby, hot shutdown, cold shutdown, and refuelling are not considered in this section. IEs due to internal fires or floods, and external events are not considered in this section.

For the initial condition, full-power operation, the plant transient condition will result in a reactor trip and challenge the Class-1 systems. Additionally, technical specification violations that require a shutdown in less than 8 hours are included as an IE. In less sudden transients, such as controlled power reductions that do not induce trips, there is a high probability that plant operators will affect an orderly plant shutdown without Class-1 system actuation. Orderly or controlled shutdowns, such as technical specification required shutdowns where the completion time is longer than 8 hours, are not considered IEs since they do not challenge the plant Class-1 systems.

Initiating event analysis is carried out in the following sequence of steps:

- Identification of candidate events
- Quantification of IE frequencies
- Grouping of candidate IEs

10.2.1.1 Identification of Candidate Events

There are two methods used to identify potential IEs. The first is to review reactor operating experience. In this approach, both industry and plant specific operating experiences are reviewed and classified to enumerate the plant trips and IEs that have actually occurred. Both the industry and the NRC have sponsored generic industry surveys of this experience. These surveys as well as plant specific data are reviewed and factored into the evaluation. Since there is no AP1000 plant operating experience available at this time, only generic operating experience can be reviewed.

In addition to reviewing operating experience, a systematic evaluation of plant systems was performed to identify IEs resulting from equipment failures. System engineer interviews were also conducted to review system and equipment failures that could result in an IE.

10.2.1.2 Quantification of Initiating Event Frequency

Initiating event frequency (IEF) data can be obtained directly from a generic data source or quantified by using fault-tree modelling. Fault-tree modelling is typically used for the quantification of support system initiating events (SSIEs). There are some unique IEs where generic data is not representative of the AP1000 plant design and does not result in the loss of a support system. In these cases, alternative methods for IEF quantification are utilized and documented. The following subsections identify the methods for generating IEFs.

10.2.1.2.1 Single Basic Event Initiators

Single Basic Event IEFs can be calculated using generic and/or plant-specific data and are incorporated into the model as a single basic event. Since there is no operational history available for AP1000 plants, only generic data is available and utilized to determine IEFs.

The primary data source for generic IEFs is NUREG/CR-6928 (Reference 10.15). Alternate data sources are used and documented if a given frequency is not available in the primary data source or if an alternate data source is more relevant for a given event than the primary data source. Justification for the use of an alternate data source is documented in the IE analysis.

All single basic event initiators shall be in units of reactor operating state year. The plant availability factor (PAF) is modelled as a basic event in the linked internal events model.

10.2.1.2.2 Support System Initiating Event Frequency

An SSIE occurs when the loss of a normally operating system results in an IE and can adversely affect one or more systems used to mitigate the IE. Loss of a support system can lead to an immediate reactor trip or a delayed reactor trip due to the consequential loss of a mitigating system. Loss of a support system that does not generate an immediate reactor trip but could result in an administrative shutdown due to a technical specification violation is not considered to be an IE and can be screened. Support system IEs are quantified using a fault tree analysis method consistent with the Electric Power Research Institute (EPRI) SSIE guidance (Reference 10.23).

10.2.1.2.3 Interfacing System Loss of Coolant Accident (ISLOCA) Event Frequency

ISLOCA refers to LOCAs outside of the containment. This type of LOCA challenges the ability to achieve a safe stable state, because the RCS inventory losses are outside containment. ISLOCAs are typically initiated by the failure of multiple pressure isolation devices in a line connected to the RCS that penetrates the containment and interfaces with low pressure piping outside containment. The failure of a high to low pressure interface at full power would result in overpressurization and potentially the subsequent failure of the low pressure system piping or components (e.g., heat exchanger tubing, pump seals, etc.). ISLOCA IE analysis can be broken down into two tasks. The first task is the identification of potential ISLOCA pathways and the second task is to quantify the IE frequency for each non screened path from task one. The ISLOCA event identification and quantification methods are consistent with the guidance provided in Reference 10.24. ISLOCAs for each pathway is quantified to generate an IEF.

10.2.1.2.4 Special Initiating Events – Others

There are some unique IEs where generic data is not representative of the AP1000 plant design and the event is not due to of a loss of a support system or an ISLOCA event. In these

cases, alternative methods for frequency calculations are utilized and documented. Relevant data from other generic sources are reviewed for applicability to the design and operation of the AP1000 plant. If generic data is not available, an IEF may be calculated using a fault tree analysis method similar to the support systems IE quantification. This method should address all possible impacts of common cause failures and should not include the contribution due to loss of a support system already quantified.

10.2.1.3 Grouping of Candidate Initiating Events

IEs are combined or grouped to maintain the number of event trees and event sequences to a manageable size and to facilitate quantification. Combining events into a common group is performed based on the similarity of plant response, success criteria, timing, and impact on mitigating systems. Each IE was reviewed using a structured and systematic process to support the grouping of initiators.

10.2.2 Identification of AP1000 Plant Initiating Events

10.2.2.1 Review of Generic Initiating Event Categories

A review was performed of the IEs identified in NUREG/CR-3862 (Reference 10.21), NUREG/CR-5750 (Reference 10.22), and NUREG/CR-6928 (Reference 10.15) to determine if they were applicable to the AP1000 plant design.

10.2.2.2 Review of AP1000 Plant Systems

A systematic evaluation of AP1000 plant systems was performed to identify IEs resulting from equipment failures.

A review for multi-unit IEs was performed. The Raw Water System (RWS) is the only shared system in the AP1000 plant; however it is not modelled as an SSIE. A loss of offsite power (LOOP) affecting multiple units at one site is the only IE identified for multi-unit impact. Note that the impact of a multi-unit LOOP IE is not currently evaluated for the AP1000 plant PSA.

In addition to the initiators from Section 10.2.2.1 that are applicable to the AP1000 plant, the following IEs were identified:

- Spurious Actuation of the ADS
- Spurious In-containment Refuelling Water Storage Tank (IRWST) Actuation
- CMT, Direct Vessel Injection (DVI), and PRHR Line Breaks
- PRHR Tube Rupture
- Reactor Vessel Rupture
- Loss of Additional Support Systems which result in Loss of Component Cooling Water System (CCS), (Loss of Heating, Ventilation, and Air Conditioning (HVAC) to the CCS Pump Room, and Loss of Central Chilled Water High Capacity System (HCS))

The following Protection and Safety Monitoring System (PMS) and Diverse Actuation System (DAS) actuation functions require further evaluation for the general transient category:

- PMS Actuation Functions
  - IRWST Injection
  - Containment Recirculation
  - CMT Injection
  - ADS Actuation
  - PRHR Actuation
  - Passive Containment Cooling Actuation
- DAS Actuation Functions
  - CMT Injection
  - PRHR Actuation
  - Passive Containment Cooling Actuation

The following IEs are typically included in operating plant PSAs but do not apply to AP1000:

- Startup of an inactive reactor coolant pump (RCP) - all RCPs are normally running while at-power.
- Failure of a pressuriser power-operated relief valve (PORV) - the AP1000 plant design does include a pressuriser PORV.
- RCP seal LOCA - the AP1000 plant RCPs are canned-motor pumps and do not have a seal around the motor shaft.

10.2.3 Initiating Events Modeled in the PSA

Table 10-1 provides a summary of the updated IEFs in units of per reactor operating state year for the AP1000 plant PSA. The IE frequencies are also provided in per reactor year in Table 10-1. The per reactor year frequencies in Table 10-1 were calculated by hand using the PAF (assumed to be 0.93). Where applicable, the associated comprehensive automated fault tree analysis software (CAFTA) database variable name or top event is also provided in Table 10-1. Each IE basic event is used in the quantification model in units of per reactor operating state year or SSIE tree. Each IE is multiplied by a PAF basic event to convert from per units of reactor operating state year to units of per reactor year in the linked model.

10.2.3.1 Large LOCA (Break size 22.86 cm (9 inches) diameter or greater)

The large LOCA event is defined as all RCS ruptures with break sizes sufficient to produce a depressurization of the RCS that allows gravity injection from the IRWST. The break size corresponding to this category is a 22.86 cm (9 inches) equivalent diameter or larger break (excluding “vessel rupture event”). The IEF for a large LOCA was calculated from the exceedance frequencies derived from the expert elicitation process documented in NUREG-1829 (Table 7.19 of Reference 10.27). AP1000 plant specific break size exceedance frequencies are interpolated from the known points in NUREG-1829 Table 7.19 using the power law fit method (Reference 10.25). For the AP1000 plant large LOCA category, the break size is greater than a given AP1000 plant effective break size; therefore, the LOCA IEF

is equal to the mean exceedance frequency for that particular AP1000 plant effective break size. Table 10-1 documents the resulting large LOCA IEF.

10.2.3.2 Medium LOCA (Break size between 10.16 and 22.86 cm (4 inches and 9 inches diameter)

The medium LOCA event is defined as all RCS ruptures with break sizes insufficient to depressurize the RCS to allow gravity injection, but sufficient to depressurize the RCS to the Normal Residual Heat Removal System (RNS) operating pressure without operation of the ADS. The break size corresponding to this category is less than 22.86 cm (9 inches) and greater than or equal to 10.16 cm (4 inches) equivalent diameter. On the basis of piping size, the range of this category includes safety injection (SI) line breaks and CMT line breaks. However, because the mitigating systems' response for these break categories is different than that for a medium LOCA, SI and CMT line breaks are evaluated using separate event trees. The IEF for a medium LOCA was calculated from the exceedance frequencies derived from the expert elicitation process documented in NUREG-1829 (Table 7.19 of Reference 10.27). AP1000 plant specific break size exceedance frequencies are interpolated from the known points in NUREG-1829 Table 7.19 using the power law fit method (Reference 10.25). For the medium AP1000 plant LOCA category, the break size ranges are between two given AP1000 plant effective break sizes; therefore, the LOCA IEF is calculated as the difference of the mean exceedance frequencies for those particular AP1000 plant effective break sizes. Table 10-1 documents the resulting medium LOCA IEF.

10.2.3.3 Small LOCA (Break size between 0.95 cm (3/8 inch) and 10.16 cm (4 inches diameter)

The small LOCA is defined as all RCS ruptures with break sizes less 10.16 cm (4 inches) equivalent diameter and greater than those producing leakage that can be made up by the Chemical and Volume Control System (CVS) (about 0.95 cm (3/8 inch) equivalent diameter, which corresponds to a break flowrate of approximately 6.3 L/sec (100 gallons per minute). The IEF for a small LOCA was calculated from the exceedance frequencies derived from the expert elicitation process documented in NUREG-1829 (Table 7.19 of Reference 10.27). AP1000 plant specific break size exceedance frequencies are interpolated from the known points in NUREG-1829 Table 7.19 using the power law fit method (Reference 10.25). For the small AP1000 plant LOCA category, the break size ranges are between two given AP1000 plant effective break sizes; therefore, the LOCA IEF is calculated as the difference of the mean exceedance frequencies for those particular AP1000 plant effective break sizes. Table 10-1 documents the resulting small LOCA IEF.

10.2.3.4 RCS Leak (Break size less than 0.95 cm (3/8 inch diameter)

The RCS Leak is defined as all RCS ruptures with break size less than 0.95 cm (3/8 inch) equivalent diameter (i.e., leaks that can be made-up by the CVS, which corresponds to a break flowrate of approximately 6.3 L/sec (100 gpm). The CVS is designed to make up RCS leaks of 6.3 L/sec (100 gpm) or less. If the CVS fails, the pressuriser water level will decrease and the event will proceed as a small LOCA. The RCS Leak IEF was determined by a review of generic industry data from NUREG/CR-6928 (Reference 10.15) for a very small LOCA. The NUREG/CR-6928 IE name for this event is IE-VSLOCA. Table 10-1 documents the RCS Leak IEF.

10.2.3.5 Spurious Actuation of the Automatic Depressurization System – ADS Stages 1-3

A spurious actuation of ADS Stages 1-3 occurs when any combination of ADS Stages 1-3 valves spuriously operate and open a flow path from the RCS into the IRWST. The frequency

for spurious actuation of the ADS Stages 1-3 MOVs is generated by a special initiator fault tree over a one year mission time. The result is documented in Table 10-1.

10.2.3.6 Spurious Actuation of the Automatic Depressurization System – ADS Stage 4

Spurious actuation of the ADS Stage 4 is defined as an inadvertent opening of one or more ADS Stage 4 valves. The frequency for spurious actuation of the ADS Stage 4 squib valves is generated by a special initiator fault tree over a one year mission time. The result is documented in Table 10-1.

10.2.3.7 Spurious IRWST Actuation

Spurious actuation of the IRWST is defined as an inadvertent opening of one or more IRWST squib valves. The frequency for spurious actuation of the IRWST squib valves is generated by a special initiator fault tree over a one year mission time. The result is documented in Table 10-1.

10.2.3.8 Core Makeup Tank Line Break

Each CMT line break is defined as all ruptures occurring in one of the lines connecting the CMT to the reactor coolant cold legs. On the basis of break size, this category is classified as a medium LOCA, but it is modelled in a different event tree from the medium LOCA because only one of the CMTs is available for mitigation, with no other systems being impacted. The CMT line break event frequencies are based on system piping information and are calculated using EPRI pipe rupture frequencies (Reference 10.28). The result is documented in Table 10-1.

10.2.3.9 Direct Vessel Injection Line Break

Each DVI line break is defined as all ruptures occurring in one of the safety injection trains and includes the DVI lines and the lines that connect the CMT, accumulator, IRWST, and the RNS injection line to the DVI lines. The DVI line break event frequencies are based on system piping information and are calculated using EPRI pipe rupture frequencies (Reference 10.28). The result is documented in Table 10-1.

10.2.3.10 Passive Residual Heat Removal Line Break

The PRHR line break event is defined as all ruptures occurring in the line connecting the reactor coolant hot leg to the PRHR heat exchanger and the lines connecting the PRHR heat exchanger to the reactor coolant cold leg. The PRHR line break event frequency is based on system piping information and is calculated using EPRI pipe rupture frequencies (Reference10.28). The result is documented in Table 10-1.

10.2.3.11 Passive Residual Heat Removal Tube Rupture

This category includes events in which a single PRHR heat exchanger tube has a complete circumferential rupture. If CVS operation or PRHR isolation fails, the PRHR tube rupture event progression is similar to that for a small LOCA. Based on the ratio of PRHR tubes to steam generator tubes, the frequency of PRHR tube rupture event is expected to be at least 29 times lower than the frequency of an SGTR. The frequency of an SGTR event, based on pressurized water reactor (PWR) generic industry data from NUREG/CR-6928 (Reference 10.15), is 3.54E-03 event per reactor operating year. The PRHR Tube Rupture

frequency was calculated by dividing the SGTR IEF in units of per reactor operating year by a factor of 29. The resulting PRHR tube rupture IEF is documented in Table 10-1.

10.2.3.12 Reactor Vessel Rupture

Reactor vessel rupture is defined as the random failure of the reactor vessel, resulting in a LOCA size/location that exceeds the passive core cooling system capability. The frequency of 2.90E-08 events per reactor year for vessel rupture is from Reference 10.26. This frequency was converted to reactor operating state year by dividing by an assumed industry average plant availability factor of 0.90. The resulting reactor vessel rupture IEF is documented in Table 10-1.

10.2.3.13 Steam Generator Tube Rupture

An SGTR event is defined as a rupture of one or more than one steam generator tubes, either as an IE (e.g., tube rupture due to high cycle fatigue or loose parts) or as a consequence of other IEs (i.e., a main steam line break or stuck-open main steam line safety valve). The SGTR IEF was determined by a review of generic industry data from NUREG/CR-6928 (Reference 10.15). The NUREG/CR-6928 IE name for this event is IE-SGTR (PWR). The generic data is applicable for the AP1000 plant, due to the similarity of the AP1000 plant steam generator design to the PWR legacy plant steam generator design on which NUREG/CR-6928 data is based. Table 10-1 documents the SGTR IEF.

10.2.3.14 Interfacing Systems LOCAs

The ISLOCA refers to a LOCA through a line connected to the RCS in which RCS inventory bypasses containment. The ISLOCA is typically initiated by the failure of pressure isolation devices in a line connected to the RCS that penetrates the containment and involves low pressure piping outside containment.

Seven ISLOCA scenarios were identified and modelled using the CAFTA fault tree approach following guidance in Reference 10.24. The seven ISLOCA scenarios and their respective containment penetration identifiers are:

- CCS RCP external heat exchanger (HX) Outlet Line, penetration P04
- CVS Spent Resin Sluice Line, penetration P05
- CVS Normal Makeup Line, penetration P07-N
- CVS passive core cooling system (PXS) Header Makeup Line, penetration P07-P
- CVS Zinc Injection Line, penetration P08
- RNS Suction Line, penetration P19
- RNS DVI Injection Line, penetration P20

The resulting ISLOCA IEFs are documented in Table 10-1.

10.2.3.15 Contribution to LOCA Event Frequencies by Other Initiating Events

Consequential LOCA due to other IEs are analysed with the event tree for the corresponding IEs. For example, during a reactor trip with a loss of secondary side cooling and loss of the PRHR system the RCS can pressurize to the RCS safety valves set point. After the safety valves are challenged, there is a possibility that the safety valves will fail to reseat. This could lead to a LOCA event. A review of LER events under the category of stuck open safety relief valve was performed. All events reviewed were a result of a safety valve failing to reseat/leaking after a test or a self-revealing maintenance error while returning to power. Therefore, a stuck open safety relief valve is not addressed as a separate IE but is addressed as a consequence if the safety valves are lifted and fail to reseat in the event tree for events where the safety valves' opening set point could be reached.

The AP1000 plant RCPs are canned-motor pumps. Primary coolant circulates between the stator and rotor for cooling. A seal around the motor shaft is not necessary; therefore, the design is not susceptible to RCP seal LOCAs due to loss of cooling and injection.

10.2.3.16 PMS Spurious PRHR Actuation

Spurious opening of the PRHR valves will result in a cooldown event to the RCS resulting in a possible reactor trip. PMS PRHR actuation will also directly cause a reactor trip. The frequency for spurious opening of the PRHR air-operated valves (AOVs) (PXS-PL-V108A/B) is generated by a special initiator fault tree over a one year mission time. The result is documented in Table 10-1.

10.2.3.17 PMS Spurious CMT Actuation

Spurious opening of the CMT injection valves could result in borated water entering the core and could result in a reactor trip. The frequency for spurious opening of the CMT injection AOVs (PXS-PL-V014A/B or PXS-PL-V015A/B) is generated by a special initiator fault tree over a one year mission time. The result is documented in Table 10-1.

10.2.3.18 Spurious IRWST Recirculation

Spurious opening of the recirculation valves could drain the IRWST into containment. If any of the IRWST squib valves indicate that they are open, then the operators are directed to start a shutdown of the reactor. This manual shutdown of the reactor is maintained as a potential reactor trip. The frequency for spurious opening of the IRWST recirculation squib valves (PXS-PL-V118A/B or PXS-PL-120A/B) is generated by a special initiator fault tree over a one year mission time. The result is documented in Table 10-1.

10.2.3.19 General Transient Sub-Groups

The general transient IEF from NUREG/CR-6928 (Reference 10.15) is 7.51E-01 per reactor operating state year. The NUREG/CR-6928 IE name for this event is IE-TRAN (PWR). The same event categorization in NUREG/CR-5750 (Reference 10.22) was also used for the development of the frequencies in NUREG/CR-6928.

To address the dependency a General Transient (GTRAN) IE could have on mitigating equipment, sub-grouping is required. Initiators that generate a safeguards signal or fail operation of main feedwater (MFW) should be separated from events that do not impact the ability for MFW to provide decay heat removal during an event.

To achieve this separation, a review of general transient events was performed so the frequency could be fractioned into sub-groups. Note that the IEs unique to the AP1000 plant, identified in Section 10.2.2.2, have been excluded from the sub-grouping since there is no applicable generic category. The three groups and the corresponding number of events identified from NUREG/CR-5750 applicable categories are as follows:

- General Transient with Main Feedwater (717 events)
- General Transient without Main Feedwater (433 events)
- General Transient with Safeguards Actuation Signal (S Signal) (34 events)

The fraction of the number of events for each sub-group over the total number of events (1184 events) was then multiplied by the GTRAN IEF from NUREG/CR-6928 provided above. The resulting frequency for each GTRAN IE sub-group is documented in Table 10-1.

10.2.3.20 Total Loss of Main Feedwater

This category includes those events in which the MFW flow to both steam generators is lost or isolated as an IE, leading to a reactor trip (including the primary and secondary power mismatch and the events that generate a safeguards actuation). The total loss of main feedwater IEF was determined by a review of generic industry data from NUREG/CR-6928 (Reference 10.15). The NUREG/CR-6928 IE name for this event is IE-LOMFW. Table 10-1 documents the total loss of MFW IEF.

10.2.3.21 Total Loss of Condenser Heat Sink

This category includes those events that result in loss of the condenser as a heat sink. This category includes inadvertent closure of all main steam isolation valves (MSIVs), loss of condenser vacuum, and unavailability of the turbine bypass. The total loss of condenser heat sink IEF was determined by a review of generic industry data from NUREG/CR-6928 (Reference 10.15). The NUREG/CR-6928 IE name for this event is IE-LOCHS (PWR). Table 10-1 documents the total loss of condenser heat sink IEF.

10.2.3.22 Total Loss of Component Cooling Water

This category consists of the complete loss of CCS flow due to either an operator error or a mechanical failure. Loss of CCS causes loss of RCP flow, which results in a reactor trip. The frequency for loss of CCS is generated by an SSIE fault tree over a 1 year mission time. The result is documented in Table 10-1.

10.2.3.23 Total Loss of Service Water System

This category consists of the complete loss of Service Water System (SWS) flow due to either an operator error or a mechanical failure. Loss of SWS results in loss of CCS. The frequency for loss of SWS is generated by a support system IE fault tree over a 1 year mission time. The result is documented in Table 10-1.

10.2.3.24 Total Loss of Compressed and Instrument Air System

The complete loss of the Compressed and Instrument Air System (CAS) causes the feedwater flow control valves to close resulting in a turbine trip/reactor trip. The loss of CAS also causes full opening of the startup feedwater (SFW) regulating valves, closure of both MSIVs and/or loss of PORV availability, and opening of the CMT valves and PRHR valves. The frequency for loss of CAS is generated by an SSIE fault tree over a 1 year mission time. The result is documented in Table 10-1.

10.2.3.25 Loss of Medium Voltage ac Power

This category includes loss of a Main alternating current (ac) Power System (ECS) ac bus due to either an operator error or a mechanical failure that could generate a reactor trip. Loss of a 6.9 kilo volt (KV) bus could result in a reactor trip due to loss of an RCP or loss of equipment supporting feedwater operation. All of the ECS buses were reviewed for possible failure modes leading to IEs. The IEF for loss of medium voltage ac power is from NUREG/CR-5750 (Reference 10.22, Table D-11, category C1). Table 10-1 documents the loss of medium voltage ac power IEF.

10.2.3.26 Loss of Low Voltage direct current (dc) Power

Loss of certain Class 1 DC and Uninterruptible Power Supply System (IDS) Class 1 dc buses can generate a reactor trip. IDS consists of the redundant Class 1 DC and ac uninterruptible power supply (UPS) power distribution systems feeding Class-1 loads. IDS provides uninterruptable power for the plant instrumentation, control, monitoring, and other vital functions required for plant startup, normal operation, and normal or emergency shutdown of the plant. All of the IDS buses were reviewed for possible failure modes leading to IEs. The frequencies for loss of IDS are generated by SSIE fault trees over a 1 year mission time. The loss of low voltage power IEF was calculated by hand by adding together the individual IDS bus IEFs. The result is documented in Table 10-1.

10.2.3.27 Loss of HVAC to the CCS Pump Room

This category consists of the complete loss of room cooling to the CCS pump room due to failure of the Turbine Building Ventilation System (VTS) South Bay Equipment Area HVAC Subsystem. Loss of room cooling to the CCS pumps results in loss of CCS. Loss of CCS causes loss of reactor coolant pump flow, which results in a reactor trip. The frequency for loss of HVAC to the CCS pumps is generated by an SSIE fault tree over a 1 year mission time. The result is documented in Table 10-1.

10.2.3.28 Loss of Central Chilled Water System HCS

This category consists of the loss of the common flow path of the Central Chilled Water System HCS which supports HVAC load to the room where the CCS pumps are located. Loss of central chilled water to this HVAC load would result in loss of room cooling to CCS pumps. Loss of room cooling to the CCS pumps results in a reactor trip. The frequency for loss of Central Chilled Water HCS is generated by an SSIE fault tree over a 1 year mission time. The result is documented in Table 10-1.

10.2.3.29 Total Loss of Offsite Power

A LOOP event is defined as an event that results from a loss of the offsite grid power (loss of the grid itself and failures of equipment that tie the plant to the grid). The total LOOP IEF was determined by a review of generic industry data from NUREG/CR-6928 (Reference 10.15). The NUREG/CR-6928 IE name for this event is IE-LOOP. Table 10-1 documents the total LOOP IEF.

10.2.3.30 Steam Line Break Downstream of the MSIVs

This category includes breaks in the main steam lines downstream of the MSIVs. The steam generator can be quickly isolated from the breaks without significant steam generator depressurization. To maximize their effect, all secondary side piping breaks are assumed to be large breaks. This is conservative because smaller breaks cause less severe scenarios with much longer times for operator actions.

The primary generic data source (Reference 10.15) does not include steam line break (SLB) outside containment frequencies. The SLB downstream of the MSIVs IEF was determined by a review of generic industry data from NUREG/CR-5750 (Reference 10.22) SLB outside containment category. A portion of the main steam line is outside containment but upstream of the MSIVs, and therefore is not isolatable. A review of the event reports identified in Table D-5 of NUREG/CR-5750 was performed for the SLB outside containment category (K1). All of the events that occurred were downstream of the MSIVs and were isolatable leaks or breaks. Table 10-1 documents the SLB downstream of MSIVs IEF.

10.2.3.31 Steam Line Break Upstream of the MSIVs

This category includes breaks in the main steam lines upstream of the MSIVs, breaks in the main feedwater lines downstream of the feedwater isolation valves, and SFW line breaks downstream of the SFW isolation valves. In these cases, the faulted steam generator cannot be isolated from the breaks. These breaks result in complete steam generator depressurization. To maximize their effect, all secondary side piping breaks are assumed to be large breaks. This is conservative because smaller breaks cause less severe scenarios with much longer times for operator actions.

The primary generic data source (Reference 10.15) does not contain information to support steam line break inside containment frequencies. SLB upstream of the MSIVs IEF was determined by a review of generic industry data from NUREG/CR-5750 (Reference 10.22) SLB inside containment. The NUREG/CR-5750 IE category for this event is K3. Table 10-1 documents the SLB upstream of MSIVs IEF.

10.2.3.32 Feedwater Line Break

This category includes breaks outside containment in the MFW lines upstream of the feedwater isolation valves, in the SFW line upstream of the SFW isolation valves, and in the condensate line that contains main turbine working fluid at or above atmospheric saturation conditions. The primary generic data source (Reference 10.15) does not contain information to support feedwater line break frequencies. The feedwater line break IEF was determined by a review of generic industry data from NUREG/CR-5750 (Reference 10.22, Table D-11). The NUREG/CR-5750 IE category for this event is K2. Table 10-1 documents the feedwater line break IEF.

10.2.3.33 Anticipated Transient without Trip (ATWT)

An ATWT event is defined as one in which the reactor trip should occur but mechanical failure of the rod control system or failure of the PMS system prevents dropping of the control rods into the core. The failure probability of the automatic and manual reactor trip is used in ATWT frequency calculation.

10.2.4 Grouping of AP1000 Plant Initiating Events

IE groups are events that have similar plant response, success criteria, timing, impact on mitigating systems, and effect on operators. To identify events with similar plant responses, the high level functions of reactivity control, RCS inventory control, RCS overpressure control, and reactor core decay heat removal were used. Table 10-2 includes a summary of the IE grouping results.

10.2.4.1 Grouping of LOCAs

Initiating events that require RCS inventory control as a primary mitigation function are defined as LOCAs. The break sizes for large, medium, small, and RCS leak were based on the thermo – hydraulic response of the AP1000 plant. No mitigation equipment is credited for the reactor vessel rupture IE. Since the RCS LOCA breaks size categories are based on the differences in the impact on mitigation equipment it is not appropriate to group any of the RCS LOCAs.

Breaks in the passive Class-1 systems connected to the RCS (CMT, DVI, and PRHR) could impact the ability of that system to perform its mitigation function. Opening of the ADS Stages 1-3 valves results in a different plant response than opening the ADS Stage 4 valves. Based on the differences in the impact on mitigation equipment none of the passive Class-1 system LOCAs were grouped.

Unlike the breaks in the RCS and breaks in the passive Class-1 systems connected to the RCS, SGTR and ISLOCA events could result in bypassing the containment. Credit for isolation of the break may also be possible for SGTR and ISLOCA events. Due to the potential for bypassing containment, the differences due to the impact of the IE on mitigation equipment and the expected operator response, grouping of ISLOCAs with SGTR is not recommended. No mitigation equipment is credited for non isolatable ISLOCA IEs.

In summary, none of the LOCA IEs were grouped except for the ISLOCA IEs and PRHR tube rupture with small LOCA. Table 10-2 lists all the LOCA IEs which are modelled in specific event trees. For each IE group, a corresponding event tree is developed except for non isolatable ISLOCA, PRHR tube rupture, and vessel rupture initiation events.

10.2.4.2 Grouping of Transients

IEs that do not require RCS inventory control as a primary mitigation function are defined as transient events. The IEs which are identified as general transients with safeguards and without safeguards all have the same expected emergency operating procedures (EOPs) to be entered by the operators. These initiators are grouped into two different categories since PRHR actuation following a safeguards signal will result in isolation of SFW and MFW. Loss of compressed air and loss of low voltage power can result in actuation of PRHR and the CMTs due to loss of power or air to the normally energized PXS AOVs. Within the general transient without MFW group there are several IEs that should not credit MFW. For example, transients due to loss of SWS or loss of CCS would result in loss of MFW.

Loss of offsite power was not grouped with the general transient events to support model development and review. It is important to understand what sequences can lead to station blackout events. Breaks in the steam lines and feedwater lines can result in rapid depressurization of the secondary side and a cooldown of the RCS. This cooldown causes an increase in reactivity and requires additional boron to be added into the RCS to mitigate the event. These events were grouped by the ability to isolate the blowdown of the steam generators.

10.3 Accident Sequence Analysis

10.3.1 Method Discussion

The Accident Sequence Analysis develops the plant response to an IE based on the operator action and system response to specific initiators. This Accident Sequence model and event tree structure includes operator actions, mitigating systems, and phenomena that can alter the accident sequence progression. The event tree structure is based on expected plant response, the EOPs, information from the safety analyses in Chapter15 of the PCSR, and insights from the previous AP1000 plant PSA model. The Success Criteria Analysis, as summarized in Section 10.4, supports the individual accident sequence paths including the functional success, mission times, and human error probability (HEP) time windows. Based on the event tree and Success Criteria models, the core damage paths are binned into a plant damage state to facilitate the Level 1/Level 2 model interface.

10.3.2 Event Tree Models

The event tree models are summarized in the following sections for each IE group. The IE groups from Table 10-2 are listed with their corresponding event tree names in Table 10-3. Table 10-4 through Table 10-28 provide descriptions for each event tree.

In the event tree descriptions, if an operator action can be taken to actuate equipment following a signal failure, then the appropriate procedure and operator action identifier are listed at the beginning of the top event description.

Plant Damage States (PDSs) for core damage sequences are defined in Section 10.10.1.

10.3.2.1 Large Loss of Coolant Accident

The LLOCA includes RCS pipe breaks inside containment with sizes sufficient to produce a depressurization of the RCS that allows gravity injection from the IRWST. The break size range for LLOCA is 22.86 cm (9 inches) up to a double-ended rupture of the hot leg. The event tree model that addresses the plant response to an LLOCA IE is LLOCA. The event tree top events are described in Table 10-4.

10.3.2.2 Medium Loss of Coolant Accident

The MLOCA event includes breaks in the RCS contained inside containment with sizes that are smaller than LLOCAs (the upper bound of MLOCAs) and larger than small LOCAs (SLOCAs) (the lower bound of MLOCAs). The MLOCA event is defined as all RCS ruptures with break sizes sufficient to allow the automatic actuation of ADS Stage 4 without the operation of the ADS Stages 1-3, and ruptures in which there is sufficient pressure decrease and time to initiate the RNS if the IRWST injection fails. In addition, void formation in the core is not sufficient to shut down the reactor; therefore, reactor trip is also required. The break size range for MLOCA is 10.16 cm (4 inches) to less than 22.86 cm (9 inches). The event tree model that addresses the plant response to an MLOCA IE is MLOCA. The event tree top events are described in Table 10-5.

10.3.2.3 Small Loss of Coolant Accident

SLOCA events are characterized by breaks in the RCS with sizes between 0.95 cm (3/8 inch) and less than 10.16 cm (4 inches). These events consist of RCS breaks having a size greater than those producing leakage that can be made up by the CVS but less than that required to depressurize the RCS sufficiently without PRHR or ADS Stages 1-3 before ADS Stage 4 can automatically open. The event tree model that addresses the plant response to an SLOCA IE is SLOCA. The event tree top events are described in Table 10-6.

10.3.2.4 RCS Leak

The RCS leakage event includes leak rates less than the flow from a 0.95 cm (3/8 inch) break (less than approximately 6.3 L/sec – 100 gpm). Typical examples of small line breaks include failed instrument process lines or tubing. The CVS is designed to make up RCS leaks of 6.3L/sec (100 gpm) or less. This function allows the plant to be taken to cold shutdown conditions without the use of Class-1 makeup systems. The controlled plant shutdown is not modelled, but if the CVS system fails, the pressuriser level will decrease and the event will proceed as a slower version of a small LOCA. This is modelled in the event tree. The event tree model that addresses the plant response to an RCS Leak IE is LEAK. The event tree top events are described in Table 10-7.

10.3.2.5 Spurious ADS Stages 1-3 Actuation

A spurious actuation of ADS Stages 1-3 occurs when any combination of ADS Stages 1-3 valves spuriously operate and open a flow path from the RCS into the IRWST. The lower bound of this initiator would be the actuation of only one ADS Stage 1 valve. The upper bound of this initiator would be the actuation of both trains of ADS Stages 1-3 valves. The most likely cause of a spurious ADS Stages 1-3 actuation would occur because of a spurious PMS signal. This spurious signal would actuate one train of ADS Stage 1, and then actuate the remaining ADS Stages 2-3 valves on that train with the appropriate time delay. The ADS Stage 1 valves are 10.16 cm (4 inches) and the Stages 2 and 3 valves are 20.32 cm (8 inches). Given the range of the equivalent break sizes that could occur, this could behave similar to an MLOCA or an LLOCA. Success Criteria Analysis demonstrates that with all six ADS Stages 1-3 valves spuriously opening, the event behaves like an MLOCA. This is the basis for the event tree development. The event tree model that addresses the plant response to a spurious ADS Stages 1-3 IE is SPADS13. The event tree top events are described in Table 10-8.

10.3.2.6 Spurious ADS Stage 4 Actuation

The spurious actuation of one or more ADS Stage 4 valves is modelled for this IE. The most realistic scenarios for spurious actuation are one ADS Stage 4 valve, both ADS Stage 4 valves in the same compartment, or all four ADS Stage 4 valves actuating. The piping to the ADS Stage 4 valves has a nominal diameter of 35.56 cm (14 inches); however, the flow is limited by the squib valve internal flow area. The minimum internal diameter for the ADS Stage 4 line from the line reducer to the squib valve (RCS-PL-V004A) is 23.47 cm (9.24inches) based on the squib valve. This is slightly above the diameter cutoff for a Medium LOCA (less than 22.86 cm (9 inches); however, there is uncertainty concerning the piping response as a result of the spurious actuation, and it is judged that the resulting transient will act similar to a Medium LOCA. For more than one ADS Stage 4 valve, the flow would correspond to an LLOCA. The event tree model that addresses the plant response to a spurious ADS 4 IE is SPADS4. The event tree top events are described in Table 10-9.

10.3.2.7 Spurious IRWST Actuation

The spurious actuation of one or more IRWST squib valves is modelled for this IE. The scenarios for spurious actuation are one to all four IRWST squib valves actuating. The spurious actuation of one or more IRWST squib valves causes a pressure transient in the piping and exposes the piping and check valves upstream of the squib valves to RCS pressure. If the check valve upstream of the squib valve fails, the result is a LOCA into the IRWST. Due to the transient, there is a possibility that the piping pressure boundary could fail resulting in a DVI LOCA with early draining of the IRWST. It is assumed that the pipe pressure boundary remains intact if the check valve remains closed. For this event, even when the pressure boundary integrity is maintained and the check valve remains closed, there is a 0.32 cm (1/8”) diameter hole in the check valve for pressure balancing so the consequence would be an RCS leak into the IRWST. The event tree model that addresses the plant response to a spurious IRWST actuation IE is SPIRWST. The event tree top events are described in Table 10-10.

10.3.2.8 CMT Line Break

This event is a failure in the piping leading to or from either CMT. This includes the piping from the Loop 2 cold legs to the CMTs and from the CMTs to the normally closed isolation valves (PXS-PL-V014A, V014B, V015A, V015B) upstream of the DVI line. The piping has a nominal diameter of 20.32 cm (8 inches). The unique feature of a break in the CMT piping is that it could range from an RCS Leak to an MLOCA with the one CMT disabled, especially for the larger break sizes. At some point, the smaller break sizes would not fail the function of the CMT but may degrade it. These breaks would not be substantially different from SLOCAs in other parts of the primary loop. Therefore, this event focuses on the larger break sizes that disable the function of one CMT. The event analysed is an MLOCA break in the piping to or from a CMT. The event tree top events are described in Table 10-11.

10.3.2.9 DVI Line Break LOCA

The DVI lines are a nominal 20.32 cm (8 inches in diameter). Each DVI line has a flow venturi built into the nozzle at the RV which is designed to limit the flow out of the vessel for a DVI line break. The venturi has an inside diameter of 10.16 cm (4 inches) making this equivalent to the low end of the MLOCA break size range. Therefore, the DVI line break can be classified as an MLOCA event, but some considerations must be made for the event progressing as an SLOCA or RCS Leak. The event tree model that addresses the plant

response to a DVI line break IE is DVILB. The event tree top events are described in Table 10-12.

10.3.2.10 PRHR Line Break

This event is a failure in the piping from the RCS Loop 1 hot leg to the PRHR heat exchanger or from the PRHR heat exchanger to the Loop 1 steam generator (SG). This piping has a nominal diameter of 35.56 cm (14 inches), and one section has a nominal diameter of 45.72 cm (18 inches). The unique feature of a break in the PRHR piping is that it could range from an RCS Leak to an LLOCA with the PRHR function disabled, especially for the larger break sizes. At some point, the smaller break sizes would not fail the function of the PRHR heat exchanger but may degrade it. These breaks would not be substantially different from SLOCAs in other parts of the primary loop. Therefore, this event focuses on the larger break sizes that disable the function of the PRHR. The event analysed is a medium to large break in the piping to or from the PRHR heat exchanger. The event tree model that addresses the plant response to a PRHR line break IE is PRHRLB. The event tree top events are described in Table 10-13.

10.3.2.11 PRHR Tube Rupture

This event is a failure of a single PRHR heat exchanger tube ranging from a small leak up to a complete circumferential tube rupture. As soon as the event initiates, the PRHR heat exchanger inlet pipe temperature begins to increase up to a value at which an alarm in the main control room is actuated. If the leak rate (as indicated by RCS mass balance) is less than the technical specification limit, the plant can continue to operate. If the leak exceeds the technical specification limit, the plant will be shut down to repair the leak. If a complete rupture of a PRHR heat exchanger tube occurs, the RCS transient is fast enough that the reactor is expected to trip and safety injection actuated before the operators are able to isolate the PRHR heat exchanger.

During a PRHR tube rupture event, decay heat removal using PRHR is credited based on the Success Criteria Analysis. This means that the PRHR tube rupture event can be modelled as a SLOCA; therefore, a separate event tree is not required.

10.3.2.12 Steam Generator Tube Rupture

The SGTR initiator covers a range of faults from a single tube double-ended guillotine rupture up to and including a five-tube double-ended guillotine rupture. After reactor trip, the ruptured SG is isolated and the RCS is cooled down and depressurized to stop the flow of RCS coolant into the secondary side of the ruptured SG. The MFW pumps are tripped on an S signal; therefore, they are not credited for this event. The event tree model that addresses the plant response to a SGTR IE is SGTR. The event tree top events are described in Table 10-14.

10.3.2.13 ISLOCA – CVS Spent Resin Sluice Line, CVS Makeup Line, or CVS Zinc Injection Line

Section 10.2 documents the analysis performed to identify ISLOCA events. Of the ISLOCA pathways identified, three have the capability of being isolated, thus terminating the LOCA outside containment. The three are the CVS spent resin sluice line, the CVS makeup line, and the CVS zinc injection line. The other ISLOCA pathways identified cannot be isolated and are modelled as going directly to core damage. The event tree model that addresses the plant

response to an ISLOCA IE is ISL-CVS. The event tree top events are described in Table 10-15.

10.3.2.14 General Transient with Safeguards Actuation

A spurious S signal causes a reactor trip and will also result in a trip of the MFW pumps. At the beginning of this IE, the RCS and secondary sides are intact. The decay heat removal systems available are the PRHR System, SFW System, and RCS depressurization using the ADS with IRWST/RNS injection and recirculation. The MFW pumps are tripped on an S signal; therefore, they are not credited for this event. The event tree model that addresses the plant response to a general transient with an S signal IE is GTRAN-WS. The event tree top events are described in Table 10-16.

10.3.2.15 General Transient, No Safeguards Actuation

This category of events includes transients that cause a reactor trip without an S signal in conjunction with the reactor trip. At the beginning of the IE, the RCS and secondary sides are intact. The decay heat removal systems available are the MFW System, SFW System, PRHR System, and RCS depressurization using the ADS with IRWST/RNS injection and recirculation. The event tree model that addresses the plant response to a general transient (no initial safeguards signal) IE is GTRAN. The event tree top events are described in Table 10-17.

10.3.2.16 Loss of Offsite Power

The LOOP event applies to a transient event that begins with the loss of electrical power from the plant switchyard (loss of the grid itself or failures of equipment that tie the plant to the grid). Restoration of the grid within the PSA time period is not modelled. The passive Class-1 systems need only battery power to actuate. Class 1 250 Vdc divisions A and D battery banks and one of the battery banks in divisions B and C are designated as 24-hour battery banks and provide power to the loads required for the first 24 hours following a loss of all ac power event. The second battery banks in divisions B and C, designated as the 72-hour battery banks, are used for those loads requiring power for 72 hours following the same event.

In addition, systems powered by the standby diesel generators (DGs) are modelled. Note that the MFW pumps are not powered by the standby DGs. A LOOP, with the subsequent failure of both trains of onsite ac power, is a station blackout (SBO) event. For an SBO, only dc power is available from the batteries; therefore, only the passive Class-1 systems can be actuated.

The event tree model that addresses the plant response to a LOOP IE is LOOP. The event tree top events are described in Table 10-18.

10.3.2.17 SLB Downstream of the MSIVs

This IE group includes breaks in the main steam lines downstream of the MSIVs, and breaks in the MFW lines upstream of the feedwater isolation valves (FWIVs). In both events, both SGs can be isolated from the breaks.

SFW is not modelled for this event. PRHR will be actuated on SG level signals for the secondary side breaks in this group. If SFW is operating along with PRHR, then combining their operation with the cooldown from the steam line break would most likely result in an RCS Low Tcold signal. This signal isolates SFW. Therefore, to cover all of the secondary

break cases in this group and to address the possibility that the secondary side break could cause a harsh environment and disable SFW, SFW is not modelled.

The event tree model that addresses the plant response to a steam line break downstream of the MSIVs IE is SLBD. This event tree is also used for a pipe break upstream of the FWIVs. The event tree top events are described in Table 10-19.

10.3.2.18 SLB Upstream of the MSIV

This IE group includes breaks of the main steam lines upstream of the MSIVs, breaks of the MFW lines downstream of the FWIVs, and SFW line breaks downstream of the SFW isolation valves. In these events, the faulted SG cannot be isolated from the break. Successful operation of the isolation valves does not prevent the faulted SG from blowing down; however, it does prevent blowdown of both SGs. The event tree model that addresses the plant response to a steam line break upstream of the MSIVs IE is SLBU. The event tree top events are described in Table 10-20.

10.3.2.19 Spurious IRWST Recirculation

A spurious opening of the PXS recirculation valves can start draining the IRWST inventory to the reactor cavity. A low IRWST level alarm provides a cue for the operator to take action to isolate IRWST injection valves. If any of the IRWST squib valves indicate that they are open, then the operators are directed to start a shutdown of the reactor. This manual shutdown of the reactor is maintained as a potential reactor trip. If the reactor is not manually shut down, there is a potential that the normal plant operation may be challenged due to the increased water level in the reactor cavity and sump. This IE mode includes the likelihood of any one recirculation valve opening and the likelihood of a common cause event resulting in all recirculation valves opening. The event tree model that addresses the plant response to a spurious IRWST recirculation IE is SPRECIRC. The event tree top events are described in Table 10-21.

10.3.2.20 Transfer Tree ATWT – Loss of MFW

The ATWT precursors encompass a spectrum of IEs and ensuing plant transient progressions. This ATWT category applies to those transient precursors where the MFW is lost as a part of the IE. The event tree model that addresses the plant response to an ATWT with loss of MFW IE is ATWT-LMFW. The event tree top events are described in Table 10-22.

10.3.2.21 Transfer Tree ATWT – MFW Available

The ATWT precursors encompass a spectrum of IEs and ensuing plant transient progressions. This ATWT category applies to those transient precursors where the MFW is available at the beginning of the IE. The event tree model that addresses the plant response to an ATWT with MFW IE is ATWT. The event tree top events are described in Table 10-23.

10.3.2.22 Transfer Tree LOCA – No Trip

Reactor trip is required in all of the LOCA event trees except LLOCA. If reactor trip fails, the LOCA event is transferred to the LOCA no trip event tree. This event tree covers various size LOCAs at various locations in the RCS, CMT, ADS, and DVI lines. Therefore, a bounding approach is taken with regard to systems and components modelled for successful plant shutdown. The event tree model that addresses the plant response to a LOCA event without a reactor trip is LOCA-NOTRIP. The event tree top events are described in Table 10-24.

10.3.2.23 Transfer Tree LOCA – Secondary Side Fault

The LOCA secondary side fault event tree is used to address certain LOCA IEs in which the secondary side failed either because the SG safety valves, SG PORVs, and turbine bypass valve failed to open resulting in a pressure boundary failure or because the SG safety valves, SG PORVs, or turbine bypass valve failed to reclose after opening, or turbine trip failed. The event becomes a LOCA with a secondary side failure. The event tree model that addresses the plant response to a LOCA event with a secondary side failure is LOCA-SSFAULT. The event tree top events are described in Table 10-25.

10.3.2.24 Transfer Tree SGTR – No Trip

This event tree addresses an SGTR without reactor trip. Because reactor trip has failed, a CMT is required to shut down the reactor. Based on the ATWT analyses and success criteria, turbine trip and secondary side pressure relief are addressed for this event. The event tree model that addresses the plant response to a SGTR event without a reactor trip is SGTR-NOTRIP. The event tree top events are described in Table 10-26.

10.3.2.25 Transfer Tree SLBD – General Transient

This event tree addresses a secondary side line break downstream of the MSIVs (or upstream of the FWIVs) with successful reactor trip and successful isolation of the break so that no further SG inventory is lost through the break. This changes the event after the initial SG blowdown to one very similar to a reactor trip without MFW. The secondary side PORVs and safety valves are not expected to be challenged for this event. The event tree model that addresses the plant response to this event is SLBD-GTRAN. The event tree top events are described in Table 10-27.

10.3.2.26 Transfer Trees for Long Term Cooling

The long term cooling event trees are transfer trees used to assess long term containment cooling for successful Level 1 sequences in which decay heat is being removed from the RCS by either containment sump recirculation or the PRHR. There are two transfer trees; LTC and LTCP. These transfer trees evaluate electric power, containment isolation, and containment cooling for those sequences that are successful in the shorter term with RCS cooling from either the PRHR heat exchanger or containment sump recirculation. These sequences depend on long term cooling from the containment shell for success. In addition, the LTCP event tree includes credit for SFW for RCS cooling upon failure of PRHR cooling. The event tree models that address the plant response to these events are LTC and LTCP. The event tree top events are described in Table 10-28.

10.4 Success Criteria Analysis

10.4.1 Introduction

The success criteria defines the AP1000 plant specific measures of success and failures which support the accident sequence analysis, systems analysis, human reliability analysis, and Level 2 analysis.

10.4.2 Definitions

Core Damage: Uncovery and heatup of the reactor core to the point at which prolonged oxidation and severe fuel damage are anticipated and involve enough of the core, if released, to result in offsite public health consequences. Core damage is defined from the MAAP4 code as having TCRHOT > 982.2 °C (1800 °F). TCRHOT specifies the peak core node temperature.

Mission Time: The time period that a system or component is required to operate in order to successfully perform its function. AP1000 plant system models for core cooling, reactivity and decay heat removal have mission times of 24 hours. The Passive Containment Cooling System (PCS) model has a mission time of 72 hours.

Safe Stable State: A plant condition, following an IE, in which RCS conditions are controllable at or near desired values.

10.4.3 Computer Codes Used

CENTS

CENTS (Reference 10.29) is an interactive, high fidelity computer code for simulation of the Nuclear Steam Supply System (NSSS). It calculates the transient behaviour of Combustion Engineering (CE) and Westinghouse designed PWRs for normal and abnormal conditions, including accidents. CENTS determines the core power and heat transfer throughout the NSSS. It also computes the thermal-hydraulic (T-H) behaviour of the reactor coolant in the primary and secondary systems. It includes the primary and secondary control systems and the balance-of-plant fluid systems.

CENTS is designed to support engineering, operations, and training functions. It supports evaluation of plant behaviour for accidents, operator actions, design, and scoping studies. It is licensed for safety analyses of PWRs. In addition, it may be used for NSSS simulations supporting optimization, procedure preparation or evaluation, determining success paths for PSA events, training, etc. The code simulates a wide range of variations in plant state, from steady state conditions to severe accidents. It provides a full range of interactions between the analyst, the reactor control systems, and the NSSS. It also allows analysis of multiple failures and the effects of operator intervention or mistakes. Examples of transients run with CENTS include: steady state, power change, pump trip, overcooling or undercooling, loss of feedwater, steam line break, feedwater line break, steam generator tube rupture, anticipated transient without scram, loss of coolant accident, letdown line break, control rod ejection, and malfunctions of the various plant components and control systems.

LOFTRAN

The LOFTRAN program (Reference 10.30) is used for studies of transient response of a pressurized water reactor system to specified perturbations in process parameters. LOFTRAN simulates a multi-loop system by a model containing a reactor vessel, hot and cold leg piping, steam generator (tube and shell sides), and pressuriser. Operation of the pressuriser heaters, spray, and safety valves are also modelled in the program. Point model neutron kinetics and the reactivity effects of the moderator, fuel, boron, and control rods are included. The secondary side of the steam generator uses a homogeneous, saturated mixture for the thermal transients and a water level correlation for indication and control. The protection and safety monitoring system is simulated to include reactor trips on high neutron flux, overtemperature ΔT, high and low pressure, low reactor coolant system flow, and high pressuriser level.

Control systems are also simulated, including rod control, steam dump, feedwater control, and pressuriser level and pressure control. The emergency core cooling system, including the accumulators, is also modelled.

For the AP1000 plant design, the LOFTRAN code allows the simulation of the PRHR heat exchanger, CMTs, and associated protection and safety monitoring system actuation logic.

MAAP4.0.7

The Modular Accident Analysis Program version 4.0.7 (Reference 10.31) is a computer code that simulates the response of light water reactor (LWR) power plants during accidents. Given a set of IEs and operator actions, MAAP4 predicts the plant's response as the accident progresses. MAAP4 possesses a dynamic benchmarking capability to ensure the code is consistent with major experiments and plant transient experiences.

The following are limitations to MAAP4:

- Core Flow Reversal in LLOCA – For break sizes ≥ 25 cm (10 inches), the flow in the core could initially reverse. MAAP4 does not model the flow reversal. There are other situations in the initial phase of the transient that MAAP4 does not model, including: steam binding, departure from nucleate boiling, detailed condensation on safety injection flow. The results of the code during the flow reversal time are not used in this analysis. Break sizes considered in the MAAP4 analysis are limited to 22.86 cm (9 inches) or less.

- Water Momentum Equation – MAAP4 does not have a complete water momentum equation for the primary system or the steam generator; the core voiding and the general two-phase distribution in the RCS during blowdown and reflood requires a fully-posed momentum equation. In the smaller LLOCAs, reflood does not occur, so the momentum equations are not needed. However, in the case of the larger LLOCAs, the design basis safety analysis will be used as a conservative estimate.

- PRHR Steam Condensate Rate – MAAP4 does not accurately model the steam condensation in the PRHR tubes. Heat removal rate through PRHR becomes time step dependent when the RCS water and steam are separated. It leads to excessively small heat removal if used with a small time step.

- Neutronics Model – MAAP does not contain a neutronics model or chemical addition model; therefore, there is no core feedback. For initiators which cause reactivity changes other than nominal decay heat, the success criteria must be developed with other codes. For example, for ATWT initiators, the success criteria were determined using LOFTRAN.

- Piping Break Locations – MAAP4 does not model RCS mixing when a LOCA has stabilized and natural circulation has been established. Analyses performed on the LLOCA show no difference between break locations on the top or the bottom of the hot leg (HL) and cold leg (CL) of the RCS piping.

- Global Pressure Model – Pressure and average water and gas temperatures are calculated via subroutine PTCAL. PTCAL computes the average gas temperature and system pressure by combining all control volumes together. The primary advantage of this method eliminates the numerical stiffness which occurs if the pressure was calculated in each small control volume.

- Simplified RCS Nodalization – Because MAAP4 has a simplified RCS nodalization (i.e., lumped cold leg nodes, no DVI nodes, no CMT nodes, no PRHR nodes), the MAAP4 T-H response for special LOCAs may be predicting non conservative results. Therefore, the event tree structure and the success criteria for special LOCA initiators have been determined via engineering judgment, and there are very few MAAP analyses for the special LOCA cases.

10.4.4 Methodology

The success criteria are determined for the event tree top node paths; they are defined as the minimum requirements per top event that fulfil the basic function which prevents core damage. The basic mitigating functions and their associated systems are:

- Reactivity Control
  - Plant Control System
  - Protection and Monitoring System
  - Diverse Actuation System
  - Chemical and Volume Control System
  - Core Makeup Tanks
- RCS Overpressure Control
  - Pressuriser size (larger than operating plants)
  - Pressuriser Safety Valves
  - Automatic Depressurization System
  - Passive Residual Heat Removal
- RCS Inventory Control
  - Chemical and Volume Control System
  - Core Makeup Tanks
  - Automatic Depressurization System
  - Normal Residual Heat Removal System
  - Accumulators
  - IRWST Gravity Injection and Recirculation
- Reactor Core Decay Heat Removal
  - Main Feedwater
  - Startup Feedwater
  - Secondary Side Pressure Relief (condenser or power-operated relief valve and main steam line safety valves)
  - Passive Residual Heat Removal
  - Normal Residual Heat Removal System
- Containment Cooling
  - Normal Containment Heat Removal (fan coolers)
  - Passive Containment Cooling

– Normal Residual Heat Removal

The minimum requirements can be met by combinations of systems (PXS, CVS, RNS, etc.), structures (containment, etc.), components (MOVs, AOVs, HXs, etc.), and/or automatic actuations or human actions (completed operator actions within the specified time window).

The methodology for the analyses can be divided into two distinct types: distinct initiators with detailed T-H results or similar initiators with modified success criteria and T-H results. For example, the MLOCA initiator is a distinct initiator with a specified response. The MAAP4 T-H results for all MLOCA success paths are determined along with the human reliability analysis (HRA) supporting information. This approach was taken for all of the IEs analysed with MAAP4. In contrast, the DVI line break LOCA is evaluated based on other LOCA results with the basis for the event tree and success criteria development defined.

Engineering judgement has been used for the following IEs: PRHR Tube Rupture, CMT Line Break, PRHR Line Break, Spurious Actuation ADS Stages 1-3, Spurious Actuation ADS Stage 4, Spurious IRWST Injection Actuation, DVI Line Break, and Spurious Containment Recirculation. Engineering judgement is used for these sections either to bound the event by other events or because the MAAP4 model lacks the detailed modelling components to accurately represent these “special LOCAs.”

The results of the T-H analyses are used to confirm the success paths of the event trees and the minimum required amount of mitigation equipment as presented in the Accident Sequence Analysis Sections 10.3.2.1 through 10.3.2.26, and define the time windows for operator actions.

10.4.5 Assumptions

The Success Criteria specific assumptions identified in the development of this model are:

1. When two or more ADS Stage 4 valves are required, it is assumed that at least one valve is required to open on the non-pressuriser loop. ADS stage 4 valves are less effective connected to the HL with the pressuriser. MAAP has a global RCS pressure model and lumped RCS nodalization which is not able to capture the injection gap phenomena. By operating at least 1 valve on the non-pressuriser loop, the phenomenon is avoided. Two ADS Stage 4 valves opening on the non-pressuriser loop will perform like one valve open on each loop.

2. A conservative 25 percent containment condensate bypass (bypassing the IRWST) is assumed for all cases unless otherwise noted.

3. CVS is assumed to automatically provide injection during RCS cool down events where the pressuriser level is expected to decrease. Current CVS design/operation will isolate CVS injection with a coincident Safeguards Signal and PZR High-1 level. Success criteria will model the CVS as follows: During an RCS cool down event, CVS will automatically ‘arm’ 1 pump and isolate the Demineralized Water Storage Tank given a Safeguards Signal. CVS will maintain the PZR level between Low-2 and Low-1, injecting water from the BAST. CVS will begin injecting when the PZR reaches Low-2. This configuration allows for automatic CVS injection should the initial PZR level be above High-1 when the Safeguards Signal is generated.

4. The SGTR HRA time windows are developed based on a single tube rupture because the expected initiator affects a single tube. Additionally, this is consistent with the design basis analysis which determines the SG margin to overfill.

10.4.6 Determination of LOCA Break Sizes

LLOCA:

The LLOCA represents breaks that are greater than or equal to a 22.86 cm (9 inches) equivalent diameter on a main coolant loop or connected line. This break size is chosen based on the ability to provide adequate PXS injection without the use of ADS assuming containment isolation operates normally. A 22.86 cm (9 inches) break size adequately depressurizes the RCS to allow for gravity injection without additional ADS. 20.32 cm (8 inches) break size cases do not allow for sufficient depressurization through the break, and the pressure head for gravity injection is not able to overcome the RCS pressure. The capability of core cooling for a 22.86 cm (9 inches) break and larger is verified by MAAP4 analyses. There are no operator actions associated with this IE in the short term because the event is fast acting; however, time for operator actions exists during recirculation.

Depressurization is not required through the ADS Stage 4 valves to allow gravity injection; however, ADS Stage 4 is required to support long term containment recirculation. The break allows for sufficient depressurization to allow gravity injection, and the PMS signals are required to actuate gravity injection from the IRWST. CMT level setpoints correspond to a series of PMS signals which actuate ADS Stages 1-3, ADS Stage 4, and gravity injection from the IRWST. In support of the LLOCA success path, one of two IRWST lines is required. One of four recirculation lines is required to support the LLOCA-001 success path.

The reduced containment pressure from successful PCS cooling of containment combined with the containment isolation failure produce a conservatively low pressure condition for PXS core cooling. In the passive plant, the RCS and containment pressures are strongly coupled following ADS actuation. At higher system pressure, the steam/water enthalpy is greater and allows the RCS to vent more effectively. More energy is released through the break and ADS at any given venting flowrate, resulting in a lower pressure differential and more efficient PXS injection and recirculation. Therefore, PCS cooling and containment isolation failure produce a lower system pressure and create a more challenging condition for passive core heat removal.

Sensitivities were run to explore different break locations. Results from these sensitivities revealed that breaks at different locations resulted in similar hottest core node temperatures.

MLOCA:

The MLOCA represents a break on a main coolant loop or connected line that is between 22.86 cm (9 inches) and 10.16 cm (4 inches) in diameter or equivalent. The bottom end of the MLOCA range has been determined by the ability of the break by itself to depressurize the RCS below 4136.85 kPa (600 psia) with the 10.16 cm (4 inches) break size to allow for successful ADS Stage 4 actuation.

The MLOCA analyses confirm the success paths of the MLOCA event tree. ADS is required for adequate RCS depressurization to allow for gravity injection or RNS injection. ADS is also required to provide a long term vent pathway.

The MLOCA cases have been run with PCS and containment isolation failure as described for LLOCA as that has been determined most limiting.

SLOCA:

The SLOCA represents a break on a main coolant loop or connected line that is between 0.95 cm (3/8 inch) to 10.16 cm (4 inches) in diameter or equivalent. The bottom end of the SLOCA has been determined by the ability of CVS to make up lost coolant from a 0.95 cm (3/8 inch) break. The CVS provides makeup for RCS leaks up to 0.95 cm (3/8 inch) diameter within the reactor coolant pressure boundary. The upper bound is determined by the bottom end of the MLOCA.

The SLOCA analyses confirm the success paths of the SLOCA event tree. PRHR is able to provide heat removal during a SLOCA and has been credited. ADS is required for adequate RCS depressurization to allow for gravity injection or RNS injection. ADS is also required to provide a long term venting pathway.

The SLOCA cases have been run with PCS as described for LLOCA and MLOCA that have been determined most limiting. 0.95 cm (3/8 inch) to 10.16 cm (4 inches) cases behave differently and the operator action windows for RNS are limited by the 10.16 cm (4 inches) break size. No clear criteria has been identified to create more specific LOCA categories from the SLOCA break range.

10.4.7 Determination of HRA Time Windows

The following information was developed to support the HRA analysis:

- Description of operator action
- Initiator
- Cue for operator action
- Time of cue with respect to time zero (Tdelay)
- Irreversible damage state
- Time of irreversible damage state with respect to time zero (TSW)
- References for cue, irreversible damage state, and MAAP run

The MAAP4 cases run have been designed to determine the most limiting scenarios to be used as inputs for the HRA. Specifically, maximum RCS depressurization, minimum injection along with the correct equipment configuration is modeled to capture the most challenging operator action timeframes. The operator time windows are presented in Table 10-32.

10.4.8 Analyses and Results

10.4.8.1 Large LOCA

The LLOCA initiator has been previously analyzed with design basis accident analysis codes. The MAAP4 code is limited in its ability to correctly model plant response for break sizes above a 22.86 cm (9 inches) equivalent diameter break during core reflood and blowdown; therefore, the minimum equipment required for the LLOCA has been taken from the DBA analysis. The MAAP cases in this analysis are confirmation runs performed for completeness of the documentation of the success criteria.

The only success path on the LLOCA event tree is LLOCA-001. Each case that was analyzed was performed conservatively with one accumulator, two CMTs, two ADS Stage 4 valves for a long term vent path, one PXS injection valve open, one PXS recirculation valve open, successful PCS water cooling and a 55.88 cm (22 inches) equivalent diameter containment

isolation failure, unless otherwise noted. The equipment assumptions for the LLOCA analysis are based on the combination of equipment that results in the minimum equipment configuration scenario to successfully mitigate a LLOCA. The minimum break size provides the least pressure relief from the break during the injection phase.

The minimum LLOCA break size is a 22.86 cm (9 inches) equivalent diameter break as determined by the smallest break size that is able to remove energy from the primary system while keeping the peak core temperature below 982.2˚ C (1800˚ F) (TCRHOT < 1800˚ F) during PXS injection without any additional depressurization from ADS. The break size was determined assuming successful containment isolation. Sensitivity analyses were performed to ensure that the 22.86 cm (9 inches break) would allow sufficient injection to keep the core below 1800˚F. For confirmatory purposes, 25.4 cm (10 inches) and 20.32 cm (8 inches) break size cases were run to verify that a 22.86 cm (9 inches) break is the lower bound for the LLOCA.

At least one accumulator is required for reactor vessel reflooding following a LLOCA IE. Automatic actuation of the ADS valves is required as manual ADS actuation is not credited in the LLOCA. The break size is sufficient for allowing PXS injection without additional ADS; however, a minimum of two ADS Stage 4 valves are required for long term core cooling.

The successful mitigation of the LLOCA requires successful opening of a PXS injection valve. The manual action to align RNS injection is not credited for the LLOCA. PXS injection is initiated on the same PMS signal as ADS Stage 4 and is driven by the head of water between the IRWST water level and the mixture level in the HL. Additionally, as the injection water boils in the core, the two-phase mixture has a lower density, and the density difference provides additional driving head for PXS injection.

For success, one out of four injection lines must be available, and one of four recirculation lines must be available in any combination of trains.

The MAAP4 analyses verifying the 22.86 cm (9 inches) break were run with PCS water cooling and containment isolation failure. PCS cools the shell around containment, resulting in lower containment pressures. The likely containment failure is of two 40.64 cm (16 inches) diameter valves and has been simulated. Cases run show that low system pressure results in the limiting scenario for PXS injection. These cases also demonstrate that the AP1000 can tolerate failure to isolate the containment and maintain sufficient water inventory to support long term core cooling.

10.4.8.2 Medium LOCA

The success paths for MLOCA are presented in the MLOCA event tree. Each success criteria analysis case for MLOCA has been analyzed with PCS in operation with 25 percent condensate bypass. Each case assumes a 55.88 cm (22 inches) equivalent diameter containment isolation failure, and the success criteria has been determined from this limiting set of conditions. The cases have been run for the upper and lower bound break sizes which are 22.86 cm (9 inches) and 10.16 cm (4 inches), respectively. All success paths assume a hot leg break located at the piping centerline. The upper end of the break range was determined by the lower end of the LLOCA. The lower end of the MLOCA break range has been determined by the 10.16 cm (4 inches) break size's ability to depressurize the RCS below 4136.85 kPa (600 psia) allowing successful ADS Stage 4 operation. 15.24 cm (6 inches) break sizes were also analyzed. These cases also demonstrate that the AP1000 can tolerate failure to isolate the containment and maintain sufficient water inventory to support long term core cooling.

The MLOCA requires ADS Stages 1-3 to actuate to depressurize the RCS for successful RNS injection. ADS Stages 1-3 also cue the operators to manually put RNS in service. ADS Stage 4 must operate to vent the RCS to allow for PXS injection and continued long term recirculation. ADS Stages 1-3 are not required for successful actuation of ADS Stage 4 as the break size will adequately depressurize the RCS. ADS Stages 1-3 can be actuated through Condition 1 or Condition 2. Condition 1 is defined as the setpoints designed in automatic PMS, which actuate ADS. Condition 2 is defined as when the level in the hot leg of the RCS reaches 16.1 percent.

RNS is manually put in service on the cue for ADS Stages 1-3. ADS Stages 1-3 cues are given in the appropriate cases to determine the time that RNS is to be aligned. The success cases assume that RNS is put in service when the ADS Stages 1-3 cue is met.

Pressuriser safety valves (SVs) may potentially stick open during their operation; because of this, any stuck open pressuriser SV in initiators other than MLOCA will transfer to the MLOCA event tree. When fully open, the SV's flow area is approximately equivalent to the break size covered in the MLOCA initiator. When an SV does not seat, it will continue to vent and depressurize the RCS just as a MLOCA would. It is for this reason that stuck open pressuriser SVs will be transferred to the MLOCA event tree. This is considered bounding as the pressuriser SVs may stick only partially open.

10.4.8.3 Small LOCA

The success paths for SLOCA are presented in the SLOCA event tree. Each case has been analyzed with PCS in operation with 25 percent condensate bypass. Each case models a 55.88cm (22 inches) equivalent diameter containment isolation failure, and the success criteria has been determined from this limiting set of conditions. The cases have been run for the upper and lower bound break sizes which are 10.16 cm (4 inches) and 0.95 cm (3/8 inches), respectively. All success paths have been run on the hot leg, where the break is located on the piping centerline. The upper end of the break range was determined by the lower end of the MLOCA. The lower end of the SLOCA break range has been determined by the ability of CVS to make up lost coolant from a 0.95 cm (3/8 inch) break. These cases also demonstrate that the AP1000 can tolerate failure to isolate the containment and maintain sufficient water inventory to support long term core cooling.

The SLOCA requires that ADS Stages 1 3 operate to depressurize the RCS to allow for gravity or RNS injection. The equipment setpoints and associated actuations for the SLOCA are the same as the MLOCA initiator.

RNS is manually put in service on the cue for ADS Stages 1-3. ADS Stages 1-3 cues are given in the appropriate cases following to determine the time that RNS is to be aligned. The success cases assume that RNS is put in service when the ADS Stages 1-3 cue is met. 10.16 cm (4 inches) cases do not see any benefit from PRHR; however, 0.95 cm (3/8 inch) breaks benefit where the RCS is depressurized, and time to core damage is extended. A 5.08 cm (2 inches) break size was also analyzed.

10.4.8.4 RCS Leak

This initiator is an RCS LOCA, 0.95 cm (3/8 inch) and smaller, which is in the nominal CVS pump makeup capacity of 6.3 L/sec (100 gpm).

If CVS and borated inventory is available, this accident can be mitigated with a controlled plant shutdown without the use of Class 1 equipment within the time described in the technical specifications.

In the event that CVS is unavailable, there will be continual RCS inventory losses. When PRHR is available to remove decay heat, its availability provides more long term success paths. In injection mode, the CMT level drops and ADS Stages 1-3 and ADS Stage 4 actuation will occur. Otherwise, the accumulators will inject and ADS Stages 1-3, and ADS Stage 4 must be actuated manually. The IRWST provides gravity injected RCS inventory makeup after the ADS Stage 4 squib valves open; RNS pumped injection provides an alternative means for RCS makeup. When the IRWST level drops, recirculation is required via passive recirculation or RNS pumped recirculation. All LEAK event tree success paths were analyzed and confirmed using the upper bound RCS leak size.

10.4.8.5 General Transients with Safeguards Actuation

This initiator is a reactor trip coincident with a Safeguards Signal. Safeguards actuation provides automatic CMT actuation, PRHR actuation, and main feedwater isolation. For successful mitigation of general transient sequences, decay heat removal is required from either SFW or PRHR.

This analysis bounds general transient events that experience a failure of MFW and/or SFW by analyzing cases that model a total loss of feedwater. A total loss of feedwater event bounds the thermal hydraulic response of general transient initiators with failures of feedwater. During a total loss of feedwater event, the SG dries out during at power operation. However, during a general transient initiator with failed MFW and/or SFW, the reactor trips and SG dry out follows. So, at the time of reactor trip, there is significantly less SG inventory in the total loss of feedwater case as compared to the general transient case.

In the event that decay heat removal is unavailable, the RCS will lose the ability to transfer heat and begin to heat up. As the RCS temperature and pressure increase, the pressuriser SVs will lift and cause an RCS inventory loss. This helps the CMT recirculation and injection driving force. In recirculation mode, the CMTs provide borated water to the reactor vessel for RCS inventory and reactivity control. In injection mode, the CMT level drops and ADS Stages 1-3 and ADS Stage 4 actuation will occur. The IRWST provides gravity injected RCS inventory makeup after the ADS Stage 4 squib valves open; pumped RNS injection provides an alternative means for RCS makeup. When the IRWST level drops, recirculation is required via passive recirculation or pumped RNS recirculation.

The success paths of the general transients with safeguards actuation (GTRAN-WS) event tree are analyzed and confirmed. In all cases, reactor trip is successful, the secondary side is not faulted, and the pressuriser SV lifts but does not stick open. The interaction between SFW and PRHR is addressed in this analysis. Each sequence has been analyzed with PCS in operation and 25 percent condensate bypass and a 55.88 cm (22 inches) diameter containment isolation failure. The success criteria have been determined from this limiting set of conditions. These cases also demonstrate that the AP1000 can tolerate failure to isolate the containment and maintain sufficient water inventory to support long term core cooling.

10.4.8.6 General Transients without Safeguards Actuation

This initiator is a reactor trip without a Safeguards Signal. In this event tree, MFW is available to the SGs. For successful mitigation of general transient sequences, decay heat removal is required from MFW, SFW, or PRHR.

This analysis bounds general transient events that experience a failure of MFW and/or SFW by analyzing cases that model a total loss of feedwater. A total loss of feedwater event bounds the thermal-hydraulic response of general transient initiators with failures of

feedwater. During a total loss of feedwater event, the SG dries out during at power operation. However, during a general transient initiator with failed MFW and/or SFW, the reactor trips and SG dry out follows. So, at the time of reactor trip, there is significantly less SG inventory in the total loss of feedwater case as compared to the general transient case.

Consistent with the system model, MFW pumps receive supply from the condenser. The condenser receives discharged steam from the SG and produces condensate. Therefore, there is a continuous supply of condensate for the MFW pumps. MAAP4 does not have the capability to model this feature; to mimic this setup, an additional condensate storage tank (CST) mass inventory is added when the CST reaches an arbitrarily low value.

In the event that decay heat removal is unavailable, the RCS will lose the ability to transfer heat and begin to heat up. As the RCS temperature and pressure increase, the pressuriser SVs will lift and cause an RCS inventory loss. This helps the CMT recirculation and injection driving force. As the CMTs inject into the RCS and their level decreases, the ADS Stages 1-3 and ADS Stage 4 actuation will occur. The IRWST provides gravity injected RCS inventory makeup after the ADS Stage 4 squib valves open; pumped RNS injection provides an alternative means for RCS makeup. When the IRWST level drops, recirculation is required via passive recirculation or pumped RNS recirculation. The interaction between SFW and PRHR is addressed in this analysis.

The success paths of the general transients without the safeguards actuation (GTRAN) event tree are analyzed and confirmed. In all cases, reactor trip is successful, the secondary side is not faulted, and the pressuriser SVs lift but do not stick open.

10.4.8.7 Steam Generator Tube Rupture

An SGTR can occur as an initiator or as an induced event from a different initiator. During an SGTR, RCS inventory is transferred through the tube rupture and into the SG secondary side. In general, the AP1000 plant design operating philosophy requires limiting the primary to secondary leakage and minimizing the radiological releases following a SGTR. Success for this initiator is defined as the termination of tube rupture break flow and prevention of core damage.

When ruptured SG isolation is successful (based on SG level setpoints) and decay heat removal is available, the RCS pressure is balanced and SGTR break flow is terminated and remains in the ruptured SG. If isolation is failed, or there is no decay heat removal, then RCS depressurization via the ADS valves helps reduce the inventory losses. This allows for recirculation to be credited when ruptured SG isolation fails.

The success criteria is valid for a single detectable tube leak up to five double-ended guillotine (DEG) tube ruptures. For the SGTR event tree success paths reactor trip is successful. SFW has been modeled in each of the cases to minimize the time for SG overfill; this way the accident progression is not changed; however, the timeline of events is moved up to be within the 24 hour mission time. Cases which include SFW as a mitigating system will also be modeled with a cooldown via the secondary side at a rate of 37.7˚ C/hr (100˚ F/hr). The interaction between SFW and PRHR is addressed in this analysis. Top event I&I involves manual identification and isolation of the ruptured steam generator. Top event OFILL isolates CVS and SFW flow to the steam generators. The success paths of the SGTR event tree are analyzed and confirmed.

10.4.8.8 Steam Line Break

Steam line break represents a DEG break on the secondary steam line. The break size is limited by the area of the venturi flow limiting insert at the top of the SG. The steam line break area has been defined by this restrictor, which is 0.13 square meter (1.4 square feet).

An SLB requires boration of the RCS to maintain core subcriticality. MAAP4 is not capable of modelling criticality; and therefore, the first 1,000 seconds of each case has been modelled by CENTS which has a criticality model and can determine any return to power after the break. Based on the CENTS runs, the return to power cases (<25percent of total power) do not result in core damage. The success criteria have been determined from cases that have acceptable return to power events which quickly turn around and stabilize with subcritical conditions.

The CENTS model has generated a bounding total power curve for the first 1,000 seconds of an SLB. The bounding total power curve accounts for the decay heat from reactor trip as well as the short return to criticality at the beginning of the accident. This return to power occurs almost immediately after reactor trip, and subsides a few hundred seconds into the accident as seen in the CENTS analysis. It is important that boration from the fast acting CMTs is introduced to the reactor immediately following reactor trip to shut the reactor down. The MAAP4 analyses incorporate the total power curve from CENTS to determine the minimum set of equipment required for an SLB.

The SLB initiator does not include any success paths that require manual actuation of ADS (via Condition 2). The return to power that is modelled in these cases is so great that the boration required to shut down the reactor must come immediately after the reactor trips, via the CMT or CVS. ADS Stages 1-3 (actuated via the low hot leg level) are unable to depressurize the RCS in time for the accumulators to mitigate the return to power.

Each sequence has been analysed with PCS in operation, 25 percent condensate bypass and a 55.88 cm (22 inches) diameter containment isolation failure. Both the SLB upstream and downstream of the MSIVs are modelled so that they vent the break effluent inside containment. Break locations that discharge to the containment or the environment are not expected to have a significant impact on results. Containment isolation failure results in the more conservative approach for determining the long term success of each case. MAAP detects low steam line pressure (which would result in SG isolation) about 13 seconds after the steam line break. For consistency, the cases have been designed so that SG isolation (if required) will occur 15 seconds after the SLB. The success criteria have been determined from this limiting set of conditions. The success paths of the SLBU and SLBD event trees are analyzed and confirmed.

10.4.8.9 Interfacing System LOCA

An Interfacing System LOCA is a break outside containment in an auxiliary system that interacts with the reactor coolant system. If the break is not isolated, the result is a loss of reactor coolant and emergency cooling water outside containment. The unmitigated loss of coolant outside containment may lead to core damage and a direct release to the environment. If isolation of the break is successful, the ISLOCA may then be successfully mitigated by the Class-1 and non-Class 1 systems of the plant. This analysis is based on (and uses scenario information from) the break pathways identified in the ISLOCA analysis.

The ISLOCA cases act like general transients after the breaks have been isolated. Therefore, the cases reference the general transient sections. All of the sequences for ISLOCA have been analyzed with PCS in operation and 25 percent condensate bypass, as well as a 55.88 cm (22 inches) equivalent diameter containment isolation failure. The interaction between SFW and PRHR is addressed in this analysis. Each of the ISLOCA pathways is described along with its corresponding success case.

CVS Spent Resin Sluice Line (P05)

In the event of a CVS spent resin sluice line over pressurization, the low pressure piping located outside of containment just before the WSS Spent Resin Tank may fail, resulting in an ISLOCA. The line is 5.08 cm (2 inches) in diameter and passes through containment penetration P05. Successful mitigation in these cases requires automatic or manual isolation on the Safeguards Signal; otherwise, the sequence will proceed to core damage and large release. Therefore, each of the success paths includes successful isolation at the time of the Safeguards Signal. The success criteria for each ISL-CVS event tree success path are analyzed and confirmed.

CVS Normal, CMT and Accumulator Makeup Lines (P07)

In the scenario where the CVS normal, CMT or accumulator makeup lines over pressurize (through containment penetration P07), the low pressure piping and makeup suction header outside containment may fail resulting in an ISLOCA. A 7.62 cm (3 inches) diameter line runs through containment penetration P07. This ISLOCA has the same event tree as the CVS Spent Resin Sluice Line. Successful mitigation in these cases requires automatic or manual isolation on the Safeguards Signal; otherwise, the sequence will proceed to core damage and large release. Therefore, each of the success paths includes successful isolation at the time of the Safeguards Signal. The success criteria for each ISL-CVS event tree success path are analyzed and confirmed.

CVS Zinc Injection Line (P08)

The zinc injection package continuously adds liquid zinc acetate solution through containment penetration P08 during normal power operation. A positive displacement pump accommodates the variations in operating pressures at the injection point. Upon failure of the positive displacement pump, a potential ISLOCA scenario will result from external leakage of the containment isolation valve outside containment or the failure of the zinc addition pump discharge check valve and external leakage of the pump. The HRA has been bounded by the previous ISLOCA pathway (P07). The success criteria for each ISL-CVS event tree success path are analyzed and confirmed.

10.4.8.10 Loss of Offsite Power

A LOOP initiator occurs when offsite ac power is lost to the reactor and its associated mitigation equipment. This analysis does not credit turbine runback.

Under normal operation, passive equipment is powered from the Class 1 250V dc batteries. For LOOP initiators, the only condition that changes is what powers the batteries. When ac power is available, the ac source is supplying power to the battery chargers, which allows the batteries to maintain charge while supplying the loads. When ac power is not available, the batteries are sufficiently sized to supply 24 hours of indication and control to Class 1 equipment. During LOOP initiators, active equipment is loaded on the SDG and supplied power from those sources.

The LOOP event tree structure and success criteria are similar to the general transient event tree, and when a secondary side fault occurs the event transfers to the SLBU event tree. The only exceptions to the information presented in these sections are ac power availability and use of PRHR. The availability of ac power and, therefore, the power source for active systems and the treatment of the passive system battery power is a difference from the general transient tree.

When a LOOP initiator occurs and the SDGs are unavailable, the plant is in SBO conditions. Because the active systems rely on the SDGs as their power source, in this scenario, the active systems are disabled. The passive systems are powered from the Class 1 batteries, which provide 24 hours of power for reactor trip and ESFAC (Engineering Safety Features Actuation Cabinets) actuation.

There is a cumulative timer, which measures the time the ac power source is unavailable; this monitors the SBO accident length. Shortly before the timer is fulfilled (at approximately 22 hours), the ADS Stage 4 and IRWST gravity injection line squib valves are fired. Based on the MAAP4 results, ADS Stages 1-3 are not required to reduce the RCS to pressures lower than 4136.85 kPa (600 psia). If the cumulative timer is disabled as is recommended in the operating procedures, then PRHR is the only system required for mitigation of this accident. PRHR serves as both decay heat removal and RCS depressurization for this accident scenario. The interaction between SFW and PRHR is addressed in this analysis. The success criteria for each LOOP event tree success path are analyzed and confirmed.

10.4.8.11 PRHR Tube Rupture

During a PRHR tube rupture, the PRHR tube is leaking RCS inventory into the IRWST. This initiator represents a detectible leak up to a single DEG break. For smaller PRHR HX tube leaks, the temperature instruments in the PRHR or IRWST will identify that hot water is leaking out of the RCS. During larger breaks of the PRHR HX tubes, the reactor will trip on low pressuriser pressure/level. As a complication of reactor trip, the secondary side relief valves lift and are expected to reclose. If the valves remain open, this initiator is treated with the secondary side fault initiators.

When PRHR HX isolation is not successful, the transient break flow continues and the resulting mitigation is similar to a SLOCA. These success paths require initial inventory control using either the CMTs or accumulators. As this accident progresses, the CMT or RCS levels will drop and ADS Stages 1-3 actuation can occur either automatically or manually. After ADS Stages 1-3 actuations occur, the ADS Stage 4 valves, IRWST gravity injection and recirculation will follow. Instances when ADS Stage 4 depressurization or IRWST gravity injection is not successful, RNS injection and pumped recirculation can provide long term RCS inventory control.

This analysis does not credit CVS as an RCS inventory source. The PRHR tubes are 1.91 cm (3/4 inch), which is greater than the CVS capability. Crediting CVS in this initiator only prolongs the time of reactor trip from low pressuriser pressure/level. CVS does not support long term normal operation with a single DEG PRHR tube rupture.

This analysis does not credit PRHR HX isolation. On the upper bound break size of the accident progression, the RCS transient is fast enough that the reactor is expected to trip, and Safeguards Signal is actuated before the operators are able to isolate the PRHR HX. There is less than 5 minutes to isolate the PRHR HX.

During a PRHR tube rupture event PRHR performance is expected to be maintained. Sensitivity cases were run with a design basis T-H code to demonstrate continual PRHR performance during a tube rupture event. Since this tube rupture break size could be a small leak up to a double ended break of a 1.91 cm (3/4 inch) tube, this event is grouped with Small LOCA since CVS makeup is not sufficient at the upper end of the break size. This IE can therefore be grouped as a small LOCA event.

10.4.8.12 CMT Line Break

A CMT line break occurs upstream of the CMT isolation valves (PXS-V014A/B and PXS-V015A/B) on the discharge line and downstream of the T-connection for the RCS CL and the CMT balance line.

When a CMT line break occurs on the discharge line, the initial CMT inventory will drain down. Following CMT drain down from a discharge line break or when a CMT line break occurs on the balance line, RCS inventory will be lost through the normally open valves PXS-V002A/B and/or ruptured area via the CL.

Because these line sizes are nominally 20.32 cm (8 inches), the upper bound break size of this event is based on the MLOCA tree. On the lower end of the break sizes, it is similar to the success paths of lower bound of RCS Leaks. It is acceptable to not include PRHR as a mitigation feature because in these cases, PRHR removes decay heat and decreases the RCS pressure. But there are still success paths without PRHR modelled in the LEAK event tree. Therefore, this initiator uses a combination of success paths from MLOCA (for the upper bound requirements) and RCS Leak (for the lower bound requirements) for the CMTLB event tree. As part of the initiator, one CMT's inventory is lost. The CMT success criteria must be reduced to one out of one available CMT.

10.4.8.13 PRHR Line Break

A PRHR line break occurs upstream of the PRHR HX inlet up to the T-connection with the RCS HL and downstream of the PRHR HX outlet to the SG CL plenum. This analysis disables the heat removal capability of PRHR for any break size in the PRHR lines. Although this is conservative, PRHR is not credited as a mitigation feature of this initiator.

At the upper bound of this initiator, a DEG of the 45.72 cm (18 inches) pipe could occur. On the other hand, at the lower bound of this initiator, a break equivalent to an RCS leak could occur. In order to develop success criteria that are valid for the entire break range, the LLOCA event tree was altered to include the necessity of reactor trip and depressurization from ADS Stages 1-3 to mitigate the smaller break sizes. Additionally, only the PXS automatic features are considered in the PRHRLB event tree as consistent with LLOCA. The PRHR line break accident progression credits only the recirculation operator action.

10.4.8.14 Spurious Actuation ADS Stages 1-3

Spurious ADS Stages 1-3 initiators occur when any combination of ADS Stages 1-3 valves spuriously operate and provide depressurization from the RCS into the IRWST. It is expected that most actuations will occur with a spurious PMS signal to one train, which would begin with the ADS Stage 1 actuation and remaining ADS Stages 2-3 valves with the appropriate time delay. However, this analysis must consider an upper and lower bound spurious actuation. The lower bound of this initiator would be the actuation of only one ADS Stage 1 valve. The upper bound of this initiator would be the actuation of both trains of all ADS

Stages 1-3 valves. The actuation of any ADS stage 1-3 valve is very unlikely due to PMS interlocks and a diverse blocker.

The event tree structure of this initiator is based on the MLOCA event tree with adjusted success criteria for ADS Stages 1-3 depressurization. For this initiator, reactor trip is required for reactivity control. Following reactivity control, the RCS also needs inventory control from any one of the CMTs or accumulators. Depending on how many ADS valves opened as part of the initiator, more ADS valves may need to open to provide depressurization to reduce the RCS pressure to less than 4136.85 kPa (600 psia) for ADS Stage 4 actuation. ADS Stage 4 actuation is followed by IRWST passive gravity injection and recirculation or RNS pumped injection and recirculation.

Based on MAAP4 runs, the spurious ADS Stages 1-3 initiator can be appropriately treated as a MLOCA with adjusted success criteria based on the SPADS13 event tree structure. The RCS pressure decrease from the spurious ADS Stages 1-3 initiator is within the range of RCS pressure from a traditional HL or CL MLOCA break.

10.4.8.15 Spurious Actuation ADS Stage 4

The spurious ADS Stage 4 initiator occurs when one or more ADS Stage 4 valves operate and open during at-power conditions. This IE has complicating factors associated with the plant response of this initiator mainly from the potential for local pipe and valve damage. The actuation of any ADS Stage 4 valve is very unlikely due to PMS interlocks and a diverse blocker.

The top portion of the SPADS4 event tree (greater than one valve spuriously operates) uses LLOCA success criteria requirements, and the bottom portion (one valve spuriously operates) uses MLOCA success criteria. There are no MAAP4 supporting T-H cases to determine the success criteria requirements for this initiator.

When two ADS Stage 4 valves spuriously operate, one valve on the opposite loop is required to meet the depressurization success criteria, and the signal for IRWST gravity injection must be provided. When four ADS Stage 4 valves spuriously operate, the depressurization success criteria is met; however, the IRWST gravity injection signal must be generated. When one ADS Stage 4 valve spuriously operates, one valve on the opposite loop is required to meet the depressurization success criteria and the signal for IRWST gravity injection must be provided.

A spurious actuation of one ADS Stage 4 valve can create an accident equivalent to a LLOCA. The opening of a valve at full RCS pressure may not work as intended. It is because of this phenomenon that the depressurization has been demonstrated with a MAAP4 run to clarify that one fully opened ADS Stage 4 valve will depressurize the RCS in about 300 seconds. With one ADS Stage 4 valve spuriously operating along with two accumulators the RCS depressurizes rapidly to nearly 689.5 kPa (100 psia).

10.4.8.16 Spurious IRWST Injection Actuation

The spurious IRWST injection valve initiator occurs when one or more IRWST gravity injection squib valves operate during at-power conditions. This IE has several complicating factors associated with the plant response of this initiator (the potential for local pipe and valve damage). There are no MAAP4 supporting T-H cases to determine the success criteria requirements for this initiator. The actuation of any IRWST injection valve is very unlikely due to PMS interlocks and the diverse blocker.

The top non-core damage path on the SPIRWST event tree (two or more valves spuriously operate) requires four out of four injection check valves to remain intact and closed after spurious actuation of the IRWST gravity injection squib valves. This path transfers to the SLOCA event tree because of pressure balancing holes in the check valves.

The bottom non-core damage paths on the SPIRWST event tree (one out of four valves spuriously operates) requires one out of one gravity injection check valve to remain intact and closed after there is spurious actuation of the IRWST squib valves on that line. If the gravity injection check valve remains intact and closed, the path transfers to the LEAK event tree. If the gravity injection check valve fails to remain intact or closed, this event is treated as a DVILB since it could result in a LOCA with loss of one injection pathway.

10.4.8.17 DVI Line Break

A DVI line break occurs upstream of the RV inlet and downstream of the CMT isolation valves, the accumulator check valves, the IRWST injection lines, and the RNS injection lines. This break range can be on the upper end, a DEG of the 20.32 cm (8 inches) portion of the line but limited by the 10.16 cm (4 inches) venturi in the RV inlet nozzle, or on the lower end, an RCS leak.

When this initiator occurs and RCS inventory is lost through the DVI line, reactor trip is required for reactivity control. RCS inventory is replaced from either the CMTs or the accumulators. In order to provide long term core cooling, the ADS Stages 1-3 valves provide depressurization to reduce the RCS pressure to less than 4136.85 kPa (600 psia) for ADS Stage 4 actuation. ADS Stage 4 actuation is followed by IRWST passive gravity injection and recirculation. Neither RNS injection nor RNS recirculation are credited in this analysis.

10.4.8.18 Spurious Containment Recirculation

The spurious containment recirculation initiator occurs when one PXS recirculation valve or a common cause failure event of all PXS recirculation valves open. Spurious actuation of the PXS recirculation squib valves can drain the IRWST inventory to the reactor cavity. The PXS recirculation line configuration includes two cavity flooding lines. Two of the four lines have a squib valve and an open motor-operated valve (MOV) in series. The other two recirculation lines have a squib valve in series with a check valve that prevents the IRWST from draining through them. Engineering judgement was used to support the success criteria. There are limited MAAP4 supporting T-H cases to determine the success criteria requirements for this unique initiator.

If the operator successfully isolates the IRWST recirculation valves within 30 minutes of the low IRWST level alarm, then the IRWST level remaining will support PRHR cooling and IRWST injection and recirculation. If the reactor trip is successful, main feedwater or startup feedwater could provide RCS cooling. A safeguards signal is not anticipated due to the inventory drained to the sump. The potential containment pressure increase due to external reactor vessel cooling (water in the cavity and the in-vessel retention design feature) is expected to be maintained lower than the containment isolation setpoint.

MAAP4 results of this analysis looked at the spurious opening of both recirculation lines opening at time 0 and isolation of the recirculation pathway after 30 minutes. After reactor trip, the run did not credit SFW or MFW for decay heat removal. PRHR was actuated on low steam generator level. CMT actuation with RCP trip occurs on low pressuriser pressure. With the RCPs tripped, there is decreased PRHR decay heat removal and the pressuriser safety valves open for a time until the decay heat subsides. With PRHR operating, successful

IRWST recirculation isolation, and successful opening and closure of the pressuriser safety valves, this event can be treated like a general transient with safeguards (safeguards signal is anticipated due to PRHR actuation on low pressuriser pressure). In the GTRAN-WS event tree, decay heat removal systems available are PRHR system, SFW system, and RCS depressurization using the ADS with IRWST/RNS injection and recirculation.

If the pressuriser safety valves stick open, the success criteria are based on the MLOCA plant response. This potential event was analysed with MAAP4. The analysis shows that based on the timing of passive injection and recirculation, a minimum of 3 out of 4 ADS Stage 4 valves are required for successful passive injection and long term core cooling by the PXS system following RCS depressurization. Gravity injection is successful if the water head in the IRWST is sufficient to overcome the friction losses and pressure drop across the piping, core, and ADS Stage 4 lines that develop from venting the two-phase steam and water flow produced by the decay heat boiling in the core. The ADS Stage 4 requirements are a function of decay heat, the time to start of injection, the time to start recirculation, and the reduced IRWST level at injection.

If the IRWST recirculation valve is isolated within 30 minutes and the reactor is not successfully tripped, the sequence is maintained as a sequence because the operators are directed to initiate a plant shutdown due to a technical specification requirement. If the reactor does not successfully trip, then the sequence can be treated as an ATWT event.

If the IRWST recirculation is not isolated and the reactor is not successfully tripped, the sequence is assigned as a core damage event. In this potential ATWT event, PRHR and passive injection is degraded due to the drained IRWST condition.

If IRWST recirculation isolation is not successful, then the IRWST will continue to drain to the reactor cavity and containment sump. Because IRWST inventory is needed to support heat removal systems like PRHR and RCS depressurization using the ADS with IRWST/RNS injection and recirculation, only the secondary side heat removal systems are credited.

10.4.8.19 Anticipated Transient Without SCRAM

The ATWT initiator occurs for a spectrum of IEs which are expected to result in a reactor trip and it does not occur. Note that DAS provides a backup means of removing power from the CRDMs to provide for control rod insertion. In order to mitigate this event the reactor power must be reduced without rod insertion. In addition, the maximum RCS pressure must be limited. Providing these two functions are interrelated.

The success criteria is the RCS pressure must remain less than 220.63 Bar (3200 psig). Limiting the RCS pressure to this value without rod insertion requires that the core power production be rapidly reduced to levels that can be removed by the MFW, SFW or PRHR. This power reduction is accomplished by:

- Reactor coolant temperature rise and associated negative reactivity feedback
- Tripping of the RCPs and associated void formation in the core

In the longer term, boron is required to completely shut down core power generation. For this function CMT operation is credited. Note that when the CMTs are actuated, the RCPs are also tripped which is important in reducing the power. In an ATWT, the CMTs will operate in a water recirculation mode.

For this specific initiator, MFW, SFW or PRHR are available for heat removal. For immediate boration CVS is not credited because there is not enough time to complete the operator action to align the system.

The interaction between SFW and PRHR is addressed in this analysis. The LOFTRAN code with its ability to model reactivity changes was used for the success criteria runs. The success criteria for each ATWT event tree success path are analyzed and confirmed.

10.4.8.20 ATWT – Loss of Main Feedwater

This event is similar to the ATWT event described in Section 10.4.8.19 except that the IE involved a loss of MFW. For this specific initiator, SFW or PRHR is available for heat removal. Otherwise, the success criteria are the same as in Section 10.4.8.19.

10.4.8.21 Long Term Cooling Analysis

The long term cooling event trees are transfer trees used to assess long term containment cooling for successful Level 1 sequences in which decay heat is being removed from the RCS by either containment sump recirculation or the PRHR. The Level 1 success criteria analysis has confirmed that these cases mitigate core damage for the first 24 hours (reaching a safe, stable state), and this analysis determines the equipment configurations that will allow for successful continued long term core cooling for at least 3 days from the start of an accident. For each case analysed, the equipment required to mitigate each accident in the short term (<24 hours) has successfully operated, and the long term heat removal ability is determined and analysed.

PCS water actuation is modelled in the cases in this analysis; the actuation setpoint used is the high containment pressure setpoint. In containment isolation failure cases where the containment pressure setpoint was not met, the containment temperature setpoint was used to actuate PCS water. Containment will eventually reach this setpoint as demonstrated in the SGTR cases where CI is failed and PCS is required to actuate.

Success is determined by a sump level analysis and by an analysis for extended PRHR cooling. Each case that uses ADS must maintain a sump water level that is above the minimum level during recirculation operation to be considered successful. This minimum water level ensures that recirculation of water through the sump is possible. For the total loss of feedwater (TLFW) cases which analyse PRHR cooling, success is based off the PRHR HX's ability to provide cooling during each case. Each case has been run for 5 day duration to determine if a case is successful for a minimum of 3 days and to determine if a case is successful past the 3 day time frame. Success using PRHR requires that the RCS temperature does not exceed 253 ˚ C (488˚ F) before 72 hours.

Representative MAAP4 runs were made for the following events:

- Large LOCA
- DVI Line Break
- TLFW
- Steam Line Break Upstream of the MSIVs
- SGTR

The success paths of the LTC and LTCP event trees are analyzed and confirmed.

10.5 Systems Analysis

10.5.1 Fault Tree Guidelines

The Systems Analysis documentation and fault trees were developed based on consistent guidance. This section aims to summarize those guidelines.

10.5.1.1 Basic Event Parameters

A basic event's failure probability or unavailability is determined by identifying the failure modes for the component and by assigning failure rates to the failure modes from the Master Type Code Table.

Demand failure probabilities for equipment, which must start or change state, are calculated using the failures per demand value multiplied by the number of demands required (Calculation Method (Type) 1). Operating equipment basic event failure probabilities are calculated using the failure rate multiplied by the mission time (Calculation Method (Type) 3), and standby equipment basic event probabilities are calculated using the failure rate multiplied by the exposure time divided by 2 plus the mission time (Calculation Method (Type) 5).

The calculation of component failure probabilities is summarized by the following examples for each method:

- Calculation Method (Type) 1: A normally closed, MOV, which is required to pass flow, may fail to open on demand.

- Calculation Method (Type) 3: A pump, which is required to run in order to mitigate an event, may fail to run for the mission time.

- Calculation Method (Type) 5: A standby, normally open, MOV, which is required to pass flow, may have transferred closed during the period of time between the previous test and the IE, or the mission time.

Instead of the calculation method (type) in CAFTA, the equation field is used with the equations corresponding to the calculation methods discussed above.

10.5.1.2 Exposure Times

Many components that need to be included in the model are normally in a standby mode; that is, they are not used until required. Often such components are assumed to have a failure rate (i.e., failure per hour) while in standby mode. Standby components are usually subjected to periodic testing. The time between tests is the length of time the component is exposed to failure without detection, and hence the term "exposure time."

For support system trains that are normally rotated during at-power operation, an exposure time will be used that is the time, or representative of the time, the component is exposed to failure without detection. This exposure time for support systems that are normally rotated is the time period between rotating pump trains. Pump trains are assumed to be rotated every two weeks. This is consistent with current plant practices.

10.5.1.3 Mission Times

The mission time is the time period that a system or component is required to operate in order to successfully perform its function. Success is defined as the plant reaching a safe, stable plant condition after the IE. The timing required to reach a safe, stable state is established by Success Criteria.

Each core damage event tree is modelled through a time frame of up to 24 hours. This time frame is selected to be consistent with the commonly accepted PRA practices, in which it is postulated that an event sequence will reach steady state conditions which will change very slowly at that time. Also assumed is the possibility of numerous and diverse recovery actions (which are not credited in the cutsets) that can be undertaken in such a time frame to further mitigate the event. Another aspect of this time frame is that it covers the actuation of all expected mitigation functions/systems needed for avoiding core damage.

Likewise, some systems required to maintain containment integrity are modelled through a 72 hour mission time.

Additionally, when developing an IE system model, a mission time of 1 year (8760 hours) is used for the initial fault to obtain an annual frequency of failure, and 72 hours is used for subsequent faults.

10.5.1.4 Naming Convention

A standard naming convention is used throughout the model. For failure basic events (component failures), the normal basic event name shall follow the convention:

SYS-SCT-CFM-XXX

where,

SYS is the unique three letter system code identified for the AP1000 plant

SCT is the specific component type from NUREG-6928 (Reference 10.15)

CFM is the component failure mode (note that TAM is used as the Test and Maintenance Identifier)

XXX is the unique component identifier

There are several unique expansions to the naming convention such as for C&I systems and electrical systems.

For a support system IE fault tree, a “-IE” or “-ST” designator is added to the end of the basic event ID to indicate basic events with a mission time of 8760 hours or 72 hours, respectively.

A standard naming convention is also used for gate names. The gate naming convention is broken into parts:

- Top Logic Names
- System Tops
- System Gates

Common cause and flag names also follow a standard naming convention using identifiers including “CCF-” and “FL-”, respectively.

10.5.1.5 Failure Modes

Failure modes for Systems Analysis are considered to:

- Include active and passive failures affecting system operability (as identified in the system success criteria). Active failures typically affect pumps, valves, relays and air compressors. Passive failures typically affect heat exchangers, valves not required to change position, and tanks.

- Exclude beneficial failures (e.g., failure of an instrument in such a fashion as to generate a required actuation signal). This failure should not be included unless omission would distort the results.

- All applicable failure modes for components on a main flow path shall be modelled.

10.5.1.6 Common Cause Failures

Failure of multiple components of similar manufacture and function due to common cause are potentially significant contributors to system failure and should be accounted for during system analysis. These types of failures are represented in fault trees as common cause failure (CCF) basic events. CCF can result in failure of a system when identical, non-diverse, and active components are used to provide redundancy. A component common cause group (CCCG) shall be defined for these cases, and basic events representing failure of two or more components due to CCF shall be incorporated into the fault tree.

The identification of CCCGs shall be performed by focusing on components that share one or more of the following criteria:

- Same design
- Same hardware
- Same function
- Same installation
- Same maintenance
- Same procedures
- Same system/component interface
- Same environment

Common cause failures are discussed in detail in Section 10.8.

10.5.1.7 Test and Maintenance

The component unavailability due to testing and maintenance, where applicable, is determined as follows:

- Based on the system Piping and Instrumentation Diagram (P&ID) and the test and maintenance procedures, the system alignment for each of the test and maintenance activities is determined. Then, it is determined whether the test requires that a component be placed in a position, which makes the component unavailable.

- For each component placed into a non-safety position, both the unavailability during testing or maintenance is modelled.

- Particular attention is given to identifying components that are isolated to facilitate maintenance of another component. An example is the closure of manual valves to perform pump maintenance.

10.5.1.8 Flow Diversions and Piping Failures

Flow paths that can divert the system fluid from the intended destination shall be evaluated to determine if they should be modelled as a failure mode.

Both active and passive components shall be considered. If necessary, piping will be modelled on a functional basis.

10.5.1.9 Mutually Exclusive

Often two events may appear in a cutset that could not occur simultaneously. To address mutually exclusive events, combinations are identified and the non-applicable cutsets are removed.

10.5.1.10 Recovery

The repair of hardware failures is not modelled in the AP1000 plant PRA except where the probability of repair is justified through an adequate analysis or examination of data.

The manual actions required to bypass failed systems or recover malfunctioning equipment are modelled as described in the HRA Section 10.6.

10.5.2 Passive Core Cooling System

10.5.2.1 System Description

The PXS consists of a PRHR heat exchanger, two accumulators, two CMTs, an IRWST, and associated valves, piping, and instrumentation. The ADS is actually a subsystem of the RCS; however, it is discussed here because of its relationship with the passive core cooling system. Additionally, the RCP breakers, which are part of the ECS, are discussed here for CMT actuation.

The RCS injection subsystem consists of CMTs, accumulators, and IRWST and associated valves, piping, and instrumentation. The safety injection from these three injection sources, as well as the containment recirculation flow paths, have a common discharge through the two DVI lines and into the reactor DVI nozzles. The DVI nozzles have a venturi shape, which reduces the loss of reactor coolant in case of a break of the DVI line, and minimizes the unrecovered pressure loss during PXS injection.

The CMTs provide RCS makeup and boration for LOCAs and non-LOCAs when the normal makeup system is unavailable or insufficient. Located inside containment, above the reactor coolant loops, two CMTs during normal operation are completely filled with cold borated water. The boron concentration in these tanks is slightly higher than in the accumulators or IRWST, and therefore the tanks provide adequate shutdown margin for safe shutdown events. The CMTs are connected to the RCS through a discharge line and a cold leg inlet pressure balance line (cold leg 2A and 2B). The pressure balance line is normally open to maintain the CMTs at RCS pressure which prevents water hammer upon initiation of CMT injection. The pressure balance line or inlet line contains a normally open MOV. The discharge line of the CMT includes two normally closed, parallel air-operated isolation valves that fail open on a loss of air or electrical power. Downstream of the parallel AOVs, the discharge line contains two in line, nozzle check valves in series, a normally open manual valve, and an orifice which is provided to allow for tuning of the CMT injection flowrate prior to initial startup. Between the check valves and the orifice is the connection from the RNS pumps to provide injection to the RCS. The CMT discharge check valves are normally full open. The purpose of the check valves in series is to prevent reverse flow from the accumulators through the CMT.

Two accumulators contain borated water and a compressed nitrogen cover gas to provide rapid injection to the RCS through each DVI line. Each accumulator discharges through a normally open MOV and two normally closed tilt-disc check valves in series. Between the MOV and the check valves is an orifice to provide tuning of the injection flow. The check valves isolate the accumulators from the RCS during normal operation.

The IRWST, located in the containment slightly above the RCS loop piping, contains cold borated water and three separate screens at the bottom. A cross-connect pipe connects all three screens to distribute flow. The area of the third screen (C) is equal to the total size of the other screens (A and B). With the addition of the cross-connect pipe, clogging of any one screen would not fail the function of the IRWST to deliver flow to the gravity injection lines. The IRWST is connected to the RCS through two gravity injection lines, with each line connecting to a DVI line. Each gravity injection line contains a normally open MOV and four isolation valves. The isolation valves are in two parallel paths, each path with one squib valve backed up by an upstream check valve. The check valve prevents a LOCA in the case of an inadvertent opening of a squib valve. The containment recirculation lines are connected to an associated gravity injection line. The containment recirculation lines have two parallel paths. One path contains a squib valve backed up by an upstream check valve, and the other path contains a squib valve backed up by an upstream normally open MOV. The path with the MOV can also be used to dump the IRWST water into containment in the case of a complete failure to cool the core.

A number of vents are provided in the roof of the IRWST around the side of the IRWST adjacent to the containment wall and next to the SG compartment. Most of the vents are designed to vent steam from the IRWST to the containment. These vents open on small pressure differentials to limit the pressure differential with the containment during accidents, such as a LOCA. This venting prevents overpressurization of the IRWST and provides a path to vent steam released by the spargers or generated by PRHR HX operation into the

containment atmosphere. A few vents are designed to vent steam from the containment to the IRWST. These vents prevent excessive external pressurization of the IRWST. Vents located near containment have hoods to direct hydrogen produced during a severe accident away from containment, and these vents have a higher opening differential pressure than other vents to preferentially cause other vents away from containment to open first.

The IRWST gutter line return contains two AOVs in series which fail closed on a loss of air or control power. Under normal operating conditions, both valves are open and excess condensate on the inside of containment shell collects, and the condensate is sent to the liquid radwaste containment sump. The condensate collected during normal operation is directed to the waste sump to prevent adverse conditions in the IRWST chemistry. When the PRHR HX activates, the valves close. This closure isolates the sump, and during an accident scenario the steam is condensed by the PCS and collected by the gutter and drained back to the IRWST. Failure to close two out of two IRWST gutter AOVs (series arrangement) would fail the PRHR function for scenarios where the RCS pressure boundary is intact, such as for a loss of main feedwater or SGTR event but not for a LOCA. Recovery of the condensate within several hours would maintain the PRHR HX heat sink for an indefinite period of time. In LOCA scenarios, the PRHR function is only required for short periods of time (only needed in a few scenarios before ADS is actuated) such that collecting condensate is not required.

The emergency core decay heat removal subsystem consists of the PRHR HX and associated valves, piping, and instrumentation. The PRHR HX is located in the IRWST which then becomes the heat sink for the HX. The HX consists of c-tubes connected at the top (inlet) and bottom (outlet) to a tubesheet and channel head that is mounted on the IRWST wall. The PRHR HX is connected to the RCS through a normally open inlet line from one RCS hot leg (hot leg 1), which contains a normally open (MOV. This is a shared line with the ADS Stage 4 valves on hot leg 1. The outlet line connects to the associated steam generator (SG) (SG 1) cold plenum. This line contains two normally closed AOVs in parallel that open on a loss of air or electric power. These valves open in response to an S Signal. The discharge line also contains a normally open manual valve downstream of the parallel AOVs. The alignment of the PRHR maintains the HX full of reactor coolant at RCS pressure and prevents water hammer upon PRHR initiation. The HX is located above the RCS loops to induce natural circulation if the RCPs are not available.

The ADS consists of four different valve stages that open sequentially to reduce RCS pressure so that long term cooling can be provided to the RCS. For ADS Stages 1-3, each valve stage consists of two lines, where each line contains two normally closed valves in series. Each stage line has an isolation valve upstream of a control valve. When ADS is actuated, the isolation valve opens first and is followed by opening of the control valve to initiate and control the flow to the IRWST. Both groups of ADS Stages 1-3 have a common inlet header connected to the pressuriser and a common discharge line connected to one of the two spargers in the IRWST. ADS Stage 4 is arranged in two identical groups and each group discharges separately into one of the two SG compartments above post-accident flood up level. ADS Stage 4 has four lines each with two valves in series, which are a normally open isolation valve in series with a squib valve. The isolation valve, upstream of the squib valve, is an MOV gate valve and is only closed during cold/refuelling shutdowns to perform maintenance or in-service testing on the squib valves.

Each RCP is powered through two Class 1 circuit breakers connected in series: ECS-ES-31, -32; -41, -42; -51, -52; and -61, -62. The circuit breakers' purpose is to satisfy tripping requirement of these pumps. The two breakers in series scheme are to ensure that the RCPs are shut down when tripping signal is initiated. Each RCP breaker receives a separate

signal from the PMS. Only one of the breakers in series receives a redundant signal from the DAS. The RCP trip switchgear room is located in the Auxiliary Building.

10.5.2.2 Assumptions and Sources of Model Uncertainty

The assumptions and uncertainties made in the development of the PRHR system models are as follows:

1. The mission time for Class 1 equipment with position indication in the main control room (MCR) is 24 hours. This length of time is based on the assumption that, if component position indication is provided in the MCR, the verification of that components position is included in the board walkdown procedure.

2. One demand was used in the model for the opening and closing of the IRWST vents. The vents could be cycled more than once in the mission time.

10.5.2.3 System Boundaries for PSA Model

The PXS system boundary consists of a PRHR HX, two accumulators, two CMTs, an IRWST, and associated valves, piping, and instrumentation. The system boundary for this system analysis also includes the DVI line to the reactor vessel boundary. The PRHR draws water from the hot leg (SG 1) and returns to SG 1. The CMTs draw water from the cold legs on loop 2. The boundary of this system analysis does not include the SGs, or parts of the RCS: specifically the reactor vessel, the pressuriser, the hot legs, or the cold legs.

The RCS model includes the ADS Stage 1-4 valves and the pressuriser safety valves.

The RCP breakers, which are part of the ECS, are part of the system boundary for CMT actuation.

In addition for the Level 2 model, four types of IRWST vents are modelled, including hooded vents, vacuum breaker hooded vents, pipe vents, and overflow vents.

10.5.2.4 Common Cause Failures

The PXS system common cause failure groups were determined consistent with the method described in Section 10.8. Unique common cause groups to note:

- Since the PXS gutter valves (PXS-PL-V130A/B) are part of the main flow path (not flow diversion) and therefore risk important to PXS, common cause is considered for fails to remain closed for these valves.

- Accumulator check valves are included in the same group since they are expected to see the same RCS pressure (Group Size of 4 – PXS-PL-V028A/B, PXS-PL-V029A/B).

- ADS Stages 2 and 3 valves are divided into two common cause groups:

  – ADS Stage 2 and 3 Isolation Valves 8” Gate Valves (Group Size of 4 – RCS-PL-V012A/B, RCS-PL-V013A/B)

  – ADS Stage 2 and 3 Control Valves 8” Globe Valves (Group Size of 4 – RCS-PL-V002A/B, RCS-PL-V003A/B)

- ADS Stage 4 Valves 14" Squib Valves (Group Size of 4 – RCS-PL-V004A/B/C/D)
- Recirculation Low Pressure 8" Squib Valves (Group Size of 2 – PXS-PL-V118A, PXS-PL-V118B)
- IRWST/Recirculation High Pressure 8" Squib Valves (Group Size of 6 – PXS-PL-V123A, PXS-PL-V125A, PXS-PL-V123B, PXS-PL-V125B, PXS-PL-V120A, PXS-PL-V120B)
- CMT outlet 8" AOVs (Group Size of 4 – PXS-PL-V014A/B, PXS-PL-V015A/B)
- CMT outlet 8" check valves (Group Size of 4 – PXS-PL-V016A/B, PXS-PL-V017A/B)
- PRHR outlet 14" AOVs (Group Size of 2 – PXS-PL-V108A/B)

10.5.3 Passive Containment Cooling System

10.5.3.1 System Description

The PCS system consists of the passive containment cooling water storage tank (PCCWST), isolation valves, a valve room, a drainage bucket, two trough and weir systems, the containment vessel, Class-1 drains, non-Class-1 drains, the passive containment cooling ancillary water storage tank (PCCAWST), two trains of recirculation pumps, a recirculation heater, an air baffle in the Shield Building, a chimney in the Shield Building, screens on the air inlets and outlets, and connections to the spent fuel pool (SFP), Demineralized Water Transfer and Storage System (DWS), and Fire Protection System (FPS).

The PCCWST is a large tank affixed to the top of the Shield Building. The PCCWST provides a sufficient amount of water for 72 hours of post-DBA containment cooling. Recirculation Pumps, a chemical addition tank, and a recirculation heater keep the PCCWST chemicals and temperature within values determined by technical specifications.

The containment vessel is the heat transfer surface for the PCS. Heat produced inside the containment vessel propagates to the atmosphere via the containment vessel. The containment vessel removes heat from the inside through convection, conduction, and radiation. The PCCWST provides flow to the containment vessel through four pipes. Each pipe penetrates to a different elevation in the PCCWST. The differing elevations of the pipes allow a passive method of flowrate control. The PCCWST also has penetrations for makeup to the SFP and FPS, and a vent to the atmosphere to ensure the water flow out does not cause a vacuum on the inside of the PCCWST and prevent the flow from meeting requirements.

Water flows from the PCCWST to a single header. The header provides flow to three trains of two isolation valves per train. The first set of isolation valves (PCS-PL-V002A/B/C) in each train is a normally open, fail as is, motor-operated gate valve. These valves provide the ability to perform testing and maintenance on the normally closed isolation valves without emptying the PCCWST. The normally open isolation valves receive a confirmatory High-2 containment pressure signal from the PMS. The normally open isolation valves are housed in the temperature controlled Valve Room directly beneath the PCCWST.

Downstream of two of the normally open isolation valves (PCS-PL-V002A/B) are normally closed, fail open, air-operated butterfly valves (PCS-PL-V001A/B). Downstream of one of the normally open isolation valves (PCS-PL-V002C) is a normally closed, fail as is, motor-operated gate valve (PCS-PL-V001C). All three of the normally closed isolation valves (PCS-PL-V001A/B/C) serve the same purpose. The valves isolate the flow of water from the PCCWST until they receive either a High containment temperature open signal from DAS or a High-2 containment pressure open signal from PMS.

10.5.3.2 Assumptions and Sources of Model Uncertainty

The assumptions and uncertainties made in the development of the PCS models are as follows:

1. The PCS troughs and weirs will provide uniform flow over the containment shell and are not subject to failure mechanisms that would prevent this. The troughs and weirs are designed to be filled with water from the distribution bucket and overflow onto the containment shell.

2. Blockage of the air flow inlets is not considered in this analysis. When water flow is available, the containment maximum pressure is not sensitive to air flow blockage.

3. The redundancy associated with the annulus inlet and the flow area associated with the chimney will provide adequate flow during any accident.

10.5.3.3 System Boundaries for PSA Model

The PCS PSA model boundary includes all flow paths from the PCCWST to the containment vessel and alignments for flow to the distribution bucket. Components modelled include tanks, MOVs, AOVs, check valves, pumps, and manual valves.

10.5.3.4 Common Cause Failures

The PCS common cause failure groups were determined consistent with the method described in Section 10.8.

10.5.4 Main and Startup Feedwater System

10.5.4.1 System Description

The Main and Startup Feedwater System (FWS) can supply feedwater to the SGs of the Steam Generator System (SGS) through two different flow paths. These flow paths are defined as follows:

- Main feedwater is defined to be feedwater that passes through the SGS main feedwater control valves (MFCVs) (SGS-PL-V250A/B). Main feedwater is always supplied from the deaerator through the main feedwater pumps.

- Startup feedwater is defined to be feedwater that passes through the SGS startup feedwater control valves (SFCVs) (SGS-PL-V255A/B). Startup feedwater can be supplied either from the deaerator through the main feedwater pumps (normal source) or from the condensate storage tank (CST) through the startup feedwater pumps (backup source).

FWS main feedwater piping begins at the outlet connections on the bottom of the Condensate System (CDS) deaerator. Feedwater from the deaerator flows through three individual lines to the suction of each of the three main feedwater pump trains. During normal operation, the deaerator contains saturated water and the height of the water level in the deaerator above the feedwater booster pumps provides the necessary net positive suction head (NPSH) for the pumps.

Three parallel trains of feedwater booster pumps and main feedwater pumps provide the motive power for main feedwater flow. The pump trains are identical in capacity and characteristics. These pumps are fixed speed motor driven and utilize the SGS main feedwater control valves to provide effective feedwater flow control. During normal full load operation, each train provides 33.3 percent of the total feedwater flow. However, with one train out of service the other two trains can provide sufficient flow to maintain power operation at up to 70 percent of full load power.

The startup feedwater pumps and their associated flow paths primarily provide backup feedwater capability in the event the booster/main feedwater pumps or their associated flow paths are lost. The startup feedwater pumps and their associated flow paths perform a defence-in-depth function of decay heat removal after a plant shutdown/trip if the main feedwater pumps are not available, such as during a LOOP event. Although it does mitigate "loss of feedwater" events, this function of the FWS is a non- Class 1system function.

10.5.4.2 Assumptions and Sources of Model Uncertainty

There were no FWS specific assumptions and uncertainties made in the development of this system model.

10.5.4.3 System Boundaries for PSA Model

The FWS consists of three MFW pump trains drawing suction from the deaerator, two SFW pump trains drawing suction from the CST, two trains of high pressure feedwater heaters, and associated valves, piping, and instrumentation. The MFW pumps normally provide flow to the MFCV; however, a cross connect allows the MFW pumps to provide flow to the SFCV if necessary. The SFW pumps provide flow to the SFCV.

10.5.4.4 Common Cause Failures

The FWS common cause failure groups were determined consistent with the method described in Section 10.8.

10.5.5 Chemical and Volume Control System

10.5.5.1 System Description

The system functions as a whole to fulfil the requirements of controlling RCS chemistry, purity, and inventory for normal plant operations. The CVS is functionally divided into six different subsystems:

Purification Loop Subsystem

This subsystem includes the regenerative and letdown heat exchangers, a flow restricting orifice, mixed and cation bed demineralizers, reactor coolant filters, and associated valves, piping, and instrumentation. The entire purification loop of the CVS is located inside

containment and provides the direct interface with the RCS. The motive force for the purification loop is the differential head across the RCPs, and continuous purification is provided without operating the CVS Makeup Pumps.

Makeup Subsystem

This subsystem includes the high head makeup pumps and associated suction and discharge piping. The makeup pumps are located outside containment in the Auxiliary Building and take suction from the boric acid storage tank (BAST), the DWS, or a combination of both through a common suction header. The discharge piping from both makeup pumps combines to form a makeup header which connects to the purification loop inside containment downstream of the reactor coolant filters. The makeup pumps are used to supply makeup water to the RCS, to introduce chemicals to the RCS, to fill and pressure test the RCS (after regular refuelling and maintenance outages), and to add borated makeup for auxiliary pressuriser spray and filling auxiliary equipment.

Letdown Subsystem

The letdown subsystem consists primarily of an effluent line off the purification loop downstream of the reactor coolant filters. When delivery of flow to the Liquid Radwaste System (WLS) is necessary, isolation valves are remotely opened to allow for diversion of purification flow through a letdown orifice to significantly drop the pressure to a value compatible with the WLS design. The letdown line functions to reduce RCS inventory during normal plant operations, power changes, startups, and shutdown.

Demineralizer Resin Sluicing and Flushing Subsystem

The demineralizer resin sluicing and flushing subsystem includes various piping flow paths and numerous valves that allow for resin fluidization, sluicing, flushing, and refilling each time a resin bed changeout is required (which typically will happen during each refuelling outage). A resin discharge header is also included to transfer spent resins from each of the demineralizers to the spent resin tanks in the WSS, located outside containment in the Auxiliary Building.

Zinc and Hydrogen Injection Subsystem

The zinc and hydrogen injection subsystem includes both the zinc and hydrogen injection packages. Piping from both the zinc and hydrogen injection packages run from the turbine hall and connect to the purification loop inside containment. The hydrogen injection point is downstream of the regenerative heat exchanger (RHX) shell side outlet line, and the zinc injection point is on the purification return line upstream of the shell side inlet of the RHX. These different injection points allow optimal mixing of the chemicals with the coolant due to the temperatures and pressures at their respective injection sites.

Auxiliary Spray Subsystem

The auxiliary spray subsystem is an additional line with isolation valves that branches off the purification return line downstream of the RHX and supplies fluid flow to the pressuriser spray nozzle when needed.

10.5.5.2 Assumptions and Sources of Model Uncertainty

No CVS specific assumptions were made in the development of this system model.

10.5.5.3 System Boundaries for PSA Model

The CVS PSA model consists of the purification loop, the makeup subsystem, the letdown line containment isolation valves (CVS-PL-V045 and V047), and the zinc injection containment isolation valves (CVS-PL-V092 and V094).

The purification loop includes the purification supply line and return line. The purification loop supply line consists of the purification stop valves (CVS-PL-V001, V002, and V003), the tube side of the regenerative heat exchanger (CVS-ME-01), the letdown heat exchanger (CVS-ME-02), and the in service mixed bed demineralizer (CVS-MV-01A). The purification loop return line includes the shell side of the regenerative heat exchanger (CVS-ME-01) and the purification return line valves (CVS-PL-V080, V081, and V082) which inject water into the RCS via the steam generator.

The makeup subsystem consists of two makeup pump trains (CVS-MP-01A/B) which draw from the BAST (CVS-MT-01) and/or the DWS supply line via a three-way blend control valve (CVS-PL-V115). The common makeup pump discharge header includes a makeup flow control valve (CVS-PL-V157), two makeup discharge header containment isolation valves (CVS-PL-V090 and V091), and other associated valves and piping which inject makeup into the purification return line upstream of the shell side of the regenerative heat exchanger.

10.5.5.4 Common Cause Failures

The CVS common cause failure groups were determined consistent with the method described in Section 10.8. Unique common cause groups to note:

- Common cause is only modelled between two of the three purification stop valves (CVS-PL-V001 and V002) which are redundant. The third isolation valve (CVS-PL-V003) is a diverse valve type.

- The letdown line outside containment isolation valve (CVS-PL-V047) has an air positioner and is diverse from the letdown line inside containment isolation valve (CVS-PL-V045). No common cause is modelled between the valves in this case.

10.5.6 Containment Hydrogen Control System

10.5.6.1 System Description

The Containment Hydrogen Control System (VLS) provides monitoring and control of the hydrogen concentrations inside containment in order to maintain containment integrity against hydrogen detonation. The system performs its functions through the use of three subsystems as discussed below.

Hydrogen Monitoring

This subsystem includes three hydrogen sensors and three pressure sensors that continuously provide hydrogen concentration levels to the main control room via three independent channels in the Plant Control System (PLS). The three hydrogen sensors are located in the upper dome of containment in order to provide a global hydrogen concentration measurement, while the pressure sensors are used to provide pressure compensation to the hydrogen sensors. For accident mitigation, this subsystem is used as a backup to the core exit temperature indication that prompts operators to start the igniters in containment. An elevated containment hydrogen level alarm, coincident with high core exit temperature, will alert the

operators to start the igniters if they have not already done so. Procedures will instruct operators to start the igniters based on core exit temperature alone.

Hydrogen Recombination

The hydrogen recombination subsystem consists of two pairs of passive autocatalytic recombiners (PARs) positioned in containment such that they are able to take advantage of the natural circulation and mixing of the containment atmosphere to optimize their efficiency and remove susceptibility to debris blockage. The PARs are designed to accommodate the relatively slow hydrogen production rate anticipated for a design basis LOCA. The PARs are entirely passive devices relying on the catalytic properties of the material (palladium or platinum) to induce catalytic oxidation of the surrounding hydrogen. Therefore, no power supplies or other supports are required. Additionally, the catalyst is not consumed during operation, nor is it subject to long-term aging degradation.

Hydrogen Ignition

This subsystem contains 66 coil-type hydrogen igniters strategically distributed throughout containment. These igniters are designed to burn hydrogen in containment whenever concentration levels increase rapidly beyond the capacity of the PARs, in order to prevent hydrogen detonation. The igniters are divided into two groups of 33, which are supplied power by separate 220/120V ac distribution panels and backed up by separate dc supplies fed through their respective inverters. Each major area in which the igniters are located includes at least one igniter from each group for redundancy. The igniters are actuated manually through PLS upon indication of core exit temperature greater than 648.9° C (1200° F), which is likely prior to RCS breach. The hydrogen monitoring subsystem discussed above provides backup indication to start the igniters. The DAS provides a diverse means of manually actuating the igniters from the MCR. There are no automatic actuations for this system. All 33 igniters in a group are actuated simultaneously via PLS, and all 66 igniters are actuated simultaneously via DAS.

10.5.6.2 Assumptions and Sources of Model Uncertainty

The VLS specific assumptions and uncertainties made in the development of this system model are as follows:

1. While the igniters are always grouped for redundancy, they are located throughout containment, including relatively isolated areas. The PSA cannot distinguish areas of hydrogen concentration; it can only make the determination that hydrogen is present in containment and the igniters are required for mitigation. Therefore, this success criterion is extended to include each area identified; system success is defined as the successful operation of one igniter in each area. This is conservative modelling since there is some likelihood associated with there being hydrogen in any given area, and the igniters in that area may not be required to mitigate the accident.

2. Though the PARs have no explicit failure modes in the PSA, credit may be taken for their ability to reduce hydrogen levels in containment and forestall or eliminate the need for the igniters. Any credit taken necessarily has some level of model uncertainty associated with it.

10.5.6.3 System Boundaries for PSA Model

The VLS model contains all 66 igniters and associated fuses and circuit breakers between the igniters and the 220/120V ac distribution panels. These fuses are included as protection for the igniters; however, for the purpose of the PSA, if a fuse spuriously breaks contact, the igniter is no longer available for accident mitigation. The panels themselves and associated backup supplies are included in other system models and linked via transfers. The VLS model also includes relays for igniter actuation. The hydrogen monitoring subsystem is not credited in the PSA. The VLS model also does not take credit for the PARs for hydrogen control.

10.5.6.4 Common Cause Failures

The igniter and associated fuse CCF groups are defined by the number of igniters/fuses in each area, and the remaining components are defined with a single group per component type. Because there are a large number of similar components in this system, the VLS CCF groups in the model would become too cumbersome for quantification. The CCF events were injected into the system model and the change in the top event probability (from its value without CCF injected) was used to calculate a beta factor. With this, the CCF was removed from the model, and a basic event that includes the beta factor ($VLS-ALL-CCF-B) was used to raise the system top probability to the value that included CCF.

10.5.7 Normal Residual Heat Removal System

10.5.7.1 System Description

The RNS includes two mechanical trains of decay heat-removal equipment. Each train includes one RNS pump and one RNS heat exchanger located in the Auxiliary Building. The two trains of equipment share a common suction line from the RCS. Each train has a discharge line to return the flow to the RCS through the two PXS DVI lines. The RNS is also interconnected with the IRWST, the SFP, and the CVS to perform support functions. In addition, the RNS includes the piping, valves, and instrumentation necessary for correct system operation.

The portions of the RNS piping that contain reactor coolant outside the RCS pressure boundary valves (RNS-PL-V001A/B, RNS-PL-V002A/B, RNS-PL-V015A/B, and RNS-PL-V017A/B); including those that are outside containment, have a design pressure and temperature high enough that full RCS system pressure is below the ultimate rupture strength of the piping.

The common suction header then branches into two parallel lines, with each line containing two normally closed MOVs in series that serve as reactor coolant pressure boundary valves. This configuration ensures both reliable RCS pressure boundary isolation and decay heat removal initiation by allowing RNS initiation after a single failure of an isolation valve to open, and also by allowing for RNS isolation after a single failure of an isolation valve to close. The isolation valve in each pair closest to the containment penetration also serves as a containment isolation valve. Each RNS/RCS suction isolation valve receives power from a Class 1 power supply (250 Vdc) and is interlocked with RCS pressure to prevent the operator from opening the valve until RCS pressure is below 31 Bar (450 psig), the normal operating pressure of the RNS suction. These valves are also interlocked to prevent them from being opened unless the isolation valves from the IRWST to the RNS pump suction header and from the RNS pump discharge header to the IRWST are closed. This prevents inadvertent

blowdown of the RCS to the IRWST. In addition, the power supply to each valve is blocked at the valve's motor control centre during plant power operations.

Once inside containment, each discharge line contains a check valve which acts as a containment isolation valve. Downstream of the check valve, each discharge line is routed to a PXS DVI line. Note that the PSA model is based on an RNS design in which there is a common discharge header through containment that then branches into two lines, each being routed to a PXS DVI line.

The RNS is capable of providing low pressure makeup from the Spent Fuel Pool Cooling System (SFS) cask loading pit (CLP) and the IRWST to the RCS. The system must be manually initiated by the operator following receipt of an ADS signal. If the RNS is available, it will provide RCS makeup once the pressure in the RCS falls below the shutoff head of the RNS pumps.

10.5.7.2 Assumptions and Sources of Model Uncertainty

The RNS specific assumptions and uncertainties made in the development of this system model are as follows:

1. There is uncertainty associated with the amount of time that the CLP is unavailable while the plant is at-power. The CLP can be unavailable for use by the RNS for accident mitigation due to fuel handling operations. The CLP is assumed to be unavailable 5percent of the time while the plant is at-power.

2. There is uncertainty associated with the response of check valve RNS-PL-V056 during switch over from CLP injection to IRWST injection. Because of RNS pump suction, check valve RNS-PL-V056 may never fully close; therefore, closing of RNS-PL-V056 as a redundant method to isolate the CLP has not been modelled. CLP isolation failure is a concern because, if the CLP is not isolated, the RNS pumps may drain down the CLP and entrain air in the RNS pump suction causing the RNS pumps to fail. Note that MOV RNS-PL-V055 can isolate the CLP and is modelled to do so.

10.5.7.3 System Boundaries for PSA Model

The boundaries for the RNS PSA model include the flow path from the hot leg suction to the DVI lines into the reactor vessel. Also included are connections to the PXS IRWST and the PXS sump as well as the CLP and its connections. For the Level 2 portion of the RNS model, the spent fuel pool and its connections are included in the RNS boundary.

10.5.7.4 Common Cause Failures

The RNS common cause failure groups were determined consistent with the method described in Section 10.8. Unique common cause groups to note:

- Check valves on the DVI lines – these four check valves are broken up into two CCF groups of two because RNS-PL-V017A/B are normal swing check valves, and RNS-PL-V015A/B are stop check valves. This diversity allows these four check valves to be in different common cause groups.

Hot leg suction MOVs – these four MOVs are broken up into two CCF groups of two because valves RNS-PL-V001A/B are subject to RCS pressure, and valves RNS-PL-V002A/B are not. Additionally, valves RNS-PL-V002A/B are containment isolation valves

so they will be tested more frequently than RNS-PL-V001A/B. This diversity allows these four MOVs to be in different common cause groups.

10.5.8 Component Cooling Water System

10.5.8.1 System Description

The CCS is divided into two redundant trains, each including one pump and one heat exchanger. The two pumps take suction from a common return header and the heat exchangers are routed to a common supply header. Each pump discharges to the respective heat exchanger, but a cross-connection at the pump discharge allows for either pump to feed either heat exchanger. The CCS heat exchangers are cooled by the SWS. The CCS heat exchangers are plate type, counterflow heat exchangers.

The CCS supplies cooling water to:

- RCP motor cooling
- RCP variable frequency drive cooling
- RNS heat exchangers (shutdown and refuelling modes only)
- Spent fuel pool cooling
- Condenser cooling for the Central Chilled Water System (VWS) high capacity water-cooled chiller units
- Letdown cooling via the CVS letdown heat exchanger
- Primary Sampling System (PSS) sample heat exchanger cooling
- WLS reactor coolant drain tank heat exchanger cooling
- CVS makeup pump miniflow heat exchanger cooling
- RNS pump seal cooling
- CAS cooling
- CDS condensate pump motor oil cooling

One train of CCS is required for normal operation. The remaining CCS pump is aligned to deliver flow to the operating heat exchanger and is started automatically if the operating CCS pump fails. All loads inside containment can be remotely isolated by automatic closure of motor-operated containment isolation valves in response to a safeguards signal.

10.5.8.2 Assumptions and Sources of Model Uncertainty

No CCS specific assumptions were made in the development of this system model.

10.5.8.3 System Boundaries for PSA Model

The CCS consists of two trains of cooling which consist of pumps, heat exchangers, and associated valves and piping. The CCS surge tank is part of the system boundary which provides makeup to the CCS. The CCS is made of common valves and piping to associated loads. Valves and piping that are part of the CCS which are specific to other systems are modelled with that system.

10.5.8.4 Common Cause Failures

The CCS common cause failure groups were determined consistent with the method described in Section 10.8.

10.5.9 Service Water System

10.5.9.1 System Description

Major elements of the SWS include two 100 percent capacity service water pumps, automatic backwash strainers, a two-cell cooling tower with a divided basin and associated piping, valves, controls, and instrumentation. The service water system is arranged into two trains of components and piping. Each train includes one service water pump, one strainer, and one cooling tower cell. Each train provides cooling to one CCS heat exchanger. SWS piping and components are located within the Turbine Building or in the yard area.

Cooled service water exiting from the cooling tower is collected in a concrete storage basin located below the tower structure. The basin is divided into halves, with each half capable of collecting the segregated flow from one tower cell.

Each service water pump provides 100 percent of the required flow to cool the CCS heat exchanger. Both service water pumps are operated simultaneously for increased capacity in order to support outage scheduling (shutdown cooling).

A check valve (SWS-PL-V025A/B) at the discharge of each pump prevents reverse flow through an idle pump during periods when the pump discharge valve is not fully closed. In the event that neither service water pump is operating (e.g., immediately following loss of normal ac power), the check valves minimize system drain down. Each pump discharge isolation valve is an MOV (SWS-PL-V002A/B) and automatically closes after the associated pump is stopped. The discharge MOV must be fully closed to start the associated pump.

The SWS normally operates in one of two basic modes of operation: single train or two trains. The SWS follows the needs of the CCS, and the mode of operation selected for use is chosen to support the current mode of CCS operation.

10.5.9.2 Assumptions and Sources of Model Uncertainty

No SWS specific assumptions were made in the development of this system model.

10.5.9.3 System Boundaries for PSA Model

The boundary of the SWS includes the main flow path of Train A and B from the cooling tower basin, through the pumps, through the CCS heat exchangers, and back to the cooling tower. The main components in the SWS include service water pumps, valves, strainers, screens, cooling tower, and cooling tower fans. The SWS boundary also includes makeup to the cooling tower basin from the RWS.

10.5.9.4 Common Cause Failures

The SWS common cause failure groups were determined consistent with the method described in Section 10.8.

10.5.10 Central Chilled Water System

10.5.10.1 System Description

The Central Chilled Water System consists of two subsystems: a High Capacity System (HCS), and a Low Capacity System (LCS). The HCS supplies cooling water to the Radiologically Controlled Area Ventilation System (VAS), Containment Recirculation Cooling System (VCS), Containment Air Filtration System (VFS), Health Physics and Hot Machine Shop HVAC System (VHS), Radwaste Building HVAC System (VRS), VTS, and the Annex/Auxiliary Building Nonradioactive Ventilation System (VXS). The HCS also provides cooling water for the Secondary Sampling System (SSS) sample cooler, the WLS vapour condenser and the Gaseous Radwaste System (WGS) gas cooler. The LCS provides chilled water to defence-in-depth HVAC cooling coils used by the Nuclear Island Nonradioactive Ventilation System (VBS) air handling units and the VAS unit coolers located in the CVS and RNS pump rooms.

High Capacity Subsystem

The high capacity subsystem consists of two 85 percent capacity chilled water pumps, two 15percent capacity chilled water pumps, two 85 percent capacity water cooled chillers , two 15percent air cooled chillers, a chemical feed tank, an expansion tank, and associated valves, piping, and instrumentation. The subsystem is arranged in two parallel mechanical trains with common supply and return headers. Each train includes one 15 percent capacity pump, one 85 percent capacity pump, one 15 percent capacity chiller, and one 85 percent capacity chiller. A cross-connection at the discharge of each pump allows for each to feed a given chiller of matching capacity.

Low Capacity Subsystem

The LCS consists of two 100 percent capacity chilled water trains. Each train consists of a chilled water pump, an air-cooled chiller, an expansion tank, and associated valves, piping, and instrumentation. A common chemical feed tank is connected to both subsystems. The system is arranged in two independent trains with separate supply and return headers. This configuration provides redundancy and independence of trains during the various modes of system operation and satisfies availability requirements. The subsystem configuration provides 100 percent redundancy during normal plant operation and following the loss of offsite power.

10.5.10.2 Assumptions and Sources of Model Uncertainty

No VWS specific assumptions were made in the development of this system model.

10.5.10.3 System Boundaries for PSA Model

The VWS consists of an HCS and an LCS. The HCS consists of two parallel trains of chilled water which feed a common header. Each train consists of an 85 percent capacity water cooled chiller pump, a 15 percent capacity air cooled chiller pump, an 85 percent capacity water cooled chiller package, a 15 percent capacity air cooled chiller package, and associated valves and piping. The VWS expansion tank on the HCS is part of the system boundary which provides makeup to the VWS HCS. DWS makeup to VWS HCS is less than 6.3 L/sec (100 gpm) and therefore is not credited in the model. The VWS is made of common valves and piping to associated HVAC loads. Valves and piping that are part of VWS which are specific to HVAC loads are modelled in the HVAC system.

The LCS consists of two independent trains of chilled water. Each train consists of a 100 percent capacity air cooled pump, a 100 percent capacity air cooled chiller package, and associated valves and piping. The VWS expansion tanks on each LCS train are part of the system boundary which provides makeup to each train of the VWS LCS. DWS makeup to VWS LCS is less than 6.3 L/sec (100 gpm) and therefore is not credited in the model. The VWS is made of common valves and piping to associated HVAC loads. Valves and piping that are part of VWS which are specific to HVAC loads are modelled in the HVAC system.

10.5.10.4 Common Cause Failures

The VWS common cause failure groups were determined consistent with the method described in Section 10.8. Unique common cause groups to note:

Common cause failure was modelled for both the 15 percent capacity portion of HCS and the LCS for air cooled pumps and air-cooled chiller packages due to similar sizing and operation.

10.5.11 Electric Power Distribution Systems (EPS)

10.5.11.1 System Description

The EPS consists of three electrical systems ECS, dc and uninterruptible power supply system (EDS), and IDS, supported by various mechanical and C&I systems. The first tier (ECS) consists of the ac power distribution systems feeding non-Class-1 loads required for unit operation. The second tier (EDS) includes the ac and dc power distribution systems supplying power to permanent non-Class 1 loads, i.e., loads that, due to their specific functions, are generally required to remain operational at all times or when the unit is shut down. The third tier (IDS) consists of the redundant Class 1 dc and ac UPS power distribution systems feeding Class-1 loads. The EPS is supported by transformers in the main generator system (ZAS), two standby DGs in the onsite standby power system (ZOS), and fuel delivery to the ZOS supplied by DOS.

To provide normal power to the plant auxiliary and service loads during normal operation, the station generated power is transmitted to the offsite transmission system with a tap to the three unit auxiliary transformers (UATs): ZAS ET-2A, 2B, 2C. A second ac power supply from the utility grid, or other power source, is provided for reserve power, maintenance, and testing of the equipment through two reserve auxiliary transformers (RATs): ZAS-ET-4A, 4B. The reserve power source is site specific.

The normal ac power supply to the ECS is provided from the station main generator. When the main generator is not available, the preferred plant auxiliary power supply is provided from the switchyard by back-feeding through the main step-up transformer (MSUT) and UATs with the generator breaker open. A reserve source of power is provided through two RATs to the ECS. In case of loss of both normal and preferred power sources as a result of a fault operating the protective relays and devices for the UATs and MSUT concurrent with a turbine generator breaker trip, the automatic bus transfer will be initiated to switch over loads from the UATs to RATs. This automatic switch over is a fast bus transfer backed up by a residual voltage transfer. The fast bus transfer is blocked during plant startup when the auxiliary boiler(s) is in operation.

The ECS is divided into two subsystems; Medium Voltage (MV) and Low Voltage (LV). The MV subsystem contains the 6.9kVac switchgear which provides power for the large ac loads including RCPs, CWS pumps, SWS pumps, CCS pumps, etc. The arrangement of the 6.9kVac 60 Hz buses permits feeding functionally redundant pumps or groups of loads from separate buses and enhances the plant operational flexibility. The 6.9kVac switchgear powers motors larger than 250HP, and the load centre transformers. There are two 6.9kVac switchgear (ECS-ES-1 and ECS ES-2) located in the Annex Building, and five switchgear (ECS-ES-3, 4, 5, 6, 7) located in the Turbine Building.

The LV subsystem begins at the MV 6.9kVac terminals of the load centre transformers, which are powered from the MV portion of the ECS, and ends at the terminals of the 480Vac 60 Hz LCs and is then further broken down into 480Vac 60 Hz MCCs. LCs and MCCs power loads such as motors, heaters, battery chargers, voltage regulating transformers, and lighting transformers.

The ECS also includes two 480Vac 60 Hz Non-Class 1 ancillary ac DGs located in the southeast corner of the Annex Building. These DGs provide power for post-accident monitoring (PAM), MCR lighting, and MCR and C&I room ventilation. The ancillary DGs are used following an extended (more than 72 hour) loss of all normal/preferred, standby, and dc backed electric power sources.

The IDS consists of the redundant Class 1 dc and ac UPS power distribution systems feeding Class-1 loads.

The IDS consists of Class 1 250Vdc and Class 1 120Vac UPS, power distribution subsystems. The IDS is designed such that the critical plant loads required for plant safe shutdown and monitoring are powered when all the onsite and offsite ac power sources at the plant are lost and cannot be recovered for a period of up to 72 hours.

The normal source of power for the Class 1 dc system is the Non-Class 1 ECS. The connection between the Class 1 system and the Non-Class 1 system is made through the battery chargers that serve as isolation devices. If the normal source of ac power is not available, the Class 1 batteries have sufficient capacity for the critical plant loads required for plant safe shutdown for a period of up to 72 hours.

The Class 1 250Vdc subsystem is divided into four independent divisions (A, B, C, and D). Each of these divisions is supplied from dedicated batteries and battery chargers.

Divisions A and D battery banks and one of the battery banks in divisions B and C are designated as 24 hour battery banks and provide power to the loads required for the first 24 hours following a loss of all ac power event or a DBA. The second battery bank in divisions B and C, designated as the 72 hour battery banks, are used for those loads requiring power for 72 hours following the same event.

The Class 1 120Vac, 60 Hz ac UPS provides power to four independent divisions of Class 1 instruments and control power buses. Divisions A and D each consist of one Class 1 inverter associated with C&I DP and a backup voltage-regulating transformer with a DP. Each inverter is powered from its respective 24 hour battery bank SB. Divisions B and C each consists of two inverters, two C&I DPs, and a backup voltage-regulating transformer with a DP shared between the divisions. The 24 hour battery bank SB powers one inverter, and the 72 hour battery bank SB powers the other inverter.

The EDS includes the ac and dc power distribution systems supplying power to permanent non-Class-1 loads i.e., loads that, due to their specific functions, are generally required to remain operational at all times or when the unit is shut down.

The EDS consists of two 125Vdc and 120Vac subsystems and one 250Vdc subsystem. The 125Vdc and 120Vac subsystems represent two separate power supply trains. The 250Vdc subsystem is dedicated to the turbine-generator dc emergency pump motors. The 250Vdc subsystem has only one dc SB bus.

Each 125Vdc subsystem consists of two separate dc SB buses for the Non-Class 1 dc loads. These two buses can be interconnected by a normally open circuit breaker at each distribution bus to enhance the power supply source availability. When the tie breakers between two buses are closed, the selection of loads to be powered is administratively controlled to stay within the battery rating. Each of the two 125Vdc subsystems include two sets of battery chargers, stationary batteries, dc distribution equipment, and associated monitoring and protection devices.

The 480Vac ECS LCs, backed by the ZOS, provides the normal ac power to the battery chargers which provide the dc power for plant operation, and at the same time maintain the associated stationary battery banks on float charge. Battery chargers for 125Vdc EDS1 and EDS3 subsystem are fed by LC ECS-EK-13; battery chargers for 125Vdc EDS2 and EDS4 are fed by LC ECS-EK-23. Both LCs are part of the ECS and DG backed.

10.5.11.2 Assumptions and Sources of Model Uncertainty

No electric power specific assumptions were made in the development of this system model.

10.5.11.3 System Boundaries for PSA Model

The ECS portion of the EPS PSA model includes the ZAS transformers (MSUT, UATs, and RATs), 6.9kVac buses, 480Vac LCs, 6.9kVac to 480Vac LC transformers, 480Vac MCCs, 120Vac DPs, 480Vac to 120Vac DP transformers, and the ancillary DGs. The ECS also accounts for all breakers between the components listed.

The IDS portion of the EPS PRSA model includes battery chargers, 24 and 72 hour batteries, 250Vdc SBs, DPs, and MCCs. The IDS also includes 120Vac UPS components consisting of inverters, static switches, regulating transformers, and 120Vac UPS DPs. The IDS also accounts for all breakers between the ECS and IDS components.

The EDS portion of the EPS PSA model includes battery chargers, 2 hour batteries, 125Vdc SBs, DPs, and MCCs. The EDS also includes 120Vac UPS components consisting of inverters, static switches, regulating transformers, and 120Vac UPS DPs.

The DG portion of the EPS PSA model includes components in the ZOS and DOS. The DOS includes all fuel oil transfer components from the 7 day tank to the 4 hour day tank. Components in the DOS include transfer pumps, strainers, valves, and moisture separators. The ZOS includes the diesel engine and generator, output breaker, air start system, oil/water jacket cooling system, exhaust system, and air intake system.

10.5.11.4 Common Cause Failures

The electric power common cause failure groups were determined consistent with the method described in Section 10.8. Unique common cause groups to note:

- The 6.9kVac and 480Vac breakers were identified as being subject to CCF. The CCF failure modes for breakers include fail to open, fail to close, and spurious operation. The 6.9kVac and 480Vac LC breakers that supply redundant equipment were included in the CCF analysis for ECS in their own respective CCF groups. Feeder breakers for mechanical components were not considered in the ECS because the breaker is within the component boundary of that mechanical component.

- Battery chargers and inverters were identified as being subject to CCF. The CCF failure mode for chargers and inverters is failed to operate. In the IDS there are two group sizes for battery chargers. One group includes four battery chargers for the 24 hour batteries, and the other group includes two chargers for the 72 hour batteries. The inverters follow the same methodology: four inverters for the 24 hour power supplies, and two inverters for the 72 hour supplies. In EDS there is a group of four battery chargers and a group of four inverters.

10.5.12 Containment Isolation

10.5.12.1 System Description

The Containment System (CNS) isolation system provides the Class 1 system function of containment isolation for containment boundary integrity and provides a barrier against the release of fission products to the atmosphere. The containment isolation system utilizes manual valves, check valves, relief valves, AOVs, and MOVs to isolate the containment atmosphere from the environment outside.

Some penetrations do not isolate solely on a containment isolation signal (T Signal), these penetrations are addressed below:

CCS – The CCS containment isolation valves (CIVs) isolate on an S Signal rather than a T Signal to maximize routine recovery and economic protection, in the event that the T Signal was generated on manual actuation of the PCS.

CVS (Charging) – The CVS makeup line CIVs will be closed based on the following Category-A signals: (a) High-2 pressuriser level (pressuriser overfill protection), (b) High SG level (SGTR – steam generator overfill protection), (c) S Signal + High pressuriser level (safeguards actuation without makeup requirements), and (d) High-2 containment radiation (core damage source term containment isolation).

RNS – The RNS CIVs are isolated on a High containment radiation signal. The High containment radiation signal indicates an event in which there is core damage, and is therefore a source term requiring containment isolation including RNS. Because the RNS is normally isolated during Modes 1, 2, and 3 and aligned only for shutdown operations, it would typically not require an isolation signal following a DBA from Modes 1, 2, and 3.

SGS Main Steam – The main steam line is isolated on a main steam line isolation signal, indicating either excessive cooldown of the reactor (which might lead to an uncontrolled return to criticality) or a challenge to the integrity of the reactor vessel due to thermal shock. In addition to limiting the reactor cooldown rate, the closure of the CIVs maintains containment integrity by limiting mass and energy addition to the containment.

SGS Main Feedwater – The main feedwater line is isolated on a feedwater isolation signal indicating excessive cooldown of the reactor, which may lead to an uncontrolled return to criticality or a challenge to the integrity of the reactor vessel due to thermal shock. The signal is generated on any condition that generates an S Signal. In addition to limiting the reactor cooldown rate, the closure of the CIVs maintains containment integrity by limiting mass and energy addition to the containment. Finally, isolation prevents overfilling the SGs with possible consequent damage to the steam system and/or turbine.

SGS Blowdown – The PMS limits the potential for SG dryout and limits the loss of the SG inventory as a heat sink under accident or transient conditions. Within the PMS, any set of conditions which initiates the PRHR system operation also isolates the blowdown system.

VFS – The VFS is isolated not only on a T Signal, but also on a High containment radiation signal to provide an immediate response to radioactive releases to containment. In addition to the normal function of the containment filtration system, the VFS vent line also provides vacuum relief capability. The vacuum relief system utilizes the vent line penetration, but performs vacuum relief through separate branch lines. The branch lines contain check valves inside containment which will remain closed during normal operation. Motor operated butterfly valves provide containment isolation on the outboard side of the vacuum relief system. The motor operated butterfly valves are normally closed during all modes of operation, and receive an automatic close signal on a T Signal and High containment radiation signal. These valves receive an open signal on a Low-2 containment pressure signal, which takes priority over containment isolation. This functionality ensures that any event requiring vacuum relief inside containment can be mitigated to protect the containment vessel.

10.5.12.2 Assumptions and Sources of Model Uncertainty

The CNS specific assumptions and uncertainties made in the development of this system model are as follows:

1. Electrical, instrumentation, and spare penetrations are not modelled in this analysis. The penetrations either have no fluid flow and very low differential pressure, or are capped at both ends. The pipe failure data is not detailed enough to represent the failure of piping with very low differential pressure and no flow.

10.5.12.3 System Boundaries for PSA Model

The CNS components credited in this model consist of the inside reactor containment (IRC) isolation valves and the outside reactor containment (ORC) isolation valves for each penetration modelled.

10.5.12.4 Common Cause Failures

The CNS common cause failure groups were determined consistent with the method described in Section 10.8.

10.5.13 Compressed and Instrument Air System

10.5.13.1 System Description

The CAS consists of three subsystems: instrument air, service air, and high-pressure air.

Instrument Air Subsystem

Instrument air supplies compressed air for AOVs, dampers, fan inlet guide vane actuators, and pneumatic instruments. Instrument air consists of two 100 percent capacity air-supply trains, which include a compressor package, a dryer package, an air receiver, and associated valves, piping, and instrumentation. Both air receiver discharge lines are connected to the instrument air distribution header. An interconnection is provided between the instrument air system and the service air system. Ball valve (CAS-PL-V017) is normally closed during power operations and during plant shutdown. If an instrument air compressor train fails during power operation, the valve may be opened to allow the service air compressors to back up the remaining instrument air compressor until the failed train is repaired. The instrument air compressors are cooled by the CCS. The instrument air compressor and dryer packages are powered from permanent and non-Class 1 buses that are backed by onsite standby diesel generators. If loss of normal ac power occurs, the "A" instrument air train is powered by the "A" train diesel, and train "B" is powered by the "B" train diesel.

Service Air Subsystem

Service air is supplied at outlets throughout the plant to power air-operated tools. Service air includes two compressor trains, each with a compressor package and an air dryer package. The service air compressor and associated equipment are powered from permanent, non-Class 1 buses. Cooling water is also supplied by the CCS.

High Pressure Air Subsystem

The high-pressure air supplies air to the Main Control Room Emergency Habitability System (VES) and fire-fighting apparatus recharge station. High-pressure air includes an air compressor and filtration package, a receiver package, and supply piping. The high-pressure air compressor package is powered from permanent, non-Class 1 electrical buses. The high-pressure air compressor is air cooled and does not require a cooling water source.

10.5.13.2 Assumptions and Sources of Model Uncertainty

The CAS specific assumptions and uncertainties made in the development of this system model are as follows:

Check valves CAS-PL-V001A/B are modelled using one demand. This was used to represent the swapping of the trains. The normal operation of the compressor starts and stops based on system pressure.

10.5.13.3 System Boundaries for PSA Model

The instrument air subsystem contains two air compressor packages, where each package includes the compressor with ac motor drive, a microprocessor-based controller, lube oil system, inlet air filter, and intercooler with moisture separator, aftercooler with moisture separator, air-side safety relief valves, and a discharge check valve. The compressors receive cooling water from the CCS. The instrument air subsystem also contains two air dryer packages. The purpose of the dryer package is to remove moisture that can damage instruments, controls, system piping, and tools. Each dryer package contains two drying towers, an inlet air prefilter, and an afterfilter. The instrument air subsystem also contains two air receivers, one in each compressor train. The air receivers function to avoid excessive cycling of the air compressor valves and to allow for surge capacity for short periods of time.

10.5.13.4 Common Cause Failures

The CAS common cause failure groups were determined consistent with the method described in Section 10.8.

10.5.14 Protection and Safety Monitoring System

10.5.14.1 System Description

The PMS serves to perform the necessary Category-A signal acquisition, calculations, setpoint comparison, coincidence logic, RT or ESF actuation functions, and component control functions. The PMS serves to achieve and maintain the plant in a safe shutdown condition.

Related sensors and the reactor trip switchgear are, for the most part, four-way redundant for C&I equipment used for reactor trip and Engineered Safety Feature (ESF) actuation functions. This redundancy permits the use of bypass logic so that a division or individual channel out of service can be accommodated by the operating portions of the protection system reverting to two out of three logic from two out of four logic. Four redundant measurements of each variable for reactor trip criteria are obtained by the use of four separate sensors. One measurement is processed by each division.

The Bistable Processor Logic (BPL) is the first level of processing in a safety path. Analogue signals are converted to digital form by analogue-to-digital converters within the division's BPL. Signal conditioning is applied to selected inputs following the conversion to digital form. Following necessary calculations and processing by the BPL, the measurements are compared against the applicable setpoint for that variable. A partial trip signal for a parameter is generated if the channel's measurement exceeds its predetermined or calculated limit. Processing of variables for reactor trip is identical in each of the four redundant divisions of the protection system.

The Local Coincidence Logic (LCL) subsystem acts to initiate a reactor trip or ESF actuation when a pre-determined condition in two out of four independent safety divisions reaches a partial trip or partial actuation state. The LCL also provides for the bypass of trip or actuation functions to accommodate periodic tests and maintenance.

The reactor trip signal from each of the four divisions of the PMS is sent to that division's reactor trip circuit breakers (RTCB). Each division controls two RTCBs. The reactor is tripped when two or more actuation divisions output a reactor trip signal, opening their breakers.

The ESF component control function is implemented with two Integrated Logic Processors (ILPs) and Component Interface Modules (CIMs) that provide a distributed interface between the Class-1 system and the plant operator for control of non-modulating Class 1 plant components. CIMs provide the capability for on/off control of individual Class 1 plant components. The CIMs receive inputs from the ILPs and from the PLS. Non-modulating control relates to the opening or closing of solenoid-operated valves and solenoid-operated pilot valves, and the opening or closing of motor-operated valves and dampers.

10.5.14.2 Assumptions and Sources of Model Uncertainty

The PMS specific assumptions and uncertainties made in the development of this system model are as follows:

1. The model is based on representative signals. The signals modelled for reactor trip include high pressuriser pressure and over temperature delta T (OTDT). Representative reactor trip signals are used based on the previous studies completed for the Pressurized Water Reactor Owners Group (PWROG). It was concluded in these studies that reactor trip actuation signals will be provided by multiple sources (plant parameters) for all initiators. In addition, these automatic actuations are backed up by an operator action to trip the reactor. Given the multiple ways the reactor can be tripped, the divisions are very small contributors to the trip signal unavailability, and the specific signals modelled will not impact the results of the reactor trip signal unavailability analysis.

2. A failure of a single cabinet fan is assumed to lead to only a small increase in cabinet temperature which would not impact the reliability of the components in the cabinet. Each cabinet includes multiple cooling fans located in various locations throughout the cabinet. It is expected that multiple fans would need to fail to cause a significant change in the reliability of the components inside the cabinet.

3. The spurious actuation fault trees modelled in the PMS include single failures that cause a spurious actuation. There is uncertainty in the failure modes identified and modelled for support actuations. For ADS Stages 1-3, two CIMs are modelled for spurious actuation (isolation and control valves). The common cause failures of the software and other modules are modelled as part of the single failure methodology for spurious actuation.

4. The Low-3 Pressuriser Pressure signal is a representative signal used in the containment isolation TOPS (over pressure protection) for long term cooling analysis (LTCA) and Level 2. The signal is representative of the safeguards signal that would occur in Level 1 sequences requiring containment isolation.

5. The IDS power supply and integral cabinet power supply panel are required for successful ILC actuation of the ESF components controlled by the PMS. This dependency on an external power supply and the integral cabinet power supply panel is modelled explicitly in each PMS TOP. However, in cases where the PMS top models the de-energization of a normally energized solenoid-operated valve (e.g., CMT, PRHR, and PCS actuation), the failure of the integral cabinet power supply panel and external power supplies was removed because failure of the power supplies results in the Class-1 components entering their safe state. There are other solenoid-operated valves (SOVs) that may have conservatively modelled the ILP power supply and SOV external power supply that were not felt to be risk significant.

10.5.14.3 System Boundaries for PSA Model

The components and type codes (TCs) included in the PMS PSA model include:

- Component Interface Module CI631 (PMS-CIM-FOP)
- Digital Input Module DI621 (PMS-DIM-FOP)
- Digital Output Module
  - PMS-DO1-FOP Type DO620 (used for PMS-PLS digital interface in the ICP and turbine trip in the LCL)
  - PMS-DO2-FOP Type DO630 (used for reactor trip (RT) model)
- Analogue Input Module
  - PMS-AI1-FOP Type AI687
  - PMS-AI2-FOP Type AI688
- Processor Module PM646A (PMS-PRM-FOP)
- Communication Interface Module (PMS-COM-FOP)
- High Speed Link (PMS-HSL-FOP)
- Safety Remote Node Controller (PMS-SRN-FOP)
- Sensors
  - Pressure (PCS-STP-FOP, RCS-STP-FOP, SGS-STP-FOP)
  - Level (PXS-STL-FOP, RCS-STL-FOP, SGS-STL-FOP)
  - Temperature (RCS-STT-FOP)
  - Neutron Detector (RXS-NDT-FOP)
- Turbine Trip Relays (PMS-RLY-FOP)
- Reactor Trip Breakers (PMS-RTB-FOP)
- Reactor Trip Matrix Termination Unit
  - Shunt Trip (PMS-RST-FOP)
  - UV Trip (PMS-RUV-FOP)
- Squib Valve Termination Unit (PXS-STU-FOP)
- Analogue Output Module
  - PMS-AOM-FOP Type AO650
- Isolation Barrier
  - PMS-IS1-FOP Analogue Output I/I Isolator (Current/Current)
  - PMS-IS2-FOP Analogue Output E/I Isolator (Voltage/Current)
  - PMS-IS3-FOP Digital Output Isolator
  - PMS-IS4-FOP Isolator for Turbine Trip
- Hand Switches on the Primary Dedicated Shutdown Panel and Secondary Dedicated Shutdown Panel (PMS-MSW-FTC)
- Power supplies within each modelled cabinet, including the power supply module, line filter, rectifier, and circuit breakers

10.5.14.4 Common Cause Failures (CCFs)

CCFs for the PMS modules are modelled using a beta factor. The PMS includes relatively large numbers of similar components that should be included together in CCF groups. Application of the alpha-factor method for such large groups would result in a substantial increase in fault tree size and complexity that is not necessary to reflect the contribution of CCF to system failure. Using the beta factor model, only global common cause events that fail all components in a common cause group are included in the model.

The failure of the PMS software is modelled as a single common cause event. Modelling and establishment of CCF groups for sensors are developed and quantified using the alpha factor method. CCF groups are established for redundant sensors based on the specific plant parameter that is being monitored. Unique functions are provided as follows:

- Each core makeup tank includes four level sensors that monitor upper tank level and are included in a CCF group of size eight to cover the sensors in both tanks.

- Similarly, each core makeup tank also includes four level sensors that monitor lower tank level and are included in a separate CCF group of size eight.

- The neutron detectors are also broken into two groups based on upper and lower detectors.

10.5.15 Diverse Actuation System

10.5.15.1 System Description

The DAS is a Class 2 system that provides backup to the PMS. The DAS provides an alternate means of initiating a reactor trip and actuating selected engineered safety features. The DAS was added to the set of AP1000 plant C&I systems to provide a means to mitigate consequences of failure to trip following an ATWT event and reduce the impact on PSA for postulated common-mode failures of PMS.

The DAS uses dedicated sensors to monitor the following six plant parameters independently of the PMS and the PLS:

- SG wide range water level
- Pressuriser water level
- Core exit thermocouple temperature
- RCS hot leg temperature
- Containment operating area temperature
- Rod control motor-generator (MG) set output voltage

In order for a DAS automatic function to be initiated, a digital output from two out of three or one out of two taken twice DAS processors is required. For example, pressuriser water level is monitored by three DAS channels. Each level channel is sent to a different DAS processor. It is necessary for two processors to produce a water level output signal to initiate an RT and CMT actuation. Note that the PSA model is currently based on two out of two logic.

10.5.15.2 Assumptions and Sources of Model Uncertainty

The DAS specific assumptions and uncertainties made in the development of this system model are as follows:

1. The master disable switch located outside the MCR, which is a component in the Operations and Control Centres System (OCS), is not expected to be used or tested at any time during maintenance or operation of the plant.

2. A failure of a single cabinet fan is assumed to lead to only a small increase in cabinet temperature which would not impact the reliability of the components in the cabinet. Each cabinet includes multiple cooling fans located in various locations throughout the cabinet. It is expected that multiple fans would need to fail to cause a significant change in the reliability of the components inside the cabinet. The processor cabinet cooling fans (front and rear doors) failure to provide circulating air when the cabinet is powered results in the cabinet retaining function with no spurious actuation.

10.5.15.3 System Boundaries for PSA Model

The DAS equipment includes the following major components:

- Dedicated sensors
- Two Processor Cabinets
- One DAS Control Panel
- One Squib Valve Controller (SVC) Cabinet

10.5.15.4 Common Cause Failures

No common cause failures were identified for non-electric power distribution DAS equipment located in the Processor Cabinets. Failure modes related to this group of equipment are single failures to the DAS system tops.

Common cause failures for the DAS relays are modelled using a beta factor. The DAS relays and manual switches include a number of similar components that should be included together in CCF groups. Application of the alpha-factor method for such groups would result in a substantial increase in fault tree size and complexity that is not necessary to reflect the contribution of CCF to system failure. Using the beta factor model, only global common cause events that fail all components in a common cause group are included in the model.

Modelling and establishment of CCF groups for sensors were developed and quantified using the alpha factor method for groups up to size eight. CCF groups are established for redundant sensors based on the specific plant parameter that is being monitored.

10.5.16 Plant Control System

10.5.16.1 System Description

PLS performs signal acquisition, calculations, setpoint comparisons, logic calculations, and component control to maintain the plant's systems during all modes of operations. The PLS accepts operator soft control manual commands from the Data Display and Processing System (DDS) and actuates the command if the plant system and control system are in the proper modes. Process variables, component status, and alarm data are generated and processed in the PLS and transmitted to the DDS for presentation and recording. The PLS can control Class 1 components via an optical interface to CIMs in the PMS. The CIM is a Class 1 component that provides command prioritization. The PLS communicates to field devices primarily via Ovation-based input/output (I/O) modules, but also utilizes Profibus and Modbus communications.

The PLS is composed of individual controllers with local and remote I/O. Each controller communicates point data via the Ovation network. Controllers can receive point data from other controllers via the Ovation network, or utilize hardwired communication via I/O.

The PLS performs the following control and monitoring functions:

- Rod position indications
- NSSS control
- Rod control
- Reactor power
- Pressuriser pressure
- Pressuriser level
- Steam generator inventory
- Reactor coolant system inventory
- Turbine steam demand control:
- Tavg
- Steam pressure
- Turbine control and protection
- Fluid systems control
- Balance of plant system control
- Electrical systems control
- Diesel generator control and load sequencing
- Ventilation systems control

PLS functions are implemented with the Emerson Ovation Control System. The system is made up of controllers that communicate with field devices using local and remote I/O modules, Profibus, and Modbus.

10.5.16.2 Assumptions and Sources of Model Uncertainty

The PLS specific assumptions and uncertainties made in the development of this system model are as follows:

1. PLS cabinets PLS-JD-DPU041 through PLS-JD-DPU048 are dual redundant controller cabinets that house two pairs of controllers with each pair acting as a redundant pair. The PLS model does not include the second set due to unavailability of the precise location.

2. A failure of a single cabinet fan is assumed to lead to only a small increase in cabinet temperature which would not impact the reliability of the components in the cabinet. Each cabinet includes multiple cooling fans located in various locations throughout the cabinet. It is expected that multiple fans would need to fail to cause a significant change in the reliability of the components inside the cabinet.

3. HVAC dependencies are not required for PLS. Failure of HVAC to a PLS cabinet room is assumed to lead to a relatively small decrease in component reliability and an insignificant impact on overall risk.

10.5.16.3 System Boundaries for PSA Model

The components and TCs included in the PLS PSA model include:

- Contact Input (Enhanced Compact SOE Input Module) (PLS-CTI-FOP)
- Relay Output Module (PLS-ROM-FOP)
- Analogue Input Module (PLS-AIM-FOP)
- Analogue Output Module (PLS-AOM-FOP)
- Resistance Temperature Detector (PLS-RTD-FOP)
- Processor Module (which includes the NIC card) (PLS-PRM-FOP)
- Profibus (PLS-PFB-FOP)
- IOIC (PLS-IOC-FOP)
- MAU (PLS-MAU-FOP)
- Remote Node Controller (PLS-RNC-FOP)
- Sensors
  - Pressure (STP-FOP-PT)
  - Level (STL-FOP-LT)
  - Temperature (STT-FOP-TE)
  - Flow (STF-FOP-FT)
- Power Distribution Module (PLS-PDM-FOP)
- 24V dc Power Supply (PLS-PWS-FOP)
- Power Line Filter (PLS-PWF-FOP)
- 5V/12V dc PCPS (PLS-CPS-FOP)

10.5.16.4 Common Cause Failures

Common cause failures for the PLS modules are modelled using a beta factor. The PLS includes relatively large numbers of similar components that should be included together in CCF groups. Application of the alpha-factor method to such large groups would result in a substantial increase in fault tree size and complexity that is not necessary to reflect the contribution of CCF to system failure. Using the beta factor model, only a global common cause event that fails all components in a common cause group is included in the model.

The failure of the PLS software is modelled as a single common cause event. Modelling and establishment of CCF groups for sensors are developed and quantified using the alpha factor method. CCF groups are established for redundant sensors based on the specific plant parameter that is being monitored.

10.5.17 Support Systems

A support system is defined as a plant system that affects the operation of two or more other plant systems, whether those systems are front line systems, support systems, or a combination of support and front line systems. Table 10-29 maps mitigating systems (left hand column) to support systems. Table 10-30 maps support systems that are supported by other support systems.

10.6 Human Reliability Analysis

10.6.1 Method Discussion

This section summarizes the HRA for the at-power internal events PSA for the AP1000 plant. The two types of human interactions that are analysed are pre-initiator (Type A) and post-initiators (Type C). The following describes these types of human interactions (HIs).

- Type A or Pre-initiators – This type of HI accounts for latent human interactions that occur during routine activities including testing, maintenance, or calibration activities that are performed before the IE. These actions by plant personnel can affect availability and safety by inadvertently disabling equipment during test and maintenance (T&M). Routine actions considered in the PSA involve restoring a component or flow path to normal configuration after completing the testing, inspection, or maintenance and ensuring that the sensing equipment is correctly aligned and calibrated for automatic response to emergency actuation conditions.

- Type C or Post-Initiators – This type of HI is a dynamic human interaction occurring after initiator occurrence. Operator actions are taken following procedures during a plant accident; plant personnel can operate standby equipment that terminates the accident, and human actions that prevent the termination of the accident fall into this category.

Type B HI includes human actions that can cause an IE (i.e., by committing an error, plant personnel can initiate an accident). Actions that can initiate plant transients are implicitly accounted for in the quantification of IE frequencies to the extent that these human actions are the cause of such events. Plant specific data are used to assign total IE frequencies of which human errors are only one cause.

HRA for pre-initiators is carried out in the following sequence of steps.

1. Identification of specific routine activities that, if not performed correctly, could impact the availability of equipment necessary for a system's PSA function.

2. Screening of routine activities identified that could impact the availability of equipment. None of these screened activities are identified as pre-initiators.

3. Assessment of the probability of pre-initiators and possible dependency between HI.

HRA for post-initiators is carried out in the following sequence of steps.

1. Identification of post-initiators through a review of relevant procedures.
2. Assessment of the probability of post-initiators and possible dependency between HI.

HRA results were documented and quantified using the EPRI HRA Calculator®. This tool is designed to step PSA analysts through the HRA tasks needed to develop and document human failure events (HFEs) and to quantify HEPs.

10.6.2 Analyses and Results

10.6.2.1 Pre-Initiators

The identification and screening of pre-initiators is performed during the systems analyses. Pre-initiators are quantified using the Techniques for Human Error Rate Prediction (THERP) methodology in the EPRI HRA Calculator. Detailed information including applicable procedures, steps, and test or maintenance periodicity are entered into the HRA Calculator for each pre-initiator. Quantification is then performed by selecting the appropriate item from the applicable THERP table.

Table 10-31 provides a summary of all of the calculated HEPs and associated error factors for each of the pre-initiators. Several of the Event IDs were developed for multiple basic events (BEs). This was done for events that impact similar equipment and have a potential error from a similar action. The consequence is the same, and the ability to recover from the error is the same. This grouping is appropriate since the HEPs would be the same if each were analysed separately.

10.6.2.2 Post-Initiators

The identification of post-initiator HFEs was performed in parallel to the PSA systems and accident sequence analyses. As event tree models that represent potential accident sequences were developed, the analyst identified operator actions that are required to be taken to mitigate an accident in accordance with the applicable procedures. Similarly, as fault tree models were developed, the system analysts identified human actions that are required to place equipment in a state necessary to support the applicable success criteria.

The identification of post-initiator HFEs was performed as follows:

- A review of the relevant procedures, including the emergency operating procedures (EOPs), abnormal operating procedures (AOPs), annunciator response procedures, system procedures, and other procedures was performed. The procedures were reviewed in the context of the IE and its associated accident sequences and mitigating systems that were modelled in the PSA.

- During the development of the system fault trees, a review of each system was performed. This included a review of the system function, human interfaces with the system, piping and instrumentation diagrams, dependencies on other systems, etc. This information was used for the identification of HFEs.

Interviews were conducted with procedure writers and plant experts to apply their knowledge and experience to gain insights into the identification of HFEs, confirm that the proposed actions to be included in the PSA are aligned with the operator training and procedures such that the action can be credited, confirm whether the failure to complete the human actions could lead to core damage, and identify potential additional actions that could be credited in the PSA.

Post-initiator HFEs are primarily quantified using the Cause-Based Decision Tree Method (CBDTM)/THERP methodology in the EPRI HRA Calculator, which considers both cognitive and execution errors.

Analysis of cognitive errors takes into account the following factors that could contribute to failure to recognize that an initiator has occurred or incorrect diagnosis:

- Availability of information to the crew
- Effectiveness in getting the attention of the crew
- Possibility of misreading or miscommunication of information
- Clarity of the information provided to the crew
- Likelihood of skipping a step
- Possibility of misinterpreting a step in the procedure
- Misleading logic in the instruction or procedure
- Possibility that the procedure will be deliberately violated

Analysis of execution errors takes into account the following factors:

- Manipulation tasks to implement an action, such as selecting the wrong control on a panel or turning a multi-position switch in the wrong direction or leaving it in the wrong setting
- Availability of confirmatory steps to ensure that the action was successfully performed
- Likelihood of skipping an execution step

Time windows for the operator actions were developed as part of the Success Criteria Analysis. The time windows associated with the HEPs are presented in Table 10-32. Table 10-33 provides a summary of all of the calculated HEPs and associated error factors for each of the post-initiators.

10.6.3 Operator Action Dependency

Dependency analysis is performed on PSA models to address dependencies between multiple HFEs. Dependencies occur between different HFEs that are present in the same cutset. No level of dependency is assigned between pre-initiator actions. All test and maintenance actives identified as possible pre-initiator actions are expected to be performed by different crews at different times. There is also no level of dependence assigned between pre--initiators

and post-initiators actions. These actions are assumed to be performed at different times and by different crews.

The level of dependency is assigned between actions based on a review of if the actions are performed by the same crew, contain common cognitive, occur during the same time, performed within the same location, and the associated stress level. If the actions do not occur within the same time window the level of dependency may vary based on the difference in time. A decision tree is used as a tool to determine the level of dependency to assign. The independent probability for the second HFE in the pair is replaced with a probability based on the level of dependency. These probabilities are 1.0, 0.5, 0.15 and 0.05 for complete, high, medium and low levels of dependency, respectively. The level of dependency is applied using the EPRI HRA Calculator, and is applied during quantification using a recovery rule file.

The dependency analysis was performed on the CDF and large early release frequency (LERF) results of the model in Section 10.20 using the EPRI HRA Calculator tool to generate the combinations of HEPs to be assessed and determine the level of dependency.

10.7 Data Analysis

10.7.1 Method Discussion

The objective of the data analysis is to provide the parameter estimates used in basic event creation which accurately represent the failure mode or unavailability of the component or train. The data analysis ensures that parameters accurately represent the configuration and operation of the plant, that component or system unavailability is accounted for, and that uncertainties in the data are understood and appropriately accounted for. The data analysis is primarily based on the information provided in NUREG/CR-6928 (Reference 10.15).

10.7.2 Identification of Component Types, Failure Modes, and Boundaries

Basic events represent the potential failure modes of components that result in a component failing to perform its intended function. Such basic events include, but are not limited to, a component failing to start, a component failing to run, a component failing when demanded, or a component being out of service due to test or maintenance. The components included in the PSA model are identified during the system analyses. Basic events are then developed to represent component failures and equipment unavailability that contribute to the failure of the system to meet specific success criteria.

In addition to identifying the component types and failure modes represented in the PSA, it is necessary to define component boundaries by specifying what “pieces” or “sub-components” are considered to be represented by the component failure data. These definitions are necessary to assure consistency between the basic events in the system models and the data analysis so that the boundaries of the components are defined identically. For example, all pieces of a motor-operated valve are typically considered to be part of a single “component” when collecting reliability data even though the valve consists of various piece parts (e.g., electric motor, gearbox, limit switches, stem, disc, valve body, etc.) that may be separately identified in the plant maintenance records. PSAs typically do not model failures of every switch, relay, or contact in a control circuit of a component because that type of detail is difficult to obtain from the plant data. Instead, failures of these “pieces” are typically included with actual failures of the components to establish a failure rate.

10.7.3 Component Grouping

The generic component failure data in NUREG/CR-6928 is primarily tabulated by component type (e.g., motor-operated pumps, circuit breakers, etc.). Component grouping is further refined according to mission type (standby or normally operating) and service condition (clean water or raw water) when supported by data. Separate groups were created for chillers, compressors, diesel generators, and fans to differentiate between standby and normally operating components. All components were grouped by system to allow plant-specific data changes in the future. In some cases, representative data must be assigned to component groups that are included in the AP1000 plant PSA model, but have no specific failure data or no specific unavailability test and maintenance data from generic sources.

10.7.4 Generic Component Failure Parameters

This section identifies the type codes used in the AP1000 plant PSA and the applicable generic component failure parameters. Each combination of system, component group, and failure mode was assigned an eleven-character type code. The component failure basic event naming convention uses the first eleven characters of the basic event for the type code. The failure parameters and source information for each type code is stored in the "TC" table of the CAFTA database. As basic events are developed during fault tree construction, CAFTA pulls the applicable information into the "BE" table of the database from the "TC" table when the first eleven characters match a type code. For example, the fault tree model for the PCS includes basic event "PCS-AOV-FTO-V001A," which represents failure of the PCCWST isolation valve PCS-PL-V001A failing to open when demanded. "PCS-AOV-FTO" is the eleven character type code for this component/failure mode combination, and CAFTA uses the failure parameter and source information in the type code table to populate the "BE" table. Type codes with generic failure parameters derived from NUREG/CR-6928 Table 5-1, are listed in Table 10-34 with their description, failure rate, units (Demand or Hour), NUREG/CR-6928 failure mode code, α value, β value, and variance.

Other sources of component failure data were used for type codes not covered in NUREG/CR-6928. These type codes are listed in Table 10-35 along with the associated failure parameter information and sources.

10.7.5 Component and Equipment Unavailability

Test and maintenance activities that remove components and equipment from service and alter the normal configuration of mechanical systems can be significant contributors to the overall unavailability of those systems. AP1000 plant specific planned or unplanned maintenance data is not available. The data analysis used generic unavailability from NUREG/CR-6928. Table 10-36 shows the variables used for unavailability as well as the description, the rate, the event code, the α variable, the β variable, and the variance from NUREG/CR-6928.

Other sources of component unavailability data were used for unavailability not covered in NUREG/CR-6928. These unavailabilities are listed in Table 10-37 along with the associated parameter information and sources.

10.7.6 C&I Data

Reliability analyses were performed for each C&I system as part of the design process to ensure satisfaction of plant availability expectations and PSA safety goals. The data developed for, and used in, the reliability analyses was also used in the PSA.

The reliability analysis for the DAS is documented in Reference 10.38. The reliability analysis includes the DAS component failure rates as well as the values used for the length of surveillance test intervals, probability of detection, and mean time to repair. The values used in the PRA are consistent with the values used in the reliability analysis. The DAS type codes and failure parameters are listed in Table 10-38.

Failure rates for PMS components are provided in Reference 10.39. The reliability analysis for the PMS is documented in Reference 10.40. The reliability analysis also includes the values used for the length of surveillance test intervals, probability of detection, and mean time to repair. The PMS type codes and failure parameters are listed in Table 10-39 (including the failure parameters for spurious PMS component failures).

Spurious actuation of the PMS is modelled in the updated PSA and, therefore, data analyses for these failure modes were considered. The design of the PMS includes an ADS blocking device in each division to prevent spurious actuation of the automatic depression system and IRWST injection due to software CCF. The block can fail in one of two ways. The first failure mode is one where the block fails to be removed and prevent a necessary actuation. The failure rate for this mode is estimated to be approximately [ ] of the total rate and is documented in Reference 10.42. The failure rate for spurious actuation due to a CIM fault was determined based on Reference 10.43 which indicates that approximately [ ] of CIM failures would lead to such an event.

The reliability analysis for the PLS is documented in Reference 10.41. The analysis also includes the component failure rates as well as the values used for the length of surveillance test intervals, probability of detection, and mean time to repair. The values used in the PSA are consistent with the values used in the reliability analysis. The PLS type codes and failure parameters are listed in Table 10-40.

10.8 Common Cause Analysis

10.8.1 Method Discussion

Components of similar manufacture and functions are subject to CCF. Common cause failure can result in failure of a system when identical, non-diverse, and active components are used to provide redundancy. Failure of two or more components in a common cause group can occur if they are of the same design, perform the same function, share the same installation and maintenance procedures, or are located in the same location or environment. In most systems modelled in the PSA, some components meet these criteria for susceptibility to CCF. The CCF groups for each system are identified during system analysis using the methodology described in NUREG/CR-5485 (Reference 10.45). If the component is subject to multiple failure modes, a CCF group is created for each failure mode.

For the AP1000 plant PSA, CCF modelling and establishment of CCF groups was performed in accordance with the guidance in NUREG/CR-5485 (Reference 10.45) and quantified using the alpha factor model. The alpha factors were derived from WCAP-16672-P (Reference 10.46). An exception to this is the application of the beta factor model for the C&I systems and the VLS due to large CCF group size. CCF groups are established for each system, component, and failure mode combination listed in Table 10-41 and Table 10-42 that is included in the AP1000 plant fault tree models.

Due to the unique systems in the AP1000 plant, and the lack of plant-specific experience, generic common cause failure groups are defined in Table 10-42. These common cause

failure groups are included in every system model where CCF is appropriate. The data for these groups is based on the alpha factors from Reference 10.46.

The CCF calculations depend on alpha factors representative of data from observed CCF events. Table 10-43 reports the CCF alpha and beta factors used in the AP1000 plant PSA, as well as their description, value, and source. Some CCF group sizes are larger than the data in the table records. When a group size was larger than the referenced data, the largest group size was used.

10.8.2 Unique Common Cause

10.8.2.1 Common Cause Variables for C&I

The PMS, PLS, and DAS include relatively large numbers of similar components that should be included together in CCF groups although DAS is simpler than the other two systems. In some cases there are dozens of the same component type used in each system. Application of the alpha factor method to such large group sizes is not practical and would result in a substantial increase in fault tree size and complexity that is not necessary to reflect the impact of CCF on system failure.

The C&I beta factor values were originally developed based on a method presented in AnnexD of the international standard IEC 61508-6 (Reference 10.47) as documented in Reference 10.48. Reference 10.50 includes PLS hardware common cause variables for the ovation data network. The data used assumed 12 fan out clusters.

C&I beta factors are summarized in Table 10-44.

In addition to the C&I beta factors used for hardware common cause, the PMS and PLS systems include a software common cause event. A desirable characteristic of the PSA would be to model software failures in a way that is consistent with the basis of how they occur and also within the context that the software is used. However, due to the lack of consensus on software reliability methods, detailed modelling of software failures was not performed for this analysis. In order to account for the potential impact of software errors on the reliability of these systems, a basic event representing failure due to common cause is included in the model for each system. No common mode failure of software between PMS and PLS is modelled because the processors and software in these two systems are from different manufacturers using different designs. Reference 10.49 includes an evaluation of software failures that was used in the PSA. The calculated failure rate is a function of several variables relative to software development. The assumptions for common cause failure of software and common cause failure of software leading to a spurious actuation are documented as areas of model uncertainty in the PSA.

Unique C&I common cause variables are summarized in Table 10-45.

10.8.2.2 Common Cause Variables for Loss of Long Term Core Cooling

PSAs should address the need for containment sump recirculation for a wide range of IEs, including non-LOCA events. Theoretically, any accident sequence that involves containment sump recirculation could have a failure path that involves a loss of long term core cooling due to inadequate gravity driven flow (PXS) or Net Positive Suction Head (NPSH) (RNS) as a result of high sump screen head losses or downstream effects. Considerations for loss of long term cooling were incorporated into the AP1000 plant during the design process and led to the conclusion that this design is less susceptible to debris-induced failure of LTCC. An

expert panel was conducted to assess the estimated probabilities used in the PSA (Reference10.51). The factors are used as common cause basic events in the PSA model. The common cause variables are summarized in Table 10-46.

10.9 Fault Tree and Core Damage Quantification Process

10.9.1 Model Quantification

Quantification of the PSA model was performed using fault tree linking at the following stages of the model building process:

- System level – to generate results for each system top event or support system model
- Accident sequence level – to generate results for each accident sequence
- Total CDF level – to generate overall results for core damage frequency

A brief description of the sequence of steps used to build the integrated model follows:

1. Accident sequence logic was generated from the event trees to create an equivalent fault tree logic model consisting of top events or system logic. Successes are accounted for in each sequence by including the applicable successful tops under an ‘A and not B’ gate.

2. Mitigating system fault tree models were merged into the model. The accident sequence event names match the names of the mitigating system models. In this manner, a system was merged into its proper location in the event sequence.

3. Support system models were merged into the model as required by the mitigating systems. The mitigating system models contain transfer gates whose names match the names of top gates in the support system. In this manner, a support system was merged into its proper location in the model.

10.9.2 Mutually Exclusive

Often two events may appear in a cutset that could not occur simultaneously. For example, maintenance events on separate trains of the same system are typically not allowed by plant technical specifications. Mutually exclusive (MUX) combinations were identified in the Systems Analyses as well as the Level 2 Analysis.

To address mutually exclusive events, combinations were identified and the non-applicable cutsets were removed from the model by means of a mutually exclusive fault tree which includes a branch for standard plant systems and a branch for site-specific systems. The MUX top event was developed using the combinations identified in the aforementioned analyses and then merged into the linked fault tree model with an ‘A and not B’ gate at a sequence organizational gate level.

10.9.3 Flags

Flags are used in the model to define system alignments/configurations, probabilities associated with IEs, and logic markers. The alignment/configuration flags are used to identify the running and standby trains at the time of the IE or to include/eliminate weather related failures such as outside temperature. Alignment/configuration flags can be set for the operating configuration once the plant is operational. For CDF and Level 2 release category

quantification, flag values are based on the fraction of time the component is expected to be running or in standby (or weather related state) during a year of operation.

Flags with the prefix "FL-L2" are used in the Level 2 model.

10.9.4 Event Tree Transfers

In some cases, an accident scenario path may have a transfer to a different event tree as a consequence of the accident progression (e.g., transient with a stuck open pressuriser safety valve transfers to a LOCA scenario). The application of transfers between event trees also reduces the size and complexity of individual event trees. The Accident Sequence Analysis (Section 10.3) identifies where transfers are in the event tree models. When transfers are used between event trees, all sequence logic is maintained. Logic flags are used to identify when a transfer is part of a sequence.

10.9.5 Treatment of Dependencies

Dependencies are addressed using different methods in the AP1000 plant PSA model. Several IE dependencies are addressed during the accident sequence development and documented in the Accident Sequence Analysis (Section 10.3). Initiating event dependencies have also been addressed in the corresponding system models. For support systems that have an SSIE tree, initiator dependencies are addressed using logic in the support system models.

SSIE dependencies are also addressed if the IE could change the possible failure modes for that system. For example, during normal operation one CCS pump is normally running with the other in standby, however, during a LOOP event the running pump would stop and have to restart or the standby pump would have to start. Therefore, the logic under the normal CCS top does not account for the requirement for both pumps to start. To account for this, these system failures that are unique to a LOOP event are modelled under an 'AND' gate with the LOOP initiator.

Support system dependencies are addressed within the system models. Section 10.5.17 provides a summary of the support system dependencies for the AP1000 plant PSA. In addition to IE and system dependencies, the dependency between HFEs is also addressed as summarized in Section 10.6.

10.9.6 Truncation Limitation

A sufficiently low truncation value was determined for the plant-level CDF calculation in order to ensure that significant cutsets and sequences were included in the final results. This was accomplished by initially quantifying the model with a truncation value of 1E-12 and iteratively reducing the truncation value by an order of magnitude until the change in CDF was less than 5 percent. Convergence was demonstrated with a truncation value of 1E-14.

10.9.7 Recoveries

The AP1000 plant passive system designs have very limited dependency on support systems. There is limited benefit from LOOP recovery and support system recoveries. Based on the low contribution to CDF from LOOP IEs and the limited benefit of restoring offsite power, a LOOP recovery factor was not addressed for this model.

10.10 Level 2 Analysis

The Level 2 analysis begins with core damage (CD) sequences from the Level 1 model development. The Level 1 core damage sequences are binned into PDSs that characterize the plant conditions that may impact the severe accident progression from the initiator conditions (high RCS pressure, low RCS pressure, or containment bypass) magnitude of hydrogen generation and release locations, and IRWST water availability.

10.10.1 Plant Damage States for Core Damage Sequences

Categorizing core damage accident scenarios provides a systematic method for interfacing the Level 1 PRA core damage analysis results with the Level 2 PRA severe accident containment integrity analyses. This modelling method provides a direct transfer of all CD sequences that result from Level 1 quantification into the Level 2 model.

A naming convention with a maximum of three-characters has been developed that defines the PDS characteristics for the AP1000 plant. The first character(s) in the naming convention defines the degree of RCS depressurization available from the IE. The second set of characters provided in the PDS name is the availability of the ADS depressurization. The availability of successful ADS is important because it gives information regarding two conditions: (1) how much RCS depressurization has occurred because of ADS actuation and (2) where hydrogen gas will be released from the RCS and accumulate in containment. The final PDS naming criteria is for PXS water availability and distribution in the containment, which is primarily influenced by PXS failures. Table 10-47 summarizes the accident sequence characteristics, initiators, placement of hydrogen generation, and water availability.

10.10.2 Level 2 Recovery and Containment Isolation Event Trees

Through automatic actuations or recovery operator actions in FR-C.1, the PXS and RCS (i.e., ADS) systems can be recovered post CD to support the RCS pressure boundary integrity, in-vessel retention (IVR) or support hydrogen mitigation. These recoveries are treated in Level 2 recovery event trees. The inputs to these trees are the PDSs described in Section 10.10.1, and the recoveries are applied based on the associated system failures in Level 1 (Table 10-48 and Table 10-49).

10.10.3 Magnitude of Release

10.10.3.1 Large Release Definition

This analysis considers containment isolation line sizes greater than 5.08 cm (2 inches) in nominal diameter are large releases from the containment. Additionally, this analysis considers large pre-existing containment leaks (Reference 10.52). Failure of the containment pressure boundary due to severe accident phenomena is classified as a large release.

This analysis also considers unisolated SGTR and ISLOCA core damage events as large releases from the containment. These sequences are treated in the bypass Containment Event Tree (CET).

10.10.3.2 Small Release Definition

This analysis considers that containment isolation line sizes less than or equal to 5.08 cm (2 inches) in nominal diameter are small releases from the containment. Additionally, this analysis considers small pre-existing containment leaks. This analysis also considers SGTR

with success of overfill protection as small releases from the containment. The overfill protection isolates CVS and SFW to both SGs. Additionally; the MFW line to the ruptured SG is isolated on a Safeguards Signal. Because this protection measure isolates flow to and from the ruptured SG but does not automatically close the MSIVs, these releases are considered small.

10.10.3.3 Containment Leakage

Severe accident scenarios that are mitigated such that the containment pressure boundary is intact and has not been pressurized beyond American Society of Mechanical Engineers (ASME) service level C pressure during the severe accident will leak at or less than the design leak rate.

10.10.4 Recovery and Containment Isolation Event Trees

The Level 2 recovery and containment isolation event tree models are described.

10.10.4.1 Is the Containment Isolation Successful?

This top examines the sequences that bypass the containment because of a containment isolation failure or a pre-existing containment crack or tear. It determines the status of containment isolation prior to CD. This top is valid for both the high pressure and low pressure CETs.

Containment isolation is required to prevent fission product releases to the environment after CD. The containment isolation failure provides a direct release pathway from the containment atmosphere to the environment.

A negative response to this question implies either a large or small containment isolation failure has occurred prior to the time of core damage and results in an early release.

10.10.4.2 Are ADS Stages 2-3 Depressurization Available?

This top examines the availability of ADS Stages 2-3 to provide RCS depressurization and a flow path for hydrogen release from the RCS into the IRWST.

The status of ADS Stages 2-3 is determined in one of two ways, either by the Level 1 actuation or by the post CD actuation. Based on the size of the ADS Stage 1 valve and the MLOCA break definition, one out of two ADS Stage 1 valves would be sufficient to reduce the RCS pressure below the main steam safety valve (MSSV) setpoints and thereby mitigate I-SGTR (Assumption 3). However, based on downstream needs (success criteria for IVR), the success criteria for this top is defined by success in the Level 1 or as a recovery of two out of four ADS Stages 2-3 valves.

10.10.4.3 Is ADS Stage 4 Depressurization Available?

This top examines the availability of ADS Stage 4 to provide a continuous RCS depressurization through discharge from the hot legs and into the containment atmosphere facilitating passive IRWST gravity injection, containment sump recirculation, and IVR. ADS Stage 4 also provides an engineered flow path for hydrogen release from the RCS into the containment loop compartments.

The status of ADS Stage 4 is determined in one of two ways, either by the Level 1 actuation or by the post CD actuation. The success criteria for this top are defined by success in the Level 1 or as a recovery of one out of four ADS Stage 4 valves.

10.10.4.4 Is the IRWST Water Injected into the RCS?

This top examines the availability and timing of IRWST water injection into the RCS.

IRWST may be injected before or after core damage. When IRWST gravity injection is successful and ADS Stage 4 is successful, the reactor cavity is flooded with water and the Reactor Vessel (RV) is submerged by the accident progression. Here, core damage is typically a result of the failure of passive recirculation. If IRWST gravity injection fails or ADS Stage 4 fails, the reactor cavity will not be flooded sufficiently to support IVR without a successful FR-C.1 operator action to flood the reactor cavity manually.

Success or failure at this node is determined by the Level 1 actuation or the post CD recovery.

10.10.4.5 Is Recirculation Successful?

This top examines the availability and timing of recirculation maintaining long term core cooling into the RCS from containment sump.

When PXS recirculation from the containment sump is successful, the reactor cavity contains water, and the sump and the IRWST are hydraulically coupled. Condensation water from the containment shell is returned to either the IRWST or the containment sump to maintain the water pool. However, if sump recirculation fails, only water from the IRWST can be injected into the RCS. As the IRWST drains, water head to maintain long term core cooling is lost and core damage occurs.

Success or failure at this node is determined by the Level 1 actuation or the post CD recovery.

10.10.5 Containment Event Tree Tops

The Level 2 containment event tree models are described.

10.10.5.1 No Induced Steam Generator Tube Rupture Occurs?

This top examines the conditions for either pressure induced or thermally induced SGTR. This top is valid for only the high pressure CETs.

Pressure induced SGTR occurs when there is a high differential pressure across the SG tubes, typically when the RCS pressure is at the pressuriser safety valve setpoint and the SG is fully depressurized. Thermally induced SGTR occurs when the RCS pressure is high and the post CD natural circulation conditions heat up the SG tubes.

This top includes the success of the SGS PORVs or MSSVs to operate as designed to relieve pressure when their setpoints are reached and to reclose, and includes the consideration that either a Pressure Induced SGTR (PI-SGTR) or a Thermally Induced SGTR (TI-SGTR) can occur if SGS fails.

TI-SGTR occurs when a creep rupture failure from a high SG tube temperature is predicted during high pressure severe accident conditions. The MAAP4 analysis concluded that a

depressurized secondary side is a prerequisite for TI-SGTR. If the secondary side is pressurized, molten debris relocation to the lower head is predicted to occur well before TI-SGTR and will challenge vessel integrity due to creep failure of the lower head. For SGS failure cases, TI-SGTR occurs before RV integrity challenge. Failure of this top leads to a large early release that bypasses the containment through the I-SGTR. HL creep failure is not predicted to occur prior to TI-SGTR or reactor vessel failure regardless of SGS success. Therefore, hot leg creep rupture failure is not credited for RCS depressurization and mitigation of high pressure phenomena. If the secondary is not depressurized, vessel failure is predicted.

PI-SGTR occurs when a large pressure differential exists across the SG tubes and a flaw exists in the SG tubes which becomes weak and fails under the stress of the pressure. Early in plant life, the SG tubes are considered to be in pristine condition (i.e., no tube flaws) so the probability that a PI-SGTR will occur is zero. TI-SGTR occurs when temperature challenges exist on the SG tubes. Because this plant does not have loop seals, full loop natural circulation is very effective at increasing the heat transfer from the core to the SG tubes and increases the probability of a thermal creep failure. The probability that a TI-SGTR will occur is one for high pressure CD scenarios when SGS fails.

10.10.5.2 Has the PXS Gutter Successfully Aligned?

This top event examines if the PXS gutter valves are successfully aligned. This top is valid for both the high pressure and low pressure CETs.

During injection, the steam in containment condenses on the containment shell and returns to the IRWST through the PXS gutters, slowing the loss of injection. This recirculation of condensate water to the IRWST has a significant effect on IVR by maintaining a flow of debris cooling water to the RV. However, if the gutter valves fail to align to the IRWST, the condensate will not be returned to the IRWST and instead will be directed to the containment sump. In the event of recirculation failure and gutter failure, the IRWST water inventory will be depleted more quickly and the RV will dry out after injection is completed.

This top event is only considered if recirculation has failed after the recovery event tree results (HP2 and LP2). The gutter valve alignment does not need to be considered for recirculation success paths because the IRWST and the containment sump are hydraulically coupled through the recirculation lines so it does not matter if the condensate is returned to the IRWST or the containment sump.

10.10.5.3 Is In-Vessel Retention Successful?

This top examines if the core debris is maintained within the RV and is valid for both the high pressure and low pressure CETs.

IVR is detailed in Section 10.12.2.1.

When molten core debris is relocated to the lower plenum of the RV, the water in the cavity cools the external surface of the RV by nucleate boiling to prevent vessel failure. The two conditions which ensure IVR are RCS depressurization by a minimum of two out of four ADS Stages 2-3 valves or one out of four ADS Stage 4 valves and RV cavity flooding to at least the 99.4 m (98’) elevation prior to the challenge to the vessel integrity. When these conditions are successful, the AP1000 plant RV retains the core debris and prevents the release of molten debris into the containment.

10.10.5.4 No Ex-Vessel High Energy Phenomena Occurs?

This top examines ex-vessel phenomena that can immediately fail the containment at vessel failure. This top is valid for both the high pressure and low pressure CETs.

Ex-Vessel Phenomena is detailed in Section 10.12.2.2.2.

At vessel failure, containment integrity may be challenged immediately by high energy phenomena that occur as a result of debris relocation to the reactor cavity. Ex-vessel steam explosion and High Pressure Melt Ejection (HPME)/Direct Containment Heating (DCH) are evaluated as potential containment failure modes. Steam explosions are postulated to occur in the reactor cavity when the RV fails and debris is ejected from it into water in the reactor cavity. A steam explosion may occur as a result of molten metal and/or oxide core debris mixing and thermally interacting with water. Steam is created at a very high rate, potentially producing a sonic pressure front and dynamic loading on local structures.

A positive response to this top implies that steam explosion does not occur or does not fail the containment integrity. A negative response implies that there is an ex-vessel steam explosion which fails containment.

10.10.5.5 Does the Ex-Vessel Core Debris Spread and Quench?

This top examines the characterizations of the Molten Core Concrete Interaction (MCCI) after RV failure. This top is valid for both the high pressure and low pressure CETs.

Core debris coolability is detailed in Section 10.12.2.5.

If IVR is not successful and the RV fails, the molten core debris will spill from the RV into the reactor cavity and onto the concrete basemat below the RV. The degree of the debris spreading on the cavity floor and potentially into the Reactor Coolant Drain Tank (RCDT) room will depend on the RV failure mode. The global lower head failure mode is expected to spread the debris throughout the cavity and RCDT room. The flow of debris from a localized failure of the lower head would have little momentum, and the spreading is expected to be limited to the reactor cavity octagon.

For either spreading pattern, the molten debris will transfer heat into the concrete floor of the cavity. Over time, the containment floor may be eroded from this molten core and concrete interaction; this phenomenon is referred to as Base Mat Melt Through (BMMT). The probability of basemat failure due to BMMT is investigated for two concrete types, limestone and basaltic. The output of the MCCI analysis is the probability of debris quenching prior to basemat failure and the timing of quench or failure. The model structure applied in the CET was compiled using a decomposition event tree which was converted to a fault tree and included in the Level 2 fault tree model.

10.10.5.6 Is the PCS Water Cooling the Containment Shell?

This top examines the availability of PCS cooling on the containment shell. This top is valid for both the high pressure and low pressure CETs.

The containment atmosphere is cooled by PCS, which condenses the steam in the containment atmosphere onto the containment shell as heat is transferred through the shell to the ambient environment. PCS water is applied to the shell external surface to enhance the cooling by evaporation to the natural circulation air flow through the PCS cooling annulus. Except for pressurization by high energy severe accident phenomena such as a hydrogen

burn, the water-cooled PCS will generally maintain the containment pressure below the design pressure. Water that is condensed on the PCS inner surface is returned to the IRWST through the PXS gutter or to the containment sump if the gutter system is not aligned.

When PCS water cooling is not available, the containment atmosphere will become steam inerted and hydrogen combustion will not be possible unless cooling is restored and steam is condensed from the atmosphere.

This top represents the availability of PCS water which provides containment cooling.

10.10.5.7 Is PRHR Providing Decay Heat Removal?

This top examines the availability of PRHR as the decay heat removal method. This top is valid for only the high pressure CETs.

PRHR provides effective decay heat removal during high pressure scenarios. When PRHR removes decay heat, the IRWST becomes saturated. Steaming in the IRWST will drive the oxygen out of the gas space and along with other conditions (described in Section 10.10.5.11); prevent deflagration to detonation transition (DDT) from occurring in the IRWST.

A positive response to this top shows that PRHR, which prevents hydrogen complications, has been met. However, a negative response to this top shows that the PRHR system is not being used and DDT must be evaluated later in the CET.

10.10.5.8 Can ADS Stage 4 Actuation Mitigate Hydrogen Complications?

This top examines the availability of ADS Stage 4 depressurization to mitigate hydrogen complications in the containment atmosphere by mixing the hydrogen uniformly in the major compartments of the containment. This top is valid for both the high pressure and low pressure CETs.

By design, the ADS Stage 4 valves play an important part in hydrogen mitigation within the containment. ADS Stage 4 provides an engineered flow path for hydrogen release from the RCS into the containment loop compartments where it is mixed in the containment, thereby reducing the complication of diffusion flame against the containment shell and preventing detonable local limits of hydrogen accumulation in small dead ended compartments, such as the IRWST. Mainly, there are two types of hydrogen generation concerns within the AP1000 plant containment: DDT and diffusion flame.

Hydrogen combustion and detonation are detailed in Section 10.12.2.3. This section also includes the conditions and failures leading to potential for DDT.

A positive response to this top implies that the ADS Stage 4 success criteria for actuation which prevents hydrogen complications has been met. However, a negative response to this top implies that the ADS Stage 4 success criteria have not been met and DDT or diffusion flame must be evaluated later in the CET.

10.10.5.9 Are the Hydrogen Igniters Providing Hydrogen Mitigation?

This top represents the availability of the hydrogen igniters (as part VLS) which mitigate hydrogen generation. This top is valid for both the high pressure and low pressure CETs.

A positive response implies that hydrogen igniter system mitigation is available; a negative response implies that the hydrogen igniter system mitigation has failed.

10.10.5.10 No Diffusion Flame Occurs which Fails the Containment?

This top examines if a diffusion flame can occur from ADS Stages 1-3 actuation and hydrogen generation in the IRWST. This top is valid for both the high pressure and low pressure CETs.

Hydrogen combustion and detonation are detailed in Section 10.12.2.3.

If the hydrogen igniters are successfully actuated, a hydrogen plume may be postulated to ignite as a diffusion flame and locally heat the containment pressure boundary if a hydrogen release pathway near the containment pressure boundary is open. A diffusion flame can occur when an inert plume of hydrogen and steam enters an oxygen rich atmosphere. The plume is ignited and burns as a standing flame at the location where the plume enters the oxygen rich compartment. When hydrogen burns at a vent near the containment pressure boundary, a thermal loading on nearby structures by radiation heat transfer and convection is produced.

A positive response to this top implies that a diffusion flame does not occur and the IRWST vents meet their success criteria. However, a negative response to this top implies that a diffusion flame occurs and fails the containment.

10.10.5.11 Containment Does Not Fail during Hydrogen Combustion?

This top examines the survivability of containment given a hydrogen combustion event occurs. This top is valid for both the high pressure and low pressure CETs.

Containment failures due to hydrogen combustion are considered for flame acceleration and deflagration to DDT in the event of igniter failure. In-vessel releases that are not well-mixed in the containment and ex-vessel scenarios may result in flame acceleration and DDT.

Hydrogen combustion and detonation are detailed in Section 10.12.2.3. This section also includes the conditions and failures leading to potential for DDT.

10.10.5.12 Does the Operator Vent the Containment?

This top examines the availability of the operators to vent the containment to reduce the containment pressure. This top is valid for both the high pressure and low pressure CETs.

During severe accident progressions when PCS is unavailable to cool the containment atmosphere, the containment will begin to pressurize. To maintain containment integrity in these cases, the operator can vent the containment to reduce the containment pressure.

A positive response to this top implies that containment venting was successful and a controlled, vent release occurs. A negative response to this top implies that containment venting was not successful.

10.10.5.13 No Containment Failure from Over Pressurization Occurs?

If PCS is failed and the containment pressure cannot be vented, it is expected that the containment overpressure failure will occur in one of two timeframes. Containment failure within 24 hours is considered to be an intermediate containment failure (LIRF release category). If containment failure does not occur at 24 hours, then a late containment failure

will occur (LATE release category). This top is valid for both the high pressure and low pressure CETs.

10.10.5.14 No Base Mat Melt Through (BMMT) Failure in 24 Hours?

In the unlikely event of unquenched MCCI, there is a small probability of BMMT that occurs prior to 24 hours. This top is valid for both the high pressure and low pressure CETs.

A positive response to this question designates a late containment failure from BMMT. A negative response to this question designates an intermediate containment failure from BMMT.

10.10.6 Assumptions and Sources of Model Uncertainty

1. This model assumes that the time to reach an irreversible state for the post core damage operator action to recover water for PCS water cooling occurs when the containment atmosphere is steam inerted or at an elevated dry hydrogen concentration of 8 percent,, whichever occurs last.

2. This model considers two RV failure modes. These failure modes determine the spreading of the molten debris. The molten material will either remain in the reactor cavity or occupy the reactor cavity and the RCDT room. A 50 percent probability for each RV failure mode is assumed.

3. This model assumes that ADS Stage 1 actuation during the Level 1 and/or Level 2 accident progression does not impact the accident sequence; however, it is noted that one out of two ADS Stage 1 valves open would be sufficient to mitigate induced SGTR.

4. Hydrogen control by PARs is credited for well-mixed in-vessel hydrogen releases. Hydrogen control by the PARs is not credited for unmixed in-vessel releases and all ex-vessel releases. For ex-vessel scenarios, PARs are not credited for mitigating long-term non-condensable flammable gas generation associated with MCCI. The uncertainty in non-condensable gas generation during MCCI is too large to credit the effectiveness of the PARs for ex-vessel scenarios. Igniters are required to control flammable gas releases from MCCI.

5. This model assumes a 25 percent condensate bypassing the PXS gutters and the IRWST for all cases unless otherwise noted. The water that bypasses the gutters is directed to the containment sump. The bypass fraction is determined by engineering judgement of systems analysis as bounding conditions during plant operation.

6. This model assumes when the reactor vessel integrity is challenged by molten core debris and the RCS pressure is at or above the secondary side valves setpoint (i.e., at the pressuriser SV setpoint), an HPME occurs.

7. This model assumes that hydrogen igniter system success is defined as one successfully operating hydrogen igniter at each igniter location.

8. This model assumes that high pressure sequences without ADS depressurization and no induced SGTR (I-SGTR) phenomena (i.e., HPME sequences) cause RV failure and have successful spreading into the RCDT.

9. This model uses the secondary side valves top L2-SGS-SS-PA-PLA which considers eighty demands on each function of the MSSV. The SG PORVs are expected to open at

the lower pressure and modulate to control pressure. If the SG PORV sticks open, the automatic closure of the block valve is credited. If the SG PORV does not open, the MSSVs would open and have eighty cycles. The number of cycles is on the upper end of the estimates provided in NUREG-1570 (Reference 10.53). This estimate of MSSV demands is applicable to the AP1000 plant design. The SG design for the AP1000 plant and legacy plants are similar.

10. For CD events initiated by SGTR with successful ruptured SG isolation, ADS Stages 2-3 failures and ADS Stage 4 failures are conservatively binned as "large" containment bypasses.

11. The ISLOCA initiator %ISL-P04 progresses directly to CD and is also considered to be a large release. This ISLOCA pathway is limited to a 0.95 cm (3/8 inch) RCP heat exchanger tube.

12. The low pressure CET includes both LLOCA and MLOCA core damage events. Depressurization for these initiators is still required in the CET to support IVR, diffusion flame, and DDT.

13. The probabilities for reactor vessel failures and the corresponding containment failures are considered to be realistic estimates. The containment integrity may be challenged immediately by high energy phenomena that occur as a result of debris relocation to the reactor cavity.

14. Analysis has shown there is a potential for DDT within the IRWST if zero, one, or two ADS Stage 4 valves are open. The analysis also shows that there is a potential for DDT within the SG compartments if less than four ADS Stage 4 valves open. In cases where both DDT conditions could exist, the more conservative ADS Stage 4 success criteria are used.

15. This model assumes that low pressure sequences with no ADS depressurization is a LERF.

10.11 Uncertainty Analysis

The EPRI CAFTA-related code UNCERT was used to propagate the parametric uncertainty associated with basic event failure parameters. This was performed using the Level 1 at-power internal events PSA quantification results that include all cutsets above the 1E-14 truncation limit. The uncertainty analysis was performed using 1000 samples, the default random seed, and the Latin Hypercube sampling method. Table 10-65 provides the CDF and LRF results based on the uncertainty run.

10.12 Severe Accident Phenomena Treatment

10.12.1 Introduction

This section describes how the AP1000 NPP containment addresses challenges from severe accident phenomena, and how the challenges are evaluated in the PSA. In the PSA, the MAAP code (Reference 10.4) is used to evaluate severe accident scenarios. Severe accident phenomenological uncertainties are treated with Risk-Oriented Accident Analysis Methodology (ROAAM) (Reference 10.70) phenomenological evaluations, with AP1000 NPP specific decomposition event tree phenomenological evaluations, or with assumptions that certain low-frequency severe accident phenomena fail the containment. The objective of

these studies is to show, with a high degree of confidence, that the AP1000 NPP containment will accommodate the effects of severe accident phenomena that are expected to occur after the onset of core damage and afterward to establish a controlled, stable condition in which no further high energy challenges to containment integrity will occur. Such evaluations demonstrate the robustness of the containment design. The controlled, stable condition for the plant is defined as the plant condition, following core damage, in which containment conditions are controllable at or near desired values.

10.12.2 Treatment of Physical Processes

The following eight issues are identified in Reference 10.69 as being representative of the phenomenological issues pertaining to severe accident conditions:

1. Loss-of-coolant accident (LOCA)
2. Fuel-coolant interaction (steam explosion)
3. Hydrogen combustion and detonation
4. Melt attack on concrete structure or containment pressure boundary
5. High-pressure melt ejection
6. Core-concrete interaction (CCI)
7. Containment pressurization from decay heat
8. Elevated temperature (equipment survivability)

The challenge to the containment integrity from a LOCA blowdown is covered in the containment design basis and is not specifically addressed here. Treatment of physical processes affecting the remaining challenges is discussed in this chapter.

10.12.2.1 In-Vessel Retention of Molten Core Debris

In-vessel retention (IVR) of core debris by external reactor vessel cooling is a severe accident mitigation attribute of the AP1000 NPP design (Reference 10.75). With the reactor vessel intact and debris retained in the lower head, phenomena such as molten core-concrete interaction and ex-vessel steam explosion, which occur as a result of core debris relocation to the reactor cavity, are prevented.

The AP1000 NPP reactor vessel insulation and containment geometry promote in-vessel retention. Engineered design features of the AP1000 NPP containment flood the containment reactor cavity region during accidents and, thereby, submerge the reactor vessel in water.

Reference 10.75 presents an AP1000 NPP-specific evaluation to determine the likelihood that sufficient heat can be removed from the outside surface of the submerged reactor pressure vessel lower head to prevent reactor vessel failure and relocation of debris to containment. The methodology used to quantify the margin to vessel failure in DOE/ID-10460 (Reference 10.70) for the AP600 was adapted to the AP1000 NPP.

Design features of the AP1000 NPP promote the long term retention of core debris within the reactor vessel lower head as outlined in Reference 10.75. The two conditions that promote IVR are RCS depressurization and reactor vessel cavity flooding prior to the challenge to the vessel integrity.

Accounting for the uncertainties in thermal-hydraulic parameters, the heat fluxes to the vessel wall from the debris bed are calculated. Failure is defined as departure from nucleate boiling on the external surface of the reactor vessel. The results of the analyses show margin to failure for the reactor vessel if it is depressurized and externally cooled by water.

10.12.2.2 Fuel-Coolant Interaction (Steam Explosions)

A steam explosion may occur as a result of molten metal or oxide core debris mixing with water and interacting thermally. Steam explosions may be postulated to occur inside the reactor vessel when debris relocates from the core region into the lower plenum and in the reactor cavity if the vessel fails and debris is ejected from it into water in the reactor cavity.

10.12.2.2.1 In-Vessel Fuel-Coolant Interaction

In-vessel steam explosions were studied extensively in the AP600 analyses. A ROAAM analysis of the AP600 reactor vessel lower head integrity under in-vessel steam explosion loading is presented in DOE/ID-10541 (Reference 10.71). Typically, in-vessel steam explosion analyses focus on the α-mode containment failure, which is induced by the reactor vessel upper head failure. The ROAAM steam explosion analysis focused on failure of the lower head, because that vessel failure mode could impair the in-vessel retention capability of the reactor vessel. The ROAAM analysis concludes that lower-head vessel failure from in-vessel steam explosion is physically unreasonable with very large margin to failure.

Based on the in-vessel core relocation scenario for the AP1000 NPP, the in-vessel steam explosion ROAAM analysis results presented for the AP600 can be extended to the AP1000 NPP. The mass flow rate, superheat, and composition of debris in the relocation from the upper core region to the lower head are expected to be essentially the same as the AP600. The geometry of the lower head of the AP1000 NPP is the same as the AP600. Therefore, it is reasonable to extend the results of the AP600 in-vessel steam explosion ROAAM analysis to the AP1000 NPP.

The results of the in-vessel steam explosion ROAAM can also be extended to containment failure induced by in-vessel steam explosions (α-mode containment failure). The likelihood for vessel failure and subsequent containment failure due to in-vessel steam explosion is so small as to be negligible. This conclusion is in agreement with the conclusions of US Nuclear Regulatory Commission (US NRC) NUREG-1116 by the US NRC-sponsored Steam Explosion Review Group (Reference 10.72).

Therefore, in the PSA containment event tree quantification, α-mode containment failure and in-vessel steam explosion-induced lower head failure are considered to be negligible.

10.12.2.2.2 Ex-Vessel Fuel-Coolant Interaction

The first level of defence for ex-vessel steam explosion is the in-vessel retention of the molten core debris. If molten debris does not relocate from the vessel to the containment, there are no conditions for ex-vessel steam explosion.

An analysis of the structural response of the reactor cavity was performed for the AP600 in GW-GL-022 (Reference 10.73, Appendix B). The analysis assumed that the IRWST water was not drained into the reactor cavity and IVR fails. As in the in-vessel steam explosion analysis, the results of this AP600 ex-vessel steam explosion analysis are extended to the AP1000 NPP. The vessel failure modes for AP600 and AP1000 NPP are the same. The initial debris mass, superheat, and composition are assumed to be the same as the AP600. The reactor cavity geometry and water depth prior to vessel failure are the same as AP600. Therefore, the results of the AP600 ex-vessel steam explosion analysis are considered to be appropriate for the AP1000 NPP.

The PSA containment event tree quantification considers the potential for ex-vessel steam explosions that challenge containment integrity for cases with successful cavity flooding (high RCS pressure) and with cavity flooding failure (low RCS pressure).

10.12.2.3 Hydrogen Combustion and Detonation

A substantial mass of hydrogen may be released to the containment due to the oxidation of zirconium cladding in the reactor vessel. If IVR is not successful and molten core debris is relocated from the reactor coolant system, additional hydrogen will be released to the containment during molten core concrete interaction. Hydrogen combustion inside the containment may be postulated to threaten the containment integrity. Hydrogen plumes may burn as diffusion flames and create challenging thermal loading to the containment pressure boundary and equipment. Hydrogen-air-steam mixtures may burn as deflagrations that pressurize the containment or accelerate to detonations that will create challenging impulse loads to the containment structures.

The AP1000 NPP containment includes design features to mitigate uncontrolled hydrogen combustion challenges to the containment integrity. The VLSis comprised of PARsand hydrogen igniters that consume hydrogen and prevent challenging hydrogen-air-steam mixtures in the containment atmosphere. The hydrogen igniters are arranged in two independently powered trains. Each train is capable of controlling the containment hydrogen according to single failure criteria. Hydrogen monitors display the containment hydrogen concentration in the control room to allow the operators to observe the containment conditions while performing severe accident management. Passive containment cooling helps to mix the containment atmosphere by natural circulation to dilute the hydrogen concentration and allow it to burn as it is released from the RCS.

The severe accident hydrogen analyses conservatively neglect hydrogen depletion by the PARs and credit the operation of the igniters for controlling hydrogen during core damage scenarios. Successful operation of the igniters ensures hydrogen will burn as it is released preventing the containment atmosphere from reaching globally flammable concentrations and detonable conditions.

The AP1000 NPP provides defence-in-depth to address over-temperature containment failure due to diffusion flames that may be postulated from the ignition of a hydrogen plume by the igniters. The first level of defence is the stage four automatic depressurization system (ADS Stage 4) lines from the RCS, which prevent significant hydrogen releases to the IRWST and Passive Core Cooling System (PXS) compartments. ADS Stage 4 vents from the RCS hot legs to the loop compartments, which are shielded from the containment shell and have a constant source of oxygen from the natural circulation in the containment. Hydrogen can be burned continuously as it is released in the loop compartments without threatening the containment integrity. If ADS Stage 4 fails, the AP1000 NPP has provided design considerations in IRWST vents to mitigate diffusion flames by preventing hydrogen plumes from burning near the containment walls. Vents from the passive injection system compartments and chemical volume and control system compartment are located sufficiently away from the containment shell and penetrations in order to mitigate the threat from hydrogen diffusion flames.

If igniter operation is successful, and multiple ADS Stage 4 squib valves fail to open, the PSA containment event tree quantification evaluates the success of the IRWST vents to properly perform to mitigate potential for diffusion flames burning near the containment pressure boundary. If the IRWST vents fail to perform their function properly, containment shell overtemperature failure is assumed to occur.

In the event of igniter failure, the likelihood of containment failure due to deflagration and detonation in the containment is evaluated. The AP1000 NPP containment structure is capable of withstanding the peak pressurization from the deflagration of hydrogen generated by 100 percent cladding oxidation without exceeding ASME service Level C pressure limits. Therefore, the probability of containment failure due to deflagration is considered to be negligible. Containment integrity challenges from uncontrolled hydrogen combustion are primarily due to detonation.

Containment failure from a directly-initiated detonation wave is not considered to be a credible event for the AP1000 NPP containment. There are no ignition sources of sufficient energy to directly initiate a detonation in the AP1000 NPP containment. DDT is considered to be the only likely mechanism to produce a detonation in the AP1000 NPP containment.

In the event of igniter failure, the likelihood of DDT in the AP1000 NPP containment is evaluated locally in confined compartments during in-vessel hydrogen generation and release to the containment. DDT is evaluated globally after vessel failure and molten core concrete interaction ex-vessel hydrogen releases. For DDT to occur, the combination of the gas mixture sensitivity to detonation and the geometric configuration potential for flame acceleration must be conducive to DDT. The potential for flame acceleration and DDT in the AP1000 NPP containment is evaluated using the State-of-the-Art (SOAR) methodology in NEA/CSNI/R (2000)7 (Reference 10.76) to characterize the conditions leading to the potential for DDT.

In addition to igniter failure, the following are conditions and failures leading to potential for DDT:

- Condition 1
  - Elevated hydrogen releases into the IRWST due to ADS-4 failures
  - The water in the IRWST is sub-cooled to quench steam due to failure of PRHR cooling of the RCS
  - ADS Stages 1-3 success and spargers submerged during hydrogen and steam release to quench steam
- Condition 2
  - Dry core conditions, no in-vessel core re-flooding
  - Concentrated hydrogen release into one compartment due to ADS-4 failures
- Condition 3
  - Ex-vessel core debris does not spread or is not quenched following reactor vessel failure

The PSA containment event tree quantification evaluates these conditions and assumes DDT occurs and the containment fails in the event the unfavourable conditions are met.

10.12.2.4 High-Pressure Core Damage and High Pressure Melt Ejection

The AP1000 NPP incorporates design features that prevent high-pressure core melt. These features include the PRHR system and the ADS. These design features provide passive primary system heat removal and RCS depressurization to prevent high pressure core damage conditions. The consequences from postulated HPME are mitigated by the containment layout which provides a tortuous pathway from the reactor cavity to the upper compartment, and no direct pathway for the impingement of debris on the containment shell. Preventing debris from being dispersed at high pressure to the upper containment mitigates direct containment heating (DCH) challenges to the containment integrity. Preventing molten debris from impinging on the containment shell mitigates debris-induced failures of the containment pressure boundary.

In high-pressure core damage scenarios, the potential exists for creep-rupture-induced failures of the RCS piping at the hot-leg nozzles, the surge line, the steam generator tubes and, in the event of molten debris relocation to the lower plenum, in the reactor vessel lower head. Hot-leg nozzle or surge line failure prior to the failures of other components results in the rapid depressurization of the RCS. Failure of the steam generator tubes results in a potential containment bypass and a large release of fission products to the environment. Failure of the lower head of the reactor vessel results in the potential for HPME.

The PSA containment event tree quantification considers the effects of primary and secondary system pressures and temperature, as well as the aging of the steam generator tubes in assessing the likelihood and timing of induced failures of the RCS hot leg, surge line, steam generator tubes, and reactor vessel lower head.

10.12.2.5 Core Debris Coolability

In accident sequences where the reactor pressure vessel failure is not prevented, core debris may be discharged into the reactor cavity. The AP1000 NPP cavity design provides area for the core debris to spread into the reactor coolant drain tank room. Condensate water from the PCS returns to the reactor cavity, thereby providing a long-term supply of water to cool the surface of the core debris.

At vessel failure, it is very likely that the cavity will be filled with water from the RCS, CMTs, and accumulators to at least the 94.82 m (83 ft) elevation. There are significant uncertainties associated with debris spreading in a water-filled cavity. Given the reliability of the ADS, the likely vessel failure modes produce a low-pressure melt ejection (LPME) to the containment and, therefore, the debris will drain by gravity from the reactor vessel to the cavity. Debris spreading is mainly a function of the uncertain vessel failure mode. Global lower-head failure releasing molten debris at a high rate would enhance spreading, while a localized failure mode would release molten debris with less momentum, which would most likely cause the debris to pile up under the reactor vessel and limit the spreading.

The PSA containment event tree quantification considers a bifurcation of the debris spreading scenarios and the likelihood of debris failing to quench and basemat melt-through in the event that debris does and does not spread effectively.

10.12.2.6 Containment Pressurization from Decay Heat

The AP1000 NPP containment is cooled via the PCS. Evaporative water cooling of the containment shell provides long-term containment cooling and limits the containment pressure to less than the design pressure for all severe accident events except hydrogen combustion (which is addressed separately). Passive containment cooling water is provided to the external surface of the containment shell at the top of the containment via a redundant, diverse system of valves and lines, including a line that can be connected to an outside water source, such as a fire truck.

In the unlikely event that water cannot be supplied to the top of the containment shell for an extended period of time, air-only cooling by air flowing through the PCS annulus provides significant cooling to the containment. However, under nominal-to-conservative environmental conditions, containment integrity by air-cooling alone cannot be assured. In this case, containment failure is predicted to occur more than 24 hours after accident initiation.

A significant amount of time is available for operator action to vent the containment under the severe accident management guidance (SAMG). Containment venting mitigates uncontrolled releases of fission products from a failed containment. The AP1000 NPP can be vented under the SAMG from a number of containment penetrations, primarily via the RNS piping to the spent fuel pool.

On the PSA containment event tree, the availability of PCS water and the operator action to successfully vent the containment is considered. The evaluation considers the effects of molten core concrete interaction and non-condensable gas generation on the timing of venting and the effect on the fission product release magnitude.

10.12.2.7 Elevated Temperatures (Equipment Survivability)

Reference 10.74 states that equipment identified as being useful to mitigate the consequences of severe accidents must be designed to provide reasonable assurance that it will continue to operate in a severe accident environment for the length of time needed to accomplish its function. Also, US Regulation Title 10 of the Code of Federal Regulations (CFR) Part 50.44 requires Class-1 equipment to continue performing its function after being exposed to a containment environment created as a consequence of generating a quantity of hydrogen equivalent to 100-percent cladding oxidation. As the AP1000 NPP design uses thermal igniters to burn hydrogen in a controlled manner, it is necessary to demonstrate that the Class-1 equipment can continue to perform its function in the high-temperature environment created by the hydrogen burning.

The functions of the equipment in containment for which credit is taken in the AP1000 NPP PSA were reviewed to determine if the equipment is required to operate in a severe accident environment and beyond design basis limits.

10.12.2.8 Summary

The potential for and the consequences of severe accident phenomena are evaluated. The preventive and mitigative features of the AP1000 NPP addressing the severe accident phenomena are discussed. This information is applied to the containment event trees and used in the quantification of the large release frequency.

10.12.3 Analysis Method

Analyses of severe accident phenomena have been performed primarily using the MAAP4 code as well as fundamental phenomenological calculations using spreadsheets and hand calculations.

10.12.4 Severe Accident Analyses

10.12.4.1 Operator Actions and Human Reliability Analysis

MAAP4 analyses are performed to define operator action time window for recovery actions and manual actuations that could be performed in the severe accident containment analysis. These actions include:

- Recovery of containment isolation
- Recovery of ADS stages 1, 2 and 3
- Recovery of ADS stage 4
- Recovery of IRWST passive injection
- Recovery of sump passive recirculation/PXS gutter valve alignment
- Operator action to flood the containment for IVR
- Operator action to actuate the hydrogen igniters
- Recovery of PCS water cooling
- Operator action to vent the containment

10.12.4.2 Long-Term Core Cooling

Success criteria for the required sump gravity head as a function of time after shutdown are established using detailed thermal-hydraulic calculation methods, and the MAAP4 code is used to establish the sequence timing and water level transients for a matrix of scenario to develop ADS and PXS success criteria for long term passive core cooling.

10.12.4.3 Induced Steam Generator Tube Rupture Analysis

MAAP4 analyses are performed for high pressure core damage scenarios to establish temperature transients for the hot leg, steam generator tubes, and reactor vessel lower head. The timing of potential for creep rupture failures is investigated for a matrix of cases varying the secondary side pressure and reactor cavity flooding to determine likely RCS failure locations based on scenario conditions.

10.12.4.4 In-Vessel Retention of Molten Core Debris

MAAP4 analyses are performed to establish scenario timing and initial conditions for detailed IVR calculations. The analyses consist of a matrix of cases varying IEs, time of core cycle, IRWST drain time, and modelling parameters.

The fundamental IVR phenomenological calculations are based on test data and are performed using spreadsheets. The spreadsheet calculations allow the inclusion of reactor vessel internals and investigation of debris bed chemistry uncertainties that are not available in the MAAP4 code modelling.

10.12.4.5 Passive Containment Cooling Water Depletion

A matrix of MAAP4 analyses are performed to establish containment pressurization rates following the loss of PCS water at the depletion of the PCS water storage tank, the depletion of the PCS ancillary water storage tank, and total PCS water delivery failure. The analyses include the effect of the ambient air temperature on the containment pressure. The analyses evaluate the times that the containment pressure reaches design pressure limit, ASME service level C pressure, and the probability of containment failure at the equilibrium pressure.

10.12.4.6 Hydrogen Flame Acceleration and Deflagration to Detonation Transition

A matrix of MAAP4 analyses is performed to establish conditional failure that may lead to the potential for flame acceleration and DDT. The analyses vary the IE and combinations of ADS and PXS failures that impact the timing and addition rate of water to the core and hydrogen release locations from the RCS to the containment. Hydrogen generation from MCCI is modelled, and the challenge from DDT is quantified.

10.12.5 Insights and Conclusions

The analyses of the severe accident phenomena for the AP1000 NPP PSA highlight the following insights and conclusions:

- Preventing reactor vessel failure reduces the challenges to the containment integrity during a severe accident. The design of the AP1000 NPP reactor vessel, vessel insulation, and reactor cavity, and the ability to flood the cavity after a severe accident promote in-vessel retention of molten core debris. The RCS must be depressurized and the IRWST water drained into the reactor cavity (if it had not already spilled into the containment) to successfully promote IVR.

- Should a failure of the reactor vessel occur, the design of the reactor cavity and the recirculation of water condensed on the PCS shell promotes long-term water cooling of core debris that exits the vessel.

- Lower head vessel failure due to in-vessel steam explosions is physically unreasonable.

- The PRHR and ADS systems are design features that can be used to prevent and mitigate high-pressure core melt, induced steam generator tube failures, and direct containment heating in a severe accident. The reactor cavity is designed to limit the amount of debris from being expelled into the lower compartments and to prevent debris impingement on the containment shell.

- Loads due to the deflagration of hydrogen equivalent to 100 percent zirconium oxidation will not challenge containment integrity. Deflagration to detonation transition is unlikely because, in addition to failure of the hydrogen control system (igniters), it requires a number of identified specific conditions to occur. Conditions resulting in the potential for DDT to threaten containment integrity are modelled in the PSA. Containment over-temperature due to hydrogen combustion is mitigated by the design, and failures leading to potential for overheating are identified and modelled in the PSA.

- PCS water cooling ensures that containment pressure will remain below the ASME Service Level C pressure limit during severe accidents. Only in the event of failure of water supply could pressure exceed this limit; in such a case a long grace time (>24 hours) is available to realign alternative water sources, for which connections have been provided. The capability to vent the containment is provided but would only be used per SAMG in case of a total loss of PCS cooling including failure to align alternate water supplies.

- The equipment needed to mitigate the consequences of a severe accident is designed to provide reasonable assurance that it will continue to operate during an accident.

10.13 Level 3 Offsite Dose Evaluation

The Level 3 Analysis has not been updated since APP-GW-GL-022 (Reference 10.1).

The potential for a release of radioactive material to the environment and significant radiation dose to members of the public is very small. This is due to the very small CDF and LRF, but also to the containment design, which provides enhanced deposition of core materials that could be released in a severe accident, and the PCS minimises the energy available to expel such materials from the containment.

The Level 3 PSA for internal events at full power was carried out by multiplying the fission product release category (RC) frequencies by the appropriate RC mean doses. The doses calculated were the following:

- Effective dose equivalent (EDE) whole-body dose and acute red bone marrow dose at ground level at the site boundary (assumed 0.8 km (0.5 miles))

- Population collective whole-body dose out to 80.5 km (50 miles)

- Downwind centre-line ground level thyroid dose at the site boundary

The first of these was for comparison with the Westinghouse dose-risk goal of <0.25 Sv (0.025 rem) at 1.E-6/yr, consistent with the EPRI advanced light water reactor (ALWR) Utility Requirements Document (URD) (Reference 10.3).

Source terms for each of six RCs (intact containment (IC), BP, containment failure early (CFE), containment failure intermediate (CFI), containment failure late (CFL), and RC for containment isolation (CI) failure) and one sensitivity case (category IC without credit for deposition in the containment annulus, designated DIRECT) were defined to be used as inputs for this analysis. In order to estimate conservatively the ground level doses at the site boundary, it was assumed that the releases were at ground level. It was also assumed conservatively that 5 percent of the iodine released from the containment was in volatile form. Results were quantified based on both a 24-hour and 72-hour exposure.

Interpretation of these results in the context of the United Kingdom (UK) risk and dose targets is to be found below in Section 10.5.

Table 10-12 shows that for the RCs CFL, IC, and the DIRECT sensitivity study, the mean whole-body EDE at the site boundary in 24 hours is less than 0.06 Sv (0.006 rem). For all other RCs (BP, CI, CFE, and CFI) the mean dose at the site boundary in 24 hours is >0.25 Sv (0.025 rem). The sum of the probabilities of the RCs, including an IC excess leakage category, is approximately 2.4E-7 events/yr for at-power conditions. The results also show

that for the RCs CFL, IC, and the DIRECT sensitivity study, the acute red bone marrow dose at the site boundary in 24 hours is <0.01 Sv (0.001 rem). For all other RCs (BP, CI, CFE, and CFI), the mean dose at the site boundary in 24 hours is >0.25 Sv (0.025 rem). Again, the sum of the probabilities of the RCs including an IC excess leakage category is approximately 2.4E-7 events/yr for at-power conditions. Thus, the Westinghouse design goal is met that limits the frequency of exceeding the 0.25 Sv (0.025 rem) whole-body EDE for an individual at the site boundary 24 hours after core damage to 1.E-6 events/yr, without any emergency protective action.

10.14 Low Power and Shutdown PSA Assessment

The LPSD PSA has not been updated since APP-GW-GL-022 (Reference 10.1).

10.14.1.1 Contribution to Annual Core Damage Frequency

This section presents the results from the assessment for internal events during low power or shutdown states for the AP1000 plant, which was carried out based on the requirements of the EPRI ALWR URD (Reference 10.3). The assessment encompassed operation when the reactor is subcritical, or at power operations at up to 5 percent of rated power.

Events occurring during hot and cold shutdown conditions are grouped and referred to as non-drained events, and events during drain down of the RCS and when the plant is at mid-loop are referred to as drained events. The following results are from the updated PSA (Reference 10.2).

The estimated CDF for these drained and non-drained states is 1.03E-7/yr. The LRF is estimated to be 1.72E-8/yr. Reference 10.1 shows the dominant contributions to the CDF by basic events. The data is also tabulated in Table 10-3 and shown diagrammatically in Figure10-3.

The dominant contributor, at 76 percent of the CDF in LPSD states, is failure of the component cooling or service water systems during the RCS drained state. This state is during mid-loop/vessel flange operation, and lasts for about 120 hours, once in every 18-month refuelling cycle. The major contributions to risk due to loss of circulating water system (CWS) or SWS are the following failures:

- CCF of all ADS fourth stage squib valves to operate
- CCF of the squib valves in recirculation lines
- CCF of the IRWST squib valves in gravity feed lines
- CCF of the strainers in the IRWST
- CCF of the recirculation sump strainers

10.14.1.2 Peak Point-in-Time Risk

The current AP1000 shutdown PSA resolves the shutdown states into non-drained, drained and refuelling states, and accounts for time spent in these modes (and not at full power). This analysis is sufficient to determine that the risk from these modes is low and that the plant Category-A features provide adequate risk mitigation. However, it does not provide the information that would be used by the plant operating staff to identify the peak point-in-time risks during shutdown. A provisional set of plant operating states (POSs) has been identified for the purpose of estimating peak point-in-time risk (in terms of instantaneous CDF associated with each POS), and bounding values for the instantaneous CDF in these POSs have been estimated.

The peak point-in-time risk occurs during the period when the RCS loops are drained and the refuelling canal has not been flooded for refuelling. During this period the PRHR HX is not available, and if the RNS fails and cannot be recovered the only credited means of providing long-term core cooling is gravity injection from the IRWST through one of two lines.

The peak point-in-time risk corresponds to an instantaneous CDF of 8.3E-6/yr, and is estimated on the basis that no equipment is deliberately taken offline for maintenance. If the maximum equipment outage permitted by the technical specifications is implemented, the instantaneous CDF increases to 1.45E-4/yr, the increase being due almost entirely to the permitted outage of one of the two IRWST gravity injection lines. Instantaneous CDF is only used for the purpose of identifying peak risks. The instantaneous CDF values significantly overestimate the AP1000 plant shutdown risk because the plant would not operate continuously for a year in a shutdown drained condition with equipment in maintenance.

10.15 Internal Flooding Analysis

The Internal Flooding Analysis is summarized based on qualitative assessment, model development and design information input. The following tasks were performed using the guidance provided in the EPRI Guidelines for Performance of Internal Flooding Probabilistic Risk Assessment (Reference 10.54). Section 10.20.5 includes a summary of results for the Internal Flood model.

10.15.1 Plant Partitioning

Flood areas were chosen to include the partitioning of the plant into physically separate areas that were considered to be independent of the flooding effects from other areas.

10.15.1.1 Doors

Doors are a key element for plant partitioning and the propagation path development. The opening direction, along with the other characteristics of doors, is important information needed to support the identification of the propagation path of a flood event from its origin to the final accumulation point. Design documents and drawings were used for the identification and categorization of doors for the plant partitioning and propagation path development tasks.

10.15.1.2 Stairwells and Elevators

Stairwells are usually marked with a single room name across multiple elevations. In order to easily distinguish stairwells from different buildings, during the flood areas' naming convention process, a three-digit number was added (indicating building), followed by the stairwell name on drawings to designate stairwell flood areas. To allow for a more refined description of the pathways among levels, stairwells were split into multiple rooms.

Elevators are all marked as ELEV across multiple elevations. In order to easily distinguish elevators from different buildings, during the naming convention process for flood areas, a three-digit number was added (indicating building), followed by the elevator designator (EL) and a cardinal locator designator (N for North, S for South, W for West, and E for East) to differentiate the different elevators in the same building. Elevators were split into multiple rooms to allow for a more refined description of the pathways among levels.

10.15.1.3 Major Structures

The major plant structures identified and included in the internal flooding probabilistic safety assessment IF-PSA are listed below. This list was extracted from a typical site plan for the single unit AP1000 plant, along with whether the structures are included in the standard design.

- Containment and Shield Building (standard design)
- Turbine Building (standard design)
- Annex Building (standard design)
- Auxiliary Building (standard design)
- SWS Cooling Towers (standard design)
- Radwaste Building (standard design)
- Plant Entrance (site-specific design)
- Circulating Water Pump Intake Structure (site-specific design)
- Diesel Generator Building (standard design)
- CWS Cooling Tower (site-specific design)
- CWS Intake Canal (site-specific design)
- Fire Water & Clearwell Storage Tank (standard design)
- Fire Water Storage Tank (standard design)
- Transformer Area (site-specific design)
- Switchyard (site-specific design)
- Condensate Storage Tank (standard design)
- Diesel Generator Fuel Oil Storage Tanks (standard design)
- Demineralized Water Storage Tank (standard design)
- Boric Acid Storage Tank (standard design)
- Plant Gas System (PGS) Bulk Gas Storage Area (site-specific design)
- Turbine Building Laydown Area (site-specific design)
- Circulating Water Pipe (site-specific design)
- Waste Water Retention Basin (site-specific design)
- Passive Containment Cooling Ancillary Water Storage Tank (standard design)
- Diesel-driven Fire Pump & Enclosure (standard design)

10.15.2 Building Qualitative Screening and Identification of Flood Areas

A high-level screening was performed to remove from further evaluation those buildings and structures that did not contain potential flood sources and PSA-related components. Table 10-50 shows all the buildings that are screened out for further analysis.

10.15.2.1 Containment and Shield Buildings

The containment and Shield Building include the annulus structures. Containment is normally isolated during at-power operation and is not considered vulnerable to flood-specific failure modes since it is qualified for the harsh environment characteristic of post-LOCA, main steam line break (MSLB) or feedwater line break (FWLB) scenarios.

During normal operations, a primary function of the Shield Building is to provide shielding and protection for the containment vessel and the radioactive systems and components located in the Containment Building. The Shield Building does not contain flood susceptible PSA-related equipment. The Shield Building is of little relevance in the internal flooding analysis; although a review of the general arrangement drawings identified the potential for some areas in the Shield Building to be involved in the propagation path for flooding scenarios originated in the Auxiliary Building. The Shield Building is therefore retained in the internal flooding analysis as a potential source of propagation to other buildings or flood areas where PSA-related equipment may be impacted.

10.15.2.2 Turbine Building

The Turbine Building is a non-Class 1 structure which is subjected to flooding from a variety of potential sources including the Circulating Water, Service Water, Condensate/Feedwater, Component Cooling Water, Turbine Building Cooling Water, Demineralized Water, and Fire Protection Systems, as well as the de-aerator storage tank. It is concluded that the Turbine Building contains equipment modelled in the PSA which can be impacted by flood sources also located in this building. Therefore the Turbine Building is retained. Since the Turbine Building is divided into a number of very large open areas, it will not be addressed on a room-by-room basis.

10.15.2.3 Annex Building

The Annex Building is divided into two areas: radiological controlled areas and non-radiological controlled areas. The Annex Building contains equipment modelled in the PSA which can be impacted by flood sources also located in the Annex Building. The Annex Building is therefore retained in the analysis and is addressed on a room by room basis.

10.15.2.4 Auxiliary Building

The plant Auxiliary Building contains radiological controlled areas and non-radiological controlled areas which are physically separated by 0.61m and 0.91m (2 and 3 feet) structural walls and floor slabs. These structural barriers are designed to prevent flooding across the boundary between these areas by locating penetrations for piping and HVAC duct above maximum flood levels, or by sealing these penetrations. Three floors are above grade and two are located below grade. The Auxiliary Building is divided into radiological controlled areas and non-radiological controlled areas.

10.15.2.5 Radwaste Building

There is no PSA-related equipment located in any area of the Radwaste Building. There are flood scenarios that can be envisioned to propagate into other critical structures from the Radwaste Building. Therefore, the Radwaste Building is retained in the internal flooding analysis to evaluate scenarios in which water from applicable fluid sources propagate to other unscreened buildings.

10.15.2.6 Diesel Generator Building

The Diesel Generator Building is a non-Class 1 structure which contains equipment modelled in the PSA which can be impacted by flood sources also located in the building.

10.15.3 Identification of Flood Sources

Flood sources were assessed and screened out from further evaluation using the following considerations:

- The floor drain system was considered capable of handling the discharge from small bore diameter pipes < 5 cm (2"). Therefore, the small bore pipes were not considered as a flood source that would threaten PSA-related components by submergence.
- No PSA components would be failed by a release of the system inventory.
- No transient IE would result from flood-induced failures or component unavailability due to the isolation of the break.

10.15.3.1 Fluid System Screening

Each unscreened system was evaluated to determine whether it could produce a spray, flood, major flood or high-energy line break (HELB) event by reviewing the system's characteristics, including temperature, pressure, system inventory, and system capacity. Table 10-51 lists all the unscreened systems, and Table 10-52 shows the screened systems and the reasons why they are screened out of further analysis.

10.15.4 Component Location and Initial Flooding Fragility Assessment

While many components may be exposed to sprays and minor floods, not all components are susceptible to water damage and failure. An assessment of the potential susceptibility of all PSA-relevant SSCs to damage by spray, flood (submergence), and temperature was performed. Additionally, this analysis assumes that equipment in the vicinity of fluid sources, as well as high energy lines, is susceptible to submergence, spray, jet impingement, pipe whip, humidity, condensation, and temperature concerns. Failures such as jet impingement, pipe whip, humidity, condensation, and temperature concerns, are addressed on a case by case basis and are documented throughout the analysis. Additionally, equipment in the vicinity of the flood sources is conservatively failed in all cases unless specifically stated otherwise, and thereby inherently includes the identified failure mechanisms. The extent to which PSA-related components are susceptible was based on system/component design and installation information.

10.15.5 Propagation Path Development

The information on flood areas and on general arrangement drawings, room numbering drawings, and door numbering drawings is used to develop propagation paths to fully address the potential impact of each internal event flood scenario.

Propagation paths are dependent on physical characteristics of rooms and structures and are generally independent from the actual flood sources. For this reason, propagation paths are described on a flood area by flood area basis and all the sources identified in each flood area will share the same potential propagation path.

Generic considerations on door fragility are used as primary input to propagation path development. The main generic guidance is the EPRI guideline Appendix D (Reference 10.54).

According to the fire protection analysis results, openings through fire barriers for pipe, conduit, and cable trays are sealed or closed to provide a fire resistance. Therefore, electrical penetrations are considered sealed for the development of propagation pathways. The sealing of cable penetrations is considered a best practice within the industry, and propagation through these penetrations via failure of the sealant is considered non-preferential for internal flooding. However, piping penetrations are still assumed unsealed for conservatism.

A compilation of all flooding events at nuclear power plants world-wide, including the US plants, has been collected from a number of sources.

10.15.6 Flood Area Naming Convention

Flood scenarios were characterized for each of the sources within a flood area that were not screened out from further evaluation. A decision tree was used to identify the flood damage states for each flood area. The following naming convention was used to identify the flood scenarios and facilitate integration of the flood scenarios into the PSA model.

The naming convention for flood damage states and flood scenarios is as follows:

%FL – Prefix for all flood initiators

eeeeee – Flood Area Number (pertains to the five digit AP1000 plant room number with a 6th position available if needed. If the 6th position is not needed, it shall contain an 'X')

B – Building designator (see below)

S## – Decision tree flood damage state

PPP – Three-letter designator that represents the flood source (see below)

N – One-letter designator that represents the affected train of the flood source (i.e., A – Train A, B – Train B, Z – Train A&B, or N – non-train designator)

M – Flood source failure mode (i.e., S – Spray, F – Flood, X – Major Flood, M – Maintenance Activity, or H – HELB)

Flood scenarios will be represented using the above naming convention. The scenario naming convention is represented below:

Position	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
	%	F	L	-	e	e	e	e	e	e	-	B	S	#	#	-	P	P	P	N	M

The designators used in this calculation note for the building and structures that required further evaluation are as follows:

T – Turbine Building
D – Diesel Generator Building
A – Auxiliary Building/Shield Building
X – Annex Building
R – Radwaste Building

Three letters are used to represent a flood source. The letters (i.e., PPP) and corresponding descriptions of flood sources (i.e., system) are shown in Table 10-53.

Using the above information, an example of the first flood scenario for the first flood area in the Auxiliary Building for a flood from the CCS (hypothetical) is: %FL-12101X-AS04CCSZF.

10.15.7 Diesel Generator Building Flood Scenario Characterization and Consequences

The Diesel Generator Building is a Class 2 structure which houses two standby diesel engine powered generators, the power conversion cycle equipment and the associated supporting equipment. These generators, separated by a three hour fire wall, provide backup power for plant operation in the event of the LOOP. There is no Class 1 equipment in the Diesel Generator Building. This building is located on a separate foundation at a distance from the Nuclear Island and other retained structures that will be further evaluated. The diesel generators are modelled in the PSA and are therefore PSA-related equipment. Review PSA indicated that no piping existed within the flood areas of this building for systems PSA. The diesels are cooled by using a closed loop cooling system cooled by the atmosphere. Any break or leakage from this would be insufficient to cause the failure of the opposite diesel generator due to the diesel generators being housed in independent compartments. Additionally, this same logic applies to any break of the Diesel Fuel Oil System. A break in any of these aforementioned systems would at most cause the loss of the one diesel generator. Loss of a single diesel generator would not cause a plant IE or an immediate plant shutdown, and the impact of such failure is already captured in the system model for the diesel generators. Therefore, the flood areas within the Diesel Generator Buildings are screened using the criteria of the ASME/ANS RA-Sa-2009 Standard SR IFSN-A15(c).

10.15.8 Annex Building Flood Scenario Characterization and Consequences

Most flood areas in the Annex Building do not contain any applicable flooding sources. Therefore, flood areas which lack any applicable flood sources will not be evaluated for scenario creation but will be retained to evaluate the impact of a flood from another flood area.

10.15.9 Auxiliary Building and Shield Building Flood Scenario Characterization and Consequences

From all the flood areas, most do not contain any applicable flooding sources. Flood areas that lack any applicable flood sources will not be evaluated for scenario creation but will be retained to evaluate the impact of a flood from another flood area (e.g., inter area propagation). 62 flood areas are retained in the Auxiliary Building.

Turbine Building Flood Scenario Characterization and Consequences

All 35 flood areas contain applicable flooding sources due to the fact that the Turbine Building is a large open area and exact location of piping cannot be easily identified.

10.15.10 Radwaste Building Flood Scenario Characterization and Consequences

The Radwaste Building is a non-Class 1, steel framed structure that houses low level waste processing and storage. The Radwaste Building includes facilities for segregated storage of various categories of waste prior to processing, for processing by mobile systems, and for storing processed waste in shipping and disposal containers. No Class 1 equipment is located in the Radwaste Building. Due to the lack of PSA-related equipment within this building, the insufficient inventory of the CCS to propagate to any building that contains PSA-related components, and due to the loss of the CCS system already being explicitly modelled, the Radwaste Building is screened out.

10.15.11 Determination of Scenario Frequencies

The flood area and pipe length information was used as input to the flooding IEFs. Flooding events were assumed to cause a direct failure of the ruptured system (except for spray events) and/or indirect failure of one or more PSA-related equipment (due to spray, submergence or steam) such that a reactor trip or plant shutdown is required. The reactor trip or plant shutdown may be a result of the system failure or the consequential failure of PSA-related equipment. This is significant for operating systems whose failure will cause a reactor trip. Depending on the location of a pressure boundary failure, certain systems may not cause a plant trip, and this was analysed on an individual basis.

There are twelve expansion joints located in the Turbine Building. Data from Reference 10.28 was examined and it was determined that the expansion joint failure rate data for CWS could be modified to produce failure rates more representative of this system. To do so, only failures from the service water systems were included. Once the applicable failures were identified, the ratio of these events to the total was used to adjust the given expansion joint failure rates (i.e., the fraction was multiplied by the failure rate).

10.16 Internal Fire Analysis

The Internal Fire Analysis is summarized based on the tasks performed using the guidance provided in NUREG/CR-6850 (Reference 10.55). Section 10.20.6 includes a summary of results for the Internal Fire model. The Fire PSA is dependent on the design information inputs, spatial information, and cable information which will evolve as the plant is constructed. Therefore, the internal fire analysis documented here is based on the best available information, assumptions and engineering judgement at the time of the analysis. The internal fire PSA also includes a limited set of refinements to demonstrate the overall process for the fire PSA which will also be further developed with future updates.

10.16.1 Plant Partitioning

The global plant analysis boundary (GPAB) was defined to include all areas of the plant associated with normal and emergency operation, support systems, and power production. The GPAB was then partitioned into fire compartments, which serve as the basic unit of analysis for the fire PSA. The general plan locations included in the internal fire analysis are: the annex building, auxiliary building (including the MCR), diesel generator building, radwaste building, turbine building, yard, and containment. The AP1000 fire compartments, their descriptions, fire frequency, and CDF are included in Table 10-54.

10.16.2 Component Selection

The component selection task identifies all initiating events, accident sequence models, and mitigating components to which a fire impact will be modelled in the fire analysis. The Internal Events analysis was reviewed for its applicability to the fire analysis. Additionally, events that were screened from the Internal Events analysis were re-evaluated for consideration in the fire analysis. The model was compared against the Fire Protection Analysis (Reference 10.56) to reconcile any differences in components, failure modes, high level success criteria, and system function differences. Single and multiple spurious events were reviewed for any modifications necessary for the fire analysis. Human actions, required instrumentation and high consequence components were all reviewed. The output of this task is a list of components that will be credited or screened in the fire PSA. Cable selection will be performed on those components credited in the fire PSA.

10.16.3 Cable Selection

Cable selection identified all cables associated with credited Fire PSA equipment and the routing/location of those cables.

The cable selection was performed by listing all cables linked to a Fire PSA piece of equipment that are directly linked or are in associated circuits. The cable selection criteria was developed to ensure that all cables that could affect the proper operation or cause the mal-operation of the Fire PSA equipment were identified and that these cables are properly related to the Fire PSA equipment whose functionality they could affect. To ensure all cables that could affect the operation of equipment are identified, the electrical or wiring diagrams were reviewed. The power, control, instrumentation, interlock, and equipment status indication cables related to the equipment were reviewed and documented. Electrical power requirements were reviewed during the Fire PSA cable selection task, and additional power supplies were identified and added to the Fire PSA equipment list as necessary.

The Fire PSA cable list provides a link between each cable and the associated Fire PSA component. The cable list also provides the information needed to identify the plant location (fire compartment and/or room) from the cable routing input.

10.16.4 Qualitative Screening

This task qualitatively screened fire compartments from further consideration if that fire compartment did not contain any credited Fire PSA equipment/cables or could not induce an automatic trip, a manual trip, or a mandate controlled shutdown prescribed by plant technical specifications. Three locations within the GPAB were qualitatively screened from the fire analysis: plant entrance, waste water retention basin and the simulator building.

10.16.5 Fire Risk Model

The fire PSA quantifies the fire risk model to calculate the fire-induced conditional core damage probability (CCDP) and Level 2 probabilities. The fire risk model integrated all model and data sources associated with each individual task. Model modifications were implemented to incorporate fire-induced initiating events, additional logic, equipment failures, and human failures.

10.16.6 Ignition Frequency

The AP1000 plant ignition source frequencies were developed based on apportioning generic fire frequencies developed from industry operating experience. The AP1000 plant Fire PSA used the updated generic ignition frequencies developed in NUREG-2169 (Reference 10.57). The fire scenario ignition frequency replaces the Internal Events initiating event frequencies during the fire PSA quantification. Fixed and transient ignition sources are reviewed and all fire compartments retained for quantitative analysis have a fire ignition frequency assigned.

10.16.7 Quantitative Screening

NUREG/CR-6850 (Reference 10.55) provides a framework and criteria for screening fire compartments from the fire analysis. The AP1000 plant fire analysis does not quantitatively screen any fire compartments. The CDF and LRF contributions of fire compartments meeting the quantitative screening criteria are retained in the fire PSA model.

10.16.8 Scoping Fire Modelling

This task identifies ignition sources that do not pose a threat to targets within a specific fire compartment. If that ignition source is a threat to a target, a severity factor is assigned which represents the probability that the target is damaged.

10.16.9 Detailed Circuit Failure Analysis

In the cable selection task, a generally conservative set of cables associated with each basic event is identified. The detailed circuit failure analysis is a refinement of the cable selection task. This task identified the specific cables that will induce the specific failures of concern for risk significant components.

10.16.10 Circuit Failure Likelihood Analysis

This task applied a conditional probability that a particular failure will occur given damage to a specific cable within a fire scenario.

10.16.11 Detailed Fire Modelling

In the detailed fire modelling task the single compartment analysis, main control room analysis, and multi-compartment analysis were performed. Single compartment analysis subdivides a fire compartment into a collection of fire scenarios, generally corresponding to individual ignition sources that are modelled to fail targets relatively local to the source. The MCR analysis assesses the risk associated with fires occurring inside the MCR including both abandonment and non-abandonment scenarios. Multi-compartment analysis assesses unsuppressed fire scenarios which grow to a size sufficient to generate a damaging hot gas layer and propagate to adjacent fire compartments.

The main control room scenarios, including abandonment and non-abandonment scenarios contribute less than 1 percent of the Fire CDF and Fire LRF. There are no locations in the plant which can result in the loss of control from the MCR. The abandonment and non-abandonment scenarios evenly contribute to the fire risk and are largely dependent on the ignition source whether abandonment may occur. If abandonment occurs, control is transferred to the remote shutdown room.

10.16.12 Fire Human Reliability Analysis

This task identified the HFEs to include in the Fire PSA, which included all HFEs from the internal events model required to mitigate fire-induced initiators and new HFEs developed specifically for fire. The Fire HRA was performed using NUREG-1921 (Reference 10.58) guidance. The fire HRA process accounted for fire impacts on credited cues, fire-generated conditions affecting the travel path to the action location, environmental conditions at the action location, and potentially increased stress due to the fire. HEPs were calculated based on a screening level approach which applied increased factors to the Internal Events HFEs. A process was developed to apply each relevant HFE to the fire cutsets and a dependency analysis was performed and applied to the model.

10.16.13 Fire Risk Quantification

This task quantified the fire-induced CDF and LRF for each fire scenario developed by the previous sections. The Fire PSA results, including significant fire risk contributors and fire risk insights, are identified and documented.

10.16.14 Fire Sensitivity Studies

This task performed sensitivity studies by varying the value of certain inputs to assess the impact on the model's output (CDF and LRF). Table 10-55 contains the results from various sensitivity studies on the internal fire results. The sensitivity studies were focused on the key sources of uncertainty of the model:

- Assumed cable routing,
    - Detailed cable routing information was not available for the site-specific systems. Not all fire scenarios linked to the assumed cable routing will be capable of failing these systems. The Fire PSA is moderately dependent on CDF and slightly dependent on LRF. The assumed routing for the offsite power supply system has the largest impact on the CDF reduction because the system is modelled to supply power to the start-up feedwater pumps to cool the steam generators.
- Severity factors,
    - Fires are unpredictable and assumptions are needed to model fire scenarios. The severity factor is the percentage of the ignition source expected to damage targets outside the source of origin. The Fire PSA is slightly dependent on the severity factor. This can be attributed to the scenarios being conservatively treated as full compartment burn or assigning very close distances between the ignition source and the nearest target.

- Detection time,
    - Manual fire detection is credited in the fire PSA for fire suppression. The detection time was reviewed to determine the uncertainty / sensitivity of the results to this input. The Fire PSA results are slightly dependent on the assumed detection time.
- Circuit failure likelihood probabilities,
    - The fire PSA incorporated conditional failure probabilities for various components. This sensitivity study demonstrates the importance of incorporating the circuit failure mode likelihood probabilities in the analysis for the Class-1 valves.
- Heat release rates,
    - The primary source of fire modelling uncertainty is the heat release rate, which directly affects the extent and timing of target damage. The Fire PSA utilised NUREG/CR-6850 (Reference 10.55) heat release rates which were higher for electrical cabinets than the latest industry guidance, which was released during the Fire PSA development. The Fire PSA electrical cabinets are currently conservative and have a moderate impact on the reported CDF and LRF.
- Automatic fire protection, and
    - Automatic detection is credited in the Fire PSA when ionization smoke detectors are present. Sprinkler systems (automatic suppression) are credited only when damaging hot gas layer temperatures are reached. The sensitivity demonstrates that crediting automatic detection and suppression has a moderate impact on CDF and a slight impact on LRF. Many scenarios are treated to damage all targets in the fire compartment and then propagate to adjacent compartments via the multi-compartment analysis. Automatic suppression is credited to mitigate hot gas layer formation and reduce the probability of fire propagating to adjacent fire compartments.
- Fire spread to multiple fire compartments.
    - The AP1000 plant fire PSA has a large number of small fire compartments modelled. The smaller fire compartments and conservative modelling of full compartment burn scenarios results in assumed multi-compartment propagation. Fires propagating to multiple fire compartments have a significant impact on the CDF and LRF. The impact is due to conservative assumptions, design reference point cable information, and the pre-operational state of the plant.

10.17 Winds, Floods, and Other External Hazards

10.17.1 Introduction

External hazards considered in the AP1000 NPP PSA are those hazards whose cause is external to all systems associated with normal and emergency operations situations. Some external hazards may not pose a significant threat of a severe accident. Some external hazards

are considered at the design stage and have a sufficiently low contribution to core damage frequency or plant risk.

Based on the list of external events requiring consideration from ASME/ANS-RA-Sa (Reference 10.61) and the preliminary qualitative screening guidelines provided in References 10.59, 10.60, and 10.62, the following list of external hazards were included for further consideration in the AP1000 NPP analysis. Note that Seismic Events and Internal Flooding are addressed separately in the AP1000 NPP PSA.

- High Winds
- Tornadoes
- External Flooding
- Transportation and Nearby Facility Accidents and Release of Chemicals from Onsite Storage
- Aircraft Impact
- External Fires
- Turbine Generated Missiles

These external hazards are addressed in this section.

Each potential site should re-evaluate the screening of each external hazard using site-specific information. Accordingly, if an external hazard cannot be screened out based on the criteria discussed in Section 10.17.2, the hazard may have to be modelled explicitly in the site-specific PSA.

Chapter 4 defines the site characteristics for which the AP1000 NPP is designed. It is very unlikely that sites with characteristics that fall within the AP1000 NPP site interface parameters defined in Chapter 4 will be unable to screen external hazards.

10.17.2 External Hazards Screening Analysis

Screening of external hazards that may impact the plant and contribute to risk can be accomplished using either qualitative or quantitative screening criteria outlined in ASME/ANS-RA-Sa (Reference 10.61). Any one of the following criteria provides an acceptable basis to qualitatively screen an external hazard:

- The event is of equal or lesser damage potential than the events for which the plant has been designed.
- The event has a significantly lower mean frequency of occurrence than another event, and the event could not result in worse consequences than those from the other event.
- The event cannot occur close enough to the plant to affect it.
- The event is included in the definition of another event.

- The event is slow in developing, and sufficient time is available to provide an adequate response.

External hazards which are not screened based on the qualitative criteria may be further assessed to determine if the following AP1000 NPP quantitative screening criteria can be satisfied:

- The current design-basis-hazard event cannot cause a core damage accident.
- The current design basis hazard event has a mean IEF of 1E-07 per year, and the mean value of the CCDP is assessed to be less than 1E-01.
- The CDF calculated using a bounding or demonstrably conservative analysis has a mean frequency less than 1E-08 per year.

The following equations can be used to determine if the hazard can be screened:

Equation 10-1

$$CDF = IEF * CCDP$$

Equation 10-2

$$IEF = CDF/CCDP$$

Where CDF is the annual core damage frequency, IEF is the annual IE frequency, and CCDP is the conditional core damage probability given the occurrence of the hazard.

Three CCDP cases were developed to assess risk associated with a particular external event based on the impact it may have on the plant. For example, high winds with speeds up to the AP1000 NPP operating basis may induce a LOOP, but are not expected to impact the availability of the Class 2 systems. High wind events with speeds that exceed the operating basis may induce a LOOP and also impact the Class 2 systems. Toxic chemical releases may impact the ability of the plant operators to respond to the event. The CCDPs for these scenarios as well as maximum site-specific IEFs that will support quantitative screening (i.e., would result in a CDF of 1E-08) were calculated. The results are presented in Table 10-58.

10.17.2.1 High Winds

As discussed in Chapter 4, the AP1000 NPP operating basis wind speed is 233.35 km/hr (145 mph). This value is assumed to be the maximum wind speed that will not challenge the non-Class 1 structures. The design basis wind speed for tornados is 482.80 km/hr (300 mph). This value is assumed to be the maximum wind speed that will not challenge the Class 1 structures. The structures protecting Category-A features of the AP1000 plant are designed for extreme winds and missiles associated with these winds. As long as the wind speed is less than these design basis wind speeds, the Category-A features of the AP1000 plant will be unaffected. In the unlikely event that the winds exceed the design values, then the integrity of the Class 1 structures may be compromised. The structures protecting non-Category-A safety functions of the AP1000 plant are designed according to Uniform Building Code or International Building Code and have some level of protection against seismic and high wind events. As long as the external event winds are less than the operating basis winds [233.35 km/hr (145 mph)], the non-Category-A features of the AP1000 plant will be unaffected. If the winds exceed the operating basis values, then the integrity of the non-Class 1 structures may be compromised.

High wind events that fall below the AP1000 NPP operating basis wind speed have the potential to induce a LOOP but would not impact any other SSCs. However, it is assumed that the site switchyard and surrounding grid are designed to withstand wind events up to the site-specific basic wind speed and that as long as the external winds are less than this value, the reliability of the switchyard and surrounding grid will be unaffected. The frequency of high wind events with speeds that exceed the site-specific basic wind speed but are below the AP1000 NPP operating basis wind speed of 233.35 km/hr (145 mph) should be determined, and the occurrence of a LOOP would be assumed. These events are not screened, but it is assumed that their frequency of occurrence is accounted for in the internal events PSA as a weather-induced LOOP.

High wind events that exceed the plant operating basis wind speed have the potential to induce a LOOP with a concurrent failure of non-Class 1 components which are not housed in Seismic Category 1 buildings.

The methodology for analysing plant risk due to high winds that exceed the AP1000 NPP operating basis wind speed is to perform a bounding or demonstrably conservative analysis to determine if the quantitative screening criterion can be met. For the AP1000 NPP, the quantitative screening criterion is that the total calculated CDF due to high winds has a mean frequency less than 1E-08 per year.

For a high wind event that exceeds the AP1000 NPP plant operating basis wind speed of 233.35 km/hr (145 mph) up to the design basis wind speed of 482.80 km/hr (300 mph), it can be conservatively assumed that the event results in a LOOP coincident with unavailability of the non-Class 1 systems. The CCDP for this scenario (CCDP Case 2) is 4.3E-06. Using Equation 10-2, the maximum IEF is determined to be 2.3E-03 per year.

Similarly, the maximum IEF for a high wind event resulting in the wind-induced unavailability of all non-Class 1 systems and all Class 1 systems (wind speed greater than 482.80 km/hr [300 mph]) can be estimated at 1E-08 per year, assuming a CCDP of 1.0. Due to the low frequency, high wind events above 482.80 km/hr (300 mph) can be screened from the total maximum IEF for high winds, and thus the total maximum IEF for high winds is determined to be 2.3E-03 per year.

The frequency of “straight line” high wind events can be determined based on information in historical weather datasets available at the US National Oceanic and Atmospheric Association (NOAA) National Climatic Data Centre website for a selected weather station surrounding the site. The annual exceedance frequency for a specific wind speed can be predicted using the Gumbel distribution which is a special case of the generalized extreme value distribution. This distribution is commonly used for predicting extreme value frequencies for parameters such as wind speed based on annual maximum observations.

High winds with wind speeds that exceed 233.35 km/hr (145 mph) are screened as a contributor to total plant risk if the total site-specific IEF is less than 2.3E-03 per year. This is a conservative result, and it is unlikely that sites selected based on the siting parameters in Chapter 4 would not be able to meet this criterion. However, sites that do not meet the screening criterion may need to perform more detailed analyses and include this hazard in the site-specific PSA.

High winds can also result due to hurricanes in coastal regions. Per the description of Table 10-60, Saffir-Simpson Scale (Hurricane), no hurricanes are expected to reach 482.80 km/hr (300 mph) winds and challenge the Class 1 systems; however, Category 3, Category 4, and Category 5 hurricane winds do exceed the operating basis of the AP1000 NPP. Additionally, the annual mean risk due to a Category 1, Category 2, and Category 3

hurricane-induced LOOP should be explicitly considered independent from the internal events PSA weather-induced LOOP due to the damage potential associated with the hurricanes. Site-specific IEFs for high winds associated with hurricanes and other causes should be determined based on information in historical weather datasets to determine if this hazard can be screened.

10.17.2.2 Tornados

Per the Operational Enhanced Fujita Scale for Tornados found on the Fujita Tornado Scale Intensity Wind Speed Relationship (Table 10-59), no tornados are expected to exceed the design basis wind speed of 482.80 km/hr (300 mph); however, EF3, EF4, and EF5 tornados do exceed the operating basis wind speed of the AP1000 NPP. Additionally, the annual mean risk due to an F0, F1, and F2 tornado-induced LOOP is explicitly considered independent from the internal events PSA weather-induced LOOP due to the damage potential associated with the tornado.

The methodology for analysing plant risk due to tornados is to perform a bounding or demonstrably conservative analysis to determine if the quantitative screening criterion can be met for the overall tornado hazard risk due to F0, F1, F2, F3, F4, and F5 tornados. For the AP1000 NPP, the quantitative screening criterion is that the total calculated CDF due to tornados has a mean frequency less than 1E-08 per year.

Using Equation 10-2, the maximum IEF for a F0, F1, and F2 tornado can be estimated at 2.6E-02 per year based on CCDP Case 1 (CCDP = 3.8E-07) for a tornado-induced LOOP.

Similarly, the maximum IEF for a F3, F4, and F5 tornado can be estimated at 2.3E-03 per year based on CCDP Case 2 (CCDP = 4.3E-06) for a tornado-induced LOOP coincident with unavailability of the non-Class 1 systems.

The total maximum IEF for tornado hazard is determined to be 2.8E-02 per year.

An analysis of tornado climatology in the United States is provided in US NRC NUREG/CR-4461 (Reference 10.64). The results include annual probabilities that wind speed exceeds a specified value given that a tornado strikes a structure. The expected annual strike probability for a structure the size of the AP1000 NPP ranges from approximately 1E-03 in the Central United States to approximately 1E-05 in the Eastern and Western United States. The methodology in US NRC NUREG/CR-4461 can be used to determine site-specific IEFs for tornados which are expected to fall within this range for most sites in the United States.

10.17.2.3 External Flooding

An external flooding analysis is performed to verify that any significant contribution to core damage frequency resulting from plant damage caused by storms, dam failure, and flash floods is considered. The analysis for external floods begins with an examination of the design basis for the plant, which is documented in PCSR Chapter 4. The AP1000 NPP is protected against floods up to the 100 m (100 feet) level. The 100 m (100 feet) level corresponds to the plant ground level. From this point, the ground is graded away from the structures. Thus, water will naturally flow away from the structures. Additionally, all seismic Category I SSCs are designed to withstand the effects of flooding. The seismic Category I SSCs below grade (below ground level) are protected against flooding by a waterproofing system. Unavailability of non-Class 1 SSCs that may potentially be impacted by external flooding events would not have a significant impact on total plant risk.

Sites with site characteristics that fall outside of the AP1000 NPP site interface parameters may be susceptible to external flooding that would exceed the 100 meter (100 feet) plant ground level are evaluated on a site-specific basis. Such sites may be vulnerable to external flooding due to hurricane surge water, dam failure, and flash floods.

The methodology for analysing plant risk due to external flooding is to perform a bounding or demonstrably conservative analysis to determine if the quantitative screening criterion can be met. For the AP1000 NPP, the quantitative screening criterion is that the total calculated CDF due to external flooding has a mean frequency less than 1E-08 per year.

For an external flooding event that exceeds the 100 meter (100 feet) level, it can be conservatively assumed that the event results in a LOOP coincident with unavailability of the non-Class 1 systems (CCDP Case 2). Using Equation 10-2 the maximum IEF for an external flooding event that exceeds the 100 meter (100 feet) level is determined to be 2.3E-03per year.

External flooding is screened for the site as a contributor to total plant risk if the site-specific IEF is less than this value. Information such as meteorological data for the site, historical flood height, and frequency data is used to determine the site-specific IEF. It is very unlikely that sites selected based on the siting parameters in Chapter 4 would not be able to meet this criterion. However, sites that do not initially meet the screening criterion could focus attention on areas, which due to their location and grading, may be susceptible to external flood damage. Site-specific information on such items as dikes, surface grading, locations of structures, and locations of equipment within the structures can be utilized to remove some of the conservatism in the initial evaluation. The resultant CCDP may be reduced and lead to meeting the quantitative screening criterion.

10.17.2.4 Transportation and Nearby Facility Accidents and Release of Chemicals from Onsite Storage

Transportation and nearby facility accidents and release of chemicals from onsite storage could result in an explosion, a flammable cloud or a toxic chemical release that could affect safe operation of the plant. A site-specific evaluation of potential accidents related to transportation routes and other facilities in the vicinity of the site is performed. The types of transportation routes to be considered include roads, railroads, and waterways. The types of facilities to be considered include industrial sites and military installations. Additionally, a review of chemicals stored onsite is performed. Many of the chemicals can be excluded from further consideration due to their properties (e.g., low volatility or low toxicity) or due to the relatively small quantities that are stored.

Sites within 8.05 kilometres (five miles) of transportation routes and industrial or military facilities need to consider potential accidents on roads, railroads, and waterways, and at nearby facilities. Evaluation of roads encompasses large truck traffic and other commercial carriers, and evaluation of waterways encompasses ship and barge traffic. The types of nearby facilities to be considered include industrial sites, other nuclear power plants at multi-unit sites, pipelines, and military installations. Hazardous materials that travel on nearby transportation routes or that are located at nearby facilities are identified and analysed based on volume and distance from the plant to verify they would not affect safe operation of the plant. Accidents on transportation routes or at nearby facilities have the potential to result in the release of toxic chemicals which may affect control room habitability, or explosions that could damage plant equipment.

A release of toxic materials into the atmosphere may compromise the safety of the plant operators, resulting in reduced operator reliability. The potential for this is determined based on site-specific evaluation of the types and volumes of material being transported or stored at nearby facilities. If the maximum calculated control room concentration subsequent to a postulated accident is less than the toxicity limit defined in US NRC Regulatory Guide 1.78 (Reference 10.65) for the material being analysed, then the hazard can be screened as a risk contributor.

The hazard could also be screened if it can be shown that the calculated CDF for such an event is less than 1E-08 per year. For sites where the toxicity limit is exceeded, the ability of operators to function may be impacted, but a toxic release would not directly lead to failure of plant equipment. The risk impact for this scenario can be calculated by assuming the occurrence of a general transient (reactor trip) with coincident failure of all operator actions included in the model. Failure of all PSA-credited operator actions obviates the need to evaluate specific toxic release events with respect to differences in the type and amount of material released and duration of the release. The CCDP for this scenario (CCDP Case 3) is 9.0E-07. Using Equation 10-2, the maximum total IEF for the hazard is determined to be 1.1E-02 per year. Transportation accidents, nearby facility accidents, and release of chemicals from onsite storage are screened separately for the site as a contributor to total plant risk if the total site-specific IEF for each hazard is less than this value. Sites that do not meet the screening criterion may need to perform more detailed analyses.

The above analysis is conservative as it does not take credit for the AP1000 NPP design feature which provides an additional level of defence against toxic airborne material. With advanced warning, the operators may actuate the passive control room habitability system. This system isolates the control room from normal HVAC and actuates a separate system supplied from compressed air containers. The compressed air slightly pressurizes the control room above atmospheric pressure, preventing the entrance of toxic material in the control room. This system is available for 72 hours, which is adequate time to withstand the event.

Explosions due to a transportation accident or release of chemicals from onsite storage, or at a nearby facility could result in an initiator as well as damage to mitigating equipment at the plant. Potential explosions to be considered include those that may occur coincident with the accident or subsequent to the accident due to a vapour cloud that may be generated as a result of the accident. The potential for an explosion is determined based on site-specific evaluation of the types and volumes of material being transported or stored onsite or at nearby facilities. For each postulated explosion, the safe equivalent distance beyond which the blast pressure would be less than 6.89kPa (1 psi), which is specified in US NRC Regulatory Guide 1.91 (Reference 10.66), is calculated. Evaluation of explosions due to a flammable vapour cloud would conservatively assume that the explosion occurs at the outer edge of the vapour cloud closest to the plant. If the distance between the point of the explosion and the plant is greater than the calculated safe equivalent distance, the hazard is screened. Sites that do not meet the screening criterion may need to perform more detailed analyses. These analyses should account for the location of the explosion relative to the plant and the potential impact on plant SSCs to calculate appropriate IEFs. Equation 10-1 and Equation 10-2 can then be used with IEFs and appropriate CCDPs to determine if the hazard can be screened on a quantitative basis using the AP1000 NPP screening criteria.

10.17.2.5 Aircraft Impact

Sites in the vicinity of airports and airways need to consider potential aircraft impacts. An aircraft impact would not inhibit the AP1000 NPP passive core cooling capability and would not impact containment integrity. However, aircraft impact could result in a LOOP or loss of some non-Class 1systems.

An evaluation of each nearby airport would account for the distance between the airport and the plant, and the total number of projected flight operations (take-offs and landings) to determine if the annual CDF for the airport is less than the AP1000 NPP criteria of 1E-08 per year.

An evaluation of airways is performed to determine the in-flight crash rate per kilometre for each type of aircraft using the airway, the number of flights of each type per year along the airway, and the airway width to determine the total annual frequency of an aircraft crashing into the site. The risk due to aircraft impacts is screened to determine if the total annual CDF for airplane crashes for the site is less than the AP1000 NPP criteria of 1E-08 per year.

US NRC Review Standard (RS)-002, Section 3.5.1.6 (Reference 10.68), provides a methodology for calculating the hazard frequency for airports and airways in the vicinity of the site. Sites where the total IEF for aircraft impact is greater than the 1E-07 per year screening criteria could conservatively assume that the impact results in a LOOP coincident with unavailability of the non-Class 1 systems. The CCDP for this scenario (CCDP Case 2) is 4.3E-06. Using Equation 10-2, the maximum total IEF for the hazard is determined to be 2.3E-03 per year. Aircraft impacts are screened as a contributor to total plant risk if the total site-specific IEF for this hazard is less than this value. Sites that do not meet the screening criterion may need to perform more detailed analyses.

10.17.2.6 External Fires

External fires in the vicinity of site could lead to high heat fluxes or smoke, and non-flammable gas or chemical-bearing clouds from the release of materials as a consequence. A site-specific evaluation of potential accidents that may result in forest fires, brush fires, and fires due to other sources is performed. Based on the postulated distance to the fire source, rate of spread, and duration, emission concentrations in the control room air intake would be calculated. These results are used to determine if the amount of toxic combustion products released poses a hazard to the control room operators. The heat flux and resultant temperature rise on plant structures due to an external fire should also be evaluated to determine if the Class-1 structures experience any thermal damage, based on the distance from the fire. If the analysis shows that the concentrations do not exceed toxicity limits, then external fires can be screened as a risk contributor. The hazard could also be screened if it can be shown that the calculated IEF for such an event is less than 1E-08 per year. For sites where the IEF screening criteria is not met and the toxicity limit is exceeded, the ability of operators to function may be impacted, but emissions from a fire would not directly lead to failure of plant equipment. The risk impact for this scenario can be calculated similar to how it was done for chemical releases as described in Section 10.17.2.4. This would be done by assuming the occurrence of a general transient (reactor trip) with coincident failure of all operator actions included in the model. The CCDP for this scenario (CCDP Case 3) is 9.0E-07. Using Equation 10-2, the maximum total IEF for the hazard is determined to be 1.1E-02 per year. External fires are screened for the site as a contributor to total plant risk if the total site-specific IEF for each hazard is less than this value. Sites that do not meet the screening criterion may need to perform more detailed analyses.

The above analysis is conservative as it does not take credit for the design of the AP1000 NPP control room HVAC design which includes smoke detectors. Any smoke detected from an onsite or offsite external fire would initiate isolation of the control room HVAC prior to toxicity limits being exceeded. With advanced warning, the operators may actuate the passive control room habitability system. This system isolates the control room from normal HVAC and actuates a separate system supplied from compressed air containers. The compressed air slightly pressurizes the control room above atmospheric pressure, preventing the entrance of toxic material in the control room. This system is available for 72 hours, which is adequate time to withstand the event.

10.17.2.7 Turbine Generated Missiles

PCSR Chapter 10, subsection 10.2.2, states that the AP1000 plant turbine-generator and associated piping, valves, and controls are located completely within the Turbine Building. There are no Class 1 systems or components located within the Turbine Building. An analysis was performed which concluded that the probability of destructive overspeed condition and missile generation, assuming the recommended inspection and test frequencies, is less than 1.00E-05 per year. In addition, orientation of the turbine generator is such that a high-energy missile would be directed at a 90 degree angle away from Class 1 structures, systems, or components. Failure of turbine-generator equipment does not preclude safe shutdown of the reactor. The turbine-generator components and instrumentation associated with turbine-generator overspeed protection are accessible under operating conditions.

US NRC Regulatory Guide 1.115 (Reference 10.67) provides a means to calculate the probability of failure of essential equipment because of turbine-generated missiles based on protection provided by turbine orientation. This probability is expressed as the product of the following three items:

- P1-the probability of turbine missile generation resulting in the ejection of turbine disk (or internal structure) fragments through the turbine casing
- P2-the probability of ejected missiles perforating intervening barriers and striking essential equipment
- P3-the probability of essential equipment that are struck failing to perform their Category-A functions

Mathematically, the probability of failure of essential equipment because of turbine missiles can be expressed as follows:

- $P4 = P1 \times P2 \times P3$

P4 is limited to less than 1.00E-07 per year, which US NRC Regulatory Guide 1.115 considers to be an acceptable risk rate for the loss of essential equipment from a single event. Considering P1, P2, and P3 in the placement of essential equipment, detailed strike and damage analyses have shown that separation of redundant equipment and special attention to turbine valve reliability have accomplished the objective of ensuring a low risk of damage from turbine missiles. As noted previously, there are no Class 1 systems or components located within the Turbine Building. Based on this, the AP1000 plant is considered to have a favourable turbine orientation and P2 x P3 can be credited to be 10^{-3} per Table 1 of US NRC Regulatory Guide 1.115. Combining this with the frequency of turbine missile generation frequency yields a value of P4 < 1.00E-08 per year. Although no Category-A functions could be impacted by this event, non-Category-A, defence-in-depth mitigating functions could be

adversely affected. Therefore, only the Class 1 systems are credited for this hazard. Using CCDP Case 2 for a LOOP coincident with failure of the non-Class 1 systems, the risk due to a turbine-generated missile can be conservatively estimated using Equation 10-1 as 4.32E-14 per year.

Based on these evaluations, the impact from a turbine-generated missile can be screened out from further considerations.

10.17.3 Conclusion

The risk due to external hazards is low for the AP1000 NPP design for sites that meet the siting parameters in PCSR Chapter 4. The AP1000 NPP design is shown to be highly robust against the external hazards discussed in this section. The design is resilient against high winds, external floods, and other external hazards that could potentially have an impact on the safe operation of the plant. Each potential site should re-evaluate the screening of each external hazard using site-specific information. Accordingly, if an external hazard cannot be screened out based on the criteria discussed in Section 10.17.2, the hazard may have to be modelled explicitly in the site-specific PSA.

The following conclusions and insights are derived from the AP1000 NPP external hazards assessment for events at power:

1. High winds were shown be of low risk to the AP1000 NPP design for sites that satisfy the siting parameters in PCSR Chapter 4. High wind events that exceed the plant operating basis wind speed of 233.35 km/hr (145 mph) have the potential to induce a LOOP with a concurrent failure of non-Class 1-related components; however, the frequency of such events is likely sufficiently low at most sites such that this hazard can be screened.

2. Tornados were shown to be of low risk to the AP1000 NPP design for sites that satisfy the siting parameters in PCSR Chapter 4. F0, F1, and F2 tornados have the potential to induce a LOOP, and F3, F4, and F5 tornados have the potential to induce a LOOP concurrent with the failure of non-Class 1components; however, the frequency of such events is likely sufficiently low at most sites such that this hazard can be screened.

3. The AP1000 NPP is designed to flooding levels described in PCSR Chapter 4. The site selection criterion provides that, for an accident that has potential consequences serious enough to affect the safety of the plant to the extent that US Regulation 10 CFR 50.34 guidelines are exceeded, the annual frequency of occurrence is significantly less than the maximum IEF required for quantitative screening as discussed in Section 10.17.2.3.

4. Transportation and nearby facilities accidents are likely able to be screened based on not being close enough to the plant to affect safe operation. Many of the chemicals that are stored onsite are likely able to be screened from further consideration due to their properties and/or the relatively small quantities that are stored.

5. An aircraft impact would not inhibit the AP1000 NPP passive core cooling capability and would not impact containment integrity. Aircraft impact could result in a LOOP or loss of some non-Class 1 systems; however, site selection criterion should demonstrate that the frequency of impact is sufficiently low and that this hazard can be screened.

6. External fires are likely able to be screened based on not being close enough to the plant to affect safe operation.

7. Turbine-generated missiles can be screened based on the bounding or demonstrably conservative analysis, which demonstrates a mean CDF less than 1E-08 per year.

A site-specific review of the generic PSA should be conducted to verify that the assumptions in the PSA bound the site-specific conditions for the applicant's site.

10.18 Seismic Margins Assessment (SMA)

The SMA has not been updated since APP-PRA-GSC-027 (Reference10.78).

A PSA-based seismic margin assessment (SMA) was performed for the AP1000 standard design and presented in Reference 10.1, Chapter 55.

The AP1000 design SMA was performed before the development of the American National Standards Institute/American Nuclear Society (ANSI/ANS) 58.21 (Reference 10.7) standard on external events PSA. Nevertheless, the adopted methodology is essentially consistent with the ANSI/ANS standard. Seismic-induced event trees were constructed, starting with structural or systems failures that could be postulated to occur as a result of a seismic event. The analysis considered all structures and components required to maintain the plant in a safe stable state (event tree top events). The maximum peak ground acceleration (pga) that gave at least 95 percent confidence of no more than 5 percent failure probability, i.e., representing high confidence of low probability of failure (HCLPF), was determined for the following:

- Each seismic event tree initiator
- Each seismic event tree core damage sequence
- The entire plant

To demonstrate margin over the design safe shutdown earthquake (SSE), a review-level earthquake was set at 1.67 times the SSE. This is consistent with the requirements of the US NRC (Reference 10.8). Since the AP1000 plant SSE is defined at 0.3g pga, the review-level earthquake for the AP1000 plant is set at 0.5g pga.

The following main assumptions are used in the development of the PSA-based seismic margins assessment model:

- The seismic event is assumed to occur while the plant is operating at full power.

- LOOP is assumed, since the ac power equipment is not seismic Category 1.

- No credit is taken for onsite emergency ac (diesel generators).

- No credit is taken for Class 2 systems.

The seismic IEs and event trees were established using a hierarchical approach to ensure that events presenting the greatest challenge to plant structures and systems were considered first.

All the structures or components postulated to initiate the accident sequences by their failure and needed to achieve safe shutdown following any such IE have been assessed. All the equipment and/or structures that are potentially driving the overall plant HCLPF are shown to

have an HCLPF value at or above 0.5g (and in most cases greater). Limiting components include the fuel and the pressuriser structure.

The min-max method is used on the IE HCLPF values to calculate the plant HCLPF values, which means that the maximum HCLPF value among the systems, structures, or components (SSCs) involved in a cut-set drive the cut-set HCLPF. The minimum, among all the relevant cut-sets, drives the HCLPF for the sequence, event tree, and overall plant. The AP1000 design PSA-based SMA confirmed that the plant-level HCLPF is 0.5g, thus, meeting the goal set by SECY-93-087 (Reference 10.8).

Multiple methods have been used to evaluate the HCLPF values for the SSCs assessed in the AP1000 design SMA. These include conservative deterministic failure margin methodology, probabilistic fragility analyses, other deterministic approaches, EPRI ALWR URD (Reference 10.3) recommended generic fragility data, design margin, code requirements, and test margins inherent to the seismic qualification testing.

Reference 10.7, Appendix D, describes a simple method to gain risk insights from the results of an SMA. Consideration of the seismic hazard curve allows a relation to be drawn between the established plant HCLPF value and a seismic return frequency. Reference 10.9, Figure 6, indicates that for a location with average UK seismicity, the return frequency of a seismic event of 0.5g is about 5E-6/yr. (Taking a high seismicity location could increase this by a factor of about 2.) Taking into account the definition of HCLPF, a further factor could be applied to allow for the actual probability of failure in the review earthquake being somewhat lower than 1, resulting in a possible estimate of between 1.E-7 and 1.E-6/yr, which is similar in magnitude to the CDF from internal events at power. More recent work by the British Geological Survey (Reference 10.10) indicates that the UK average seismic hazard curve (Reference 10.9) is about one order of magnitude too conservative. At this stage, this is taken only to add confidence to the above conclusions, since revised seismic assessment will be required at a later stage in the application process, and the seismic hazard curve for the specific location can then be applied.

The topic of seismic events is dealt with in more detail in Chapter 12.

10.19 Spent Fuel Pool Risk Assessment

The Spent Fuel Pool Risk Assessment has not been updated since UKP-GW-GL-743 (Reference 10.2) and is based on the APP-GW-GL-022 (Reference 10.1) internal events PSA.

Assessment of Spent Fuel Damage Frequency

A SFP PSA was conducted to estimate the AP1000 SFP fuel damage frequency (FDF) (Reference 10.2). The FDF of the AP1000 SFP was quantified to be 1.59E-10 occurrence per year using fault tree analysis, and includes the following events leading to potential fuel uncover/large radiation release:

- Loss of complete cooling during normal conditions (5.76E-12/yr.)
- Loss of complete cooling at refuelling only outage and at-power just after refuelling (1.55E-12/yr.)
- Loss of complete cooling at refuelling full core off-loads (8.19E-13/yr.)
- Loss of offsite power sequences leading to station blackout (2.69E-11/yr.)

  - Normal conditions
  - Refuelling only outage and at-power just after refuelling
  - Refuelling full core off-load

- Loss of component cooling/service water system (1.24E-10/yr.)

The main contributor to the failure of the AP1000 SFS is the loss of component cooling/service water system due to failure of the CCS or the SWS. The CCS provides cooling to both SFS HXs and the normal RNS HX. The RNS can provide backup cooling of the SFP. Note that the AP1000 design provides an alternate means of cooling the RNS HX using fire water.

Possible contribution to FDF from fuel transfer canal drain line rupture is not considered in this analysis. The level of water in the fuel transfer canal is closely monitored during fuel transfer operations. If a loss of water level is noted, fuel transfer is halted, and the one fuel rod assembly being moved is placed where impact of a loss of water level is minimised.

The CCF analysis uses the beta factor method, and follows the approach described in Section 29.3.1 of the UK AP1000 PSA report (Reference 10.1). The human error analysis uses the THERP method (Reference 10.6).

In the worst scenario of a seismic event (assuming water in the pool is initially drained to the level of the SFP cooling system connection simultaneous with a station blackout) immediately following a refuelling full core off-load, water in the pool could reach saturation in 1.4 hours. The time before reaching saturation during a seismic event at-power following a refuelling is at least 6.5 hours. The operator has enough time to align the different cooling and makeup sources if needed.

The EPRI guidance for fault tree modelling of SSIEs (Reference 10.11) has been used. The time-dependent failures that start the sequence of events that cause the IE are assigned a mission time of one year (for example, the loss of operating SFS train A during normal conditions). This ensures that the quantification results are expressed as a frequency instead of a probability. The time-dependent secondary failures in the sequence of events that cause the IE are assigned a mission time of 24 hours (for example, the loss of the standby SFS train B during normal conditions). A multiplier representing the fraction of time the system operates in a given configuration over a year is added at the top of each SSIE.

This quantification for FDF is determined by a PSA model that assumes that fuel damage occurs when makeup water cannot be provided. The AP1000 Abnormal Operating Procedures include mitigation actions for loss of SFP cooling that are credited in the current PSA analysis, including recovery of the failed SFP cooling function and water addition to the SFP using the fire water system to prevent fuel uncovery. These additional recoveries, quantified in the PSA, are quite possible due to the existence of alarms to alert the plant operating staff to the loss of SFP cooling, the existence of proceduralised actions to mitigate the loss of SFP cooling and SFP inventory loss, and the large amount of time between the alarm and the actual fuel uncovery. Thus, source term addition because of the fuel damage frequency could be overestimated by the quantified fuel damage frequency.

AP1000 SFP is located outside the reactor containment building, and fuel damage in the SFP is, therefore, considered to result in a release outside containment. The comparable LRF quantified in the “UK AP1000 PSA” is 1.95E-08 events per year (Reference 10.1). The AP1000 Level 3 PSA analysis was performed using the LRF results from the Level 1 and Level 2 PSA (Reference 10.1). The FDF value is 0.82 percent of the LRF value.

The fission product release for an SFP fuel damage event would be significantly different than the fission product release assumed for an at-power core damage event such as that analysed in the AP1000 Level 3 PSA. The differences and their effect on consequences can be characterised as follows:

- SFP fission product inventory would consist of long-lived radionuclides as opposed to the mix of short- and long-lived radionuclides for an at-power core damage event. When evacuation is considered in the Level 3 analysis, the offsite consequences of a large release are dominated by the shorter-lived radionuclides.

- The SFP fuel damage fission product inventory is primarily non-volatile species, some of which will deposit within the spent fuel building and not be released to atmosphere while others will deposit rapidly in areas within the controlled site area. Thus, the offsite consequences will be reduced compared to a large release from an at-power core damage event.

- The SFP fuel damage inventory will include multiple cores as opposed to a single core for a large release from an at-power event. This will result in the potential release of larger quantities of long-lived radionuclides compared to the large release from an at-power condition.

- The SFP fuel damage event may take place in an oxidizing environment as opposed to a reducing environment for an at-power core damage event. This can result in different radionuclide chemical species being formed. WASH-1400 analyses showed that a large release from a core damage accident in an oxidizing environment can have slightly greater health consequences compared to a large release from a core damage event in a reducing environment.

Due to the very low fuel damage frequency, the potential releases from spent fuel damage are below the UK numerical targets.

10.19.1 Assessment of Spent Fuel Pool Boiling Frequency

In addition to the FDF quantified for the SFP, an assessment of the AP1000 SFP boiling frequency has also been conducted for the UK AP1000 plant (Reference 10.12), which took into account the latest design changes relative to the systems that interact with the SFP. The boiling frequency of the AP1000 SFP was quantified to be 4.42E-04 occurrence per year using a similar fault tree analysis approach for the estimate of the FDF, and includes the following events:

- Loss of offsite power with plant trip and subsequent failure of both trains of the onsite standby diesel generators (with an estimated frequency of 7.69E-06/yr)

- Loss of both trains of SFS, plus the loss of both RNS trains

- Loss of both trains of CCS

- Loss of both trains of SWS

The SFP boiling frequency contribution from loss of offsite power is calculated by multiplying the frequency of loss of offsite power used in Reference 10.38 (3.59E-02/yr) by the probability of failing to recover offsite power in 8 hours, and by the probability of failure of the diesels to start and run for 24 hours.

An updated frequency for loss of the CCS /SWS (Reference 10.13) was used to estimate the SFP boiling frequency.

The SFP boiling contribution from pipe breaks is 2.77E-06/yr (Reference 10.12).

The loss of SFP cooling due to loss of the SFS and RNS trains documented in the FDF estimate (Reference 10.14) was modified to remove unnecessary conservatism and simplifications in the model of the defence-in-depth systems, and to reflect the AP1000 plant 50 Hz standard design as updated, including for example the capability to align the fire protection system to provide an alternative means of cooling for the RNS and SFS heat exchangers in case of loss of both CCS/SWS trains. The SFP boiling contribution from the loss of SFS and RNS

The modification also corrected some errors in the FDF model, and used reliability data from NUREG/CR-6928 (Reference 10.15).

10.20 PSA Results and Insights

10.20.1 Introduction

This section summarizes the use of the AP1000 NPP PSA in the design process, PSA results and insights, plant features important to reducing risk, and PSA input to the general design assessment process.

The AP1000 NPP is expected to achieve a higher standard of severe accident safety performance than current operating plants, because of the adoption of simple passive Class 1 SSCs and because both prevention and mitigation of severe accidents have been addressed during the design stage, taking advantage of PSA insights, PSA success criteria analysis, severe accident research, and severe accident analysis. Since PSA considerations have been integrated into the AP1000 NPP design process from the beginning, many of the traditional PSA insights relating to current operating plants are not at issue for the AP1000 NPP. The Level 1, Level 2, and Level 3 results show that addressing PSA issues in the design process leads to a low level of risk. The PSA results indicate that the AP1000 NPP design meets the higher expectations and goals for new generation passive PWRs.

The CDF and LRF for at-power internal events (excluding seismic, fire, and flood events) are 1.7E-07 events per reactor-year and 1.7E-08 events per reactor-year, respectively. These frequencies are at least two orders of magnitude less than a typical pressurized water reactor plant currently in operation. This reduction in risk is due to many plant design features, with the dominant reduction coming from highly reliable and redundant passive Class 1 systems that impact both at-power and shutdown risks. These passive systems are much less dependent on operator action and support systems than plant systems in current operating plants.

The CDF and LRF for at-power internal flood events are 4.4E-09 events per reactor-year and 1.2E-09 events per reactor-year, respectively. These frequencies are also at least two orders of magnitude less than a typical pressurized water reactor plant currently in operation. This reduction in risk is due to consideration of potential flood sources and propagation paths during the design of the AP1000 NPP structures that contain Class 1 equipment as well as the use of simple passive SSCs that are less dependent on support systems than systems in current operating plants.

The CDF and LRF for at-power internal fire events are 6.7E-07 events per reactor-year and 5.6E-08 events per reactor-year, respectively. This includes contribution from all credible

fire sources and unscreened fire compartments within the fire PSA global plant analysis boundary.

As discussed in Section 10.16, the external events evaluation concludes that there are no external hazards with an initiation frequency high enough to require further quantification.

The PSA based Seismic Margin Assessment (Section 10.18) provides results in terms of acceleration to show the plant is sufficiently robust for seismic events.

A synopsis of the insights gained from the PSA about the AP1000 NPP design includes:

- The AP1000 NPP design benefits from the high level of redundancy and diversity of the passive Class 1 systems. The passive systems have been shown to be reliable; their designs are simple so that a limited number of components are required to function.

- The AP1000 NPP is less dependent on non-Class 1 systems than current plants or advanced light water reactor evolutionary plants.

- The non-Class 1 support systems (ac power, component cooling water, service water, and instrument air) have a limited role in the plant risk profile because the passive Class 1 systems do not require cooling water or ac power.

- The AP1000 NPP is less dependent on human actions than current plants or advanced light water reactor evolutionary plants. Even when no credit is taken for operator actions, the AP1000 NPP meets the United States Nuclear Regulatory Commission (US NRC) safety goal, whereas current plants may not.

- Single system or component failures are not overly important due to the redundancy and diversity of Class 1 systems in the design. For example, the following lines of defence are available for reactor coolant system (RCS) makeup:

  – CVS

  – CMTs

  – Partial automatic depressurization system in combination with normal residual heat removal

  – Full automatic depressurization system with accumulators and in-containment refuelling water storage tank

  – Full automatic depressurization system with core makeup tanks and in-containment refuelling water storage tank

- Typical current PSA dominant IEs are significantly less important for the AP1000 NPP. For example, the RCP seal LOCA event has been eliminated as a core damage initiator since AP1000 NPP uses sealless reactor coolant pumps. Another example is the LOOP event. The station blackout and loss of offsite power event is a minor contributor compared to legacy plants to AP1000 NPP since the passive Class 1 systems do not require the support of ac power.

- Passive Class 1 systems are available in all shutdown modes. Planned maintenance of passive features is only performed during shutdown modes when that feature is not risk important. In addition, planned maintenance of non-Class 1 defence-in-depth features used during shutdown is performed at power when these systems are less risk important.

- The potential for containment isolation and containment bypass is lessened by having fewer penetrations to allow fission product release. In addition, normally open and risk important penetrations are fail-closed, thus eliminating the dependence on C&I and batteries for these penetrations.

- The reactor vessel lower head has no vessel penetrations, thus eliminating penetration failure as a potential vessel failure mode. Preventing the relocation of molten core debris to the containment eliminates the occurrence of several severe accident phenomena, such as ex-vessel fuel-coolant interactions and core-concrete interaction, which may threaten the containment integrity. Therefore, AP1000 NPP, through the prevention of core debris relocation to the containment, significantly reduces the likelihood of containment failure.

- The potential for the spreading of fires and floods to Class 1 equipment is reduced by the AP1000 NPP layout.

10.20.2 Use of PSA in the Design Process

The AP1000 NPP design has evolved over a period of years, including the work done for the AP600 design. PSA techniques have been used since the beginning in an iterative process to optimize the AP600/AP1000 NPP with respect to public safety. Each of these iterations has included:

- Development/refinement of the PSA model
- Use of the model to identify weaknesses
- Quantification of PSA benefits of alternate designs and operational strategies
- Adoption of selected design and operational improvements.

The scope and detail of the PSA model has increased from the early studies as the plant design has matured. This iterative design process has resulted in a number of design and operational improvements.

10.20.3 Core Damage Frequency from Internal Initiating Events at Power

Internal IEs are transient and accident initiators that are caused by plant system, component, or operator failures. External IEs, which include internal fire and flooding events and events at shutdown, are discussed in other subsections.

The AP1000 NPP mean plant core damage frequency for internal IEs at power is calculated to be 1.7E-07 events per year. Forty-four separate IEs were defined to accurately represent the AP1000 NPP design. Of these IEs 22 are loss-of-coolant accidents and 22 are transients. Initiating events unique to the AP1000 NPP design have been defined and evaluated, including direct vessel injection line breaks, core makeup tank line breaks, and passive residual heat removal heat exchanger (HX) tube ruptures and line breaks, and spurious actuation of core makeup tanks, passive residual heat removal, depressurizing valves, and IRWST injection and circulation. The resulting core damage frequency is very small; a value of 1.7E-07 means that only one core damage event is expected in 5.8 million plant-years of

operation. This core damage frequency value is two orders of magnitude (i.e., 100 times) smaller than corresponding values typically calculated for current pressurized water reactors.

The contribution of IEs to the total plant core damage frequency is summarized in Table 10-61. Figure 10-3 illustrates the relative contributions to core damage frequency from the various at-power IEs.

The top five IEs contribute 70 percent of the total at-power plant core damage frequency. The remaining IEs contribute a total of approximately 30 percent to the core damage frequency from internal events. The dominant IEs are:

- Small Loss-of-Coolant Accident
- Reactor Vessel Rupture
- Spurious IRWST Recirculation
- Loss of Offsite Power
- Steam generator tube rupture

Within this group of events, each of the first three contributes 8 percent or more to the total core damage frequency. These three events account for approximately 58 percent of the total core damage frequency. The next five events each contribute less than 4 percent to the total core damage frequency and account for an additional 15 percent to the total core damage frequency.

The results show a very low core damage frequency dominated by primarily rare events (IEs that are not expected to occur during the lifetime of a plant). This indicates that the AP1000 NPP design is robust with respect to its ability to withstand challenges from more frequent events (e.g., transients) and that adequate protection against the more severe events is provided through the defence-in-depth features.

The CDF uncertainty results show an approximately normal distribution when displayed on a log scale. This indicates that the overall uncertainty associated with CDF can be represented by a lognormal distribution. The range between the 5th and 95th percentiles indicates an error factor of approximately 3 for a lognormal distribution.

10.20.3.1 Dominant Core Damage Sequences

The dominant sequences which contribute approximately 90 percent of the total are given in Table 10-62.

The top five dominant accident sequences make up nearly 50 percent of the core damage frequency. These sequences are:

1. Sequence SLOCA-008 is the most dominant contributor to CDF at 13.4 percent. This sequence is a small LOCA followed by successful reactor trip, secondary side pressure relief, actuation of PRHR, and CMT injection. ADS Stages 2-3 are successful; however, ADS Stage 4 fails which prevents gravity injection from the IRWST. Core damage occurs due to failure of injection via the RNS.

2. The second dominant sequence is SPRECIRC-37 which contributes 9.5 percent to the total CDF. This sequence represents a spurious PXS recirculation actuation followed by failure of the operator to isolate the recirculation pathway, success of reactor trip, and successful secondary side pressure relief. MFW and SFW fail which prevents successful secondary side heat removal. PRHR decay heat removal and passive and active injection

are not credited due to the reduced IRWST level. With failure of both passive and active decay heat removal the sequence goes to core damage.

3. The third most dominant sequence is SLOCA-002 and contributes 8.8 percent to the total CDF. A small LOCA occurs followed by successful reactor trip, secondary side pressure relief, and actuation of PRHR and CMT injection. ADS Stages 2-3 and ADS Stage 4 are successful, as is gravity injection from the IRWST. Core damage occurs due to failure of recirculation via the containment sump.

4. Sequence SLOCA-005 is the fourth most dominant sequence and contributes 8.0 percent to the total CDF. This sequence represents a small LOCA followed by successful reactor trip, secondary side pressure relief, and actuation of PRHR and CMT injection. ADS Stages 2-3 and ADS Stage 4 are successful, but, gravity injection from the IRWST and RNS injection from the IRWST fail.

5. Sequence SLOCA-022 is the fifth most dominant sequence and contributes 6.8 percent to the total CDF. This sequence represents a small LOCA followed by successful reactor trip, secondary side pressure relief, and actuation of PRHR. CMT injection fails. ADS Stages 2-3 are successful, but ADS Stage 4 fails. Core damage occurs due to subsequent failure of injection via the RNS.

10.20.3.2 Sensitivity Analyses Summary for At-Power Core Damage

Importance and sensitivity analyses were performed on the core damage model for internal IEs at power.

The analyses were chosen to address the following issues:

- Importance of individual basic events and their effect on plant core damage frequency
- Importance of Class 1 and non-Class 1 systems in maintaining a low plant core damage frequency
- Effect of human reliabilities as a group on plant core damage frequency

The sensitivity analyses results show that:

- The common cause failure basic events, particularly those associated with Class 1 systems, are important individually, and also as a group for plant core damage frequency. This is expected for a plant with highly redundant Class 1 systems, for which individual component random failure contributions are of reduced significance.
- A sensitivity analysis is made for the unavailability of all non-Class-1 systems. The plant CDF obtained is 1.4E-04. This sensitivity analysis shows that the passive Class-1 and non – Class-1 systems are needed to support the current low level of core damage frequency for internal events.
- The most important systems by risk achievement worth (RAW) and risk reduction worth (RRW) are the PMS, RCS, PXS, and PCS. The only non-Class 1 systems identified by the importance measures were RNS and ECS.

- If no credit is taken for operator actions, the plant core damage frequency is 1.8E-05 events per year. This compares well with core damage frequencies for existing plants where credit is taken for operator actions.

- If the squib valve component failure probability is increased by a factor of 10, the resulting plant core damage frequency is 7.33E-07 events per year. This sensitivity case included recalculating squib valve CCF equations based on the increased component failure probability.

10.20.4 Large Release Frequency for Internal Initiating Events at Power

The results of the Level 2 (containment response) analysis for the internal IEs PSA at power demonstrate that the AP1000 NPP containment design is robust in its ability to prevent releases following a severe accident and that the risk to the public due to severe accidents for AP1000 NPP is very low. The LRF of the AP1000 NPP can be divided into two types of failures: 1) initially failed containment, in which the integrity of the containment is either failed due to the IE or never achieved from the beginning of the accident; and 2) containment failure induced by high-energy severe accident phenomena. The total of these failures is the overall large release frequency. LRF is composed of three release categories: 1) LERF, 2) large intermediate release frequency (LIRF), and 3) large venting release frequency (LVRF). The LERF category includes releases to the environment which are greater than nominal containment leakage and occur during core relocation. The LIRF category includes releases to the environment which are greater than nominal containment leakage and occur after core relocation, but within 24 hours of core damage. The LVRF category includes releases to the environment from a containment vent which are greater than nominal containment leakage. The total of these frequencies is the overall LRF.

The overall LRF for AP1000 NPP is 1.7E-08 events per year. This is approximately 10 percent of the core damage frequency for internal IEs at power. The ability of the containment to prevent releases (i.e., the containment effectiveness) is approximately 90 percent.

The LRF uncertainty results show an approximately normal distribution when displayed on a log scale. The range between the 5th and 95th percentiles indicates a lognormal error factor of approximately 10 for the LRF release category.

10.20.4.1 Plant Damage State Importance

Each of the PDSs was evaluated and the top state by frequency was a high pressure scenario with ADS Stages 1-3 actuation and failure of IRWST injection (H2I) with 30 percent of core damage. Second and third highest by frequency PDS were high pressure scenarios with failure of ADS Stages 1-4 actuation (HN) or partial automatic depressurization system with failure of passive and active (normal residual heat removal systems) IRWST injection (H1I). The “H” designators indicate the RCS pressure at the initiation of the event is considered high. The top three by frequency PDS contribute over 70 percent of core damage.

10.20.4.2 Dominant Contributors to Large Release Frequency Sequences

The LRF is dominated by the LERF-BYPASS category with 32 percent of the LRF. The second dominant LRF is LERF-EV2 with 26 percent. The dominant component failures by RAW are primarily due to common cause failure of PMS components which prevent automatic actuation of the Class 1 systems. The most significant operator error by RAW is the failure to recognize the need to actuate PRHR.

The dominant IE in the LERF is SLOCA which contributes approximately 29 percent. The next most dominant contributor is a SGTR which contributes approximately 28 percent to the total LERF.

10.20.5 Results of Internal Flooding Assessment

The AP1000 NPP design philosophy of minimizing the number of potential flooding sources along with the physical separation of redundant Class 1 components and systems from each other and from non-Class 1 components, minimizes the consequences of internal flooding. The core damage frequencies from flooding events at power are not an appreciable contributor to the overall AP1000 NPP core damage frequency. The CDF and LRF for at-power internal flood events are 4.4E-09 events per reactor-year and 1.2E-09 events per reactor-year, respectively.

10.20.6 Results of Internal Fire Assessment

The AP1000 NPP design philosophy of separation of Class 1 circuits and equipment along with physical separation of redundant Class 1 components and systems from each other and from non-Class 1 components minimizes the consequences of internal fires. The CDF and LRF for at-power internal fire events are 6.7E-07 events per reactor-year and 5.6E-08 events per reactor-year, respectively. This includes contribution from all credible fire sources and unscreened fire compartments within the fire PSA global plant analysis boundary. The fire-induced CDF is driven by the fire failing DAS combined with independent failure of the automatic and manual PMS. If only the automatic PMS signal fails, the manual operator actions to respond to this loss of automatic signal fail. This loss of redundant signaling capability fails many sequences required to mitigate core damage such as PRHR, CMT injection, steam generator cooling, and depressurization. LRF results are driven by fire-induced loss of the VLS hydrogen igniters, as well as fire-induced failures to isolate containment. Figure 10-1 shows the Internal Fire CDF by building or location. Figure 10-2 shows the Internal Fire LRF by building or location. The top fire compartments contributing to CDF are discussed in Table 10-56. The top fire compartments contributing to LRF are discussed in Table 10-57.

The results from the Fire PSA led to evaluations in the ALARP assessment centred on cable routing, separation of hydrogen igniter power supplies, ADS valve cable design, and fire protection system detection and suppression. The at-power Fire PSA results demonstrate that the CDF and LRF are below the Basic Safety Level (BSL) and Basic Safety Objective (BSO) Target 8, and therefore a graded approach is appropriate to demonstrate ALARP considerations for the at-power Fire PSA (refer to Section 10.23). Therefore, it is recognised that although ALARP is not directly required for the Fire PSA, it was performed to show how potential enhancements with small plant impacts were considered.

10.21 Review of Uncertainties

The PSA results are subject to some uncertainty, arising from various limitations in the way they were derived. This section reviews those limitations, and shows that the resulting uncertainty does not affect the conclusions drawn in this report from the results.

Limitations that could affect the PSA results are considered under the following categories:

- Limitations in scope
- Limitations in methodology
- Uncertainty in the validity of assumptions

- Uncertainties in reliability data
- Uncertainties in CCF data
- Uncertainties in Level 2/Level 3 source terms
- Uncertainties in the underpinning deterministic analysis

10.21.1 Limitations in Scope

10.21.1.1 Non-reactor Faults

The PSA does not (by definition) consider sources of radiation outside the reactor. However, the risks and dose-frequencies from accidents involving such sources are assessed separately in Chapter 9 of this PCSR and added to the corresponding figures for reactor accidents to allow a further comparison with the UK numerical targets to be made.

10.21.1.2 Seismic

As noted in Section 10.4.10 above, so far, only an SMA has been done, and not a Seismic PSA.

10.21.1.3 External Hazards

When a complete treatment of external hazards is included in the PSA, it is inevitable that the CDF and the LRF will increase, since they will then take into account additional IEs. The main reason for expecting that this increase will be small is that the design of the AP1000 is exceptionally robust against loss of external provisions. Excepting seismic events (which are treated separately), in general, the main threat from external hazards comes from their potential to disable either the external grid (and at the same time increase the chance of failure of the diesel generators) or the service water/component cooling water ultimate heat sink. The risk importance of the diesel generators and the component cooling/service water systems is very low because the passive Class-1 systems require neither ac power nor cooling to heat exchangers or to pumps. Furthermore, those passive systems are housed within the reactor containment and as such, have the best possible protection from external influences. In addition, the passive Class-1 systems are fail safe (requiring no electrical power or C&I) for non-LOCA faults.

The consequences of this robustness are already demonstrated in the PSA, as can be seen in Figure 10-2. Although the PSA assumes IE frequencies of greater than 1E-1/yr for both LOOP and loss of service water/component cooling, the contribution to CDF from each of these events is less than 1E-9/yr. It is inconceivable that external initiators having the same net effect could have frequencies of comparable magnitude, and their contribution to CDF will, therefore, be much less.

10.21.1.4 Human Factors Scope Limitations

Since the PSA model was developed, the human factors (HF) aspects of the AP1000 design safety case have been significantly revised, and this revision is continuing. As a consequence of the revisions, limited HEPs used in the PSA have been substantiated by human factors (refer to Chapter 13).

10.21.2 Limitations in Methodology

10.21.2.1 Methodology for Level 3 Dosimetry

The calculation of doses in the Level 3 treatment of the PSA was performed using a methodology which does not comply with current UK guidelines (Reference 10.1) in the following two significant ways:

- Dose coefficients are based on ICRP30, rather than on ICRP72, as required by Reference 10.1.

- No account is taken of doses from groundshine and ingestion, which must be considered according to Reference 10.1.

From a detailed comparison of representative calculations performed according to the two different approaches, it is estimated that an upper bound to the dose "as it would be calculated following the UK guidelines" is obtained by multiplying the dose as calculated in the PSA by a factor of six. This is explained in more detail above in Section 10.5, where the adjustment is made for the purpose of comparison with the ONR numerical targets.

10.21.3 Uncertainty in Level 2/Level 3 Source Terms

The source terms and Level 3 analysis have not been updated and, therefore, do not reflect the updated Plant Damage States of the Level 2 internal events model.

The Level 2 PSA identified six containment end states, or RCs. For each RC, a single combination of PDS and CET path was selected for the calculation of a source term. A single source term was calculated for each RC.

For the RCs "intact containment" and "bypassed containment", it was relatively straightforward to identify a single PDS/CET path whose resulting best estimate source term would be bounding in terms of overall dose, even though it was not separately bounding in terms of quantity of each isotope released (Reference 10.5).

For the four RCs that involved containment failure, there were large numbers of PDS/CET paths that were similar in terms of the parameters affecting the best estimate source term development. To identify from all of these the one best estimate source term that was bounding in terms of dose would have required a large number of complicated deterministic calculations, each followed by a dose calculation. This was considered to be impractical, but more importantly, it was also considered to be unnecessary because the variation in source term between PDS/CET paths was believed to be small compared with the uncertainty in the finally calculated source term due to the inherent uncertainty in the calculation process, i.e., in the analysis of fission product transport from fuel to environment. In other words, the variations in best estimate source term are far overshadowed by the change in source term for fission product modelling uncertainties. The procedure adopted, therefore, was to select a single representative PDS/CET path for each RC, and then to perform a detailed sensitivity analysis to determine the effect on the calculated source term of varying the important modelling options and assumptions in the fission product transport analysis (Reference 10.5). The set of options and assumptions that gave the largest source term was then used to perform the definitive source term calculation.

As a consequence of following this procedure for the four failed containment RCs, there is high confidence that the source terms finally assigned to the end states bound any real release

because of the use of conservative modelling assumptions throughout the fission product transport analysis. This remains true, even though it is also likely that there are other PDS/CET paths which would have given slightly greater calculated source terms with the same set of modelling assumptions (and would, therefore, be even more bounding). In other words, numerical manipulations of the source term to obtain an absolute worst case, bounding source term considering all uncertainties would provide no further insights related to design or operational changes. Therefore, the existing analyses are adequate to demonstrate that the risks are ALARP.

10.22 Planned Update to the Reactor PSA

The next planned update to the AP1000 plant PSA will be to support site licensing of the AP1000 plant in the UK. The PSA will be updated to reflect a DRP that includes site specific design and address UK site licensing requirements to work towards the UK Technical Assessment Guides (TAGs).

Key items for future consideration include the following:

1. There is an uncertainty concerning the piping response to a spurious actuation of one or more ADS Stage 4 valves at-power. The piping is not designed for valve actuation at full RCS pressure. To construct the event tree, assumptions were made regarding the consequences of spurious actuation.

2. For the spurious IRWST actuation IE, there is an uncertainty of the plant consequences that result if the check valve(s) upstream of the spuriously opened IRWST squib valve(s) have an internal failure. The check valve failure would result in a LOCA into the IRWST. This condition has not been evaluated and is taken to core damage if two or more sets of valves (IRWST squib and its check valve) fail. The failure of one IRWST valve and its check valve is treated as a DVI LOCA.

3. Common cause of all PMS and PLS software are modelled. There is currently no accepted methodology for modelling and quantifying software reliability. It is not known whether the scope and level of detail of these failures is appropriate or whether all possible failures have been accounted for.

10.23 Conclusions

As the PSA continues to evolve and move toward a site-specific PSA, the safety assessment principles (SAPs, Reference 10.77) are also reviewed and assessed. Not all SAPs that use probabilistic methods are documented, but a subset to summarize the PSA results are documented here. PSA methods are used throughout the design process to support and compliment deterministic methods as documented with other safety cases. As the PSA develops into a site-specific PSA, the SAPs will continue to be used to enhance the PSA.

SAP	Description	PSA Comments
FA.10	*"Suitable and sufficient PSA should be performed as part of the fault analysis and design development and analysis."*	PSA is used as an integral part of the design and analysis. The scope and depth of the PSA at this stage of the design is documented throughout Chapter 10. A comprehensive PSA has been developed but will continue to evolve as the design develops and moves toward site-licensing.
FA.11	*"PSA should reflect the current design and operation of the facility or site."*	At this point in the design, a site-specific PSA has not been evaluated. However, the overall goal of the generic design PSA to influence the design and support the overall risk assessment of the plant has been achieved.
FA.12	*"PSA should cover all significant sources of radioactivity, all permitted operating states and all relevant initiating faults."*	The scope of the PSA will continue to evolve as site-licensing approaches. Some areas in Chapter 10 have not been updated for the generic design assessment.
FA.13	*"The PSA model should provide an adequate representation of the facility and/or site."*	The PSA is a comprehensive model and analysis that assesses the design and generic site.
FA.14	*"PSA should be used to inform the design process and help ensure the safe operation of the site and its facilities."*	The PSA has been used in ALARP activities and has been used to understand the overall risk of the plant to support design decisions.
FA.15	*"Fault states, scenarios and sequences beyond the design basis that have the potential to lead to a severe accident should be analysed."*	The severe accident analysis (SAA) uses a systematic approach to analysis beyond design basis states and scenarios.
FA.16	*"Severe accident analysis should be used in the consideration of further risk-reducing measures."*	SAA has been used in the overall design process as part of ALARP assessments and design investigations.
FA.25	*"The severe accident analysis should be performed in a manner complementary to the DBA and PSA, so that each type of analysis informs the others in a mutually consistent manner within the facility's safety case."*	The SAA has and will continue to be used as part of the PSA which will continue to assess against the fault study's conclusions.

The essence of demonstrating that risks have been reduced ALARP is to show that the costs of improving safety any further would be grossly disproportionate to the effort of implementing improvements compared to the current design. From Reference 10.77, paragraph 698, "It is ONR's policy that a new facility or activity should at least meet the BSLs. However, even if the BSLs are met, the risks may not be ALARP; in such cases the designer/dutyholder must reduce the risks further. Deciding when the level of risk is ALARP needs to be justified by the designer/dutyholder on a case-by-case basis, applying the legal test of gross disproportion. A graded approach should be used so that the higher the risk (or hazard), the greater the degree of disproportion applied, and the more robust the argument needed to justify not implementing additional safety measures."

Additionally, paragraph 710, states "The BSOs also recognise that there is a level beyond which further consideration of the safety case would not be a reasonable use of ONR

resources, compared with the benefit of applying these resources to areas of higher risk. Inspectors therefore need not seek further improvements from the designer/dutyholder but can confine themselves to assessing the validity of the arguments presented."

The CDF and LRF values for the at-power PSA results (Internal Events, Internal Flooding, and Internal Fire) which assess the total per reactor year core damage or large early releases are summarized below:

	CDF	LRF
At-Power Internal Events	1.7E-07	1.7E-08
At-Power Internal Flooding	4.4E-09	1.2E-09
At-Power Internal Fire	6.7E-07	5.6E-08
Total At-Power PSA (sum of listed contributors)	**8.4E-07**	**7.4E-08**

Target 8 is the target for the total predicted frequencies of accidents on an individual facility per annum which would give doses to a person off the site. These targets were compared to the CDF and LRF values for the at-power PSA results (Internal Events, Internal Flooding, and Internal Fire).

BSL Target 8 1E-04 pa

BSO Target 8 1E-06 pa

Target 9 is the target for the total risk of 100 or more fatalities, either immediate or eventual, from accidents at the site resulting in exposure to ionising radiation. This parameter will be highly site specific and cannot be calculated precisely in a generic assessment. Nevertheless, a simplified assessment can be made that assumes that all large releases (i.e., with the containment not intact) will result in more than 100 fatalities, either immediate or eventual, and no other events will result in that number of fatalities. In this case, these targets were compared to the total LRF value for the at-power PSA results (Internal Events, Internal Flooding, and Internal Fire).

BSL Target 9 1E-05 pa

BSO Target 9 1E-07 pa

The AP1000 at-power PSA risk demonstrates margin to the Target 8 and Target 9 BSO as shown above. Since it is anticipated that the AP1000 plant at-power PSA will continue to meet the BSO, there is little need to further reduce the AP1000 at-power PSA risk.

10.24 References

10.1 Westinghouse Report APP-GW-GL-022, Rev. 8, "AP1000 Probabilistic Risk Assessment," August 2009.

10.2 Westinghouse Report UKP-GW-GL-743, Rev. 1, "AP1000 PRA Spent Fuel Evaluation," January 2010.

10.3 EPRI ALWR URD, Rev. 7, "Advanced Light Water Reactor Utility Requirements Document," Electric Power Research Institute, December 1995.

10.4 MAAP4 User's Manual, Electric Power Research Institute, June 1999.

10.5 Westinghouse Document UKP-GW-GL-082, Rev. 0, "AP1000 Severe Accident Phenomenological Roadmap," January 2011.

10.6 NRC NUREG/CR-1278, "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications," 1983.

10.7 ANSI/ANS 58.21-2007, "External Events PRA Methodology," American National Standards Society, March 2007.

10.8 SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs," US Nuclear Regulatory Commission, April 2, 1993 (Addendum dated July 21, 1993).

10.9 J. Irving, "Seismic Qualification of Safety Related Nuclear Plant and Equipment 'Seismic Hazard in the UK,' *IMechE*, 1984.

10.10 CR/07/125, British Geological Survey Technical Report, "Eurocode 8 Seismic Hazard Zoning Maps for the UK," RMW Musson and SL Sargeant, 2007.

10.11 Westinghouse Document WCAP-16872-NP, Rev. 0, "Pilot Implementation of EPRI Guidance for Fault Tree Modelling of Support System Initiating Events," March 2008.

10.12 Westinghouse Report UKP-PRA-GSC-002, Rev. A, "Spent Fuel Pool Boiling Frequency for the UK AP1000™ Plant," January 2011.

10.13 Westinghouse Report UKP-PRA-GSC-001, Rev. A, "Update of the Loss of CCS/SWS Frequency for the UK AP1000™ Plant", November 2010.

10.14 Westinghouse Report APP-PRA-GSC-400, Rev. C, "AP1000 Spent Fuel Pool Probabilistic Risk Assessment (PRA)," January 2010.

10.15 NUREG/CR-6928, "Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants," U.S. Nuclear Regulatory Commission, February 2007.

10.16 Not used

10.17 Not used

10.18 Not used

10.19 Not used

10.20 Not used

10.21 NUREG/CR-3862, "Development of Transient Initiating Event Frequencies for Use in Probabilistic Risk Assessments," U.S. Nuclear Regulatory Commission, May 1985.

10.22 NUREG/CR-5750, "Rates of Initiating Events at U.S. Nuclear Power Plants: 1987-1995," U.S. Nuclear Regulatory Commission, December 1998.

10.23 EPRI Report 1013490, "Support System Initiating Events: Identification and Quantification Guideline," Electric Power Research Institute, December 2006.

10.24 Westinghouse Document WCAP-17154-P, Revision 0, "ISLOCA Risk Model," April 2010.

10.25 S. A. Eide, D. M. Rasmuson, C. L. Atwood, "Estimating Loss-of-Coolant Accident Frequencies for the Standardized Plant Analysis Risk Models," Proceedings of ANS PSA 2008 Topical Meeting, Knoxville, Tennessee, September 7-11, 2008.

10.26 OG-09-36, "White Paper on Consideration of Reactor Vessel Failure in Plant-Specific PRA Models for PWRs," January 2009.

10.27 NUREG-1829, "Estimating Loss-of-Coolant Accident (LOCA) Frequencies through the Elicitation Process," U.S. Nuclear Regulatory Commission, April 2008.

10.28 EPRI Report TR-1021086, Revision 2, "Pipe Rupture Frequencies for Internal Flooding PRAs," Electric Power Research Institute, November 2010.

10.29 Westinghouse Document WCAP-16248-P, Revision 0, Volume 1, "User's Manual for the CENTS Code," April 2004.

10.30 Westinghouse Document WCAP-7907-P-A/WCAP-7907-A, "LOFTRAN Code Description," April 1984.

10.31 Report Number FAI/07-54, "Transmittal Document for MAAP4 Code Revision MAAP 4.0.7; MAAP4 User's Manual," May 2007.

10.32 NUREG/CR-5500, Vol. 2, "Reliability Study: Westinghouse Reactor Protection System, 1984–1995," U.S. Nuclear Regulatory Commission, December 1998.

10.33 Westinghouse Document WCAP-15691, Revision 5, "Joint Applications Report for Containment Integrated Leak Rate Test Interval Extension," March 2004.

10.34 NUREG/CR-4639, Volume 5, Revision 4, "Nuclear Computerized Library for Assessing Reactor Reliability (NUCLARR)." U.S. Nuclear Regulatory Commission, September 1994.

10.35 Westinghouse Document WCAP-15376-P-A, Revision 1, "Risk-Informed Assessment of the RTS and ESFAS Surveillance Test Intervals and Reactor Trip Breaker Test and Completion Times," March 2003.

10.36 Westinghouse Letter LTR-AMLRS-11-31, Revision 0, "White Paper on Spurious Actuation Frequency of the Automatic Depressurization System (ADS) Stage 4 Valves due to Internal Rupture," April 2011.

10.37 Westinghouse Letter LTR-RIAM-12-44, Revision 0, “Spurious Actuation of AP-1000 IRWST 8” Squib Valve,” May 2012.

10.38 Westinghouse Document APP-GW-JJ-005, Revision 0, “AP1000 Diverse Actuation System Reliability Analysis Report,” October 2012.

10.39 Westinghouse Document WNA-AR-00211-GEN, Revision 2, “Protection and Safety Monitoring System MTBF Summary Report,” February 2012.

10.40 Westinghouse Document CPP-PMS-AR-001, Revision 0, “China AP1000 Protection and Safety Monitoring System Reliability Analysis,” March 2012. Note: The PMS reliability data available at the time of the PSA update was China specific. In a future update to the PSA, the APP reliability data will be used.

10.41 Westinghouse Document WNA-AR-00039-GEN, Revision 1, “Ovation DCS Platform Reliability,” June 2010.

10.42 Westinghouse Document APP-GW-GEE-2411, Revision 0, “ADS Diverse Actuation Block,” March 2011. Note: The block device modelled in the updated PSA is based on the design change proposal due to the timing of the update. In a future update to the PSA, the updated PMS references incorporating the block reliability will be used.

10.43 Westinghouse Document APP-GW-JJ-002, Revision 4, “FMEA of AP1000 Protection and Safety Monitoring System,” November 2011.

10.44 Westinghouse Document CN-AP1000-234 (APP-PRA-F5-001), Revision 0, “Shutdown Calculations to Support AP1000 ATWS PRA Analysis,” December 2012.

10.45 NUREG/CR-5485, “Guidelines on Modelling Common-Cause Failure in Probabilistic Risk Assessment,” U.S. Nuclear Regulatory Commission, November 1998.

10.46 Westinghouse Document WCAP-16672-P, Revision 1, “Common Cause Failure Parameter Estimates for the PWROG,” June 2008.

10.47 IEC 61508-6 Ed. 1 [2000-04] "Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3."

10.48 Westinghouse Document WNA-CN-00067-SSP, Revision 3/APP, “TWICE – Fault Tree Analysis of Reactor Trip System,” August 2009.

10.49 Westinghouse Document CN-PRRA-92-319, Revision 0, “AP600 PRA: Dependent Failures Notebook (Appendix E),” June 1992.

10.50 Westinghouse Document WNA-AR-00177-GEN, Revision 1, “Reliability Analysis of the Ovation Data Network,” June 2011.

10.51 Westinghouse Letter LTR-RAM-I-12-075, Revision 0, "Expert Panel for Estimating Reference Probabilities for Debris-Induced Failure of Long Term Core Cooling for the AP1000 Plant," January 2013.

10.52 Westinghouse Document WCAP-15691, Revision 5, "Joint Applications Report for Containment Integrated Leak Rate Test Interval Extension," March 2004.

10.53 NUREG-1570, "Risk Assessment of Sever Accident-Induced Steam Generator Tube Rupture," U.S. Nuclear Regulatory Commission, March 1998.

10.54 EPRI 1019194, "Guidelines for Performance of Internal Flooding Probabilistic Risk Assessment," Electric Power Research Institute," December 2009.

10.55 US NRC NUREG/CR-6850, "EPRI/NRC–RES Fire PRA Methodology for Nuclear Power Facilities," Electric Power Research Institute, September 2005.

10.56 Westinghouse Document APP-GW-N4R-003, Revision H, "Fire Protection Analysis Report," July 2014.

10.57 US NRC NUREG-2169 (EPRI 3002002936), "Nuclear Power Plant Fire Ignition Frequency and Non-Suppression Probability Estimation Using the Updated Fire Events Database," Electric Power Research Institute, Palo Alto, CA, and U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research, Washington, D.C., January 2015.

10.58 US NRC NUREG-1921 (EPRI TR-1023001), *EPRI/NRC-RES Fire Human Reliability Analysis Guidelines*, Electric Power Research Institute, Palo Alto, CA, and U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research, Rockville, MD: July 2012.

10.59 "Individual Plant Examination of External Events (IPEEE) for Severe Accident Vulnerabilities – 10 CFR 50.54(f)," Generic Letter 88-20, Supplement 4, June 28, 1991.

10.60 US NRC NUREG-1407, "Procedural and Submittal Guidance for the Individual Plant Examination of External Events (IPEEE) for Severe Accident Vulnerabilities," June 1991.

10.61 ASME/ANS-RA-Sa 2009, "Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications," American Society of Mechanical Engineers.

10.62 US NRC Regulatory Guide 1.200, "An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk Informed Activities," Revision 2.

10.63 National Weather Service, "The Saffir-Simpson Hurricane Scale," June 22, 2006, http://www.nhc.noaa.gov/aboutsshs.shtml.

10.64 US NRC NUREG/CR-4461, "Tornado Climatology of the Contiguous United States," Revision 2.

10.65 US NRC Regulatory Guide 1.78, "Evaluating the Habitability of a Nuclear Power Plant Control Room During a Postulated Hazardous Chemical Release," Revision 1, December 2001.

10.66 US NRC Regulatory Guide 1.91, "Evaluation of Explosions Postulated to Occur on Transportation Routes Near Nuclear Power Plants," Revision 1, February 1978.

10.67 US NRC Regulatory Guide 1.115, "Protection against Turbine Missiles," Revision 2, January 2012.

10.68 RS-002, USNRC Review Standard (RS)-002, "Processing Applications for Early Site Permits," May 3, 20014, Section 3.5.1.6, "Aircraft Hazards."

10.69 Letter from D. A. Ward, Advisory Committee on Reactor Safeguards, to K. A. Carr, Chairman, Nuclear Regulatory Commission, "Proposed Criteria to Accommodate Severe Accidents in Containment Design," dated May 17, 1991.

10.70 DOE/ID-10460, Theofanous, T. G., et al., "In-Vessel Coolability and Retention of a Core Melt," July 1995.

10.71 DOE/ID-10541, Theofanous, T. G., et al., "Lower Head Integrity Under In-Vessel Steam Explosion Loads," July 1996.

10.72 US NRC NUREG-1116, "A Review of the Current Understanding of the Potential for Containment Failure From In-Vessel Steam Explosions," 1985.

10.73 Westinghouse Document GW-GL-022, Revision 8, "AP600 Probabilistic Risk Assessment," September 1998.

10.74 Attachment to letter from D. M. Crutchfield, Office of Nuclear Reactor Regulation, to E. E. Kintner, Advanced Light Water Reactor Steering Committee, "Major Technical and Policy Issues Concerning the Evolutionary and Passive Plant Designs," dated February 27, 1992.

10.75 Westinghouse Document APP-PRA-GSC-304, Revision 0, "AP1000 In-Vessel Retention of Molten Core Debris," July 2003.

10.76 NEA/CSNI/R(2000)7, "Flame Acceleration and Deflagration-to-Detonation Transition in Nuclear Safety, State-of-the-Art Report by a Group of Experts," Organization for Economic and Cooperative Development Nuclear Energy Agency, August 2000.

10.77 ONR "Safety Assessment Principles for Nuclear Facilities," Revision 0, Office for Nuclear Regulations, 2014.

10.78 Westinghouse Document APP-PRA-GSC-027, Revision 2, "AP1000 PRA-BASED SEISMIC MARGIN ASSESSMENT UPDATE," February 2011.

Table 10-1. Initiating Event Frequency Summary

Event Description	Basic Event Name	IEF (Per Reactor Operating State Year)	IEF (Per Reactor Year)	Section
Large LOCA	%LLOCA	8.37E-07	7.78E-07	10.2.3.1
Medium LOCA	%MLOCA	7.30E-06	6.79E-06	10.2.3.2
Small LOCA	%SLOCA	3.01E-03	2.80E-03	10.2.3.3
RCS Leak	%LEAK	1.55E-03	1.44E-03	10.2.3.4
Spurious ADS Stages 1-3 Actuation	%SPADS13			10.2.3.5
Spurious ADS Stage 4 Actuation	%SPADS4			10.2.3.6
Spurious IRWST Actuation	%SPIRWST			10.2.3.7
CMT A Line Break	%CMTLB-A			10.2.3.8
CMT B Line Break	%CMTLB-B			10.2.3.8
DVI Line A Break	%DVILB-A			10.2.3.9
DVI Line B Break	%DVILB-B			10.2.3.9
PRHR Line Break	%PRHRLB			10.2.3.10
PRHR Tube Rupture	%PRHRTR			10.2.3.11
Reactor Vessel Rupture	%RVR			10.2.3.12
SGTR	%SGTR	3.54E-03	3.29E-03	10.2.3.13
Interfacing System LOCA-Non Isolatable	%ISL-P04			10.2.3.14
	%ISL-P19			
	%ISL-P20			
Interfacing System LOCA-Isolatable (CVS)	%ISL-P05			10.2.3.14
	%ISL-P07-N			
	%ISL-P07-P			
	%ISL-P08			
PMS Spurious PRHR Actuation	%SPPRHR			10.2.3.16
PMS Spurious CMT Actuation	%SPCMT			10.2.3.17

Table 10-1. Initiating Event Frequency Summary (cont.)

Event Description	Basic Event Name	IEF (Per Reactor Operating State Year)	IEF (Per Reactor Year)	Section
Spurious IRWST Recirculation	%SPRECIRC	[	]	10.2.3.18
General Transient With Main Feedwater	%GTRAN-WFW	4.55E-01	4.23E-01	10.2.3.19
General Transient Without Main Feedwater	%GTRAN-WOFW	2.75E-01	2.56E-01	10.2.3.19
General Transient With S Signal	%GTRAN-WS	2.16E-02	2.01E-02	10.2.3.19
Total Loss of Main Feedwater	%LMFW	9.59E-02	8.92E-02	10.2.3.20
Total Loss of Condenser Heat Sink	%LCOND	8.11E-02	7.54E-02	10.2.3.21
Total Loss of Component Cooling Water	%CCS			10.2.3.22
Total Loss of Service Water	%SWS			10.2.3.23
Total Loss of Compressed and Instrument Air	%CAS			10.2.3.24
Loss of Medium Voltage AC Power	%MVAC	1.85E-02	1.72E-02	10.2.3.25
Loss of Low Voltage Power	%IDSA-DD-1			10.2.3.26
	%IDSB-DD-1			
	%IDSC-DD-1			
	%IDSD-DD-1			
Loss of HVAC to the CCS Pumps Room	%VTS-T2			10.2.3.27
Loss of VWS HCS	%VWS-HCS			10.2.3.28
Total Loss of Offsite Power	%LOOP	3.59E-02	3.34E-02	10.2.3.29
SLB Downstream of the MSIVs	%SLBD	1.00E-02	9.30E-03	10.2.3.30
SLB Upstream of the MSIVs	%SLBU	1.00E-03	9.30E-04	10.2.3.31
Feedwater Line Break	%FWLB	3.43E-03	3.19E-03	10.2.3.32

Table 10-2. Summary of Initiating Event Grouping

IE Type	Group	Initiating Event Name
LOCAs	LLOCA	Large LOCA
	MLOCA	Medium LOCA
	SLOCA	Small LOCA
	RCS Leak	RCS Leak
	Spurious ADS Stages 1-3 Actuation	Spurious ADS Stages 1-3 Actuation
	Spurious ADS Stage 4 Actuation	Spurious ADS Stage 4 Actuation
	Spurious IRWST Actuation	Spurious IRWST Actuation
	CMT Line Break	CMT Line Break
	DVI Line Break	DVI Line Break
	PRHR Line Break	PRHR Line Break
	PRHR Tube Rupture	PRHR Tube Rupture
	Reactor Vessel Rupture	Reactor Vessel Rupture
	SGTR	SGTR
	Interfacing System LOCA – Non Isolatable	CCS RCP external HX outlet line ISLOCA (P04)
		RNS suction line ISLOCA (P19)
		RNS DVI injection lines ISLOCA (P20)
	Interfacing System LOCA – Isolatable (CVS)	CVS spent resin sluice line ISLCOA (P05)
		CVS normal makeup line ISLOCA (P07-N)
		CVS PXS header makeup line ISLOCA (P07-P)
		CVS zinc injection line ISLOCA (P08)

Table 10-2. Summary of Initiating Event Grouping (cont.)

IE Type	Group	Initiating Event Name
Transients	General Transient with S Signal – GTRAN-WS	PMS Spurious PRHR Actuation
		PMS Spurious CMT Actuation
		General Transient With Safeguards Signal
		Loss of Low Voltage Power
		Total Loss of Compressed and Instrument Air
	General Transient without Safeguards – GTRAN	General Transient Without Main Feedwater
		Total Loss of Main Feedwater
		Total Loss of Condenser Heat Sink
		Total Loss of Component Cooling Water
		Total Loss of Service Water
		General Transient With Main Feedwater
		Loss of Medium Voltage AC Power
		Loss of HVAC to CCS Pump Room
		Loss of Central Chilled Water HCS
	Loss of Offsite Power – LOOP	Total Loss of Offsite Power
	SLB Downstream of the MSIVs – SLBD	SLB Downstream of the MSIVs
		Feedwater Line Break
	SLB Upstream of the MSIVs – SLBU	SLB Upstream of the MSIVs
	Spurious IRWST Recirculation	Spurious IRWST Recirculation

Table 10-3. Summary of Initiating Event Grouping With Event Trees

Group	Event Tree Name
LLOCA	LLOCA
MLOCA	MLOCA
SLOCA	SLOCA
RCS Leak	LEAK
Spurious ADS Stages 1-3	SPADS13
Spurious ADS Stage 4	SPADS4
Spurious IRWST	SPIRWST
CMT Line Break	CMTLB
DVI Line Break	DVILB
PRHR Line Break	PRHRLB
PRHR Tube Rupture	SLOCA
Reactor Vessel Rupture	(CD assumed, no event tree)
SGTR	SGTR
ISLOCA – Non Isolatable	(CD assumed, no event tree)
ISLOCA – Isolatable (CVS)	ISL-CVS
General Transient with S signal – GTRAN-WS	GTRAN-WS
General Transient without S signal – GTRAN	GTRAN
Loss of Offsite Power – LOOP	LOOP
SLB Downstream of the MSIVs – SLBD	SLBD
SLB Upstream of the MSIVs – SLBU	SLBU
Spurious IRWST Recirculation	SPRECIRC

Table 10-4. LLOCA Event Tree Description

Top Event	Top Event Description
ACC	The accumulators are designed to deliver a large volume of borated water to the reactor vessel (RV) at a high flowrate in the event of an LLOCA. The success of this top event (ACC-1) requires one out of two accumulators to inject into the direct vessel injection (DVI) line, when the RCS pressure is below the accumulator pressure. Failure of this top event leads to core damage because the core reflood does not occur in time.
CMT	The success of this top event (CMT-2-PA-DA) requires two out of two core makeup tanks (CMTs) to inject. Each CMT must inject through one out of two parallel valves on the discharge piping, and at least one must provide a CMT actuation signal to ADS. Failure of this top event leads directly to core damage because there is insufficient water inventory for the core and insufficient time for operator action.
IRWST	The success of this top event (IRWST-1-PA) requires one out of four gravity injection line squib valves to actuate and provide IRWST injection into the RV via the DVI lines. Failure of this top event leads directly to core damage because there is insufficient water inventory for the core and insufficient time for operator action.
ADS4	For the most likely LLOCA sequences, the ADS Stage 4 valves are not required for successful IRWST gravity injection because the size of the LOCA sufficiently reduces the RCS pressure. However, there are conditions for which ADS relief is required. Once the break in the RCS is covered by the rising water level in containment, an open ADS Stage 4 valve is required to ensure there is adequate flow out of the RCS for proper core cooling. In addition, if containment isolation fails, an ADS Stage 4 valve is required to ensure that the RCS pressure is low enough for IRWST injection and recirculation. The success criteria for this top event (ADS4-2L-PA) are one out of two ADS Stage 4 valves on each loop (two out of four total) actuating and providing a signal for IRWST gravity injection and recirculation. If ADS4 fails, the sequence goes to core damage because there is insufficient RCS venting for the passive recirculation function.
RECIRC	This top event is associated with containment sump recirculation on a Protection and Safety Monitoring System (PMS) signal or operator action HEPO-RECIRC using E-1. The success of this top event (RRWST-1-PX-DM) requires one out of four containment sump recirculation line squib valves to actuate and provide flow into the RV via the DVI lines. Failure of this top event leads to core damage because long term cooling is not established.

Table 10-5. MLOCA Event Tree Description

Top Event	Top Event Description
REACTOR TRIP	This top event is associated with PMS and Diverse Actuation System (DAS) reactor trip signals and operator action HEPO-RT using E-0. Void formation is not sufficient to shut down the reactor core. Reactor trip (RT-PX-DX-LOCA) is successful when the control rods are inserted into the core and reactivity control is achieved. Failure of this top event results in a transfer to reactor trip failure event tree LOCA-NOTRIP.
CMT	Due to timing considerations, credit is not taken for operator action to actuate the CMTs. The success of this top event (CMT-1-PA-DA) requires one out of two CMTs to inject through one out of two parallel valves on the discharge piping and a CMT actuation signal to ADS. The CMTs will be actuated automatically either through the PMS or DAS. If this top event fails, then accumulator injection is required to provide water to the RCS.
ACC	For MLOCAs, the accumulators provide a source of water when the CMTs fail, prior to injection from the IRWST, to maintain water in the core. The success of this top event (ACC-1) requires one out of two accumulators to inject into the DVI line, when the RCS pressure is below the accumulator pressure. Failure of this top event leads directly to core damage because it is addressed only on the failure path of top event CMT.
ADS23	This top event is associated with ADS Stages 1-3 actuation on a PMS signal or operator action HEPO-ADS-C1 or HEPO-ADS-C2 using E-1 or the Foldout Page for E-1. The success criteria for ADS23 (ADS23-2-PX-DM-C1, ADS23-2-PM-DM-C2) are two out of four ADS Stages 2 and 3 valves open and discharge into the IRWST. ADS23-2-PX-DM-C1 is used on the CMT success path because both automatic and manual actuations via the PMS are possible. ADS23-2-PM-DM-C2 is used on the CMT failure path because automatic actuation via the PMS will not occur because either the signal fails or the CMT valves fail and the CMT Low level input to actuate ADS will not be generated. Failure of this top event can lead to a non-core damage state if top event ADS4 is successful.
ADS4	This top event is associated with ADS Stage 4 actuation on a PMS signal or operator action HEPO-ADS4-C1 or HEPO-ADS4-C2 using E-1 or the Foldout Page for E-1. The success criteria for this top event (ADS4-2L-PX-DM-C1, ADS4-2L-PM-DM-C2) are one out of two ADS Stage 4 valves on each loop (two out of four total) actuating and providing a signal for IRWST gravity injection and recirculation. ADS4-2L-PX-DM-C1 is used when top event CMT is successful because both automatic and manual actuations via the PMS are possible. ADS4-2L-PM-DM-C2 is used when top event CMT fails because there is no automatic PMS actuation and the operator action is based on RCS hot leg level. Failure of top event ADS4 leads directly to core damage on the failure paths of ADS23 because there is insufficient RCS depressurization for IRWST or RNS injection. On success paths of ADS23, failure of ADS4 does not lead directly to core damage because there is sufficient RCS depressurization to allow RNS injection to be successful.

Table 10-5. MLOCA Event Tree Description (cont.)

Top Event	Top Event Description
IRWST	This top event is associated with IRWST gravity injection actuation on a PMS ADS Stage 4 actuation signal or operator action HEPO-INJ using E-1. The success of this top event (IRWST-1-PX-DM) requires one out of four gravity injection line squib valves to actuate and provide IRWST injection into the RV via the DVI lines. Failure of this top event does not directly lead to core damage because ADS Stage 4 has successfully depressurized the RCS and there is sufficient time for the operator to establish injection through the RNS.
RNS	This top event is associated with using the RNS to provide low pressure injection to the RCS with operator action HEPO-RNSINJ and HEPO-RNSIRWST using ES-1.3. Success for this top event (RNS-1-PLM-L) includes successful operator action and the equipment functioning to align and start one out of two RNS pumps to take suction from the cask loading pit (CLP), then to realign the RNS pump to take suction from the IRWST to maintain flow into the RV through one out of two DVI lines. Failure of this top event leads directly to core damage because the RNS is addressed when IRWST injection is not available.
RECIRC	This top event is associated with containment sump recirculation on a PMS signal or operator action HEPO-RECIRC using E-1. The success of this top event (RRWST-1-PX-DM) requires one out of four containment sump recirculation line squib valves to actuate and provide flow into the RV via the DVI lines. Failure of this top event leads to core damage because long term cooling is not established.

Table 10-6. SLOCA Event Tree Description

Top Event	Top Event Description
REACTOR TRIP	This top event is associated with PMS and DAS reactor trip signals and operator action HEPO-RT using E-0. Void formation is not sufficient to shut down the reactor core. Reactor trip (RT-PX-DX-LOCA) is successful when the control rods are inserted into the core and reactivity control is achieved. Failure of this top event results in a transfer to reactor trip failure event tree LOCA-NOTRIP.
SS FAULT	Because the SLOCA, especially on the small end of the break size range, can be a slow depressurization of the RCS, the initial part of the event is similar to a transient with a safeguards actuation signal (S signal). After reactor trip the secondary side relief valves will likely be challenged. The success for this top event (SGS-SS-PA-PLA) is defined as one out of two power-operated relief valves (PORVs) opening, or one out of two safety valves (the two with the lowest set pressure) opening and relieving steam, or one turbine bypass valve dumping steam to the condenser. In addition, turbine trip (steam flow stopped to both the high pressure and low pressure turbines) must be successful. Because more than one PORV or main steam safety valve (MSSV) may open after a reactor trip, the success for the valves reclosing is one PORV or block valve on each steam line reclose and two out of two MSSVs reclose. Credit is not taken for the operator to close the PORV block valve. Failure of this top event, the required valves failing to open or failing to reclose, results in a transfer to secondary side failure event tree LOCA-SSFAULT.
PRHR	This top event is associated with the PRHR heat exchanger actuation on a PMS or DAS signal or operator action HEPO-PRHR using E-0. The success of this top event (PRHR-PX-DX-L) requires one out of two of the PRHR heat exchanger control valves to open and establish flow through the PRHR heat exchanger. In addition, one out of two IRWST gutter isolation valves must close to return condensate to the IRWST to sustain long term cooling. Failure of this top event requires RCS depressurization and IRWST or RNS injection to prevent core damage.
CMT	This top event is associated with CMT actuation on a PMS or DAS signal or operator action HEPO-CMT using E-0. The success of this top event (CMT-1-PX-DX) requires one out of two CMTs to inject through one out of two parallel valves on the discharge piping, four out of four reactor coolant pumps (RCPs) to trip, and a CMT actuation signal to ADS. If this top event fails, then accumulator injection is required to provide water to the RCS prior to injection from the IRWST.

Table 10-6. SLOCA Event Tree Description (cont.)

Top Event	Top Event Description
ADS23	This top event is associated with ADS Stages 1-3 actuation on a PMS signal or operator action HEPO-ADS-C1 or HEPO-ADS-C2 using E-1 or the Foldout Page for E-1. There are three branch names and two sets of success criteria for ADS23 (ADS23-2-PX-DM-C1, ADS23-2-PM-DM-C2, ADS23-3-PX-DM-C1). The success criteria for ADS23-2-PX-DM-C1 and ADS23-2-PM-DM-C2 are two out of four ADS Stages 2 and 3 valves open and discharge into the IRWST. ADS23-2-PX-DM-C1 is used on the top CMT success path because both automatic and manual actuations via the PMS are possible. ADS23-2-PM-DM-C2 is used on the CMT failure paths because automatic actuation via the PMS will not occur because either the signal fails or the CMT valves fail and the CMT Low level input to actuate ADS will not be generated. The success criteria for ADS23-3-PX-DM-C1 are three out of four ADS Stages 2 and 3 valves open and discharge into the IRWST. If top events PRHR and CMT are successful and ADS23 fails, core damage can be prevented by successful operation of ADS4 and IRWST or RNS injection.
ACC	For SLOCAs, the accumulators provide a source of water when the CMTs fail, prior to injection from the IRWST, to maintain water in the core. The success of this top event (ACC-1) requires one out of two accumulators to inject into the DVI line, when the RCS pressure is below the accumulator pressure. Failure of this top event leads directly to core damage because it is addressed only on the failure paths of top event CMT.
ADS4	This top event is associated with ADS Stage 4 actuation on a PMS signal or operator action HEPO-ADS4-C1 or HEPO-ADS4-C2 using E-1 or the Foldout Page for E-1. The success criteria for this top event (ADS4-2L-PX-DM-C1, ADS4-2L-PM-DM-C2) are one out of two ADS Stage 4 valves on each loop (two out of four total) actuating and providing a signal for IRWST gravity injection and recirculation. ADS4-2L-PX-DM-C1 is used when top event CMT is successful because both automatic and manual actuations via the PMS are possible. ADS4-2L-PM-DM-C2 is used when top event CMT fails because there is no automatic PMS actuation and the operator action is based on RCS hot leg level. Failure of ADS4 does not lead directly to core damage if sufficient RCS depressurization has occurred to enable RNS injection to be successful.
IRWST	This top event is associated with IRWST gravity injection actuation on a PMS ADS Stage 4 actuation signal or operator action HEPO-INJ using E-1. The success of this top event (IRWST-1-PX-DM) requires one out of four gravity injection line squib valves to actuate and provide IRWST injection into the RV via the DVI lines. Failure of this top event does not directly lead to core damage because ADS Stage 4 has successfully depressurized the RCS and there is sufficient time for the operator to establish injection through the RNS.

Table 10-6. SLOCA Event Tree Description (cont.)

Top Event	Top Event Description
RNS	This top event is associated with using the RNS to provide low pressure injection to the RCS with operator action HEPO-RNSINJ and HEPO-RNSIRWST using ES-1.3. Success for this top event (RNS-1-PLM-L) includes successful operator action and the equipment functioning to align and start one out of two RNS pumps to take suction from the cask loading pit (CLP), then to realign the RNS pump to take suction from the IRWST to maintain flow into the RV through one out of two DVI lines. Failure of this top event leads directly to core damage because the RNS is addressed when IRWST injection is not available.
RECIRC	This top event is associated with containment sump recirculation on a PMS signal or operator action HEPO-RECIRC using E-1. The success of this top event (RRWST-1-PX-DM) requires one out of four containment sump recirculation line squib valves to actuate and provide flow into the RV via the DVI lines. Failure of this top event leads to core damage because long term cooling is not established.

Table 10-7. LEAK Event Tree Description

Top Event	Top Event Description
REACTOR TRIP	This top event is associated with PMS and DAS reactor trip signals and operator action HEPO-RT using E-0. An RCS Leak initiator not mitigated by CVS requires a reactor trip. Reactor trip (RT-PX-DX-LOCA) is successful when the control rods are inserted into the core and reactivity control is achieved. Failure of this top event results in a transfer to reactor trip failure event tree LOCA-NOTRIP.
SS FAULT	Because the RCS leak is a slow depressurization of the RCS, the initial part of the event is similar to a transient with an S signal. After reactor trip the secondary side relief valves will likely be challenged. The success for this top event (SGS-SS-PA-PLA) is defined as one out of two PORVs opening, or one out of two safety valves (the two with the lowest set pressure) opening and relieving steam, or one turbine bypass valve dumping steam to the condenser. In addition, turbine trip (steam flow stopped to both the high pressure and low pressure turbines) must be successful. Because more than one PORV or MSSV may open after a reactor trip, the success for the valves reclosing is one PORV or block valve on each steam line reclose and two out of two MSSVs reclose. Credit is not taken for the operator to close the PORV block valve. Failure of this top event, the required valves failing to open or failing to reclose, results in a transfer to secondary side failure event tree LOCA-SSFAULT.
PRHR	This top event is associated with the PRHR heat exchanger actuation on a PMS or DAS signal or operator action HEPO-PRHR using E-0. The success of this top event (PRHR-PX-DX-L) requires one out of two of the PRHR heat exchanger control valves to open and establish flow through the PRHR heat exchanger. In addition, one out of two IRWST gutter isolation valves must close to return condensate to the IRWST to sustain long term cooling. Failure of this top event requires RCS depressurization and IRWST or RNS injection to prevent core damage.
CMT	This top event is associated with CMT actuation on a PMS or DAS signal or operator action HEPO-CMT using E-0. The success of this top event (CMT-1-PX-DX-BD) requires one out of two CMTs to inject through one out of two parallel valves on the discharge piping, four out of four RCPs to trip, and a CMT actuation signal to ADS. If this top event fails, then accumulator injection is required to provide water to the RCS prior to injection from the IRWST.

Table 10-7. LEAK Event Tree Description (cont.)

Top Event	Top Event Description
ADS23	This top event is associated with ADS Stages 1-3 actuation on a PMS signal or operator action HEPO-ADS-C1 or HEPO-ADS-C2 using E-1 or the Foldout Page for E-1. There are different success criteria for ADS23 (ADS23-2-PX-DM-C1, ADS23-2-PM-DM-C2, ADS23-3-PX-DM-C1). For ADS23-2-PX-DM-C1 and ADS23-2-PM-DM-C2, success is two out of four ADS Stages 2 and 3 valves open and discharge into the IRWST. ADS23-2-PX-DM-C1 is used on the top CMT success path because both automatic and manual actuations via the PMS are possible. ADS23-2-PM-DM-C2 is used on the CMT failure paths because automatic actuation via the PMS will not occur because either the signal fails or the CMT valves fail and the CMT Low level input to actuate ADS will not be generated. For ADS23-3-PX-DM-C1, success is three out of four ADS Stages 2 and 3 valves open and discharge into the IRWST. This is used when top event PRHR fails and top event CMT is successful to achieve the necessary RCS depressurization prior to ADS Stage 4 actuation. If top events PRHR and CMT are successful and ADS23 fails, core damage can be prevented by successful operation of ADS4 and IRWST or RNS injection.
ACC	For this event, the accumulators provide a source of water when the CMTs fail, prior to injection from the IRWST, to maintain water in the core. The success of this top event (ACC-1) requires one out of two accumulators to inject into the DVI line, when the RCS pressure is below the accumulator pressure. Failure of this top event leads directly to core damage because it is addressed only on the failure paths of top event CMT.
ADS4	This top event is associated with ADS Stage 4 actuation on a PMS signal or operator action HEPO-ADS4-C1 or HEPO-ADS4-C2 using E-1 or the Foldout Page for E-1. The success criteria for this top event (ADS4-2L-PX-DM-C1, ADS4-2L-PM-DM-C2) are one out of two ADS Stage 4 valves on each loop (two out of four total) actuating and providing a signal for IRWST gravity injection and recirculation. ADS4-2L-PX-DM-C1 is used when top event CMT is successful because both automatic and manual actuations via the PMS are possible. ADS4-2L-PM-DM-C2 is used when top event CMT fails because there is no automatic PMS actuation and the operator action is based on RCS hot leg level. Failure of ADS4 does not lead directly to core damage if sufficient RCS depressurization has occurred to enable RNS injection to be successful.
IRWST	This top event is associated with IRWST gravity injection actuation on a PMS ADS Stage 4 actuation signal or operator action HEPO-INJ using E-1. The success of this top event (IRWST-1-PX-DM) requires one out of four gravity injection line squib valves to actuate and provide IRWST injection into the RV via the DVI lines. Failure of this top event does not directly lead to core damage because ADS Stage 4 has successfully depressurized the RCS and there is sufficient time for the operator to establish injection through the RNS.

Table 10-7. LEAK Event Tree Description (cont.)

Top Event	Top Event Description
RNS	This top event is associated with using the RNS to provide low pressure injection to the RCS with operator action HEPO-RNSINJ and HEPO-RNSIRWST using ES-1.3. Success for this top event (RNS-1-PLM-L) includes successful operator action and the equipment functioning to align and start one out of two RNS pumps to take suction from the cask loading pit (CLP), then to realign the RNS pump to take suction from the IRWST to maintain flow into the RV through one out of two DVI lines. Failure of this top event leads directly to core damage because the RNS is addressed when IRWST injection is not available.
RECIRC	This top event is associated with containment sump recirculation on a PMS signal or operator action HEPO-RECIRC using E-1. The success of this top event (RRWST-1-PX-DM) requires one out of four containment sump recirculation line squib valves to actuate and provide flow into the RV via the DVI lines. Failure of this top event leads to core damage because long term cooling is not established.

Table 10-8. SPADS13 Event Tree Description

Top Event	Top Event Description
REACTOR TRIP	This top event is associated with PMS and DAS reactor trip signals and operator action HEPO-RT using E-0. Void formation is not sufficient to shut down the reactor core. Reactor trip (RT-PX-DX-LOCA) is successful when the control rods are inserted into the core and reactivity control is achieved. Failure of this top event results in a transfer to reactor trip failure event tree LOCA-NOTRIP.
CMT	Similar to the MLOCA event, credit is not taken for operator action to actuate the CMTs due to timing considerations. The success of this top event (CMT-1-PA-DA) requires one out of two CMTs to inject through one out of two parallel valves on the discharge piping, four out of four RCPs to trip, and a CMT actuation signal to ADS. If this top event fails, then accumulator injection is required to provide water to the RCS.
ACC	For this event, the accumulators provide a source of water when the CMTs fail, prior to injection from the IRWST, to maintain water in the core. The success of this top event (ACC-1) requires one out of two accumulators to inject into the DVI line, when the RCS pressure is below the accumulator pressure. Failure of this top event leads directly to core damage because it is addressed only on the failure paths of top event CMT.
ADS23	This top event is associated with ADS Stages 1-3 actuation on a PMS signal or operator action HEPO-ADS-C1 or HEPO-ADS-C2 using E-1 or the Foldout Page for E-1. The spurious opening of some number of ADS Stages 1-3 valves initiates this event. The success criteria require two out of four ADS Stages 2 and 3 valves (similar to what is required for the traditional MLOCA) in addition to the valve(s) that opened causing the IE. If all of the ADS Stages 1-3 valves spuriously open, then there is no failure of this top event. The success criteria for ADS23 (ADS23-2-PX-DM-C1, ADS23-2-PM-DM-C2) are two out of four ADS Stages 2 and 3 valves open and discharge into the IRWST in addition to the valve(s) that opened causing the IE. ADS23-2-PX-DM-C1 is used on the CMT success path because both automatic and manual actuations via the PMS are possible. ADS23-2-PM-DM-C2 is used on the CMT failure path because automatic actuation via the PMS will not occur because either the signal fails or the CMT valves fail and the CMT Low level input to actuate ADS will not be generated.

Table 10-8. SPADS13 Event Tree Description (cont.)

Top Event	Top Event Description
ADS4	This top event is associated with ADS Stage 4 actuation on a PMS signal or operator action HEPO-ADS4-C1 or HEPO-ADS4-C2 using E-1 or the Foldout Page for E-1. The success criteria for this top event (ADS4-2L-PX-DM-C1, ADS4-2L-PM-DM-C2) are one out of two ADS Stage 4 valves on each loop (two out of four total) actuating and providing a signal for IRWST gravity injection and recirculation. ADS4-2L-PX-DM-C1 is used when top event CMT is successful because both automatic and manual actuations via the PMS are possible. ADS4-2L-PM-DM-C2 is used when CMT fails because there is no automatic PMS actuation and the operator action is based on RCS hot leg level. Failure of ADS4 leads directly to core damage on the failure paths of ADS23 because there is insufficient RCS depressurization for IRWST or RNS injection. On success paths of ADS23, failure of ADS4 does not lead directly to core damage because there is sufficient RCS depressurization to allow RNS injection to be successful.
IRWST	This top event is associated with IRWST gravity injection actuation on a PMS signal or operator action HEPO-INJ using E-1. The success of this top event (IRWST-1-PX-DM) requires one out of four gravity injection line squib valves to actuate and provide IRWST injection into the RV via the DVI lines. Failure of this top event does not directly lead to core damage because ADS Stage 4 has successfully depressurized the RCS and there is sufficient time for the operator to establish injection through the RNS.
RNS	This top event is associated with using the RNS to provide low pressure injection to the RCS with operator action HEPO-RNSINJ and HEPO-RNSIRWST using ES-1.3. Success for this top event (RNS-1-PLM-L) includes successful operator action and the equipment functioning to align and start one out of two RNS pumps to take suction from the cask loading pit (CLP), then to realign the RNS pump to take suction from the IRWST to maintain flow into the RV through one out of two DVI lines. Failure of this top event leads directly to core damage because the RNS is addressed when IRWST injection is not available.
RECIRC	This top event is associated with containment sump recirculation on a PMS signal or operator action HEPO-RECIRC using E-1. The success of this top event (RRWST-1-PX-DM) requires one out of four containment sump recirculation line squib valves to actuate and provide flow into the RV via the DVI lines. Failure of this top event leads to core damage because long term cooling is not established.

Table 10-9. SPADS4 Event Tree Description

Top Event	Top Event Description
# ADS4 VALVES	This branch in the event tree separates the tree into different events based on the number of ADS Stage 4 valves that spuriously open. The top branch (SPADS4-2-IE) models either two ADS Stage 4 valves in the same compartment or all four ADS Stage 4 valves spuriously opening which results in an LLOCA. The top branch does not require a reactor trip because the LLOCA event has sufficient void formation in the core to shut down the reactor. The bottom branch (SPADS4-1-IE) models one ADS Stage 4 valve spuriously opening which results in an MLOCA event.
REACTOR TRIP	This top event is associated with PMS and DAS reactor trip signals and operator action HEPO-RT using E-0. For an MLOCA, void formation is not sufficient to shut down the reactor core, a reactor trip is required. Reactor trip (RT-PX-DX-LOCA) is successful when the control rods are inserted into the core and reactivity control is achieved. Failure of this top event results in a transfer to reactor trip failure event tree LOCA-NOTRIP.
CMT	There are two sets of success criteria for this top event. For the top portion of the event tree, the success of this top event (CMT-2-PA-DA) requires two out of two CMTs to inject. Each CMT must inject through one out of two parallel valves on the discharge piping and at least one provides a CMT actuation signal to ADS. Failure of this top event leads directly to core damage because there is insufficient water inventory for the core and insufficient time for operator action. For the bottom portion of the event tree, the success of this top event (CMT-1-PA-DA) requires one out of two CMTs to inject through one out of two parallel valves on the discharge piping, four out of four RCPs to trip, and a CMT actuation signal to ADS. For this case, the CMTs will be actuated automatically either through the PMS or DAS. Similar to the MLOCA event, credit is not taken for operator action to actuate the CMTs due to timing considerations. If this top event fails, then accumulator injection is required to provide water to the RCS.
ACC	For LLOCAs, the accumulators provide the initial reflooding of the core. The CMTs alone do not have sufficient volume to mitigate an LLOCA. For MLOCAs, the accumulators provide a source of water when the CMTs fail, prior to injection from the IRWST, to maintain water in the core. The success of this top event (ACC-1) requires one out of two accumulators to inject into the DVI line, when the RCS pressure is below the accumulator pressure. Failure of this top event leads directly to core damage because there is insufficient makeup to the core.
ADS23	This top event is associated with ADS Stages 1-3 actuation on a PMS signal or operator action HEPO-ADS-C1 or HEPO-ADS-C2 using E-1 or the Foldout Page for E-1. The success criteria for ADS23 (ADS23-2-PX-DM-C1, ADS23-2-PM-DM-C2) are two out of four ADS Stages 2 and 3 valves open and discharge into the IRWST. ADS23-2-PX-DM-C1 is used on the CMT success path because both automatic and manual actuations via the PMS are possible. ADS23-2-PM-DM-C2 is used on the CMT failure path because automatic actuation via the PMS will not occur because either the signal fails or the CMT valves fail and the CMT Low level input to actuate ADS will not be generated. Failure of this top event can lead to a non-core damage state if top event ADS4 is successful.

Table 10-9. SPADS4 Event Tree Description (cont.)

Top Event	Top Event Description
ADS4	This top event is associated with ADS Stage 4 actuation on a PMS signal or operator action HEPO-ADS4-C1 or HEPO-ADS4-C2 using E-1 or the Foldout Page for E-1. The success criteria for this top event (ADS4-1-PA-S4, ADS4-1-PX-DM-S4-C1, ADS4-1-PM-DM-S4-C2) depend on the number of ADS Stage 4 valves that spuriously open. If two valves spuriously open, then the success criteria are one out of two ADS Stage 4 valves on the other loop actuating and providing a signal for IRWST gravity injection and recirculation (ADS4-1-PA-S4). If all four valves spuriously open, then only the signals for IRWST gravity injection and recirculation are required (ADS4-1-PA-S4). If one valve spuriously opens, then the success criteria are one out of two ADS Stage 4 valves on the other loop actuating and providing a signal for IRWST gravity injection and recirculation (ADS4-1-PX-DM-S4-C1, ADS4-1-PM-DM-S4-C2). ADS4-1-PX-DM-S4-C1 is used when top event CMT is successful because both automatic and manual actuations via the PMS are possible. ADS4-1-PM-DM-S4-C2 is used when top event CMT fails because there is no automatic PMS actuation and the operator action is based on RCS hot leg level. In the top portion of the event tree, failure of ADS4 leads directly to core damage because there is insufficient RCS venting for the passive recirculation function or the signal to open the IRWST valves fails. In the bottom portion of the event tree failure of ADS4 does not lead directly to core damage if ADS23 is successful because there is sufficient RCS depressurization to allow RNS injection to be successful.
IRWST	This top event is associated with IRWST gravity injection actuation on a PMS signal or operator action HEPO-INJ using E-1. There are two sets of success criteria for this top event (IRWST-1-PA, IRWST-1-PX-DM). For both sets, the success of this top event requires one out of four gravity injection line squib valves to actuate and provide IRWST injection into the RV via the DVI lines. No credit is taken for operator action for IRWST-1-PA because it is part of an LLOCA event. IRWST-1-PX-DM is modelled for an MLOCA event and credit for operator action is taken. In the bottom portion of the event tree, failure of this top event does not directly lead to core damage because ADS Stage 4 has successfully depressurized the RCS and there is sufficient time for the operator to establish injection through the RNS.
RNS	This top event is associated with using the RNS to provide low pressure injection to the RCS with operator action HEPO-RNSINJ and HEPO-RNSIRWST using ES-1.3. Success for this top event (RNS-1-PLM-L) includes successful operator action and the equipment functioning to align and start one out of two RNS pumps to take suction from the cask loading pit (CLP), then to realign the RNS pump to take suction from the IRWST to maintain flow into the RV through one out of two DVI lines. Failure of this top event leads directly to core damage because the RNS is addressed when IRWST injection is not available.
RECIRC	This top event is associated with containment sump recirculation on a PMS signal or operator action HEPO-RECIRC using E-1. The success of this top event (RRWST-1-PX-DM) requires one out of four containment sump recirculation line squib valves to actuate and provide flow into the RV via the DVI lines. Failure of this top event leads to core damage because long term cooling is not established.

Table 10-10. SPIRWST Event Tree Description

Top Event	Top Event Description
# IRWST VALVES	This branch identifies the number of IRWST squib valves that spuriously open. The top branch (SPIRWST-2-IE) represents two or more IRWST squib valves spuriously opening. The bottom branch (SPIRWST-1-IE) represents one IRWST squib valve spuriously opening.
PXS CKV	This top event determines whether the check valve(s) upstream of the spuriously opened IRWST squib valve(s) remains intact and closed. In the top part of the event tree, success for this top event (IRWST-4-CKV) is four out of four check valves remain intact and closed. This bounds the cases of two or three valves spuriously opening. Success of this top event is transferred to the SLOCA event tree because the check valves are leaking RCS inventory into the IRWST through the 1/8” diameter hole in each check valve. Failure of this top event goes to core damage because of the uncertainty in the consequences that result from a larger LOCA into the IRWST, and because of failure of the piping upstream of the check valves, which is not designed for RCS pressure. In the bottom part of the event tree, success for this top event (IRWST-1-CKV) is one out of one IRWST check valve remains intact and closed. Success of this top event is transferred to the LEAK event tree because only one check valve is leaking into the IRWST. Failure of this top event is transferred to the DVILB event tree because the plant response is expected to be similar to failing a DVI line.

Table 10-11. CMTLB Event Tree Description

Top Event	Top Event Description
REACTOR TRIP	This top event is associated with PMS and DAS reactor trip signals and operator action HEPO-RT using E-0. Void formation is not sufficient to shut down the reactor core. Reactor trip (RT-PX-DX-LOCA) is successful when the control rods are inserted into the core and reactivity control is achieved. Failure of this top event results in a transfer to reactor trip failure event tree LOCA-NOTRIP.
CMT	This top event is associated with CMT actuation on a PMS or DAS signal or operator action HEPO-CMT using E-0. For this event, one CMT is unavailable due to the pipe break. Similar to the MLOCA event, credit is not taken for operator action to actuate the CMTs due to timing considerations. The success of this top event (CMT-1-PA-DA) requires one out of one CMT (without the broken pipe) to inject through one out of two parallel valves on the discharge piping, four out of four RCPs to trip, and a CMT actuation signal to ADS. If this top event fails, then accumulator injection is required to provide water to the RCS.
ACC	For this event, the accumulators provide a source of water when the CMTs fail, prior to injection from the IRWST, to maintain water in the core. The success of this top event (ACC-1) requires one out of two accumulators to inject into the DVI line, when the RCS pressure is below the accumulator pressure. Failure of this top event leads directly to core damage because it is addressed only on the failure path of top event CMT. If ACC fails, then there is no RCS makeup available prior to depressurization for IRWST injection and core damage occurs.
ADS23	This top event is associated with ADS Stages 1-3 actuation on a PMS signal or operator action HEPO-ADS-C1 or HEPO-ADS-C2 using E-1 or the Foldout Page for E-1. There are two sets of success criteria for ADS23 (ADS23-3-PX-DM-C1, ADS23-2-PM-DM-C2). The success criteria for ADS23-3-PX-DM-C1 are three out of four ADS Stages 2 and 3 valves open and discharge into the IRWST. For ADS23-2-PM-DM-C2 the success criteria are two out of four ADS Stages 2 and 3 valves open and discharge into the IRWST. ADS23-3-PX-DM-C1 is used on the CMT success path because both automatic and manual actuations via the PMS are possible. ADS23-2-PM-DM-C2 is used on the CMT failure path because automatic actuation via the PMS will not occur because either the signal fails or the CMT valves fail and the CMT Low level input to actuate ADS will not be generated. Failure of this top event leads directly to core damage because RCS depressurization and IRWST or RNS injection does not occur quickly enough to prevent core damage.

Table 10-11. CMTLB Event Tree Description (cont.)

Top Event	Top Event Description
ADS4	This top event is associated with ADS Stage 4 actuation on a PMS signal or operator action HEPO-ADS4-C1 or HEPO-ADS4-C2 using E-1 or the Foldout Page for E-1. The success criteria for this top event (ADS4-2L-PX-DM-C1, ADS4-2L-PM-DM-C2) are one out of two ADS Stage 4 valves on each loop (two out of four total) actuating and providing a signal for IRWST gravity injection and recirculation. ADS4-2L-PX-DM-C1 is used when top event CMT is successful because both automatic and manual actuations via the PMS are possible. ADS4-2L-PM-DM-C2 is used when top event CMT fails because there is no automatic PMS actuation and the operator action is based on RCS hot leg level. Failure of ADS Stage 4 does not lead directly to core damage because there is sufficient RCS depressurization to allow RNS injection to be successful.
IRWST	This top event is associated with IRWST gravity injection actuation on a PMS signal or operator action HEPO-INJ using E-1. The success of this top event (IRWST-1-PX-DM) requires one out of four gravity injection line squib valves to actuate and provide IRWST injection into the RV via the DVI lines. Failure of this top event does not directly lead to core damage because ADS Stage 4 has successfully depressurized the RCS and there is sufficient time for the operator to establish injection through the RNS.
RNS	This top event is associated with using the RNS to provide low pressure injection to the RCS and operator action HEPO-RNSINJ and HEPO-RNSIRWST using ES-1.3. Success for this top event (RNS-1-PLM-L) includes successful operator action and the equipment functioning to align and start one out of two RNS pumps to take suction from the CLP, then to realign the RNS pump to take suction from the IRWST to maintain flow into the RV through one out of two DVI lines. Failure of this top event leads directly to core damage because the RNS is addressed when IRWST injection is not available.
RECIRC	This top event is associated with containment sump recirculation on a PMS signal or operator action HEPO-RECIRC using E-1. The success of this top event (RRWST-1-PX-DM) requires one out of four containment sump recirculation line squib valves to actuate and provide flow into the RV via the DVI lines or to the suction line to the RNS. Failure of this top event leads to core damage because long term cooling is not established.

Table 10-12. DVILB Event Tree Description

Top Event	Top Event Description
REACTOR TRIP	This top event is associated with PMS and DAS reactor trip signals and operator action HEPO-RT using E-0. Void formation is not sufficient to shut down the reactor core. Like the MLOCA, this initiator requires a reactor trip. Reactor trip (RT-PX-DX-LOCA) is successful when the control rods are inserted into the core and reactivity control is achieved. Failure of this top event results in a transfer to reactor trip failure event tree LOCA-NOTRIP.
CMT	This top event is associated with CMT actuation on a PMS or DAS signal or operator action HEPO-CMT using E-0. The success of this top event (CMT-1-PA-DA) requires one out of one CMT (on the non-faulted DVI line) to inject through one out of two parallel valves on the discharge piping, four out of four RCPs to trip, and a CMT actuation signal to ADS. If this top event fails, then accumulator injection is required to provide water to the RCS.
ACC	For this event, the accumulators provide a source of water when the CMTs fail, prior to injection from the IRWST, to maintain water in the core. The success of this top event (ACC-1) requires one out of one accumulator (on the non-faulted DVI line) to inject into the DVI line, when the RCS pressure is below the accumulator pressure. Failure of this top event leads directly to core damage because it is addressed only on the failure path of top event CMT. If ACC fails, then there is no RCS makeup available prior to depressurization for IRWST injection and core damage occurs.
ADS23	This top event is associated with ADS Stages 1-3 actuation on a PMS signal or operator action HEPO-ADS-C1 or HEPO-ADS-C2 using E-1 or the Foldout Page for E-1. There are two sets of success criteria for ADS23 (ADS23-3-PX-DM-C1, ADS23-2-PM-DM-C2). The success criteria for ADS23-3-PX-DM-C1 are three out of four ADS Stages 2 and 3 valves open and discharge into the IRWST. For ADS23-2-PM-DM-C2, the success criteria are two out of four ADS Stages 2 and 3 valves open and discharge into the IRWST. ADS23-3-PX-DM-C1 is used on the CMT success path because both automatic and manual actuations via the PMS are possible. ADS23-2-PM-DM-C2 is used on the CMT failure path because automatic actuation via the PMS will not occur because either the signal fails or the CMT valves fail and the CMT Low level input to actuate ADS will not be generated. To cover a range of DVI line break sizes, top event ADS23 success for RCS depressurization is required to successfully actuate ADS4. Therefore, failure of this top event leads directly to core damage.
ADS4	This top event is associated with ADS Stage 4 actuation on a PMS signal or operator action HEPO-ADS4-C1 or HEPO-ADS4-C2 using E-1 or the Foldout Page for E-1. The success criteria for this top event (ADS4-3-PX-DM-C1, ADS4-3-PM-DM-C2) are three out of four ADS Stage 4 valves actuating and providing a signal for IRWST gravity injection and recirculation. ADS4-3-PX-DM-C1 is used when top event CMT is successful because both automatic and manual actuations via the PMS are possible. ADS4-3-PM-DM-C2 is used when top event CMT fails because there is no automatic PMS actuation and the operator action is based on RCS hot leg level. Failure of ADS4 leads directly to core damage because there is insufficient RCS depressurization for IRWST injection.

Table 10-12. DVILB Event Tree Description (cont.)

Top Event	Top Event Description
IRWST	This top event is associated with IRWST gravity injection actuation on a PMS signal or operator action HEPO-INJ using E-1. The success of this top event (IRWST-1-PX-DM) requires one out of two gravity injection line squib valves (on the non-faulted DVI line) to actuate and provide IRWST injection into the RV. Failure of this top event leads directly to core damage because RNS is unavailable for this event.
RECIRC	This top event is associated with containment sump recirculation on a PMS signal or operator action HEPO-RECIRC using E-1. The success of this top event (RRWST-1-PX-DM) requires one out of four containment sump recirculation line squib valves to actuate and provide flow into the RV via the DVI lines. Failure of this top event leads to core damage because long term cooling is not established.

Table 10-13. PRHRLB Event Tree Description

Top Event	Top Event Description
REACTOR TRIP	This top event is associated with PMS and DAS reactor trip signals and operator action HEPO-RT using E-0. Because this event covers a range of break sizes, it is modelled that void formation is not sufficient to shut down the reactor core; therefore, reactor trip is required. Reactor trip (RT-PX-DX-LOCA) is successful when the control rods are inserted into the core and reactivity control is achieved. Failure of this top event results in core damage because an ATWS event requires decay heat removal and the PRHR heat exchanger function fails due to the line break.
CMT	The success of this top event (CMT-2-PA-DA) requires two out of two CMTs to inject, four out of four RCPs to trip, and a CMT actuation signal to ADS. Each CMT must inject through one out of two parallel valves on the discharge piping. Failure of this top event leads directly to core damage because there is insufficient water inventory for the core and insufficient time for operator action.
ADS23	The success criteria for ADS23 (ADS23-3-PA) are three out of four ADS Stages 2 and 3 valves open and discharge into the IRWST. Failure of this top event leads directly to core damage because depressurization and IRWST injection does not occur in time to prevent core damage.
ACC	To cover a range of break sizes, it is modelled that the CMTs alone do not have sufficient volume to mitigate the loss of RCS inventory. The success of this top event (ACC-1) requires one out of two accumulators to inject into the DVI line, when the RCS pressure is below the accumulator pressure.
ADS4	The success criteria for this top event (ADS4-2L-PA) are one out of two ADS Stage 4 valves on each loop (two out of four total) actuating and providing a signal for IRWST gravity injection and recirculation. Failure of ADS4 leads directly to core damage because there is insufficient RCS depressurization for IRWST injection.
IRWST	The success of this top event (IRWST-1-PA) requires one out of four gravity injection line squib valves to actuate and provide IRWST injection into the RV via the DVI lines. Failure of this top event leads directly to core damage because no credit is taken for the operator to establish injection through the RNS.
RECIRC	This top event is associated with containment sump recirculation on a PMS signal or operator action HEPO-RECIRC using E-1. Operator action is included for this top event because switching from IRWST injection to recirculation will occur after more than 2 hours. The success of this top event (RRWST-1-PX-DM) requires one out of four containment sump recirculation line squib valves to actuate and provide flow into the RV via the DVI lines. Failure of this top event leads to core damage because long term cooling is not established.

Table 10-14. SGTR Event Tree Description

Top Event	Top Event Description
REACTOR TRIP	This top event is associated with PMS and DAS reactor trip signals and operator action HEPO-RT using E-0. Reactor trip (RT-PX-DX-LOCA) is successful when the control rods are inserted into the core and reactivity control is achieved. Failure of this top event results in a transfer to a reactor trip failure event tree.
SS FAULT	The success for this top event (SGS-SS-PA-PLA) is defined as one out of two PORVs opening, or one out of two safety valves (the two with the lowest set pressure) opening and relieving steam, or one turbine bypass valve dumping steam to the condenser. In addition, turbine trip (steam flow stopped to both the high pressure and low pressure turbines) must be successful. Because more than one PORV or MSSV may open after a reactor trip, the success for the valves reclosing is one PORV or block valve on each steam line reclose and two out of two MSSVs reclose, or one turbine bypass valve recloses. Credit is not taken for the operator to close the PORV block valve. Failure of this top event, the required valves failing to open or failing to reclose, results in core damage if top event CMT also fails because the plant conditions are beyond those modelled in the success criteria analyses.
CMT	This top event is associated with CMT actuation on a PMS or DAS signal or operator action HEPO-CMT using E-0. The success of this top event (CMT-1-PX-DX, CMT-1-PA-DA) requires one out of two CMTs to inject through one out of two parallel valves on the discharge piping, four out of four RCPs to trip, and a CMT actuation signal to ADS. CMT-1-PX-DX is used on the success path of top event SS FAULT because there is sufficient time for operator action to initiate the CMTs. If CMT-1-PX-DX fails, then an accumulator is required on the RCS depressurization paths to provide RCS inventory makeup to prevent core damage. CMT-1-PA-DA is used on the failure path of top event SS FAULT because the path is treated like the secondary side break event trees and requires automatic actuation of the CMTs. Failure of CMT-1-PA-DA leads to core damage because a CMT is required to operate for secondary side break conditions.
PRHR	This top event is associated with PRHR actuation on a PMS signal or operator action HEPO-PRHR using E-0. The success of this top event (PRHR-PX-DM) requires one out of two of the PRHR heat exchanger control valves to open and establish flow through the PRHR heat exchanger. In addition, one out of two IRWST gutter isolation valves must close to return condensate to the IRWST to sustain long-term cooling. Failure of this top event requires SFW or RCS depressurization via the ADS valves and IRWST or RNS injection/recirculation to prevent core damage.

Table 10-14. SGTR Event Tree Description (cont.)

Top Event	Top Event Description
SFW	This top event is associated with SFW actuation on a PLS signal or operator action HEPO-SFWS using E-0, operator action HEPO-SFWCD using ES-0.4 to perform the plant cooldown with SFW, and operator action for refilling the CST following the CST alarm response procedure. The success of this top event (SFW-1-PLX-C-SGTR) requires one out of two SFW pumps providing flow through the SFCV to the intact SG removing decay heat from the RCS and the operator action to control the cooldown. In addition, one out of two blowdown isolation valves close on the intact steam generator, and one SG PORV must operate to dump the steam from the intact SG. This top event also includes the refill of the CST. Failure of this top event requires RCS depressurization via the ADS valves and IRWST or RNS injection/recirculation to prevent core damage.
I&I	This top event is associated with operator action HEPO-SGI using E-3 to isolate the faulted SG. The success of this top event (SGI-1-PLM) requires the ruptured SG to be isolated by the closure of the valves listed in E-3 including CVS isolation to the ruptured SG. In addition, the MFW line to the ruptured SG must be isolated (this occurs on the S signal). SG cooldown using SFW is not credited if this top event fails because SFW may be isolated on a High SG level signal. If this top event fails, core damage can be prevented by successful SG overfill protection and PRHR operation, or by RCS depressurization via the ADS valves and IRWST or RNS injection/recirculation.
OFILL	This top event is associated with the PMS automatic protection features to prevent SG overfill and operator action HEPO-OFILL using E-3. The success of this top event (SGI-1-PX) requires the termination of CVS, and SFW flow to both SGs. In addition, the MFW line to the ruptured SG must be isolated (this occurs on the S signal). If this top event fails, RCS depressurization via the ADS valves and IRWST or RNS injection/recirculation is needed to prevent core damage.
ADS23	This top event is associated with ADS Stages 1-3 actuation on a PMS signal or operator action HEPO-ADS-C1-SGTR or HEPO-ADS-C2-SGTR using E-3. The success criteria for ADS23 (ADS23-2-PX-DM-C1-SGTR, ADS23-2-PM-DM-C2-SGTR) are two out of four ADS Stages 2 and 3 valves open and discharge into the IRWST. The event tree branch names include a "–SGTR" because the associated operator action for the SGTR event is based on E-3. ADS23-2-PX-DM-C1-SGTR is used on the CMT success path because both automatic and manual actuations via the PMS are possible. ADS23-2-PM-DM-C2-SGTR is used on the CMT failure path because automatic actuation via the PMS will not occur because either the signal fails or the CMT valves fail and the CMT Low level input to actuate ADS will not be generated. Failure of this top event leads to core damage.
ACC	For this event, the accumulators provide a source of water when the CMTs fail, prior to injection from the IRWST, to maintain water in the core. The success of this top event (ACC-1) requires one out of two accumulators to inject into the DVI line, when the RCS pressure is below the accumulator pressure. Failure of this top event leads directly to core damage because it is addressed only when top event CMT has failed.

Table 10-14. SGTR Event Tree Description (cont.)

Top Event	Top Event Description
ADS4	This top event is associated with ADS Stage 4 actuation on a PMS signal or operator action HEPO-ADS4-C1 or HEPO-ADS4-C2 using E-1 or the Foldout Page for E-1. The success criteria for this top event (ADS4-2L-PX-DM-C1, ADS4-2L-PM-DM-C2) are one out of two ADS Stage 4 valves on each loop (two out of four total) actuating and providing a signal for IRWST gravity injection and recirculation. ADS4-2L-PX-DM-C1 is used when CMT is successful because both automatic and manual actuations via the PMS are possible. ADS4-2L-PM-DM-C2 is used when top event CMT fails because there is no automatic PMS actuation and the operator action is based on RCS hot leg level. Failure of ADS4 leads directly to core damage.
IRWST	This top event is associated with IRWST gravity injection actuation on a PMS signal or operator action HEPO-INJ using E-1. The success of this top event (IRWST-1-PX-DM) requires one out of four gravity injection line squib valves to actuate and provide IRWST injection into the RV via the DVI lines. Failure of top event IRWST does not directly lead to core damage because sufficient RCS depressurization occurs and there is sufficient time for the operator to establish injection through the RNS.
RNS	This top event is associated with using the RNS to provide low pressure injection to the RCS and operator action HEPO-RNSINJ and HEPO-RNSIRWST using ES-1.3. Success for this top event (RNS-1-PLM-L) includes successful operator action and the equipment functioning to align and start one out of two RNS pumps to take suction from the CLP, then to realign the RNS pump to take suction from the IRWST to maintain flow into the RV through one out of two DVI lines. Failure of this top event leads directly to core damage because top event RNS is addressed when IRWST injection is not available.
RECIRC	This top event is associated with containment sump recirculation on a PMS signal or operator action HEPO-RECIRC using E-1. The success of this top event (RRWST-1-PX-DM) requires one out of four containment sump recirculation line squib valves to actuate and provide flow into the RV via the DVI lines or to the suction line to the RNS. Failure of this top event leads to core damage because long-term cooling is not established.

Table 10-15. ISL-CVS Event Tree Description

Top Event	Top Event Description
ISO	This top event is associated with a PMS signal to isolate CVS and operator action HEPO-CVSISO using ECA-1.1 or HEPO-CVSISO-Z using E-0. This top event is for the isolation of the RCS leak outside containment. On a PMS Low-1 pressuriser water level signal valves CVS-PL-V001, -002, and -003 close to prevent uncovering of the pressuriser heater elements. The success of this top event (CVSISO-PX-CIE) varies based on the specific CVS ISLOCA event. The system fault tree logic addresses the appropriate success criteria for the specific ISLOCA event. Failure of this top event leads to core damage because RCS inventory is continually lost outside containment.
REACTOR TRIP	This top event is associated with PMS and DAS reactor trip signals and operator action HEPO-RT using in E-0. Reactor trip (RT-PX-DX-LOCA) is successful when the control rods are inserted into the core and reactivity control is achieved. Failure of this top event results in a transfer to the ATWS-LMFW event tree.
SS FAULT	Because the ISLOCA, especially on the small end of the break size range, can be a slow depressurization of the RCS, the initial part of the event is similar to a transient with an S signal. After reactor trip and isolation of the leak, the secondary side relief valves will likely be challenged. The success for this top event (SGS-SS-PA-PLA) is defined as one out of two PORVs opening, or one out of two safety valves (the two with the lowest set pressure) opening and relieving steam, or one turbine bypass valve dumping steam to the condenser. In addition, turbine trip (steam flow stopped to both the high pressure and low pressure turbines) must be successful. Because more than one PORV or MSSV may open after a reactor trip, the success for the valves reclosing is one PORV or block valve on each steam line reclose and two out of two MSSVs reclose, or one turbine bypass valve recloses. Credit is not taken for the operator to close the PORV block valve. Failure of this top event, the required valves failing to open or failing to reclose, results in a transfer to steam line break (SLB) upstream of the main steam isolation valves (MSIVs) event tree SLBU.
PRHR	This top event is associated with the PRHR heat exchanger actuation on a PMS or DAS signal or operator action HEPO-PRHR using E-0. The success of this top event (PRHR-PX-DX) requires one out of two of the PRHR heat exchanger control valves to open and establish flow through the PRHR heat exchanger. In addition, one out of two IRWST gutter isolation valves must close to return condensate to the IRWST to sustain long term cooling. Failure of this top event requires Startup Feedwater (SFW) or RCS depressurization and IRWST or RNS injection to prevent core damage.

Table 10-15. ISL-CVS Event Tree Description (cont.)

Top Event	Top Event Description
SFW	This top event is associated with SFW actuation on a Plant Control System (PLS) signal or operator action HEPO-SFWS following E-0 or HEPO-SFWM following FR-H.1, and operator action for refilling the condensate storage tank (CST) following the CST alarm response procedure. The success of this top event (SFW-1-PLX-C) for decay heat removal requires one out of two SFW pumps providing flow through one out of two startup feedwater control valves (SFCVs) to one out of two steam generators (SGs), and one out of two blowdown isolation valves close on the SG loop. One SG PORV or one MSSV must operate to dump the steam from the SG. In addition, the CST must be refilled. Failure of this top event requires RCS depressurization via the ADS valves and IRWST or RNS injection/recirculation to prevent core damage.
PZR SV	Success of this top event (PZRSV-2) is the opening of one out of two pressuriser safety valves and the closing of two out of two pressuriser safety valves. Failure of this top event results in a transfer to the MLOCA event tree.
CMT	This top event is associated with CMT actuation on a PMS or DAS signal or operator action HEPO-CMT-GT using FR-H.1. The success of this top event (CMT-1-PX-DX-GT) requires one out of two CMTs to inject through one out of two parallel valves on the discharge piping, four out of four RCPs to trip, and a CMT actuation signal to ADS. If this top event fails, then accumulator injection is required to provide water to the RCS prior to injection from the IRWST.
ADS23	This top event is associated with ADS Stages 1-3 actuation on a PMS signal or operator action HEPO-ADS-GT using FR-H.1. There are different success criteria for ADS23 (ADS23-3-PX-DM-GT, ADS23-2-PM-DM-GT). The success criteria for ADS23-3-PX-DM-GT are three out of four ADS Stages 2 and 3 valves open and discharge into the IRWST. This is used when top event PRHR fails and top event CMT is successful to achieve the necessary RCS depressurization prior to ADS Stage 4 actuation. ADS23-3-PX-DM-GT is used on the CMT success path because both automatic and manual actuations via the PMS are possible. The success criteria for ADS23-2-PM-DM-GT are two out of four ADS Stages 2 and 3 valves open and discharge into the IRWST. ADS23-2-PM-DM-GT is used on the CMT failure path because automatic actuation via the PMS will not occur because either the signal fails or the CMT valves fail and the CMT Low level input to actuate ADS will not be generated. Failure of this top event leads directly to core damage because decay heat removal has been lost and the RCS pressure is not low enough to successfully use the ADS Stage 4 valves.
ACC	For this event, the accumulators provide a source of water when the CMTs fail, prior to injection from the IRWST, to maintain water in the core. The success of this top event (ACC-1) requires one out of two accumulators to inject into the DVI line, when the RCS pressure is below the accumulator pressure. Failure of this top event leads directly to core damage because it is addressed only on the failure paths of top event CMT.

Table 10-15. ISL-CVS Event Tree Description (cont.)

Top Event	Top Event Description
ADS4	This top event is associated with ADS Stage 4 actuation on a PMS signal or operator action HEPO-ADS4-C1 or HEPO-ADS4-C2 using E-1 or the Foldout Page for E-1. The success criteria for this top event (ADS4-2L-PX-DM-C1, ADS4-2L-PM-DM-C2) are one out of two ADS Stage 4 valves on each loop (two out of four total) actuating and providing a signal for IRWST gravity injection and recirculation. ADS4-2L-PX-DM-C1 is used when top event CMT is successful because both automatic and manual actuations via the PMS are possible. ADS4-2L-PM-DM-C2 is used when top event CMT fails because automatic actuation via the PMS is not available. ADS4 is only modelled on the success paths of ADS23; therefore, failure of ADS4 does not lead directly to core damage because RNS injection and recirculation is possible due to the depressurization of the RCS by the ADS Stages 2 and 3 valves.
IRWST	This top event is associated with IRWST gravity injection actuation on a PMS signal or operator action HEPO-INJ using E-1 (note that E-1 would be entered from FR-H., or E-0). The success of this top event (IRWST-1-PX-DM) requires one out of four gravity injection line squib valves to actuate and provide IRWST injection into the RV via the DVI lines. Failure of this top event does not directly lead to core damage because ADS Stage 4 has successfully depressurized the RCS and there is sufficient time for the operator to establish injection through the RNS.
RNS	This top event is associated with using the RNS to provide low pressure injection to the RCS and operator action HEPO-RNSINJ and HEPO-RNSIRWST using ES-1.3. Success for this top event (RNS-1-PLM-L) includes successful operator action and the equipment functioning to align and start one out of two RNS pumps to take suction from the CLP, then to realign the RNS pump to take suction from the IRWST to maintain flow into the RV through one out of two DVI lines. Failure of this top event leads directly to core damage because top event RNS is addressed when IRWST injection is not available.
RECIRC	This top event is associated with containment sump recirculation on a PMS signal or operator action HEPO-RECIRC using E-1. The success of this top event (RRWST-1-PX-DM) requires one out of four containment sump recirculation line squib valves to actuate and provide flow into the RV via the DVI lines or to the suction line to the RNS. Failure of this top event leads to core damage because long term cooling is not established.

Table 10-16. GTRAN-WS Event Tree Description

Top Event	Top Event Description
REACTOR TRIP	This top event is associated with PMS and DAS reactor trip signals and operator action HEPO-RT using E-0. Note that a spurious S signal will also cause a reactor trip in the PMS. Reactor trip (RT-PX-DX-LOCA) is successful when the control rods are inserted into the core and reactivity control is achieved. RT-PX-DM-LOCA is used because the IE is a spurious S signal. Failure of this top event results in a transfer to the ATWS-LMFW event tree.
SS FAULT	The success for this top event (SGS-SS-PA-PLA) is defined as one out of two PORVs opening, or one out of two safety valves (the two with the lowest set pressure) opening and relieving steam, or one turbine bypass valve dumping steam to the condenser. In addition, turbine trip (steam flow stopped to both the high pressure and low pressure turbines) must be successful. Because more than one PORV or MSSV may open after a reactor trip, the success for the valves reclosing is one PORV or block valve on each steam line reclose and two out of two MSSVs reclose, or one turbine bypass valve recloses. Credit is not taken for the operator to close the PORV block valve. Failure of this top event, the required valves failing to open or failing to reclose, results in a transfer to SLB upstream of the MSIVs event tree SLBU.
PRHR	This top event is associated with the PRHR heat exchanger actuation on a PMS or DAS signal or operator action HEPO-PRHR using E-0. The success of this top event (PRHR-PX-DX) requires one out of two of the PRHR heat exchanger control valves to open and establish flow through the PRHR heat exchanger. In addition, one out of two IRWST gutter isolation valves must close to return condensate to the IRWST to sustain long term cooling. Failure of this top event requires SFW or RCS depressurization and IRWST or RNS injection to prevent core damage.
SFW	This top event is associated with SFW actuation on a PLS signal or operator action HEPO-SFWS following E-0 or HEPO-SFWM following FR-H.1, and operator action for refilling the CST following the CST alarm response procedure. The success of this top event (SFW-1-PLX-C) for decay heat removal requires one out of two SFW pumps providing flow through one out of two SFCVs to one out of two SGs and one out of two blowdown isolation valves close on the SG loop. One SG PORV or one MSSV must operate to dump the steam from the SG. In addition, the CST must be refilled. Failure of this top event requires RCS depressurization via the ADS valves and IRWST or RNS injection/recirculation to prevent core damage.
PZR SV	Success of this top event (PZRSV-2) is the opening of one out of two pressuriser safety valves and the closing of two out of two pressuriser safety valves. Failure of this top event results in a transfer to the MLOCA event tree.

Table 10-16. GTRAN-WS Event Tree Description (cont.)

Top Event	Top Event Description
CMT	This top event is associated with CMT actuation on a PMS or DAS signal or operator action HEPO-CMT-GT using FR-H.1. The success of this top event (CMT-1-PX-DX-GT) requires one out of two CMTs to inject through one out of two parallel valves on the discharge piping, four out of four RCPs to trip, and a CMT actuation signal to ADS. No credit is taken for CMT actuation on the S signal that initiated the event. If this top event fails, then accumulator injection is required to provide water to the RCS prior to injection from the IRWST.
ADS23	This top event is associated with ADS Stages 1-3 actuation on a PMS signal or operator action HEPO-ADS-GT using FR-H.1. There are different success criteria for ADS23 (ADS23-2-PM-DM-GT, ADS23-3-PX-DM-GT). For ADS23-2-PM-DM-GT, success is two out of four ADS Stages 2 and 3 valves open and discharge into the IRWST. ADS23-2-PM-DM-GT is used on the CMT failure paths because automatic actuation via the PMS will not occur because either the signal fails or the CMT valves fail and the CMT Low level input to actuate ADS will not be generated. For ADS23-3-PX-DM-GT, success is three out of four ADS Stages 2 and 3 valves open and discharge into the IRWST. This is used when top event PRHR fails and top event CMT is successful to achieve the necessary RCS depressurization prior to ADS Stage 4 actuation. Failure of this top event leads directly to core damage because RCS depressurization and IRWST or RNS injection does not occur quickly enough to prevent core damage.
ACC	For this event, the accumulators provide a source of water when the CMTs fail, prior to injection from the IRWST, to maintain water in the core. The success of this top event (ACC-1) requires one out of two accumulators to inject into the DVI line, when the RCS pressure is below the accumulator pressure. Failure of this top event leads directly to core damage because it is addressed only on the failure paths of top event CMT.
ADS4	This top event is associated with ADS Stage 4 actuation on a PMS signal or operator action HEPO-ADS4-C1 or HEPO-ADS4-C2 using E-1 or the Foldout Page for E-1. The success criteria for this top event (ADS4-2L-PX-DM-C1, ADS4-2L-PM-DM-C2) are one out of two ADS Stage 4 valves on each loop (two out of four total) actuating and providing a signal for IRWST gravity injection and recirculation. ADS4-2L-PX-DM-C1 is used when top event CMT is successful because both automatic and manual actuations via the PMS are possible. ADS4-2L-PM-DM-C2 is used when top event CMT fails because there is no automatic PMS actuation and the operator action is based on RCS hot leg level. ADS4 is only modelled on the success paths of ADS23; therefore, failure of ADS4 does not lead directly to core damage because RNS injection and recirculation is possible due to the depressurization of the RCS by the ADS Stages 2 and 3 valves.

Table 10-16. GTRAN-WS Event Tree Description (cont.)

Top Event	Top Event Description
IRWST	This top event is associated with IRWST gravity injection actuation on a PMS signal or operator action HEPO-INJ using E-1. The success of this top event (IRWST-1-PX-DM) requires one out of four gravity injection line squib valves to actuate and provide IRWST injection into the RV via the DVI lines. Failure of this top event does not directly lead to core damage because ADS Stage 4 has successfully depressurized the RCS and there is sufficient time for the operator to establish injection through the RNS.
RNS	This top event is associated with using the RNS to provide low pressure injection to the RCS and operator action HEPO-RNSINJ and HEPO-RNSIRWST using ES-1.3. Success for this top event (RNS-1-PLM-L) includes successful operator action and the equipment functioning to align and start one out of two RNS pumps to take suction from the CLP, then to realign the RNS pump to take suction from the IRWST to maintain flow into the RV through one out of two DVI lines. Failure of this top event leads directly to core damage because top event RNS is addressed when IRWST injection is not available.
RECIRC	This top event is associated with containment sump recirculation on a PMS signal or operator action HEPO-RECIRC using E-1. The success of this top event (RRWST-1-PX-DM) requires one out of four containment sump recirculation line squib valves to actuate and provide flow into the RV via the DVI lines or to the suction line to the RNS. Failure of this top event leads to core damage because long term cooling is not established.

Table 10-17. GTRAN Event Tree Description

Top Event	Top Event Description
REACTOR TRIP	This top event is associated with PMS and DAS reactor trip signals and operator action HEPO-RT using E-0. Reactor trip (RT-PX-DX) is successful when the control rods are inserted into the core and reactivity control is achieved. Failure of this top event results in a transfer to the ATWS event tree.
SS FAULT	The success for this top event (SGS-SS-PA-PLA) is defined as one out of two PORVs opening, or one out of two safety valves (the two with the lowest set pressure) opening and relieving steam, or one turbine bypass valve dumping steam to the condenser. In addition, turbine trip (steam flow stopped to both the high pressure and low pressure turbines) must be successful. Because more than one PORV or MSSV may open after a reactor trip, the success for the valves reclosing is one PORV or block valve on each steam line reclose and two out of two MSSVs reclose, or one turbine bypass valve recloses. Credit is not taken for the operator to close the PORV block valve. Failure of this top event, the required valves failing to open or failing to reclose, results in a transfer to SLB upstream of the MSIVs event tree SLBU.
MFW	This top event is associated with MFW cooling using the PLS or operator action HEPO-MFW using ES 0.1. The loss of MFW IE, and support system IEs that result in the loss of MFW, fail this top event and are addressed in the system fault tree logic and the logic for the quantification model. The success of this top (MFW-1-PLX) event is one booster/MFW pump supplying water through two out of two SFCVs (one per loop) to two out of two SGs and one turbine bypass valve dumping steam to the condenser. Failure of this top event requires decay heat removal from the SFW system, the PRHR system, or RCS depressurization via the ADS valves and IRWST or RNS injection/recirculation to prevent core damage.
SFW	This top event is associated with SFW actuation on a PLS signal or operator action HEPO-SFWX using ES-0.1 and operator action for refilling the CST following the CST alarm response procedure. The success of this top event (SFW-1-PLX) for decay heat removal requires one out of two SFW pumps providing flow through two out of two SFCVs (one per loop) to two out of two SGs, and one out of two blowdown isolation valves close on each loop. One SG PORV or one MSSV must operate to dump the steam from the SG. In addition, the CST must be refilled. Failure of this top event requires operation of the PRHR system or RCS depressurization via the ADS valves and IRWST or RNS injection/recirculation to prevent core damage.
PRHR	This top event is associated with the PRHR heat exchanger actuation on a PMS or DAS or operator action HEPO-PRHR-GT using ES-0.1. The success of this top event (PRHR-PX-DX-GT) requires one out of two of the PRHR heat exchanger control valves to open and establish flow through the PRHR heat exchanger. In addition, one out of two IRWST gutter isolation valves must close to return condensate to the IRWST to sustain long term cooling. Failure of this top event requires RCS depressurization and IRWST or RNS injection to prevent core damage.

Table 10-17. GTRAN Event Tree Description (cont.)

Top Event	Top Event Description
PZR SV	Success of this top event (PZRSV-2) is the opening of one out of two pressuriser safety valves and the closing of two out of two pressuriser safety valves. Failure of this top event results in a transfer to the MLOCA event tree.
CMT	This top event is associated with CMT actuation on a PMS or DAS signal or operator action HEPO-CMT-GT using FR-H.1. The success of this top event (CMT-1-PX-DX-GT) requires one out of two CMTs to inject through one out of two parallel valves on the discharge piping, four out of four RCPs to trip, and a CMT actuation signal to ADS. If this top event fails, then accumulator injection is required to provide water to the RCS prior to injection from the IRWST.
ADS23	This top event is associated with ADS Stages 1-3 actuation on a PMS signal or operator action HEPO-ADS-GT using FR-H.1. There are different success criteria for ADS23 (ADS23-2-PM-DM-GT, ADS23-3-PX-DM-GT). For ADS23-2-PM-DM-GT, success is two out of four ADS Stages 2 and 3 valves open and discharge into the IRWST. ADS23-2-PM-DM-GT is used on the CMT failure path because automatic actuation via the PMS will not occur because either the signal fails or the CMT valves fail and the CMT Low level input to actuate ADS will not be generated. For ADS23-3-PX-DM-GT, success is three out of four ADS Stages 2 and 3 valves open and discharge into the IRWST. This is used when top event PRHR fails and top event CMT is successful to achieve the necessary RCS depressurization prior to ADS Stage 4 actuation. Failure of this top event leads directly to core damage because RCS depressurization and IRWST or RNS injection does not occur quickly enough to prevent core damage.
ACC	For this event, the accumulators provide a source of water when the CMTs fail, prior to injection from the IRWST, to maintain water in the core. The success of this top event (ACC-1) requires one out of two accumulators to inject into the DVI line, when the RCS pressure is below the accumulator pressure. Failure of this top event leads directly to core damage because it is addressed only on the failure paths of top event CMT.
ADS4	This top event is associated with ADS Stage 4 actuation on a PMS signal or operator action HEPO-ADS4-C1 or HEPO-ADS4-C2 using E-1 or the Foldout Page for E 1. The success criteria for this top event (ADS4-2L-PX-DM-C1, ADS4-2L-PM-DM-C2) are one out of two ADS Stage 4 valves on each loop (two out of four total) actuating and providing a signal for IRWST gravity injection and recirculation. ADS4-2L-PX-DM-C1 is used when top event CMT is successful because both automatic and manual actuations via the PMS are possible. ADS4-2L-PM-DM-C2 is used when top event CMT fails because there is no automatic PMS actuation and the operator action is based on RCS hot leg level. ADS4 is only modelled on the success paths of ADS23; therefore, failure of ADS4 does not lead directly to core damage because RNS injection and recirculation is possible due to the depressurization of the RCS by the ADS Stages 2 and 3 valves.

Table 10-17. GTRAN Event Tree Description (cont.)

Top Event	Top Event Description
IRWST	This top event is associated with IRWST gravity injection actuation on a PMS signal or operator action HEPO-INJ using E-1. The success of this top event (IRWST-1-PX-DM) requires one out of four gravity injection line squib valves to actuate and provide IRWST injection into the RV via the DVI lines. Failure of this top event does not directly lead to core damage because ADS Stage 4 has successfully depressurized the RCS and there is sufficient time for the operator to establish injection through the RNS.
RNS	This top event is associated with using the RNS to provide low pressure injection to the RCS and operator action HEPO-RNSINJ and HEPO-RNSIRWST using ES-1.3. Success for this top event (RNS-1-PLM-L) includes successful operator action and the equipment functioning to align and start one out of two RNS pumps to take suction from the CLP, then to realign the RNS pump to take suction from the IRWST to maintain flow into the RV through one out of two DVI lines. Failure of this top event leads directly to core damage because top event RNS is addressed when IRWST injection is not available.
RECIRC	This top event is associated with containment sump recirculation on a PMS signal or operator action HEPO-RECIRC using E-1. The success of this top event (RRWST-1-PX-DM) requires one out of four containment sump recirculation line squib valves to actuate and provide flow into the RV via the DVI lines or to the suction line to the RNS. Failure of this top event leads to core damage because long term cooling is not established.

Table 10-18. LOOP Event Tree Description

Top Event	Top Event Description
REACTOR TRIP	For the LOOP event, power is lost to the control rod drive mechanisms and the rods fall into the core. If the rods fail to insert, then there is a mechanical binding issue and no operator action is modelled. Reactor trip (RT-LP) is successful when the control rods are inserted into the core and reactivity control is achieved. For RT-LP, a trip signal is not required because power is lost to the control rods. Failure of this top event results in a transfer to the ATWS-LMFW event tree.
NO SBO	This top event is associated with starting the standby DGs on a PLS signal or operator action HEPO-SDG using AOP-323. The success of this top event (SBO-1-PLX) is the starting and running of one out of two of the standby DGs. Failure of this top event results in SBO conditions (no onsite or offsite ac power).
SS FAULT	The success for this top event (SGS-SS-PA-PLA) is defined as one out of two safety valves (the two with the lowest set pressure) opening and relieving steam. In addition, turbine trip (steam flow stopped to both the high pressure and low pressure turbines) must be successful. Because more than MSSV may open after a reactor trip, the success for the valves reclosing is two out of two MSSVs reclose. Failure of this top event, the required valves failing to open or failing to reclose, results in a transfer to SLB upstream of the MSIVs event tree SLBU.
SFW	This top event is associated with SFW actuation by a PLS signal or operator action HEPO-SFWX using ES-0.1and operator action for refilling the CST following the CST alarm response procedure. The success of this top event (SFW-1-PLX) for decay heat removal requires one out of two SFW pumps providing flow through two out of two SFCVs (one per loop) to two out of two SGs, and one out of two blowdown isolation valves close on each loop. One SG PORV or one MSSV must operate to dump the steam from the SG. In addition, the CST must be refilled. Failure of this top event requires the PRHR system or RCS depressurization via the ADS valves and IRWST or RNS injection/recirculation to prevent core damage.
PRHR	This top event is associated with the PRHR heat exchanger actuation on a PMS or DAS signal or operator action HEPO-PRHR-GT using ES-0.1. The success of this top event (PRHR-PX-DX-LP, PRHR-SB) requires one out of two of the PRHR heat exchanger control valves to open and establish flow through the PRHR heat exchanger. In addition, one out of two IRWST gutter isolation valves must close to return condensate to the IRWST to sustain long term cooling. PRHR-PX-DX-LP is used when the diesel generators are successful. PRHR-SB is used for SBO conditions. Failure of this top event requires RCS depressurization and IRWST or RNS injection to prevent core damage.

Table 10-18. LOOP Event Tree Description (cont.)

Top Event	Top Event Description
DISABLE TIMER	This top event (22HRTIMER) is associated with the operator action HEPO-22HRTIMER for SBO conditions to turn off the retentive timer that would actuate ADS at approximately 22 hours into the SBO event using AOP-323. ADS actuation is not required if PRHR is successful so the success path of this top event transfers to long term cooling event tree LTCP. Failure of this top event means that the 22 hour timer sends an actuation signal to ADS Stages 1-4. ADS actuation requires that top events CMT (or ACC), IRWST, and RECIRC be addressed.
PZR SV	Success of this top event (PZRSV-2) is the opening of one out of two pressuriser safety valves and the closing of two out of two pressuriser safety valves. Failure of this top event results in a transfer to the MLOCA event tree.
CMT	This top event is associated with CMT actuation on PMS or DAS signal or operator action HEPO-CMT-GT using FR-H.1. The success of this top event (CMT-1-PX-DX-LOOP, CMT-1-SB) requires one out of two CMTs to inject through one out of two parallel valves on the discharge piping, and a CMT actuation signal to ADS. CMT-1-PX-DX-LOOP is used when the DGs are successful. CMT-1-SB is used for the SBO portion of the tree. If this top event fails, then accumulator injection is required to provide water to the RCS prior to injection from the IRWST.
ADS23	This top event is associated with ADS Stages 1-3 actuation on a PMS signal or operator action HEPO-ADS-GT using FR-H-1. There are different success criteria for ADS23 (ADS23-2-PM-DM-GT, ADS23-3-PX-DM-GT, ADS23-3-PX, ADS23-2-PM). For ADS23-2-PM-DM-GT and ADS23-2-PM, success is two out of four ADS Stages 2 and 3 valves open and discharge into the IRWST. They are both used on the CMT failure paths because automatic actuation via the PMS will not occur because either the signal fails or the CMT valves fail and the CMT Low level input to actuate ADS will not be generated. ADS23-2-PM is used for SBO conditions because the DAS battery is only designed for 2 hours so DAS actuation is not modelled. For ADS23-3-PX-DM-GT and ADS23-3-PX, success is three out of four ADS Stages 2 and 3 valves open and discharge into the IRWST. This is used when top event PRHR fails and top event CMT is successful to achieve the necessary RCS depressurization prior to ADS Stage 4 actuation. ADS23-3-PX-DM-GT and ADS23-3-PX are used on the CMT success paths because both automatic and manual actuations via the PMS are possible. ADS23-3-PX is used for SBO conditions because the DAS battery is only designed for 2 hours so DAS actuation is not modelled. Failure of this top event leads directly to core damage because RCS depressurization and IRWST or RNS injection does not occur quickly enough to prevent core damage.
ACC	For this event, the accumulators provide a source of water when the CMTs fail, prior to injection from the IRWST, to maintain water in the core. The success of this top event (ACC-1) requires one out of two accumulators to inject into the DVI line, when the RCS pressure is below the accumulator pressure. Failure of this top event leads directly to core damage because it is addressed only on the failure paths of top event CMT.

Table 10-18. LOOP Event Tree Description (cont.)

Top Event	Top Event Description
ADS4	This top event is associated with ADS Stage 4 actuation on a PMS signal or operator action HEPO-ADS4-C1 or HEPO-ADS4-C2 using E-1 or the Foldout Page for E-1. The success criteria for this top event (ADS4-2L-PX-DM-C1, ADS4-2L-PM-DM-C2, ADS4-2L-PX-C1, ADS4-2L-PM-C2) are one out of two ADS Stage 4 valves on each loop (two out of four total) actuating and providing a signal for IRWST gravity injection and recirculation. ADS4-2L-PX-C1 and ADS4-2L-PM-C2 are used for SBO conditions because the DAS battery is only designed for 2 hours so DAS actuation is not modelled. ADS4-2L-PX-DM-C1 and ADS4-2L-PX-C1 are used when top event CMT is successful because both automatic and manual actuations via the PMS are possible. ADS4-2L-PM-DM-C2 and ADS4-2L-PM-C2 are used when top event CMT fails because there is no automatic PMS actuation and the operator action is based on RCS hot leg level. ADS4 is only modelled on the success paths of ADS23; therefore, except for SBO conditions, failure of ADS4 does not lead directly to core damage because RNS injection and recirculation is possible due to the depressurization of the RCS by the ADS Stages 2 and 3 valves. For SBO conditions, both top events ADS23 and ADS4 must be successful to prevent core damage.
IRWST	This top event is associated with IRWST gravity injection actuation on a PMS signal or operator action HEPO-INJ using E-1. The success of this top event (IRWST-1-PX-DM, IRWST-1-PX) requires one out of four gravity injection line squib valves to actuate and provide IRWST injection into the RV via the DVI lines. IRWST-1-PX is used for SBO conditions because the DAS battery is only designed for 2 hours so DAS actuation is not modelled. Except for SBO conditions, failure of this top event does not directly lead to core damage because ADS Stage 4 has successfully depressurized the RCS and there is sufficient time for the operator to establish injection through the RNS. For SBO conditions, the RNS system does not have power, therefore, the IRWST is the only source for injection after the ADS valves are actuated and its failure leads to core damage.
RNS	This top event is associated with using the RNS to provide low pressure injection to the RCS and operator action HEPO-RNSINJ and HEPO-RNSIRWST using ES-1.3. Success for this top event (RNS-1-PLM-L) includes successful operator action and the equipment functioning to align and start one out of two RNS pumps to take suction from the CLP, then to realign the RNS pump to take suction from the IRWST to maintain flow into the RV through one out of two DVI lines. Failure of this top event leads directly to core damage because top event RNS is addressed when IRWST injection is not available.
RECIRC	This top event is associated with containment sump recirculation on a PMS signal or operator action HEPO-RECIRC using E-1. The success of this top event (RRWST-1-PX-DM, RRWST-1-PX) requires one out of four containment sump recirculation line squib valves to actuate and provide flow into the RV via the DVI lines or to the suction line to the RNS. RRWST-1-PX is used for SBO conditions because the DAS battery is only designed for 2 hours so DAS actuation is not modelled. RRWST-1-PX-DM is used for top event ADS4 success paths because automatic opening of the recirculation valves will occur in the PMS on a Low-3 level signal from the IRWST and an ADS Stage 4 actuation signal. Failure of this top event leads to core damage because long term cooling is not established.

Table 10-19. SLBD Event Tree Description

Top Event	Top Event Description
REACTOR TRIP	A large steam line break is a rapid transient that requires a quick reactor trip. To bind this event, no credit is taken for the operator to manually trip the reactor. Reactor trip (RT-PA-DA) is successful when the control rods are inserted into the core and reactivity control is achieved. Note that for this transient, additional boration is needed to counter the effects of a steam line break cooldown. The boration is addressed in top events CMT and CVS. Failure of this top event results in core damage if SG isolation fails because the plant conditions are beyond those considered in the ATWS success criteria analyses.
ISO	The success of this top event (SGI-2-PA) is closure of one out of one MSIV on each loop, one MFW isolation valve, control valve, or check valve on each loop, and one out of two SG blowdown isolation valves on each loop. In addition, the SG PORV or block valve on both SGs must close to keep the SGs intact. On the reactor trip success path, successful isolation changes the transient to a loss of feedwater type transient and transfers to transient without MFW event tree SLBD-GTRAN. On the reactor trip failure path, successful isolation transfers to the ATWS-LMFW event tree because the break has been isolated and the event is similar to one of the ATWS events. Also on the reactor trip failure path, isolation failure results in core damage because the plant conditions are beyond those considered in the ATWS success criteria analyses.
PRHR	This top event is associated with the PRHR heat exchanger actuation on a PMS or DAS signal or operator action HEPO-PRHR using E-0. The success of this top event (PRHR-PX-DX) requires one out of two of the PRHR heat exchanger control valves to open and establish flow through the PRHR heat exchanger. In addition, one out of two IRWST gutter isolation valves must close to return condensate to the IRWST to sustain long term cooling. Failure of this top event requires RCS depressurization and IRWST or RNS injection to prevent core damage.
CMT	The success of this top event (CMT-1-PA-DA) requires one out of two CMTs to inject through one out of two parallel valves on the discharge piping, four out of four RCPs to trip, and a CMT actuation signal to ADS. If this top event fails, then core damage can be prevented if PRHR and CVS injection are successful.
CVS	The need for this top event is based on the steam line break IE and mitigating the reactivity effects of the cooldown with boration from the CVS pump. If the CMTs fail to inject, boration can be provided by the CVS pumps taking suction from the BAST. The success of this top event (CVS-1-PLA) requires one out of two CVS pumps injecting from the BAST into the RCS. If this top event fails, the reactivity control is not adequate and the path goes to core damage.
PZR SV	The pressuriser safety valves are modelled to address the RCS pressure increase due to the return to power from a large steam line break cooldown. They also address a potential RCS pressure increase that may occur for the feedwater line break event. Success of this top event (PZRSV-2) is the opening of one out of two pressuriser safety valves and the closing of two out of two pressuriser safety valves. Failure of this top event results in a transfer to the MLOCA event tree.

Table 10-19. SLBD Event Tree Description (cont.)

Top Event	Top Event Description
ADS23	This top event is associated with ADS Stages 1-3 actuation on a PMS signal or operator action HEPO-ADS-C1 using E-1 or the Foldout Page for E-1. The success criteria for ADS23 (ADS23-2-PX-DM-C1) are two out of four ADS Stages 2 and 3 valves open and discharge into the IRWST. ADS23-2-PX-DM-C1 is used on the CMT success paths because both automatic and manual actuations via the PMS are possible. Because this event tree covers both steam line and the feedwater line breaks, failure of this top event leads directly to core damage because decay heat removal has been lost.
ADS4	This top event is associated with ADS Stage 4 actuation on a PMS signal or operator action HEPO-ADS4-C1 using E-1 or the Foldout Page for E-1. The success criteria for this top event (ADS4-2L-PX-DM-C1) are one out of two ADS Stage 4 valves on each loop (two out of four total) actuating and providing a signal for IRWST gravity injection and recirculation. ADS4-2L-PX-DM-C1 is used when top event CMT is successful because both automatic and manual actuations via the PMS are possible. ADS4 is only modelled on the success paths of ADS23; therefore, failure of ADS4 does not lead directly to core damage because RNS injection and recirculation is possible due to the depressurization of the RCS by the ADS Stages 2 and 3 valves.
IRWST	This top event is associated with IRWST gravity injection actuation on a PMS signal or operator action HEPO-INJ using E-1 (note that E-1 would be entered from FR-H.1 or E-0). The success of this top event (IRWST-1-PX-DM) requires one out of four gravity injection line squib valves to actuate and provide IRWST injection into the RV via the DVI lines. Failure of this top event does not directly lead to core damage because ADS Stage 4 has successfully depressurized the RCS and there is sufficient time for the operator to establish injection through the RNS.
RNS	This top event is associated with using the RNS to provide low pressure injection to the RCS and operator action HEPO-RNSINJ and HEPO-RNSIRWST using ES-1.3. Success for this top event (RNS-1-PLM-L) includes successful operator action and the equipment functioning to align and start one out of two RNS pumps to take suction from the CLP, then to realign the RNS pump to take suction from the IRWST to maintain flow into the RV through one out of two DVI lines. Failure of this top event leads directly to core damage because top event RNS is addressed when IRWST injection is not available.
RECIRC	This top event is associated with containment sump recirculation on IRWST Low-3 level and operator action HEPO-RECIRC using E-1. The success of this top event (RRWST-1-PX-DM) requires one out of four containment sump recirculation line squib valves to actuate and provide flow into the RV via the DVI lines or to the suction line to the RNS. Failure of this top event leads to core damage because long term cooling is not established.

Table 10-20. SLBU Event Tree Description

Top Event	Top Event Description
REACTOR TRIP	A large steam line break is a rapid transient that requires a quick reactor trip. To bind this event, no credit is taken for the operator to manually trip the reactor. Reactor trip (RT-PA-DA) is successful when the control rods are inserted into the core and reactivity control is achieved. Note that for this transient, additional boration is needed to counter the effects of a steam line break cooldown. The boration is addressed in top events CMT and CVS. Failure of this top event results in core damage because the plant conditions are beyond those considered in the ATWS success criteria analyses.
ISO	The success of this top event (SGI-1-PA) is closure of one out of two MSIVs and, on the faulted SG, closure of the MFW isolation valve or the main feedwater control valve (MFCV), the SFW control or isolation valve, and one out of two SG blowdown isolation valves. In addition, the SG PORV or block valve on the intact SG must close to keep the SG intact. The sequences on the failure path of this top event are tracked because these represent two SGs blowing down inside containment.
PRHR	This top event is associated with the PRHR heat exchanger actuation on a PMS or DAS signal and operator action HEPO-PRHR using E-0. The success of this top event (PRHR-PX-DX) requires one out of two of the PRHR heat exchanger control valves to open and establish flow through the PRHR heat exchanger. In addition, one out of two IRWST gutter isolation valves must close to return condensate to the IRWST to sustain long term cooling. Failure of this top event requires RCS depressurization and IRWST or RNS injection to prevent core damage.
CMT	The success of this top event (CMT-1-PA-DA) requires one out of two CMTs to inject through one out of two parallel valves on the discharge piping, four out of four RCPs to trip, and a CMT actuation signal to ADS. If this top event fails, then core damage can be prevented if PRHR and CVS injection are successful.
CVS	The need for this top event is based on the steam line break IE and mitigating the reactivity effects of the cooldown with boration from the CVS pump. If the CMTs fail to inject, boration can be provided by the CVS pumps taking suction from the boric acid storage tank (BAST). The success of this top event (CVS-1-PLA) requires one out of two CVS pumps injecting from the BAST into the RCS. If this top event fails, the reactivity control is not adequate and the path goes to core damage.
PZR SV	The pressuriser safety valves are modelled to address the RCS pressure increase due to the return to power from a large steam line break cooldown. They also address a potential RCS pressure increase that may occur for the feedwater line break event. Success of this top event (PZRSV-2) is the opening of one out of two pressuriser safety valves and the closing of two out of two pressuriser safety valves. Failure of this top event results in a transfer to the MLOCA event tree.

Table 10-20. SLBU Event Tree Description (cont.)

Top Event	Top Event Description
ADS23	This top event is associated with ADS Stages 1-3 actuation on a PMS signal or operator action HEPO-ADS-C1 using E-1 or the Foldout Page for E-1. The success criteria for ADS23 (ADS23-2-PX-DM-C1) are two out of four ADS Stages 2 and 3 valves open and discharge into the IRWST. ADS23-2-PX-DM-C1 is used on the CMT success paths because both automatic and manual actuations via the PMS are possible. Because this event tree covers both steam line and the feedwater line breaks, failure of this top event leads directly to core damage because decay heat removal has been lost.
ADS4	This top event is associated with ADS Stage 4 actuation on a PMS signal or operator action HEPO-ADS4-C1 using E-1 or the Foldout Page for E-1. The success criteria for this top event (ADS4-2L-PX-DM-C1) are one out of two ADS Stage 4 valves on each loop (two out of four total) actuating and providing a signal for IRWST gravity injection and recirculation. ADS4-2L-PX-DM-C1 is used when top event CMT is successful because both automatic and manual actuations via the PMS are possible. ADS4 is only modelled on the success paths of ADS23; therefore, failure of ADS4 does not lead directly to core damage because RNS injection and recirculation is possible due to the depressurization of the RCS by the ADS Stages 2 and 3 valves.
IRWST	This top event is associated with IRWST gravity injection actuation on a PMS signal or operator action HEPO-INJ using E-1 (note that E-1 would be entered from FR-H.1 or E-2). The success of this top event (IRWST-1-PX-DM) requires one out of four gravity injection line squib valves to actuate and provide IRWST injection into the RV via the DVI lines. Failure of this top event does not directly lead to core damage because ADS Stage 4 has successfully depressurized the RCS and there is sufficient time for the operator to establish injection through the RNS.
RNS	This top event is associated with using the RNS to provide low pressure injection to the RCS and operator action HEPO-RNSINJ and HEPO-RNSIRWST using ES-1.3. Success for this top event (RNS-1-PLM-L) includes successful operator action and the equipment functioning to align and start one out of two RNS pumps to take suction from the CLP, then to realign the RNS pump to take suction from the IRWST to maintain flow into the RV through one out of two DVI lines. Failure of this top event leads directly to core damage because top event RNS is addressed when IRWST injection is not available.
RECIRC	This top event is associated with containment sump recirculation on a PMS signal or operator action HEPO-RECIRC using E-1. The success of this top event (RRWST-1-PX-DM) requires one out of four containment sump recirculation line squib valves to actuate and provide flow into the RV via the DVI lines or to the suction line to the RNS. Failure of this top event leads to core damage because long term cooling is not established.

Table 10-21. SPRECIRC Event Tree Description

Top Event	Top Event Description
IRWST RECIRC ISO	This top event (RRWSTISO-4-PLM) is associated with the operator action HEPO-RRWSTISO to isolate the recirculation paths after spurious opening of the recirculation squib valves by closing valves PXS-PL-V117A&B and PXS-PL-121A&B using alarm response procedure PXS-401.
REACTOR TRIP	This top event is associated with PMS and DAS reactor trip signals and operator action HEPO-RT using E-0. Reactor trip (RT-PX-DX) is successful when the control rods are inserted into the core and reactivity control is achieved. If IRWST isolation is successful then failure of this top event is transferred to the ATWS event tree. If IRWST isolation fails, then failure of this top event is conservatively assigned core damage.
SS FAULT	The success for this top event (SGS-SS-PA-PLA) is defined as one out of two PORVs opening, or one out of two safety valves (the two with the lowest set pressure) opening and relieving steam, or one turbine bypass valve dumping steam to the condenser. In addition, turbine trip (steam flow stopped to both the high pressure and low pressure turbines) must be successful. Because more than one PORV or MSSV may open after a reactor trip, the success for the valves reclosing is one PORV or block valve on each steam line reclose and two out of two MSSVs reclose, or one turbine bypass valve recloses. Credit is not taken for the operator to close the PORV block valve. If IRWST isolation is successful then failure of this top event is transferred to the SLBU event tree. If IRWST isolation fails, then failure of this top event is conservatively assigned core damage.
MFW	This top event is associated with MFW cooling using the PLS or operator action HEPO-MFW using ES-0.1. The success of this top (MFW-1-PLX) event is one booster/MFW pump supplying water through two out of two SFCVs (one per loop) to two out of two SGs and one turbine bypass valve dumping steam to the condenser. Failure of this top event requires SFW or RCS depressurization and IRWST or RNS injection to prevent core damage.
SFW	This top event is associated with SFW actuation on a PLS signal or operator action HEPO-SFWX using ES-0.1 and operator action for refilling the CST following the CST alarm response procedure. The success of this top event (SFW-1-PLX) for decay heat removal requires one out of two SFW pumps providing flow through two out of two SFCVs (one per loop) to two out of two SGs, and one out of two blowdown isolation valves close on each loop. One SG PORV or one MSSV must operate to dump the steam from the SG. In addition, the CST must be refilled. If the IRWST is not isolated, failure of this top event leads to core damage because the IRWST has lost its inventory and is not available for passive injection.
PZR SV	Success of this top event (PZRSV-2) is the opening of one out of two pressuriser safety valves and the closing of two out of two pressuriser safety valves. Failure of this top event leads to event tree logic based on the MLOCA event tree.

Table 10-21. SPRECIRC Event Tree Description (cont.)

Top Event	Top Event Description
CMT	The success of this top event (CMT-1-PA-DA) requires one out of two CMTs to inject through one out of two parallel valves on the discharge piping, four out of four RCPs to trip, and a CMT actuation signal to ADS. If this top event fails, then accumulator injection is required to provide water to the RCS prior to injection from the IRWST.
ACC	For this event, the accumulators provide a source of water when the CMTs fail, prior to injection from the IRWST, to maintain water in the core. The success of this top event (ACC-1) requires one out of two accumulators to inject into the DVI line, when the RCS pressure is below the accumulator pressure. Failure of this top event leads directly to core damage because it is addressed only on the failure paths of top event CMT.
ADS23	This top event is associated with ADS Stages 1-3 actuation on a PMS signal or operator action HEPO-ADS-C1 or HEPO-ADS-C2 using E-1 or the Foldout Page for E-1. The success criteria for ADS23 (ADS23-2-PX-DM-C1, ADS23-2-PM-DM-C2) are two out of four ADS Stages 2 and 3 valves open and discharge into the IRWST. ADS23-2-PX-DM-C1 is used on the CMT success path because both automatic and manual actuations via the PMS are possible. ADS23-2-PM-DM-C2 is used on the CMT failure path because automatic actuation via the PMS will not occur because either the signal fails or the CMT valves fail and the CMT Low level input to actuate ADS will not be generated. Failure of this top event can lead to a non-core damage state if top event ADS4 is successful.
ADS4	This top event is associated with ADS Stage 4 actuation on a PMS signal or operator action HEPO-ADS4-C1 or HEPO-ADS4-C2 using E-1 or the Foldout Page for E-1. The success criteria for this top event (ADS4-3-PX-DM-C1, ADS4-3-PM-DM-C2) are three out of four ADS Stage 4 valves actuating and providing a signal for IRWST gravity injection and recirculation. ADS4-3-PX-DM-C1 is used when top event CMT is successful because both automatic and manual actuations via the PMS are possible. ADS4-3-PM-DM-C2 is used when top event CMT fails because there is no automatic PMS actuation and the operator action is based on RCS hot leg level. Failure of top event ADS4 leads directly to core damage on the failure paths of ADS23 because there is insufficient RCS depressurization for IRWST or RNS injection. On success paths of ADS23, failure of ADS4 does not lead directly to core damage because there is sufficient RCS depressurization to allow RNS injection to be successful.
IRWST	This top event is associated with IRWST gravity injection actuation on a PMS ADS Stage 4 actuation signal or operator action HEPO-INJ using E-1. The success of this top event (IRWST-1-PX-DM) requires one out of four gravity injection line squib valves to actuate and provide IRWST injection into the RV via the DVI lines. Failure of this top event does not directly lead to core damage because ADS Stage 4 has successfully depressurized the RCS and there is sufficient time for the operator to establish injection through the RNS.

Table 10-21. SPRECIRC Event Tree Description (cont.)

Top Event	Top Event Description
RNS	This top event is associated with using the RNS to provide low pressure injection to the RCS and operator action HEPO-RNSINJ and HEPO-RNSIRWST using ES-1.3. Success for this top event (RNS-1-PLM-L) includes successful operator action and the equipment functioning to align and start one out of two RNS pumps to take suction from the CLP, then to realign the RNS pump to take suction from the IRWST to maintain flow into the RV through one out of two DVI lines. Failure of this top event leads directly to core damage because top event RNS is addressed when IRWST injection is not available.
RECIRC	This top event is associated with containment sump recirculation on a PMS signal or operator action HEPO-RECIRC using E-1. The success of this top event (RRWST-1-PX) requires one out of four containment sump recirculation line squib valves to actuate and provide flow into the RV via the DVI lines or to the suction line to the RNS. Failure of this top event leads to core damage because long term cooling is not established.

Table 10-22. ATWS-LMFW Event Tree Description

Top Event	Top Event Description
TURBINE TRIP	The success for this top event (MSS-TT-PA-DA) is the isolation of steam flow to the high and low pressure turbines by the closure of the appropriate combination of turbine control, stop, reheat stop, and intercept valves. Failure of this top event goes directly to core damage because the ATWS success criteria require turbine trip to aid in the negative reactivity feedback to the reactor to limit the RCS pressure increase.
SS FAULT	The success for this top event (SGS-SS-PA-PLA-ATWS) is defined as the six lowest set pressure MSSVs open and reclose, or two SG PORVs open and reclose and five of the six lowest set pressure MSSVs open and reclose. Credit is not taken for the steam dump to the condenser and credit is not taken for the operator to close the PORV block valve. Failure of this top event, the required valves failing to open or failing to reclose, results in core damage because the plant conditions are beyond what are considered in the success criteria analyses.
SFW	This top event is associated with SFW actuation by a PLS signal and operator action for refilling the CST following the CST alarm response procedure. The success of this top event (SFW-1-PLA-ATWS) for decay heat removal requires one out of two SFW pumps providing flow through two out of two SFCVs (one per loop) to two out of two SGs, and one out of two blowdown isolation valves close on each loop. One SG PORV or one MSSV must operate to dump the steam from the SG. In addition, the CST must be refilled. Failure of this top event requires operation of the PRHR, a CMT, and the pressuriser safety valves.
PRHR	The success of this top event (PRHR-PA-DA-ATWS) requires one out of two of the PRHR heat exchanger control valves to open and establish flow through the PRHR heat exchanger. In addition, one out of two IRWST gutter isolation valves must close to return condensate to the IRWST to sustain long term cooling. Failure of this top event leads to core damage because core cooling cannot be established in time to prevent RCS over pressurization.
PZR SV (OPEN)	Success of this top event (PZRSV-2-ATWS) is the opening of two out of two pressuriser safety valves. Failure of this top event results in core damage because RCS pressure relief is required to keep the pressure below 220.63 Bar (3200 psig).
PZR SV (CLOSE)	Success of this top event (PZRSV-2C-ATWS) is the closing of two out of two pressuriser safety valves. Failure of this top event transfers to the LOCA-NO TRIP event tree.
CMT	The success of this top event (CMT-1-PA-DA-ATWS) requires one out of two CMTs to inject through one out of two parallel valves on the discharge piping and four out of four RCPs to trip. If this top event fails, then core damage results due to insufficient reactivity control and subsequent RCS over pressurization.
NO SBO	This top event is associated with starting the standby DGs on a PLS signal or operator action HEPO-SDG using AOP-323. The success of this top event (SBO-1-PLX) is the starting and running of one out of two of the standby DGs. Failure of this top event results in SBO conditions (no onsite or offsite ac power).

Table 10-22. ATWS-LMFW Event Tree Description (cont.)

Top Event	Top Event Description
DISABLE TIMER	This top event (22HRTIMER) is associated with the operator action HEPO-22HRTIMER for SBO conditions to turn off the retentive timer that would actuate ADS at approximately 22 hours into the SBO event using AOP-323. ADS actuation is not required if PRHR is successful so the success path of this top event transfers to long term cooling event tree LTC. Failure of this top event means that the 22 hour timer sends an actuation signal to ADS Stages 1-4. ADS actuation requires that top events IRWST and RECIRC be addressed. Note that at this point in the event tree, top event CMT has already been addressed and this branch occurs on the success path of CMT.
ADS4	This top event is associated with ADS Stage 4 actuation on a PMS signal or operator action HEPO-ADS4-C1 using E-1 or the Foldout Page for E-1. The success criteria for this top event (ADS4-2L-PX-C1) are one out of two ADS Stage 4 valves on each loop (two out of four total) actuating and providing a signal for IRWST gravity injection and recirculation. ADS4-2L-PX-C1 is used for SBO conditions because the DAS battery is only designed for 2 hours so DAS actuation is not modelled. ADS4-2L-PX-C1 is used because top event CMT is successful so both automatic and manual actuations via the PMS are possible. Failure of ADS4 leads directly to core damage because RNS injection and recirculation is not possible due to the SBO conditions.
IRWST	This top event is associated with IRWST gravity injection actuation on a PMS signal or operator action HEPO-INJ using E-1. The success of this top event (IRWST-1-PX) requires one out of four gravity injection line squib valves to actuate and provide IRWST injection into the RV via the DVI lines. Failure of this top event leads directly to core damage because the RNS system does not have power due to the SBO conditions and the IRWST is the only source for injection after the ADS valves are actuated.
RECIRC	This top event is associated with containment sump recirculation on a PMS signal or operator action HEPO-RECIRC using E-1. The success of this top event (RRWST-1-PX) requires one out of four containment sump recirculation line squib valves to actuate and provide flow into the RV via the DVI lines. Failure of this top event leads to core damage because long term cooling is not established.

Table 10-23. ATWS Event Tree Description

Top Event	Top Event Description
TURBINE TRIP	The success for this top event (MSS-TT-PA-DA) is the isolation of steam flow to the high and low pressure turbines by the closure of the appropriate combination of turbine control, stop, reheat stop, and intercept valves. Failure of this top event goes directly to core damage because the ATWS success criteria require turbine trip to aid in the negative reactivity feedback to the reactor to limit the RCS pressure increase.
SS FAULT	The success for this top event (SGS-SS-PA-PLA-ATWS) is defined as the six lowest set pressure MSSVs open and reclose, or two SG PORVs open and reclose and five of the six lowest set pressure MSSVs open and reclose. Credit is not taken for the steam dump to the condenser and credit is not taken for the operator to close the PORV block valve. Failure of this top event, the required valves failing to open or failing to reclose, results in core damage because the plant conditions are beyond what are considered in the success criteria analyses.
MFW	The success of this top (MFW-1-PLA-ATWS) event is one booster/ MFW pump supplying water through the SFCV to two out of two SGs and one turbine bypass valve dumping steam to the condenser. Failure of this top event requires decay heat removal from the SFW system or the PRHR system to prevent core damage.
SFW	This top event is associated with SFW actuation on a PLS signal, and operator action for refilling the CST following the CST alarm response procedure. The success of this top event (SFW-1-PLA-ATWS) for decay heat removal requires one out of two SFW pumps providing flow through two out of two SFCVs (one per loop) to two out of two SGs, and one out of two blowdown isolation valves close on each loop. One SG PORV or one MSSV must operate to dump the steam from the SG. In addition, the CST must be refilled. Failure of this top event requires operation of the PRHR, a CMT, and the pressuriser safety valves.
PRHR	The success of this top event (PRHR-PA-DA-ATWS) requires one out of two of the PRHR heat exchanger control valves to open and establish flow through the PRHR heat exchanger. In addition, one out of two IRWST gutter isolation valves must close to return condensate to the IRWST to sustain long term cooling. Failure of this top event leads to core damage because core cooling cannot be established in time to prevent RCS over pressurization.
PZR SV (OPEN)	Success of this top event (PZRSV-2-ATWS) is the opening of two out of two pressuriser safety valves. Failure of this top event results in core damage because RCS pressure relief is required to keep the pressure below 22063 kPa (3200 psig).
PZR SV (CLOSE)	Success of this top event (PZRSV-2C-ATWS) is the closing of two out of two pressuriser safety valves. Failure of this top event transfers to the LOCA-NO TRIP event tree.
CMT	The success of this top event (CMT-1-PA-DA-ATWS) requires one out of two CMTs to inject through one out of two parallel valves on the discharge piping and four out of four RCPs to trip. If this top event fails, then core damage results due to insufficient reactivity control and subsequent RCS over pressurization.

Table 10-23. ATWS Event Tree Description (cont.)

Top Event	Top Event Description
NO SBO	This top event is associated with starting the standby DGs on a PLS signal or operator action HEPO-SDG using AOP-323. The success of this top event (SBO-1-PLX) is the starting and running of one out of two of the standby DGs. Failure of this top event results in SBO conditions (no onsite or offsite ac power).
DISABLE TIMER	This top event (22HRTIMER) is associated with the operator action HEPO-22HRTIMER for SBO conditions to turn off the retentive timer that would actuate ADS at approximately 22 hours into the SBO event using AOP-323. ADS actuation is not required if PRHR is successful so the success path of this top event transfers to long term cooling event tree LTC. Failure of this top event means that the 22 hour timer sends an actuation signal to ADS Stages 1-4. ADS actuation requires that top events IRWST and RECIRC be addressed. Note that at this point in the event tree top event CMT has already been addressed, and this branch occurs on the success path of CMT.
ADS4	This top event is associated with ADS Stage 4 actuation on a PMS signal or operator action HEPO-ADS4-C1 using E-1 or the Foldout Page for E-1. The success criteria for this top event (ADS4-2L-PX-C1) are one out of two ADS Stage 4 valves on each loop (two out of four total) actuating and providing a signal for IRWST gravity injection and recirculation. ADS4-2L-PX-C1 is used for SBO conditions because the DAS battery is only designed for 2 hours so DAS actuation is not modelled. ADS4-2L-PX-C1 is used because top event CMT is successful so both automatic and manual actuations via the PMS are possible. Failure of ADS4 leads directly to core damage because RNS injection and recirculation is not possible due to the SBO conditions.
IRWST	This top event is associated with IRWST gravity injection actuation on a PMS signal or operator action HEPO-INJ using E-1. The success of this top event (IRWST-1-PX) requires one out of four gravity injection line squib valves to actuate and provide IRWST injection into the RV via the DVI lines. Failure of this top event leads directly to core damage because the RNS system does not have power due to the SBO conditions and the IRWST is the only source for injection after the ADS valves are actuated.
RECIRC	This top event is associated with containment sump recirculation on a PMS signal or operator action HEPO-RECIRC using E-1. The success of this top event (RRWST-1-PX) requires one out of four containment sump recirculation line squib valves to actuate and provide flow into the RV via the DVI lines. Failure of this top event leads to core damage because long term cooling is not established.

Table 10-24. LOCA-NOTRIP Event Tree Description

Top Event	Top Event Description
TURBINE TRIP	To be consistent with the ATWS event tree model this top event is included in the event tree. The success for this top event (MSS-TT-PA-DA) is the isolation of steam flow to the high and low pressure turbines by the closure of the appropriate combination of turbine control, stop, reheat stop, and intercept valves. Failure of this top event goes directly to core damage because the ATWS success criteria require turbine trip to aid in the negative reactivity feedback to the reactor to limit the RCS pressure increase.
SS FAULT	To be consistent with the ATWS event tree model, this top event is included in the event tree. The success for this top event (SGS-SS-PA-PLA-ATWS) is defined as the six lowest set pressure MSSVs open and reclose, or two SG PORVs open and reclose and five of the six lowest set pressure MSSVs open and reclose. Credit is not taken for the steam dump to the condenser and credit is not taken for the operator to close the PORV block valve. Failure of this top event, the required valves failing to open or failing to reclose, results in core damage because the plant conditions are beyond what are considered in the success criteria analyses.
PRHR	The success of this top event (PRHR-PA-DA-L) requires one out of two of the PRHR heat exchanger control valves to open and establish flow through the PRHR heat exchanger. In addition, one out of two IRWST gutter isolation valves must close to return condensate to the IRWST to sustain long term cooling. Failure of this top event leads to core damage because the plant conditions are beyond what are considered in the success criteria analyses.
PZR SV (OPEN)	Success of this top event (PZRSV-2-ATWS) is the opening of two out of two pressuriser safety valves. Failure of this top event results in core damage. This approach is taken to be consistent with the success paths in the ATWS event trees and because the plant conditions are beyond what are considered in the success criteria analyses.
CMT	The success of this top event (CMT-1-PA-DA-ATWS) requires one out of two CMTs to inject through one out of two parallel valves on the discharge piping and four out of four RCPs to trip. Failure of this top event leads to core damage because there is insufficient makeup to the RCS and insufficient reactivity control.
ADS23	This top event is associated with ADS Stages 1-3 actuation on a PMS signal or operator action HEPO-ADS-C1 using E-1 or the Foldout Page for E-1. The success criteria for ADS23 (ADS23-2-PX-DM-C1) are two out of four ADS Stages 2 and 3 valves open and discharge into the IRWST. ADS23-2-PX-DM-C1 is used on the CMT success path because both automatic and manual actuations via the PMS are possible. Failure of this top event leads to core damage because insufficient RCS depressurization occurs to permit IRWST injection.

Table 10-24. LOCA-NOTRIP Event Tree Description (cont.)

Top Event	Top Event Description
ADS4	This top event is associated with ADS Stage 4 actuation on a PMS signal or operator action HEPO-ADS4-C1 using E-1 or the Foldout Page for E-1. The success criteria for this top event (ADS4-2L-PX-DM-S4-C1) are one out of two ADS Stage 4 valves on each loop (two out of four total) actuating and providing a signal for IRWST gravity injection and recirculation. ADS4-2L-PX-DM-S4-C1 is used when top event CMT is successful because both automatic and manual actuations via the PMS are possible. Failure of this top event does not lead directly to core damage because this top event is addressed on the success path of top events PRHR and ADS23; therefore, there is sufficient RCS depressurization for RNS injection.
IRWST	This top event is associated with IRWST gravity injection actuation on a PMS signal or operator action HEPO-INJ using E-1. The success of this top event (IRWST-1-PX-DM) requires one out of four gravity injection line squib valves to actuate and provide IRWST injection into the RV via the DVI lines. Failure of this top event does not lead directly to core damage because this top event is addressed on the success path of top events PRHR, ADS23, and ADS4; therefore, there is sufficient RCS depressurization and time for the operator to establish injection through the RNS.
RNS	This top event is associated with using the RNS to provide low pressure injection to the RCS and operator action HEPO-RNSINJ and HEPO-RNSIRWST using ES-1.3. Success for this top event (RNS-1-PLM-L) includes successful operator action and the equipment functioning to align and start one out of two RNS pumps to take suction from the CLP, then to realign the RNS pump to take suction from the IRWST to maintain flow into the RV through one out of two DVI lines. Failure of this top event leads directly to core damage because top event RNS is addressed when IRWST injection is not available.
RECIRC	This top event is associated with containment sump recirculation on a PMS signal or operator action HEPO-RECIRC using E-1. The success of this top event (RRWST-1-PX-DM) requires one out of four containment sump recirculation line squib valves to actuate and provide flow into the RV via the DVI lines or to the suction line to the RNS. Failure of this top event leads to core damage because long term cooling is not established.

Table 10-25. LOCA-SSFAULT Event Tree Description

Top Event	Top Event Description
CMT	The success of this top event (CMT-1-PA-DA) requires one out of two CMTs to inject through one out of two parallel valves on the discharge piping, four out of four RCPs to trip, and a CMT actuation signal to ADS. Failure of this top event leads to core damage because there is insufficient makeup to the RCS and insufficient reactivity control for the cooldown aspect of this event.
ADS23	This top event is associated with ADS Stages 1-3 actuation on PMS signal or operator action HEPO-ADS-C1 using E-1 or the Foldout Page for E-1. The success criteria for ADS23 (ADS23-3-PX-DM-C1) are three out of four ADS Stages 2 and 3 valves open and discharge into the IRWST. ADS23-3-PX-DM-C1 is used on the CMT success path because both automatic and manual actuations via the PMS are possible. Failure of this top event leads to core damage because insufficient RCS depressurization occurs to permit IRWST injection.
ADS4	This top event is associated with ADS Stage 4 actuation on a PMS signal or operator action HEPO-ADS4-C1 using E-1 or the Foldout Page for E-1. The success criteria for this top event (ADS4-2L-PX-DM-C1) are one out of two ADS Stage 4 valves on each loop (two out of four total) actuating and providing a signal for IRWST gravity injection and recirculation. ADS4-2L-PX-DM-C1 is used when top event CMT is successful because both automatic and manual actuations via the PMS are possible. Failure of top event ADS4 does not lead directly to core damage because there is sufficient RCS depressurization for RNS injection.
IRWST	This top event is associated with IRWST gravity injection actuation on a PMS signal or operator action HEPO-INJ using E-1. The success of this top event (IRWST-1-PX-DM) requires one out of four gravity injection line squib valves to actuate and provide IRWST injection into the RV via the DVI lines. Failure of this top event does not lead directly to core damage because ADS Stage 4 has successfully depressurized the RCS and there is sufficient time for the operator to establish injection through the RNS.
RNS	This top event is associated with using the RNS to provide low pressure injection to the RCS and operator action HEPO-RNSINJ and HEPO-RNSIRWST using ES-1.3. Success for this top event (RNS-1-PLM-L) includes successful operator action and the equipment functioning to align and start one out of two RNS pumps to take suction from the CLP, then to realign the RNS pump to take suction from the IRWST to maintain flow into the RV through one out of two DVI lines. Failure of this top event leads directly to core damage because top event RNS is addressed when IRWST injection is not available.
RECIRC	This top event is associated with containment sump recirculation on a PMS signal or operator action HEPO-RECIRC using E-1. The success of this top event (RRWST-1-PX-DM) requires one out of four containment sump recirculation line squib valves to actuate and provide flow into the RV via the DVI lines. Failure of this top event leads to core damage because long term cooling is not established.

Table 10-26. SGTR-NOTRIP Event Tree Description

Top Event	Top Event Description
TURBINE TRIP	To be consistent with the ATWS event tree model, this top event is included in the event tree. The success for this top event (MSS-TT-PA-DA) is the isolation of steam flow to the high and low pressure turbines by the closure of the appropriate combination of turbine control, stop, reheat stop, and intercept valves. Failure of this top event goes directly to core damage because the ATWS success criteria require turbine trip to aid in the negative reactivity feedback to the reactor to limit the RCS pressure increase.
SS FAULT	To be consistent with the ATWS event tree model, this top event is included in the event tree. The success for this top event (SGS-SS-PA-PLA-ATWS) is defined as the six lowest set pressure MSSVs open and reclose, or two SG PORVs open and reclose and five of the six lowest set pressure MSSVs open and reclose. Credit is not taken for the steam dump to the condenser and credit is not taken for the operator to close the PORV block valve. Failure of this top event, the required valves failing to open or failing to reclose, results in core damage because the plant conditions are beyond what are considered in the success criteria analyses.
CMT	The success of this top event (CMT-1-PA-DA-ATWS) requires one out of two CMTs to inject through one out of two parallel valves on the discharge piping and four out of four RCPs to trip. If this top event fails, then the result is core damage because the CMT is needed for reactivity control due to the failure of reactor trip.
PRHR	The success of this top event (PRHR-PA-DA) requires one out of two of the PRHR heat exchanger control valves to open and establish flow through the PRHR heat exchanger. In addition, one out of two IRWST gutter isolation valves must close to return condensate to the IRWST to sustain long-term cooling. Failure of this top event leads to core damage.
OFILL	The success of this top event (SGI-1-PA-SGTR) requires the termination of CVS, and SFW flow to both SGs. In addition, the MFW line to the ruptured SG must be isolated (this occurs on the S signal). The failure of this event leads to core damage because the plant conditions are beyond what are considered in the success criteria analyses.
PZR SV (OPEN)	Success of this top event (PZRSV-2-ATWS) is the opening of two out of two pressuriser safety valves. Failure of this top event results in core damage based on the success criteria results for the ATWS event.
PZR SV (CLOSE)	Success of this top event (PZRSV-2C-ATWS) is the closing of two out of two pressuriser safety valves. Failure of this top event results in core damage because the plant conditions are beyond those considered in the ATWS success criteria analyses.

Table 10-27. SLBD-GTRAN Event Tree Description

Top Event	Top Event Description
PRHR	This top event is associated with the PRHR heat exchanger actuation on PMS or DAS signal or operator action HEPO-PRHR using E-0. The success of this top event (PRHR-PX-DX) requires one out of two of the PRHR heat exchanger control valves to open and establish flow through the PRHR heat exchanger. In addition, one out of two IRWST gutter isolation valves must close to return condensate to the IRWST to sustain long term cooling. Failure of this top event requires RCS depressurization and IRWST or RNS injection to prevent core damage.
PZR SV	Success of this top event (PZRSV-2) is the opening of one out of two pressuriser safety valves and the closing of two out of two pressuriser safety valves. Failure of this top event results in a transfer to the MLOCA event tree.
CMT	This top event is associated with CMT actuation on a PMS or DAS signal or operator action HEPO-CMT-GT using FR-H.1. The success of this top event (CMT-1-PX-DX-GT) requires one out of two CMTs to inject through one out of two parallel valves on the discharge piping, four out of four RCPs to trip, and a CMT actuation signal to ADS. If this top event fails, then core damage can be prevented if top events ADS23 and ACC are successful.
ADS23	This top event is associated with ADS Stages 1-3 actuation on a PMS signal or operator action HEPO-ADS-GT using FR-H-1. There are different success criteria for ADS23 (ADS23-2-PM-DM-GT, ADS23-3-PX-DM-GT). For ADS23-2-PM-DM-GT, success is two out of four ADS Stages 2 and 3 valves open and discharge into the IRWST. ADS23-2-PM-DM-GT is used on the CMT failure path because automatic actuation via the PMS will not occur because either the signal fails or the CMT valves fail and the CMT Low level input to actuate ADS will not be generated. For ADS23-3-PX-DM-GT, success is three out of four ADS Stages 2 and 3 valves open and discharge into the IRWST. This is used when top event PRHR fails and top event CMT is successful to achieve the necessary RCS depressurization prior to ADS Stage 4 actuation. Failure of this top event leads directly to core damage because RCS depressurization and IRWST or RNS injection does not occur quickly enough to prevent core damage.
ACC	For this event, the accumulators provide a source of water when the CMTs fail, prior to injection from the IRWST, to maintain water in the core. The success of this top event (ACC-1) requires one out of two accumulators to inject into the DVI line, when the RCS pressure is below the accumulator pressure. Failure of this top event leads directly to core damage because it is addressed only on the failure path of top event CMT.

Table 10-27. SLBD-GTRAN Event Tree Description (cont.)

Top Event	Top Event Description
ADS4	This top event is associated with ADS Stage 4 actuation on a PMS signal or operator action HEPO-ADS4-C1 or HEPO-ADS4-C2 using E-1or the Foldout Page for E-1. The success criteria for this top event (ADS4-2L-PX-DM-C1, ADS4-2L-PM-DM-C2) are one out of two ADS Stage 4 valves on each loop (two out of four total) actuating and providing a signal for IRWST gravity injection and recirculation. DS4-2L-PX-DM-C1 is used when top event CMT is successful because both automatic and manual actuations via the PMS are possible. ADS4-2L-PM-DM-C2 is used if top event CMT fails because automatic actuation via the PMS is not available. ADS4 is only modelled on the success paths of ADS23; therefore, failure of ADS4 does not lead directly to core damage because RNS injection and recirculation is possible due to the depressurization of the RCS by the ADS Stages 2 and 3 valves.
IRWST	This top event is associated with IRWST gravity injection actuation on a PMS signal or operator action HEPO-INJ using E-1 (note that E-1 would be entered from FR-H.1). The success of this top event (IRWST-1-PX-DM) requires one out of four gravity injection line squib valves to actuate and provide IRWST injection into the RV via the DVI lines. Failure of this top event does not directly lead to core damage because ADS Stage 4 has successfully depressurized the RCS and there is sufficient time for the operator to establish injection through the RNS.
RNS	This top event is associated with using the RNS to provide low pressure injection to the RCS and operator action HEPO-RNSINJ and HEPO-RNSIRWST using ES-1.3. Success for this top event (RNS-1-PLM-L) includes successful operator action and the equipment functioning to align and start one out of two RNS pumps to take suction from the CLP, then to realign the RNS pump to take suction from the IRWST to maintain flow into the RV through one out of two DVI lines. Failure of both IRWST and RNS injection results in loss of all low pressure injection to cool the reactor and to mitigate the loss of RCS inventory through the ADS valves.
RECIRC	This top event is associated with containment sump recirculation on a PMS signal or operator action HEPO-RECIRC using E-1. The success of this top event (RRWST-1-PX-DM) requires one out of four containment sump recirculation line squib valves to actuate and provide flow into the RV via the DVI lines or to the suction line to the RNS. Failure of this top event leads to core damage because long term cooling is not established.

Table 10-28. LTC and LTCP Event Tree Description

Top Event	Top Event Description
NO SBO	This top event is associated with starting the standby DGs on a PLS signal or operator action HEPO-SDG using AOP-323 if ac power is lost. This top event is used to check if SBO conditions exist. The success of this top event (SBO-1-PLX) is the starting and running of one out of two of the standby DGs. Failure of this top event results in SBO conditions (no onsite or offsite ac power). ForSBO conditions, the containment isolation valves will close either from the loss of power or from the subsequent loss of instrument air and top event CI is not addressed.
CI	This top event is associated with Containment Isolation (CI) actuation on a PMS or DAS signal or operator action HEPO-CNT using E-0. The Containment System (CNS) Isolation System provides the Category -A function of containment isolation for containment boundary integrity and provides a barrier against the release of fission products to the atmosphere. The success criteria for CI (CI-PX-DX) are the closure of one isolation valve on each of the lines listed in E-0 and closure of applicable containment hatches and doors. Failure of this top event does not lead directly to core damage as long as Passive Containment Cooling System (PCS) is successful.
PCS	This top event is associated with PCS actuation on a PMS or DAS signal or operator action HEPO-PCS using FR-Z.1. The success criteria for PCS (PCS-1-PX-DX, PCS-1-PM-DX, PCS-1-SB) are flow from one out of three flow paths to the distribution bucket, or makeup water provided to the distribution bucket from the PCS recirculation pumps, for 72 hours. Failure of this top event results in core damage, except as indicated below.
SFW	This top event is associated with SFW actuation on a PLS signal or operator action HEPO-SFWS following E-0 or HEPO-SFWM following FR-H.1, and operator action for refilling the CST. This top event is modelled in transfer tree LTCP to recover core cooling via SFW if PCS fails. This is a long term recovery. The success of this top event (SFW-1-PLX-C) for decay heat removal requires one out of two SFW pumps providing flow through one out of two SFCVs to one out of two SGs, and one out of two blowdown isolation valves close on the SG loop. One SG PORV or one MSSV must operate to dump the steam from the SG. In addition, the CST must be refilled. Failure of this top event leads to core damage because it is the recovery of failed PCS and long term core cooling.

Table 10-29. System Dependency Matrix – Mitigating Systems

			Support Systems														
			CAS	**CCS**	**CDS**	**DAS**	**DWS**	**ECS**	**EDS**	**IDS**	**MSS**	**PLS**	**PMS**	**PXS[1]**	**SGS[1]**	**TCS**	**VAS**
			Compressed and Instrument Air Systems	Component Cooling Water System	Condensate System	Diverse Actuation System	Demineralized Water Transfer and Storage System	Main AC Power System	Non-Class 1 DC and UPS System	Class 1 DC and UPS System	Main Steam System	Plant Control System	Protection and Safety Monitoring System	Passive Core Cooling System	Steam Generator System	Turbine Building Closed Cooling Water System	Radiologically Controlled Area Ventilation System
Mitigating Systems	CNS	Containment System				X				X			X				
	CVS	Chemical and Volume Control System	X				X	X	X	X		X	X				X
	FWS	Main and Startup Feedwater System	X		X		X	X			X	X			X	X	
	PCS	Passive Containment Cooling System				X		X[4]		X		X	X				
	PXS	Passive Core Cooling System[3]				X		X[2]		X			X				
	RCS	Reactor Coolant System				X				X			X				
	RNS	Normal Residual Heat Removal System		X				X		X		X	X	X			X
	SGS	Steam Generator System	X							X	X	X	X				
	VLS	Containment Hydrogen Control System				X			X			X					

Notes:

1. This system is not a support system but used as a transfer to a system.
2. ECS is a dependency for PXS as it is used for the RCP breakers for CMT injection. The ac power modelled in the PSA is for control power to the RCP breakers to open.
3. It is noted that PRHR and CMT are fail safe. The accumulator sub-system of PXS does not require any support systems for actuation. Only ADS and IRWST require dc power for support.
4. Main AC power system provides motive power to PCS-PL-V001C and the PCS pumps and is therefore modelled in the PCS, but not required for successful PCS. PCS-PL-V001C serves the same purpose as normally closed, fail open air operated valves, PCS-PL-V001A/B.

Table 10-30. System Dependency Matrix – Support Systems

			SUPPORT SYSTEMS																							
			CAS	CCS	CDS	CMS	CWS	DAS	DTS	DWS	ECS	EDS	GSS	IDS	MSS	MTS	PLS	PMS	RWS	SWS	TOS	VBS	VTS	VWS	VXS	VZS	ZRS
			Compressed and Instrument Air Systems	Component Cooling Water System	Condensate System	Condenser Air Removal System	Circulating Water System	Diverse Actuation System	Demineralized Water Treatment System	Demineralized Water Transfer and Storage System	Main AC Power System	Non-Class 1 DC and UPS System	Gland Seal System	Class 1 DC and UPS System	Main Steam System	Main Turbine System	Plant Control System	Protection and Safety Monitoring System	Raw Water System	Service Water System	Main Turbine Control and Diagnostics System	Nuclear Island Nonradioactive Ventilation System	Turbine Building Ventilation System	Central Chilled Water System	Annex/Aux Building Nonradioactive Ventilation System	Diesel Generator Building Heating and Ventilation System	Offsite Retail Power System
SUPPORT SYSTEMS	CAS	Compressed and Instrument Air Systems		X							X						X										
	CCS	Component Cooling Water System	X							X	X						X			X			X				
	CDS	Condensate System	X	X		X	X			X	X		X				X										
	CMS	Condenser Air Removal System	X				X			X	X																
	CWS	Circulating Water System									X								X								
	DAS	Diverse Actuation System										X															
	DOS	Standby Diesel and Auxiliary Boiler Fuel Oil System									X	X					X										
	DTS	Demineralized Water Treatment System	X								X								X								

Table 10-30. System Dependency Matrix – Support Systems (cont.)

			SUPPORT SYSTEMS																							
			CAS	CCS	CDS	CMS	CWS	DAS	DTS	DWS	ECS	EDS	GSS	IDS	MSS	MTS	PLS	PMS	RWS	SWS	TOS	VBS	VTS	VWS	VXS	VZS	ZRS
			Compressed and Instrument Air Systems	Component Cooling Water System	Condensate System	Condenser Air Removal System	Circulating Water System	Diverse Actuation System	Demineralized Water Treatment System	Demineralized Water Transfer and Storage System	Main AC Power System	Non-Class 1 DC and UPS System	Gland Seal System	Class 1 DC and UPS System	Main Steam System	Main Turbine System	Plant Control System	Protection and Safety Monitoring System	Raw Water System	Service Water System	Main Turbine Control and Diagnostics System	Nuclear Island Nonradioactive Ventilation System	Turbine Building Ventilation System	Central Chilled Water System	Annex/Aux Building Nonradioactive Ventilation System	Diesel Generator Building Heating and Ventilation System	Offsite Retail Power System
SUPPORT SYSTEMS	DWS	Demineralized Water Transfer and Storage System	X						X		X	X					X								X		
	ECS	Main AC Power System																								X	
	EDS	Non-Class 1 DC and UPS System									X															X	
	GSS	Gland Seal System													X												
	IDS	Class 1 DC and UPS System																									
	MSS1	Main Steam System	X		X							X					X										
	MTS	Main Turbine System													X						X						
	PLS	Plant Control System										X						X^2									
	PMS	Protection and Safety Monitoring System						X^1				X^3		X													

Table 10-30. System Dependency Matrix – Support Systems (cont.)

			SUPPORT SYSTEMS																							
			CAS	CCS	CDS	CMS	CWS	DAS	DTS	DWS	ECS	EDS	GSS	IDS	MSS	MTS	PLS	PMS	RWS	SWS	TOS	VBS	VTS	VWS	VXS	VZS	ZRS
			Compressed and Instrument Air Systems	Component Cooling Water System	Condensate System	Condenser Air Removal System	Circulating Water System	Diverse Actuation System	Demineralized Water Treatment System	Demineralized Water Transfer and Storage System	Main AC Power System	Non-Class 1 DC and UPS System	Gland Seal System	Class 1 DC and UPS System	Main Steam System	Main Turbine System	Plant Control System	Protection and Safety Monitoring System	Raw Water System	Service Water System	Main Turbine Control and Diagnostics System	Nuclear Island Nonradioactive Ventilation System	Turbine Building Ventilation System	Central Chilled Water System	Annex/Aux Building Nonradioactive Ventilation System	Diesel Generator Building Heating and Ventilation System	Offsite Retail Power System
SUPPORT SYSTEMS	RWS	Raw Water System									X																X
	SWS	Service Water System	X								X						X		X								
	TCS	Turbine Building Closed Cooling Water System	X				X			X	X	X															
	TOS	Main Turbine Control and Diagnostics System						X										X									
	VAS	Radiologically Controlled Area Ventilation System									X						X							X			
	VBS	Nuclear Island Nonradioactive Ventilation System									X						X							X			
	VTS	Turbine Building Ventilation System	X								X													X			

Table 10-30. System Dependency Matrix – Support Systems (cont.)

SUPPORT SYSTEMS			SUPPORT SYSTEMS																							
			CAS	CCS	CDS	CMS	CWS	DAS	DTS	DWS	ECS	EDS	GSS	IDS	MSS	MTS	PLS	PMS	RWS	SWS	TOS	VBS	VTS	VWS	VXS	VZS	ZRS
			Compressed and Instrument Air Systems	Component Cooling Water System	Condensate System	Condenser Air Removal System	Circulating Water System	Diverse Actuation System	Demineralized Water Treatment System	Demineralized Water Transfer and Storage System	Main AC Power System	Non-Class 1 DC and UPS System	Gland Seal System	Class 1 DC and UPS System	Main Steam System	Main Turbine System	Plant Control System	Protection and Safety Monitoring System	Raw Water System	Service Water System	Main Turbine Control and Diagnostics System	Nuclear Island Nonradioactive Ventilation System	Turbine Building Ventilation System	Central Chilled Water System	Annex/Aux Building Nonradioactive Ventilation System	Diesel Generator Building Heating and Ventilation System	Offsite Retail Power System
VWS	Central Chilled Water System		X	X							X	X					X					X	X		X		
VXS	Annex/Aux Building Nonradioactive Ventilation System		X								X	X					X							X			
VZS	Diesel Generator Building Heating and Ventilation System										X						X										
ZOS	Onsite Standby Power System										X						X									X	
ZRS	Offsite Retail Power System																										

Note:

1. ECS is a dependency for PXS as it is used for the RCP breakers for CMT injection.
2. PMS is modelled as a support to PLS in the PSA model to show the interface in the linked model for the PMS-PLS interface.
3. Non-Class 1 dc and UPS power supply system is noted as a dependency for PMS Category-A functions. The sequence of events (SOE) subsystem of PMS is the only subsystem that requires the non-class 1 and UPS power supply system. A specific isolation barrier in the PMS-PLS interface is powered through the SOE subsystem and therefore is modelled in this unique case for PMS.

Table 10-31. Pre-Initiator Quantification Summary

Event ID	BE Name(s)	Description	Total HEP	Error Factor
HEPE-CCS-XVM-LC-V105	HEPE-CCS-XVM-LC-V105	CROSS CONNECT VALVE CCS-PL-V105 LEFT CLOSED		
HEPE-CDS-XVM-CL	HEPE-CDS-XVM-CL-V01A	OPERATOR FAILS TO RE-OPEN CDS PUMP ISOLATION VALVE		
	HEPE-CDS-XVM-CL-V01B			
	HEPE-CDS-XVM-CL-V01C			
	HEPE-CDS-XVM-CL-V03A			
	HEPE-CDS-XVM-CL-V03B			
	HEPE-CDS-XVM-CL-V03C			
HEPE-CDS-XVM-CL-V046	HEPE-CDS-XVM-CL-V46A	OPERATOR FAILS TO RE-OPEN CDS SEAL INECTION ISOLATION VALVE		
	HEPE-CDS-XVM-CL-V46B			
	HEPE-CDS-XVM-CL-V46C			
HEPE-CVS-AOV-OP-V089	HEPE-CCS-XVM-LC-V089	VALVE CVS-PL-V089 LEFT OPEN		
HEPE-CVS-XVM-OP	HEPE-CVS-XVM-OP-V040	VALVE CVS-PL-V015A, V040, OR V041 LEFT OPEN AFTER DEMINERALIZER RESIN TRANSFER		
	HEPE-CVS-XVM-OP-V041			
	HEPE-CVS-XVM-OP-V15A			
HEPE-FWS-XVM-LC-V014	HEPE-FWS-XVM-LC-V14A	MINI-FLOW LINE RECIRCULATION VALVE FWS-PL-V014A OR B LEFT CLOSED		
	HEPE-FWS-XVM-LC-V14B			

Table 10-31. Pre-Initiator Quantification Summary (cont.)

EVENT ID	BE NAME(S)	DESCRIPTION	Total HEP	Error Factor
HEPE-FWS-XVM-LO-V015	HEPE-FWS-XVM-LO-V15A	TEST LINE RECIRCULATION VALVE FWS-PL-V015A OR B LEFT OPEN		
	HEPE-FWS-XVM-LO-V15B			
HEPE-MSS-XVM-CL	HEPE-MSS-XVM-CL-V075	STEAM DUMP ISOLATION VALVE LEFT CLOSED		
HEPE-PCS-XVM-CL-V023	HEPE-PCS-XVM-CL-V023	PCS MANUAL VALVE PCS-PL-V023 UNINTENTIONALLY LEFT CLOSED		
HEPE-PXS-SOV-OP	HEPE-PXS-SOV-OP-V21A	ACCUMULATOR NITROGEN VALVE PXS-PL-V021A OR B LEFT OPEN		
	HEPE-PXS-SOV-OP-V21B			
HEPE-SWS-FNG-LC	HEPE-SWS-FNG-LC-B01	CROSS CONNECT FLANGE SWS-PY-B01 OR B02 LEFT CLOSED		
	HEPE-SWS-FNG-LC-B02			
HEPE-SWS-XVM-LC	HEPE-SWS-XVM-LC-V036	CROSS CONNECT VALVE SWS-PL-V036 OR V083 LEFT CLOSED		
	HEPE-SWS-XVM-LC-V083			
HEPE-TCS-XVM-CL	HEPE-TCS-XVM-CL-V097	TCS-PL-V097 OR V098 LEFT CLOSED FOLLOWING T&M		
	HEPE-TCS-XVM-CL-V098			

Table 10-32. Post-Initiator Operator Action Time Windows

BE ID	T(sw)[1]	T(d)[2]	T(1/2)[3]	T(M)[4]	T(rec)[5]	Description
HEPO-22HRTIMER						OPERATOR FAILS TO DISABLE 22 HR TIMER
HEPO-ADS4-C1						OPERATOR FAILS TO DEPRESSURIZE THE RCS WITH THE ADS STAGE 4 ON LOW CMT LEVEL
HEPO-ADS4-C2						OPERATOR FAILS TO DEPRESSURIZE THE RCS WITH THE ADS STAGE 4 ON LOW HL LEVEL
HEPO-ADS-C1						OPERATOR FAILS TO DEPRESSURIZE RCS WITH THE ADS STAGES 1 – 3 ON CMT LEVEL
HEPO-ADS-C1-SGTR						OPERATOR FAILS TO DEPRESSURIZE THE RCS WITH THE ADS STAGES 1 – 3 ON CMT LEVEL DURING A SGTR
HEPO-ADS-C2						OPERATOR FAILS TO DEPRESSURIZE THE RCS WITH THE ADS STAGES 1 – 3 ON LOW HL LEVEL
HEPO-ADS-C2-SGTR						OPERATOR FAILS TO DEPRESSURIZE THE RCS WITH THE ADS STAGES 1 – 3 ON LOW HL LEVEL DURING A SGTR
HEPO-ADS-GT						OPERATOR FAILS TO DEPRESSURIZE THE RCS WITH THE ADS STAGES 1 – 3 ON LOSS OF HEAT SINK CUE
HEPO-ANC-DG						OPERATOR FAILS TO START ANCILLARY DG AND LOAD PCS RECIRCULATION PUMPS
HEPO-CCSFAN						OPERATOR FAILS TO LOAD THE CCS AHU FANS ONTO THE SDG FOLLOWING A LOOP
HEPO-CMT						OPERATOR FAILS TO MANUALLY START CMT INJECTION

Table 10-32. Post-Initiator Operator Action Time Windows (cont.)

BE ID	T(sw)[1]	T(d)[2]	T(1/2)[3]	T(M)[4]	T(rec)[5]	Description
HEPO-CMT-GT						OPERATOR FAILS TO MANUALLY START CMT INJECTION DURING A LOSS OF HEAT SINK EVENT
HEPO-CNT						OPERATOR FAILS TO MANUALLY ISOLATE CONTAINMENT
HEPO-CST						OPERATOR FAILS TO REFILL THE CST
HEPO-CSTFILL						OPERATOR FAILS TO REFILL THE CST WITH FIRE TRUCK
HEPO-CVSISO						OPERATOR FAILS TO MANUALLY ISOLATE CVS DURING AN ISLOCA EVENT
HEPO-CVSISO-Z						OPERATOR FAILS TO MANUALLY ISOLATE CVS ZINC INJECTION LINE DURING AN ISLOCA EVENT
HEPO-INJ						OPERATOR FAILS TO ACTUATE IRWST INJECTION
HEPO-L2-ADS13						OPERATOR FAILS TO DEPRESSURIZE THE RCS WITH THE ADS STAGES 1 – 3 VALVES ON LOSS OF CORE COOLING CUE
HEPO-L2-CAVFLD						OPERATOR FAILS TO FLOOD RV CAVITY FOR IVR ON LOSS OF CORE COOLING CUE
HEPO-L2-CNT						OPERATOR FAILS TO MANUALLY ISOLATE CONTAINMENT
HEPO-L2-H2I						OPERATOR FAILS TO MANUALLY ACTUATE HYDROGEN IGNITERS

Table 10-32. Post-Initiator Operator Action Time Windows (cont.)

BE ID	T(sw)[1]	T(d)[2]	T(1/2)[3]	T(M)[4]	T(rec)[5]	Description
HEPO-L2-IRWST						OPERATOR FAILS TO ACTUATE IRWST INJECTION ON LOSS OF CORE COOLING CUE
HEPO-L2-PCS						OPERATOR FAILS TO ACTUATE PCS
HEPO-L2-PXSGUT						OPERATOR FAILS TO CLOSE IRWST GUTTER DRAIN VALVES ON LOSS OF CORE COOLING CUE
HEPO-L2-RECIRC						OPERATOR FAILS TO MANUALLY OPEN THE PXS RECIRCULATION VALVES ON LOSS OF CORE COOLING CUE
HEPO-MFW						OPERATOR FAILS TO ALIGN MFW AFTER A REACTOR TRIP
HEPO-OFILL						OPERATOR FAILS TO ISOLATE RUPTURED SG (ON HIGH-3 NR SG LEVEL – PMS BACK-UP)
HEPO-PCS						OPERATOR FAILS TO ACTUATE PCS
HEPO-PCSDIST						OPERATOR FAILS TO SUPPLY WATER DIRECTLY TO THE PCS DISTRIBUTION BUCKET
HEPO-PRHR						OPERATOR FAILS TO ACTUATE PRHR DURING AN EVENT W/ S SIGNAL
HEPO-PRHR-GT						OPERATOR FAILS TO ACTUATE PRHR DURING AN EVENT W/O S SIGNAL
HEPO-RECIRC						OPERATOR FAILS TO MANUALLY OPEN THE PXS RECIRCULATION VALVES
HEPO-RNSINJ						OPERATOR FAILS TO ALIGN RNS FOR INJECTION

Table 10-32. Post-Initiator Operator Action Time Windows (cont.)

BE ID	T(sw)[1]	T(d)[2]	T(1/2)[3]	T(M)[4]	T(rec)[5]	Description
HEPO-RNSIRWST						OPERATOR FAILS TO ALIGN THE IRWST FOR RNS INJECTION
HEPO-RRWSTISO						OPERATOR FAILS TO ISOLATE IRWST RECIRC FOLLOWING SPURIOUS RECIRC ACTUATION
HEPO-RT						OPERATOR FAILS TO MANUALLY TRIP THE REACTOR
HEPO-RWS						OPERATOR FAILS TO START STANDBY RIVER WATER PUMP
HEPO-SDG						OPERATOR FAILS TO MANUALLY START THE DIESEL GENERATOR
HEPO-SFWCD						OPERATOR FAILS TO MANUALLY CONTROL THE PORV SETPOINT FOR COOLDOWN DURING SGTR
HEPO-SFWS						OPERATOR FAILS TO MANUALLY START SFW PUMP DURING AN S SIGNAL EVENT
HEPO-SFWX						OPERATOR FAILS TO MANUALLY START SFW PUMP
HEPO-SGI						OPERATOR FAILS TO ISOLATE RUPTURED SG
HEPO-SWSFAN						OPERATOR FAILS TO START STANDBY SWS COOLING TOWER FAN

Notes:

1. T(sw) = total time available (minutes)
2. T(d) = time until cue is received (minutes)
3. T(1/2) = time to diagnose the cue (minutes)
4. T(M) = time to perform the action following diagnosis of cue (minutes)
5. T(rec) = time available for recovery (T(sw) – (T(d) + T(1/2) + T(M))) (minutes)

Table 10-33. Post-Initiator Quantification Summary

Event ID	Description	Total HEP	Error Factor
HEPO-22HRTIMER	OPERATOR FAILS TO DISABLE 22 HR TIMER		
HEPO-ADS4-C1	OPERATOR FAILS TO DEPRESSURIZE THE RCS WITH THE ADS STAGE 4 ON LOW CMT LEVEL		
HEPO-ADS4-C2	OPERATOR FAILS TO DEPRESSURIZE THE RCS WITH THE ADS STAGE 4 ON LOW HL LEVEL		
HEPO-ADS-C1	OPERATOR FAILS TO DEPRESSURIZE RCS WITH THE ADS STAGES 1 – 3 ON CMT LEVEL		
HEPO-ADS-C1-SGTR	OPERATOR FAILS TO DEPRESSURIZE THE RCS WITH THE ADS STAGES 1 – 3 ON CMT LEVEL DURING A SGTR		
HEPO-ADS-C2	OPERATOR FAILS TO DEPRESSURIZE THE RCS WITH THE ADS STAGES 1 – 3 ON LOW HL LEVEL		
HEPO-ADS-C2-SGTR	OPERATOR FAILS TO DEPRESSURIZE THE RCS WITH THE ADS STAGES 1 – 3 ON LOW HL LEVEL DURING A SGTR		
HEPO-ADS-GT	OPERATOR FAILS TO DEPRESSURIZE THE RCS WITH THE ADS STAGES 1 – 3 ON LOSS OF HEAT SINK CUE		
HEPO-ANC-DG	OPERATOR FAILS TO START ANCILLARY DG AND LOAD PCS RECIRCULATION PUMPS		
HEPO-CCSFAN	OPERATOR FAILS TO LOAD THE CCS AHU FANS ONTO THE SDG FOLLOWING A LOOP		
HEPO-CMT	OPERATOR FAILS TO MANUALLY START CMT INJECTION		
HEPO-CMT-GT	OPERATOR FAILS TO MANUALLY START CMT INJECTION DURING A LOSS OF HEAT SINK EVENT		
HEPO-CNT	OPERATOR FAILS TO MANUALLY ISOLATE CONTAINMENT		
HEPO-COG-CONT	OPERATOR FAILS TO DIAGNOSE HIGH CONTAINMENT PRESSURE		

Table 10-33. Post-Initiator Quantification Summary (cont.)

Event ID	Description	Total HEP	Error Factor
HEPO-COG-CORECOOLING	OPERATOR FAILS TO DIAGNOSE INADEQUATE CORE COOLING		
HEPO-COG-HEATSINK	OPERATOR FAILS TO DIAGNOSE A LOSS OF HEAT SINK EVENT		
HEPO-COG-LOOP	OPERATOR FAILS TO DIAGNOSE A LOSS OF OFFSITE POWER EVENT		
HEPO-COG-SGTR	OPERATOR FAILS TO DIAGNOSE A SGTR EVENT		
HEPO-CST	OPERATOR FAILS TO REFILL THE CST		
HEPO-CSTFILL	OPERATOR FAILS TO REFILL THE CST WITH FIRE TRUCK		
HEPO-CVSISO	OPERATOR FAILS TO MANUALLY ISOLATE CVS DURING A ISLOCA EVENT		
HEPO-CVSISO-Z	OPERATOR FAILS TO MANUALLY ISOLATE CVS ZINC INJECTION LINE DURING A ISLOCA EVENT		
HEPO-INJ	OPERATOR FAILS TO ACTUATE IRWST INJECTION		
HEPO-L2-ADS13	OPERATOR FAILS TO DEPRESSURIZE THE RCS WITH THE ADS STAGES 1 – 3 VALVES ON LOSS OF CORE COOLING CUE		
HEPO-L2-CAVFLD	OPERATOR FAILS TO FLOOD RV CAVITY FOR IVR ON LOSS OF CORE COOLING CUE		
HEPO-L2-CNT	OPERATOR FAILS TO MANUALLY ISOLATE CONTAINMENT		
HEPO-L2-H2I	OPERATOR FAILS TO MANUALLY ACTUATE HYDROGEN IGNITERS		
HEPO-L2-IRWST	OPERATOR FAILS TO ACTUATE IRWST INJECTION ON LOSS OF CORE COOLING CUE		
HEPO-L2-PCS	OPERATOR FAILS TO ACTUATE PCS		
HEPO-L2-PXSGUT	OPERATOR FAILS TO CLOSE IRWST GUTTER DRAIN VALVES ON LOSS OF CORE COOLING CUE		
HEPO-L2-RECIRC	OPERATOR FAILS TO MANUALLY OPEN THE PXS RECIRCULATION VALVES ON LOSS OF CORE COOLING CUE		

Table 10-33. Post-Initiator Quantification Summary (cont.)

Event ID	Description	Total HEP	Error Factor
HEPO-MFW	OPERATOR FAILS TO ALIGN MFW AFTER A REACTOR TRIP		
HEPO-OFILL	OPERATOR FAILS TO ISOLATE RUPTURED SG (ON HIGH-3 NR SG LEVEL – PMS BACK-UP)		
HEPO-PCS	OPERATOR FAILS TO ACTUATE PCS		
HEPO-PCSDIST	OPERATOR FAILS TO SUPPLY WATER DIRECTLY TO THE PCS DISTRIBUTION BUCKET		
HEPO-PRHR	OPERATOR FAILS TO ACTUATE PRHR DURING AN EVENT W/ S SIGNAL		
HEPO-PRHR-GT	OPERATOR FAILS TO ACTUATE PRHR DURING AN EVENT W/O S SIGNAL		
HEPO-RECIRC	OPERATOR FAILS TO MANUALLY OPEN THE PXS RECIRCULATION VALVES		
HEPO-RNSINJ	OPERATOR FAILS TO ALIGN RNS FOR INJECTION		
HEPO-RNSIRWST	OPERATOR FAILS TO ALIGN THE IRWST FOR RNS INJECTION		
HEPO-RRWSTISO	OPERATOR FAILS TO ISOLATE IRWST RECIRC FOLLOWING SPURIOUS RECIRC ACTUATION		
HEPO-RT	OPERATOR FAILS TO MANUALLY TRIP THE REACTOR		
HEPO-RWS	OPERATOR FAILS TO START STANDBY RIVER WATER PUMP		
HEPO-SDG	OPERATOR FAILS TO MANUALLY START THE DIESEL GENERATOR		
HEPO-SFWCD	OPERATOR FAILS TO MANUALLY CONTROL THE PORV SETPOINT FOR COOLDOWN DURING SGTR		
HEPO-SFWS	OPERATOR FAILS TO MANUALLY START SFW PUMP DURING AN S SIGNAL EVENT		
HEPO-SFWX	OPERATOR FAILS TO MANUALLY START SFW PUMP		
HEPO-SGI	OPERATOR FAILS TO ISOLATE RUPTURED SG		

Table 10-33. Post-Initiator Quantification Summary (cont.)

Event ID	Description	Total HEP	Error Factor
HEPO-SWSFAN	OPERATOR FAILS TO START STANDBY SWS COOLING TOWER FAN		

Table 10-34. Generic Component Failure Parameters From NUREG/CR-6928 (Reference 10.15)

Type Code	Description	Mean	Demand (d) or Hourly (h)	Failure Mode from NUREG/CR-6928	α	β	Variance
ABT-FOP	Automatic Bus Transfer Switch Fail to operate	3.05E-03	d	ABT FTOP	0.500	1.635E+02	1.84E-05
ADU-FOP	Air Dryer Unit Fail to operate	5.00E-06	h	ADU FTOP	0.300	6.000E+04	8.33E-11
AHU-RFR	Air Handling Unit (Running) Fail to run	1.37E-05	h	AHU RUN FTR	0.300	2.190E+04	6.26E-10
AHU-RFS	Air Handling Unit (Running) Fail to start	2.73E-03	d	AHU RUN FTS	0.300	1.096E+02	2.45E-05
AHU-SF1	Air Handling Unit (Standby) Fail to run during first hour of operation	2.28E-03	h	AHU STBY FTR<1H	0.300	1.316E+02	1.73E-05
AHU-SFR	Air Handling Unit (Standby) Fail to run after first hour of operation	3.80E-06	h	AHU STBY FTR>1H	0.500	1.314E+05	2.90E-11
AHU-SFS	Air Handling Unit (Standby) Fail to start	8.29E-04	d	AHU STBY FTS	0.360	4.339E+02	1.90E-06
AOV-ELL	Air-Operated Valve External leak large	9.01E-10	h	AOV ELL	0.300	3.329E+08	2.71E-18
AOV-FCX	Air-Operated Valve Fail to control	3.00E-06	h	AOV FC	0.300	1.000E+05	3.00E-11
AOV-FRC	Air-Operated Valve Fail to remain closed	1.82E-07	h	AOV SO	0.300	1.648E+06	1.10E-13
AOV-FTC	Air-Operated Valve Fail to close	1.11E-03	d	AOV FTO/C	1.005	9.044E+02	1.22E-06
AOV-FTO	Air-Operated Valve Fail to open	1.11E-03	d	AOV FTO/C	1.005	9.044E+02	1.22E-06
AOV-ILL	Air-Operated Valve Internal leak large	4.84E-09	h	AOV ILL	0.300	6.198E+07	7.81E-17
AOV-ILS	Air-Operated Valve Internal leak small	2.42E-07	h	AOV ILS	0.661	2.731E+06	8.86E-14

Table 10-34. Generic Component Failure Parameters From NUREG/CR-6928 (Reference 10.15) (cont.)

Type Code	Description	Mean	Demand (d) or Hourly (h)	Failure Mode from NUREG/CR-6928	α	β	Variance
AOV-SOX	Air-Operated Valve Spurious operation	1.82E-07	h	AOV SO	0.300	1.648E+06	1.10E-13
BAT-FOP	Battery Fail to operate	1.86E-06	h	BAT FTOP	0.427	2.296E+05	8.10E-12
BCH-FOP	Battery Charger Fail to operate	5.08E-06	h	BCH FTOP	1.585	3.120E+05	1.63E-11
BUS-FOP	Bus Fail to operate	4.34E-07	h	BUS FTOP	0.502	1.157E+06	3.75E-13
CBK-FTC	Circuit Breaker Fail to close	2.55E-03	d	CBK FTO/C	0.698	2.730E+02	9.26E-06
CBK-FTO	Circuit Breaker Fail to open	2.55E-03	d	CBK FTO/C	0.698	2.730E+02	9.26E-06
CBK-SOX	Circuit Breaker Spurious operation	1.71E-07	h	CBK SO	1.983	1.160E+07	1.47E-14
CHL-RFR	Chiller (Running) Fail to run	9.42E-05	h	CHL RUN FTR	0.489	5.191E+03	1.81E-08
CHL-RFS	Chiller (Running) Fail to start	9.83E-03	d	CHL RUN FTS	0.818	8.240E+01	1.16E-04
CKV-FCX	Check Valve Fail to control	3.61E-07	h	HOV SO	0.300	8.310E+05	4.34E-13
CKV-FTC	Check Valve Fail to close	1.04E-04	d	CKV FTC	0.500	4.818E+03	2.15E-08
CKV-FTO	Check Valve Fail to open	1.30E-05	d	CKV FTO	0.500	3.855E+04	3.36E-10
CKV-ILL	Check Valve Internal leak large	2.96E-08	h	CKV ILL	0.300	1.014E+07	2.92E-15
CKV-ILS	Check Valve Internal leak small	1.48E-06	h	CKV ILS	0.300	2.027E+05	7.30E-12
CRD-FOP	Control Rod Drive Fail to operate	1.32E-05	d	CRD FTOP	0.500	3.791E+04	3.48E-10
CTF-RFR	Cooling Tower Fan (Running) Fail to run	5.95E-07	h	CTF RUN FTR	0.500	8.399E+05	7.09E-13

Table 10-34. Generic Component Failure Parameters From NUREG/CR-6928 (Reference 10.15) (cont.)

Type Code	Description	Mean	Demand (d) or Hourly (h)	Failure Mode from NUREG/CR-6928	α	β	Variance
CTF-RFS	Cooling Tower Fan (Running) Fail to start	1.08E-04	d	CTF RUN FTS	0.500	4.618E+03	2.34E-08
DDP-SF1	Diesel Driven Pump (Standby) Fail to run during first hour of operation	1.58E-03	h	DDP STBY FTR<=1H	0.300	1.899E+02	8.32E-06
DDP-SFR	Diesel Driven Pump (Standby) Fail to run after first hour of operation	9.48E-05	h	DDP STBY FTR>1H	0.300	3.165E+03	2.99E-08
DDP-SFS	Diesel Driven Pump (Standby) Fail to start	3.88E-03	d	DDP STBY FTS	0.300	7.702E+01	4.94E-05
EDG-SFR	Emergency Diesel Generator (Standby) Fail to run after first hour of operation	8.48E-04	h	EDG STBY FTR>1H	2.010	2.370E+03	3.58E-07
EDG-SFS	Emergency Diesel Generator (Standby) Fail to start	4.53E-03	d	EDG STBY FTS	1.075	2.362E+02	1.89E-05
EDG-SLR	Emergency Diesel Generator (Standby) Fail to load and run during first hour of operation	2.90E-03	d	EDG STBY FTLR	1.410	4.866E+02	5.90E-06
FAN-RFR	Fan (Running) Fail to run	1.08E-05	h	FAN RUN FTR	0.652	6.037E+04	1.79E-10
FAN-RFS	Fan (Running) Fail to start	1.79E-03	d	FAN RUN FTS	0.300	1.673E+02	1.06E-05
FAN-SF1	Fan (Standby) Fail to run during first hour of operation	1.91E-03	h	FAN STBY FTR<1H	0.348	1.822E+02	1.05E-05
FAN-SFR	Fan (Standby) Fail to run after first hour of operation	1.11E-04	h	FAN STBY FTR>1H	8.500	7.643E+04	1.46E-09
FAN-SFS	Fan (Standby) Fail to start	2.89E-03	d	FAN STBY FTS	0.300	1.035E+02	2.75E-05

Table 10-34. Generic Component Failure Parameters From NUREG/CR-6928 (Reference 10.15) (cont.)

Type Code	Description	Mean	Demand (d) or Hourly (h)	Failure Mode from NUREG/CR-6928	α	β	Variance
FLT-PLC	Filter Plug (Filter)	9.86E-08	h	FLT PLG (CLEAN)	0.500	5.069E+06	1.95E-14
HOV-FCX	Hydraulic-Operated Valve Fail to control	3.00E-06	h	HOV FC	0.300	1.000E+05	3.00E-11
HOV-FTC	Hydraulic-Operated Valve Fail to close	1.51E-03	d	HOV FTO/C	0.300	1.984E+02	7.55E-06
HOV-FTO	Hydraulic-Operated Valve Fail to open	1.51E-03	d	HOV FTO/C	0.300	1.984E+02	7.55E-06
HOV-SOX	Hydraulic-Operated Valve Spurious operation	3.61E-07	h	HOV SO	0.300	8.310E+05	4.34E-13
HTX-PCR	Heat Exchanger Plug/Foul (CCW or RHR HTX)	6.45E-07	h	HTX PLG CCW/RHR	1.416	2.195E+06	2.94E-13
HTX-SLL	Heat Exchanger Shell External leak large	3.50E-09	h	HTX SHELL ELL	0.300	8.566E+07	4.09E-17
HTX-SLS	Heat Exchanger Shell External leak small	5.00E-08	h	HTX SHELL ELS	0.500	9.993E+06	5.01E-15
HTX-TLL	Heat Exchanger Tube External leak large	3.48E-08	h	HTX TUBE ELL	0.300	8.621E+06	4.04E-15
HTX-TLS	Heat Exchanger Tube External leak small	2.32E-07	h	HTX TUBE ELS	0.300	1.293E+06	1.79E-13
INV-FOP	Inverter Fail to operate	5.28E-06	h	INV FTOP	1.203	2.278E+05	2.32E-11
MDC-RFR	Motor-Driven Compressor (Running) Fail to run	9.16E-05	h	MDC RUN FTR	1.423	1.553E+04	5.90E-09
MDC-RFS	Motor-Driven Compressor (Running) Fail to start	1.33E-02	d	MDC RUN FTS	0.364	2.700E+01	4.63E-04

Table 10-34. Generic Component Failure Parameters From NUREG/CR-6928 (Reference 10.15) (cont.)

Type Code	Description	Mean	Demand (d) or Hourly (h)	Failure Mode from NUREG/CR-6928	α	β	Variance
MDP-RFR	Motor-Driven Pump (Running) Fail to run	4.54E-06	h	MDP RUN FTR	1.655	3.645E+05	1.25E-11
MDP-RFS	Motor-Driven Pump (Running) Fail to start	2.23E-03	d	MDP RUN FTS	0.881	3.942E+02	5.62E-06
MDP-SF1	Motor-Driven Pump (Standby) Fail to run during first hour of operation	3.78E-04	h	MDP STBY FTR<1H	1.703	4.505E+03	8.39E-08
MDP-SFR	Motor-Driven Pump (Standby) Fail to run after first hour of operation	5.80E-06	h	MDP STBY FTR>1H	0.500	8.619E+04	6.73E-11
MDP-SFS	Motor-Driven Pump (Standby) Fail to start	1.47E-03	d	MDP STBY FTS	0.909	6.175E+02	2.37E-06
MOD-FRC	Motor-Operated Damper Fail to remain closed	3.40E-07	h	MOD SO	0.500	1.472E+06	2.31E-13
MOD-FTC	Motor-Operated Damper Fail to close	1.14E-03	d	MOD FTO/C	0.500	4.398E+02	2.57E-06
MOD-FTO	Motor-Operated Damper Fail to open	1.14E-03	d	MOD FTO/C	0.500	4.398E+02	2.57E-06
MOD-SOX	Motor-Operated Damper Spurious operation	3.40E-07	h	MOD SO	0.500	1.472E+06	2.31E-13
MOS-PLG	Motor-Operated Strainer Plug (Other)	7.38E-06	h	STR PLG	0.300	4.065E+04	1.82E-10
MOS-SOX	Motor-Operated Strainer Spurious operation	4.45E-08	h	MOV SO	0.500	1.124E+07	3.96E-15
MOV-ELL	Motor-Operated Valve External leak large	9.84E-10	h	MOV ELL	0.300	3.049E+08	3.23E-18

Table 10-34. Generic Component Failure Parameters From NUREG/CR-6928 (Reference 10.15) (cont.)

Type Code	Description	Mean	Demand (d) or Hourly (h)	Failure Mode from NUREG/CR-6928	α	β	Variance
MOV-FCX	Motor-Operated Valve Fail to control	3.00E-06	h	MOV FC	0.300	1.000E+05	3.00E-11
MOV-FTC	Motor-Operated Valve Fail to close	1.07E-03	d	MOV FTO/C	1.277	1.192E+03	8.95E-07
MOV-FTO	Motor-Operated Valve Fail to open	1.07E-03	d	MOV FTO/C	1.277	1.192E+03	8.95E-07
MOV-ILL	Motor-Operated Valve Internal leak large	3.34E-09	h	MOV ILL	0.300	8.982E+07	3.72E-17
MOV-ILS	Motor-Operated Valve Internal leak small	1.67E-07	h	MOV ILS	0.434	2.599E+06	6.43E-14
MOV-PLG	Motor-Operated Valve Plug (Other)	6.36E-09	h	XVM PLG	0.500	7.856E+07	8.10E-17
MOV-SOX	Motor-Operated Valve Spurious operation	4.45E-08	h	MOV SO	0.500	1.124E+07	3.96E-15
MSW-FTC	Manual Switch Fail to close	1.26E-04	d	MSW FTO/C	0.500	3.958E+03	3.19E-08
MSW-FTO	Manual Switch Fail to open	1.26E-04	d	MSW FTO/C	0.500	3.958E+03	3.19E-08
ORF-PLG	Orifice Plug (Other)	1.00E-06	h	ORF PLG	0.300	3.000E+05	3.33E-12
PDP-ELL	Positive Displacement Pump External leak large	9.03E-09	h	PDP ELL	0.300	3.324E+07	2.72E-16
PDP-RFR	Positive Displacement Pump (Running) Fail to run	8.32E-06	h	PDP RUN FTR	0.300	3.606E+04	2.31E-10
PDP-RFS	Positive Displacement Pump (Running) Fail to start	3.34E-03	d	PDP RUN FTS	0.519	1.549E+02	2.13E-05

Table 10-34. Generic Component Failure Parameters From NUREG/CR-6928 (Reference 10.15) (cont.)

Type Code	Description	Mean	Demand (d) or Hourly (h)	Failure Mode from NUREG/CR-6928	α	β	Variance
PDP-SF1	Positive Displacement Pump (Standby) Fail to run during first hour of operation	4.24E-04	h	PDP STBY FTR<1H	0.500	1.180E+03	3.59E-07
PDP-SFR	Positive Displacement Pump (Standby) Fail to run after first hour of operation	2.54E-05	h	PDP STBY FTR>1H	0.300	1.180E+04	2.15E-09
PDP-SFS	Positive Displacement Pump (Standby) Fail to start	2.99E-03	d	PDP STBY FTS	0.500	1.664E+02	1.78E-05
POD-FTO	Pneumatic-Operated Damper Fail to open	1.02E-03	d	POD FTO/C	0.500	4.919E+02	2.06E-06
POD-SOX	Pneumatic-Operated Damper Spurious operation	1.21E-07	h	POD SO	0.500	4.135E+06	2.92E-14
PRV-FRC	Power-Operated Relief Valve Fail to remain closed	4.63E-07	h	PORV SO	0.300	6.479E+05	7.15E-13
PRV-FTC	Power-Operated Relief Valve Fail to close	1.09E-03	d	PORV FTC	0.500	4.592E+02	2.36E-06
PRV-FTO	Power-Operated Relief Valve Fail to open	7.25E-03	d	PORV FTO	0.435	5.957E+01	1.18E-04
PRV-SOX	Power-Operated Relief Valve Spurious operation	4.63E-07	h	PORV SO	0.300	6.479E+05	7.15E-13
RBM-FTC	Reactor Trip Breaker (Mechanical) Fail to close	1.54E-05	d	RTB (BME) FTO/C	0.500	3.245E+04	4.75E-10
RBM-FTO	Reactor Trip Breaker (Mechanical) Fail to open	1.54E-05	d	RTB (BME) FTO/C	0.500	3.245E+04	4.75E-10

Table 10-34. Generic Component Failure Parameters From NUREG/CR-6928 (Reference 10.15) (cont.)

Type Code	Description	Mean	Demand (d) or Hourly (h)	Failure Mode from NUREG/CR-6928	α	β	Variance
RLY-FOP	Relay Fail to operate	2.48E-05	d	RLY FTOP	0.500	2.013E+04	1.23E-09
SOV-FOD	Solenoid-Operated Valve Fail on demand	9.54E-04	d	SOV FTO/C	0.471	4.932E+02	1.93E-06
SOV-FTC	Solenoid-Operated Valve Fail to close	9.54E-04	d	SOV FTO/C	0.471	4.932E+02	1.93E-06
SOV-FTO	Solenoid-Operated Valve Fail to open	9.54E-04	d	SOV FTO/C	0.471	4.932E+02	1.93E-06
SOV-ILL	Solenoid-Operated Valve Internal leak large	5.56E-09	h	SOV ILL	0.300	5.396E+07	1.03E-16
SOV-ILS	Solenoid-Operated Valve Internal leak small	2.78E-07	h	SOV ILS	0.357	1.284E+06	2.17E-13
SOV-SOX	Solenoid-Operated Valve Spurious operation	9.23E-08	h	SOV SO	0.300	3.250E+06	2.84E-14
STF-FOP	Sensor/Transmitter (Flow) Fail to operate	8.15E-04	d	STF FTOP	0.500	6.132E+02	1.32E-06
STL-FOP	Sensor/Transmitter (Level) Fail to operate	8.15E-04	d	STL FTOP	0.500	6.132E+02	1.32E-06
STP-FOP	Sensor/Transmitter (Pressure) Fail to operate	1.17E-04	d	STP FTOP	0.500	4.278E+03	2.73E-08
STR-PLG	Strainer Plug (Other)	7.38E-06	h	STR PLG	0.300	4.065E+04	1.82E-10
STT-FOP	Sensor/Transmitter (Temperature) Fail to operate	4.32E-04	d	STT FTOP	0.500	1.157E+03	3.73E-07
SVV-FTC	Safety Valve Fail to close	6.76E-05	d	SVV FTC	0.500	7.394E+03	9.14E-09

Table 10-34. Generic Component Failure Parameters From NUREG/CR-6928 (Reference 10.15) (cont.)

Type Code	Description	Mean	Demand (d) or Hourly (h)	Failure Mode from NUREG/CR-6928	α	β	Variance
SVV-FTO	Safety Valve Fail to open	2.47E-03	d	SVV FTO	0.300	1.212E+02	2.01E-05
SVV-SOX	Safety Valve Spurious operation	2.12E-07	h	SVV SO	0.300	1.415E+06	1.50E-13
TFM-FOP	Transformer Fail to operate	9.04E-07	h	TFM FTOP	0.314	3.473E+05	2.60E-12
TNK-PLL	Tank Pressurized External leak large	2.75E-09	h	TNK PRES ELL	0.300	1.092E+08	2.52E-17
TNK-PLS	Tank Pressurized External leak small	3.93E-08	h	TNK PRES ELS	0.500	1.274E+07	3.08E-15
TNK-ULL	Tank Unpressurized External leak large	2.23E-09	h	TNK UNPR ELL	0.300	1.344E+08	1.66E-17
TNK-ULS	Tank Unpressurized External leak small	3.19E-08	h	TNK UNPR ELS	0.500	1.567E+07	2.04E-15
TSA-PLG	Traveling Screen Assembly Plug (Other)	4.68E-06	h	TSA PLG	0.502	1.073E+05	4.36E-11
XVM-ELL	Manual Valve External leak large	3.12E-09	h	XVM ELL	0.300	9.620E+07	3.24E-17
XVM-FTC	Manual Valve Fail to close	7.43E-04	d	XVM FTO/C	0.500	6.722E+02	1.10E-06
XVM-FTO	Manual Valve Fail to open	7.43E-04	d	XVM FTO/C	0.500	6.722E+02	1.10E-06
XVM-ILL	Manual Valve Internal leak large	1.33E-09	h	XVM ILL	0.300	2.250E+08	5.93E-18
XVM-ILS	Manual Valve Internal leak small	6.67E-08	h	XVM ILS	0.500	7.499E+06	8.89E-15
XVM-PLG	Manual Valve Plug (Other)	6.36E-09	h	XVM PLG	0.500	7.856E+07	8.10E-17

Table 10-35. Generic Component Failure Parameters From Other Sources

Type Code	Description	Mean	Demand (d) or Hourly (h)	Other Source	α	β	Variance
CTR-FTI	Control Rod Fail to insert	6.6E-07	d	NUREG/CR-5500 (Reference 10.32), Page E-27(1)	(2)	(2)	1.2E-12
CTV-LPL	Containment Vessel Pre-existing leak large	[ ]	[ ]	WCAP-15691 (Reference 10.33), Table 5-5	[ ]	[ ]	[ ]
CTV-SPL	Containment Vessel Pre-existing leak small	[ ]	[ ]	WCAP-15691 (Reference 10.33), Table 5-5	[ ]	[ ]	[ ]
FUS-SOX	Fuse Spurious operation	1.30E-07	h	NUREG/CR-4639 (Reference 10.34), Appendix A; Fuse	4.8	4.00E-07	3.00E-15
IGN-FOP	Hydrogen Igniter Fail to operate	[ ]	[ ]	Manufacturer Data	[ ]	[ ]	[ ]
MOV-BLK	Motor-Operated Valve blocked	[ ]	[ ]	Expert Judgment	[ ]	[ ]	[ ]
NDT-FOP	Neutron Detector/Transmitter Fail to operate	[ ]	[ ]	WCAP-15376-P-A (Reference 10.35), App D	[ ]	[ ]	[ ]
PXS-CKV-FOP	PXS Injection Line Check Valve Fail to operate	7.10E-07	Note 4	NUREG/CR-6928 (Reference 10.15) – Based on data for check valve failing due to large internal leakage	0.3	4.23E+05	1.68E-12
PXS-EOV-FTO	PXS Explosive-Operated Valve Fail to open	[ ]	[ ]	AP1000 Plant Design Reference	[ ]	[ ]	[ ]
PXS-EOV-RPI	PXS Explosive Operated Valve (IRWST Injection Line) Rupture	[ ]	[ ]	LTR-RIAM-12-44 (Reference 10.37)	[ ]	[ ]	[ ]

Table 10-35. Generic Component Failure Parameters From Other Sources (cont.)

Type Code	Description	Mean	Demand (d) or Hourly (h)	Other Source	α	β	Variance
RCS-EOV-RPA	RCS Explosive Operated Valve (ADS Stage 4) Rupture	[ ]	[ ]	LTR-AMLRS-11-31 (Reference 10.36)	[ ]	[ ]	[ ]
SRV-FTC	Safety Relief Valve Fail to close	3.14E-03	d	NUREG/CR-4639 (Reference 10.34), Appendix A; Relief Valve	0.57	1.81E+02	1.71E-05
SRV-FTO	Safety Relief Valve Fail to open	1.03E-02	d	NUREG/CR-4639 (Reference 10.34), Appendix A; Relief Valve	0.43	4.11E+02	2.39E-04
SRV-SOX	Safety Relief Valve Fail to operate	7.06E-07	h	NUREG/CR-4639 (Reference 10.34), Appendix A; Relief Valve	1.16	1.64E+06	4.30E-13
TCV-FOP	Temperature Control Valve Fail to operate	1.24E-04	h	NUREG/CR-4639 (Reference 10.34), Appendix A; Valves Unknown Operator	13	1.08E+05	1.15E-09
VHO-FOP, VOF-FOP, VPV-FOP, VVB-FOP	Vent Fail to operate	3.05E-03	d	NUREG/CR-4639 (Reference 10.34), Appendix A; Damper Unknown Operator	2.79	9.10E+02	3.33E-06

Notes:
1. [
]
2. Lognormal distribution
3. [ ]
4. [ ]

Table 10-36. Generic Unavailability From NUREG/CR-6928 (Reference 10.15)

Variable Name	Description	Unavailability	Event Code from NUREG/CR-6928	α	β	Variance
!CAS-MDC-TAM	CAS Motor-Driven Compressor Unavailable Due To Test and/or Maintenance	1.30E-02	MDC-TM	0.500	3.796E+01	3.25E-04
!CCS-HTX-TAM	CCS Heat Exchanger Unavailable Due To Test and/or Maintenance (CCW)	7.23E-03	HTX-TM (CCW)	1.000	1.373E+02	5.15E-05
!CCS-MDP-TAM	CCS Motor-Driven Pump Unavailable Due To Test and/or Maintenance (CCW)	5.91E-03	MDP-TM (CCW)	1.288	2.166E+02	2.68E-05
!CDS-MDP-TAM	CDS Motor-Driven Pump Unavailable Due To Test and/or Maintenance (AFWS)	3.95E-03	MDP-TM (AFWS)	2.387	6.019E+02	6.50E-06
!CVS-MDP-TAM	CVS Motor-Driven Pump Unavailable Due To Test and/or Maintenance (HPSI)	4.12E-03	MDP-TM (HPSI)	2.348	5.676E+02	7.19E-06
!CWS-MDP-TAM	CWS Motor-Driven Pump Unavailable Due To Test and/or Maintenance (Other)	7.51E-03	MDP-TM (Other)	1.000	1.322E+02	5.55E-05
!DTS-MDP-TAM	DTS Motor-Driven Pump Unavailable Due To Test and/or Maintenance (Other)	7.51E-03	MDP-TM (Other)	1.000	1.322E+02	5.55E-05
!DWS-MDP-TAM	DWS Motor-Driven Pump Unavailable Due To Test and/or Maintenance (Other)	7.51E-03	MDP-TM (Other)	1.000	1.322E+02	5.55E-05
!ECS-BAC-TAM	ECS AC Bus Unavailable Due To Test and/or Maintenance	2.15E-04	BAC-TM	0.500	2.325E+03	9.24E-08
!EDS-BCH-TAM	EDS Battery Charger Unavailable Due To Test and/or Maintenance	2.20E-03	BCH-TM	0.500	2.268E+02	9.61E-06

Table 10-36. Generic Unavailability From NUREG/CR-6928 (Reference 10.15) (cont.)

Variable Name	Description	Unavailability	Event Code from NUREG/CR-6928	α	β	Variance
!FPS-MDP-TAM	FPS Motor-Driven Pump Unavailable Due To Test and/or Maintenance (Other)	7.51E-03	MDP-TM (Other)	1.000	1.322E+02	5.55E-05
!FWS-MDP-TAM	FWS Motor-Driven Pump Unavailable Due To Test and/or Maintenance (AFWS)	3.95E-03	MDP-TM (AFWS)	2.387	6.019E+02	6.50E-06
!IDS-BCH-TAM	IDS Battery Charger Unavailable Due To Test and/or Maintenance	2.20E-03	BCH-TM	0.500	2.268E+02	9.61E-06
!PCS-MDP-TAM	PCS Motor-Driven Pump Unavailable Due To Test and/or Maintenance (Other)	7.51E-03	MDP-TM (Other)	1.000	1.322E+02	5.55E-05
!RNS-HTX-TAM	RNS Heat Exchanger Unavailable Due To Test and/or Maintenance (RHR-PWR)	5.18E-03	HTX-TM (RHR-PWR)	2.748	5.278E+02	9.69E-06
!RNS-MDP-TAM	RNS Motor-Driven Pump Unavailable Due To Test and/or Maintenance (Other)	7.51E-03	MDP-TM (Other)	1.000	1.322E+02	5.55E-05
!RWS-MDP-TAM	RWS Motor-Driven Pump Unavailable Due To Test and/or Maintenance (Other)	7.51E-03	MDP-TM (Other)	1.000	1.322E+02	5.55E-05
!SWS-CTF-TAM	SWS Cooling Tower Fan Unavailable Due To Test and/or Maintenance	1.86E-03	CTF-TM	0.500	2.683E+02	6.88E-06
!SWS-MDP-TAM	SWS Motor-Driven Pump Unavailable Due To Test and/or Maintenance	1.30E-02	MDP-TM (ESW)	1.000	7.592E+01	1.65E-04
!TCS-HTX-TAM	TCS Heat Exchanger Unavailable Due To Test and/or Maintenance (CCW)	7.23E-03	HTX-TM (CCW)	1.000	1.373E+02	5.15E-05
!TCS-MDP-TAM	TCS Motor-Driven Pump Unavailable Due To Test and/or Maintenance (CCW)	5.91E-03	MDP-TM (CCW)	1.288	2.166E+02	2.68E-05

Table 10-36. Generic Unavailability From NUREG/CR-6928 (Reference 10.15) (cont.)

Variable Name	Description	Unavailability	Event Code from NUREG/CR-6928	α	β	Variance
!VAS-AHU-TAM	VAS Air Handling Unit Unavailable Due To Test and/or Maintenance	2.48E-03	AHU-TM	0.500	2.011E+02	1.22E-05
!VBS-AHU-TAM	VBS Air Handling Unit Unavailable Due To Test and/or Maintenance	2.48E-03	AHU-TM	0.500	2.011E+02	1.22E-05
!VTS-AHU-TAM	VTS Air Handling Unit Unavailable Due To Test and/or Maintenance	2.48E-03	AHU-TM	0.500	2.011E+02	1.22E-05
!VTS-FAN-TAM	VTS Fan Unavailable Due To Test and/or Maintenance	2.00E-03	FAN-TM	0.500	2.495E+02	7.95E-06
!VWS-CHL-TAM	VWS Chiller Unavailable Due To Test and/or Maintenance (Other)	1.98E-02	CHL-TM	0.500	2.482E+01	7.35E-04
!VWS-MDP-TAM	VWS Motor-Driven Pump Unavailable Due To Test and/or Maintenance (Other)	7.51E-03	MDP-TM (Other)	1.000	1.322E+02	5.55E-05
!VXS-AHU-TAM	VXS Air Handling Unit Unavailable Due To Test and/or Maintenance	2.48E-03	AHU-TM	0.500	2.011E+02	1.22E-05
!VZS-AHU-TAM	VZS Air Handling Unit Unavailable Due To Test and/or Maintenance	2.48E-03	AHU-TM	0.500	2.011E+02	1.22E-05
!VZS-FAN-TAM	VZS Fan Unavailable Due To Test and/or Maintenance	2.00E-03	FAN-TM	0.500	2.495E+02	7.95E-06

Table 10-36. Generic Unavailability From NUREG/CR-6928 (Reference 10.15) (cont.)

Variable Name	Description	Unavailability	Event Code from NUREG/CR-6928	α	β	Variance
!ZOS-EDG-TAM	ZOS Diesel Generator Unavailable Due To Test and/or Maintenance	1.34E-02	EDG-TM (EPS)	3.586	2.640E+02	4.92E-05
!ZRS-BAC-TAM	ZRS AC Bus Unavailable Due To Test and/or Maintenance	2.15E-04	BAC-TM	0.500	2.325E+03	9.24E-08
!ZRS-EDG-TAM	ZRS Diesel Generator Unavailable Due To Test and/or Maintenance	1.34E-02	EDG-TM (EPS)	3.586	2.640E+02	4.92E-05

Table 10-37. Generic Unavailability From Other Sources

Variable Name	Description	Unavailability	Source	α	β	Variance
!MSS-HOV-TAM	MSS Hydraulic-Operated Valve Unavailable Due To Test and/or Maintenance	[ ]	System Design Engineer Input	[ ]	[ ]	[ ]
!SGS-MOV-BLK	SGS Motor-Operated Valve Blocked	[ ]	Engineering Judgment	[ ]	[ ]	[ ]
!CVS-AOV-SML	CVS Air-Operated Simultaneous Actuation of Makeup and Letdown	[ ]	AP1000 Plant Design Reference	[ ]	[ ]	[ ]
!LOOP-MT	LOOP Event During Mission Time	9.84E-05	NUREG/CR-6928 (Reference 10.15)	1.580	4.40E+01	6.12E-09

Table 10-38. DAS Component Failure and Unavailability Parameters (Reference 10.38)

Type Code	Description	Unavailability	α	β	Variance
!DAS-AUT-TAM	DAS Test And Maintenance Unavailability For All Automatic Functions				
DAS-ALS-FOP	DAS ALS Backplane Fail To Operate				
DAS-ATS-FOP	DAS Automatic Transfer Switch Fail To Operate				
DAS-CP1-FOP	DAS Core Processing Board ALS-102 Fail To Operate				
DAS-ELF-FOP	DAS Electric Line Filter Fail To Operate				
DAS-IP2-FOP	DAS Input Processing Board ALS-311 Fail To Operate				
DAS-IP3-FOP	DAS Input Processing Board ALS-321 Fail To Operate				
DAS-OP1-FOP	DAS Output Processing Board ALS-402 Fail To Operate				
DAS-PSA-FOP	DAS 48V DC, 300W DAS Control Power Supply Fail To Operate				
DAS-PSB-FOP	DAS 48V DC, 150W DAS Loads Power Supply Fail To Operate				
DAS-PSC-FOP	DAS 24V DC, 150W DAS Sensor Power Supply Fail To Operate				
DAS-PSD-FOP	DAS 24V DC, 600W DAS Squib Controllers Power Supply Fail To Operate				
DAS-SVC-FOP	DAS Squib Valve Controller Fail To Operate				
DAS-UPS-FOP	DAS UPS Fails To Operate				

Table 10-39. PMS Component Failure and Unavailability Parameters (Reference 10.39)

Type Code	Description	Unavailability	α	β	Variance
!PMS-BPL-TAM	PMS BPL Unavailable Due To Test Or Maintenance				
PMS-ABD-FBR	PMS ADS Block Device Fail To Be Removed				
PMS-ABD-SIE	PMS ADS Block Device Fails To Block Spurious Operation				
PMS-AF1-FOP	PMS AF100 (Communication Highway) Fail To Operate				
PMS-AI1-FOP	PMS Analogue Input Module (AI687) Fail To Operate				
PMS-AI2-FOP	PMS Analogue Input Module (AI688) Fail To Operate				
PMS-AOM-FOP	PMS Analogue Output Module Fail To Operate				
PMS-CIM-FOP	PMS Component Interface Module Fail To Operate				
PMS-CIM-SOX	PMS Component Interface Module Fault Results In Spurious Actuation				
PMS-COM-FOP	PMS Communications Interface Module (CI631) Fail To Operate				
PMS-CTI-FOP	PMS Contact Inputs Fail To Operate				
PMS-DIM-FOP	PMS Digital Input Module Fail To Operate				
PMS-DO1-FOP	PMS Digital Output Module (DO620) Fail To Operate				
PMS-DO2-FOP	PMS Digital Output Module (DO630) Fail To Operate				
PMS-HSL-FOP	PMS High Speed Link Fail To Operate				

Table 10-39. PMS Component Failure and Unavailability Parameters (Reference 10.39) (cont.)

Type Code	Description	Unavailability	α	β	Variance
PMS-IS1-FOP	PMS ISB Analogue Output I/I Isolator (Current/Current) Fail To Operate				
PMS-IS2-FOP	PMS ISB Analogue Output E/I Isolator (Voltage/Current) Fail To Operate				
PMS-IS3-FOP	PMS ISB Digital Output Fail To Operate				
PMS-IS4-FOP	PMS BCC Turbine Trip Isolation Barrier Assembly Fail To Operate				
PMS-PRM-FOP	PMS Processor Module Fail To Operate				
PMS-PS1-FOP	PMS 24V, 10A QUINT Fail to Operate				
PMS-PS2-FOP	PMS 24V, 20A QUINT Fail to Operate				
PMS-PWF-FOP	PMS Line Filter Fail to Operate				
PMS-RCT-FOP	PMS Rectifier Fail to Operate				
PMS-RNC-FOP	PMS Remote Node Controller Fail To Operate				
PMS-RST-FOP	PMS Reactor Trip Matrix Termination Unit Shunt Trip Fail To Operate				
PMS-RUV-FOP	PMS Reactor Trip Matrix Termination Unit Undervoltage Trip Fail To Operate				
PMS-SRD-FOP	PMS Safety-Related Display Fail to Operate				
PMS-SRN-FOP	PMS Safety Remote Node Controller Fail To Operate				
PMS-STU-FOP	PMS Squib Valve Termination Unit Fail To Operate				

Table 10-40. PLS Component Failure and Unavailability Parameters (Reference 10.41)

Type Code	Description	Unavailability	α	β	Variance
PLS-AIM-FOP	HART High Performance Analogue Input Fail to Operate				
PLS-AOM-FOP	HART High Performance Analogue Output Fail to Operate				
PLS-CPS-FOP	PCPS (power supply to CPU) Fail to Operate				
PLS-CTI-FOP	Enhanced Compact SOE Input Module (contact inputs) Fail to Operate				
PLS-IOC-FOP	IOIC Interface Fail to Operate				
PLS-MAU-FOP	Media Attachment Unit Fail to Operate				
PLS-PDM-FOP	Power Distribution Module Fail to Operate				
PLS-PFB-FOP	Profibus Fail to Operate				
PLS-PRM-FOP	OCR400 Controller Fail to Operate				
PLS-PSA-FOP	24V Power Supply Fail to Operate				
PLS-PWF-FOP(1)	Power Line Filter Fail to Operate				
PLS-RNC-FOP	Remote Node Controller Fail to Operate				
PLS-ROM-FOP	Relay Output Module Fail to Operate				
PLS-RTD-FOP	Resistance Temperature Detector				
PLS-WST-FOP(2)	PLS Workstation Display Fail to Operate				

Notes:
1. Data is from Reference 10.40.
2. [ ]

Table 10-41. System/Component Specific Common Cause Groups

System/Component	Failure Mode
Diesel Generators SWS Motor-Driven Pumps SFW Motor-Driven Pumps RNS Motor-Driven Pumps	Fail to Start
	Fail to Run
480V ac Breakers 4.16/6.9kV Breakers dc Breakers Reactor Trip Circuit Breakers MSS MSIVs	Fail to Open
	Fail to Close
	Spurious Operation
Battery Chargers	No Output
	High Output
SWS Motor-Operated Valves SFW Motor-Operated Valves RNS Motor-Operated Valves SFW Air-Operated Valves	Fail to Open
	Fail to Close
	Fail to Remain Closed
SWS Air-Operated Valves	Fail to Open
SWS Check Valves SFW Check Valves	Fail to Close
	Fail to Open
RNS Check Valves	Fail to Close
	Fail to Remain Closed
RNS Air-Operated Valves	Fail to Open
	Fail to Close
SWS Air-Operated Valves	Fail to Open
SWS Check Valves	Fail to Close
SWS Strainers	Plugging
RCS Primary Safety Valves	Fail to Remain Closed
MSS Steam Relief Valves Steam Generator PORVs (ADVs)	Fail to Open
	Fail to Close
	Spurious Operation
	Fail to Remain Closed

Table 10-42. Generic Common Cause Groups

Component	Failure Mode
All driven equipment (diesel generators, pumps, chillers, compressors, fans, inverters)	Fail to Start
	Fail to Run
All air, hydraulic, motor, and solenoid-operated valves and dampers	Fail to Open
	Fail to Close
	Fail to Remain Closed
All check valves	Fail to Open
	Fail to Close
RCS ADS Stage 4 Explosive-Operated Valves	Fail to Open
PXS High Pressure Injection and Recirculation Explosive-Operated Valves	Fail to Open
PXS Low Pressure Recirculation Explosive-Operated Valves	Fail to Open
Heat exchangers	Plug

Table 10-43. Common Cause Alpha And Beta Factor Variables (Reference 10.46)

Variable Name	Description	Value	α	β	Variance
#ECS-BKF-FTC-22	CCF Failure ECS BKF Fail to Close Group Size Of 2, Alpha Factor 2				
#ECS-BKF-FTO-22	CCF Failure ECS BKF Fail to Open Group Size Of 2, Alpha Factor 2				
#ECS-BKF-SOX-22	CCF Failure ECS BKF Spurious Operation Group Size Of 2, Alpha Factor 2				
#ECS-BKS-FTC-22	CCF Failure ECS BKS Fail to Close Group Size Of 2, Alpha Factor 2				
#ECS-BKS-FTC-42	CCF Failure ECS BKS Fail to Close Group Size Of 4, Alpha Factor 2				
#ECS-BKS-FTC-43	CCF Failure ECS BKS Fail to Close Group Size Of 4, Alpha Factor 3				
#ECS-BKS-FTC-44	CCF Failure ECS BKS Fail to Close Group Size Of 4, Alpha Factor 4				
#ECS-BKS-FTO-22	CCF Failure ECS BKS Fail to Open Group Size Of 2, Alpha Factor 2				
#ECS-BKS-FTO-42	CCF Failure ECS BKS Fail to Open Group Size Of 4, Alpha Factor 2				
#ECS-BKS-FTO-43	CCF Failure ECS BKS Fail to Open Group Size Of 4, Alpha Factor 3				
#ECS-BKS-FTO-44	CCF Failure ECS BKS Fail to Open Group Size Of 4, Alpha Factor 4				
#ECS-BKS-FTO-82	CCF Failure ECS BKS Fail to Open Group Size Of 8, Alpha Factor 2				
#ECS-BKS-FTO-83	CCF Failure ECS BKS Fail to Open Group Size Of 8, Alpha Factor 3				

Table 10-43. Common Cause Alpha And Beta Factor Variables (Reference 10.46) (cont.)

Variable Name	Description	Value	α	β	Variance
#ECS-BKS-FTO-88	CCF Failure ECS BKS Fail to Open Group Size Of 8, Alpha Factor 8				
#ECS-BKS-SOX-22	CCF Failure ECS BKS Spurious Operation Group Size Of 2, Alpha Factor 2				
#ECS-BKS-SOX-42	CCF Failure ECS BKS Spurious Operation Group Size Of 4, Alpha Factor 2				
#ECS-BKS-SOX-43	CCF Failure ECS BKS Spurious Operation Group Size Of 4, Alpha Factor 3				
#ECS-BKS-SOX-44	CCF Failure ECS BKS Spurious Operation Group Size Of 4, Alpha Factor 4				
#EDS-BCH-FOP-42	CCF Failure EDS BCH Fail to Operate Group Size Of 4, Alpha Factor 2				
#EDS-BCH-FOP-43	CCF Failure EDS BCH Fail to Operate Group Size Of 4, Alpha Factor 3				
#EDS-BCH-FOP-44	CCF Failure EDS BCH Fail to Operate Group Size Of 4, Alpha Factor 4				
#EDS-EDG-SFR-22	CCF Failure ECS EDG (Standby) Fail to Run After First Hour of Operation Group Size Of 2, Alpha Factor 2				
#ECS-EDG-SFS-22	CCF Failure ECS EDG (Standby) Fail to Start Group Size Of 2, Alpha Factor 2				
#ECS-EDG-SLR-22	CCF Failure ECS EDG (Standby) Fail to Load and Run During First Hour of Operation Group Size Of 2, Alpha Factor 2				
#FWS-CKV-FTO-22	CCF Failure FWS CKV Fail to Open Group Size Of 2, Alpha Factor 2				

Table 10-43. Common Cause Alpha And Beta Factor Variables (Reference 10.46) (cont.)

Variable Name	Description	Value	α	β	Variance
#FWS-MDP-SF1-22	CCF Failure FWS MDP Fail to Start And Run 1 Hour Group Size Of 2, Alpha Factor 2				
#FWS-MDP-SFR-22	CCF Failure FWS MDP Fail to Run Group Size Of 2, Alpha Factor 2				
#FWS-MDP-SFS-22	CCF Failure FWS MDP Fail to Start Group Size Of 2, Alpha Factor 2				
#FWS-MOV-FRC-22	CCF Failure FWS MOV Spurious Op Group Size Of 2, Alpha Factor 2				
#FWS-MOV-FTO-22	CCF Failure FWS MOV Fail to Open Group Size Of 2, Alpha Factor 2				
#GEN-GEN-DMD-22	Generic CCF Demand Failure Group Size Of 2, Alpha Factor 2				
#GEN-GEN-DMD-32	Generic CCF Demand Failure Group Size Of 3, Alpha Factor 2				
#GEN-GEN-DMD-33	Generic CCF Demand Failure Group Size Of 3, Alpha Factor 3				
#GEN-GEN-DMD-42	Generic CCF Demand Failure Group Size Of 4, Alpha Factor 2				
#GEN-GEN-DMD-43	Generic CCF Demand Failure Group Size Of 4, Alpha Factor 3				
#GEN-GEN-DMD-44	Generic CCF Demand Failure Group Size Of 4, Alpha Factor 4				
#GEN-GEN-DMD-52	Generic CCF Demand Failure Group Size Of 5, Alpha Factor 2				
#GEN-GEN-DMD-53	Generic CCF Demand Failure Group Size Of 5, Alpha Factor 3				

Table 10-43. Common Cause Alpha And Beta Factor Variables (Reference 10.46) (cont.)

Variable Name	Description	Value	α	β	Variance
#GEN-GEN-DMD-55	Generic CCF Demand Failure Group Size Of 5, Alpha Factor 5				
#GEN-GEN-DMD-62	Generic CCF Demand Failure Group Size Of 6, Alpha Factor 2				
#GEN-GEN-DMD-63	Generic CCF Demand Failure Group Size Of 6, Alpha Factor 3				
#GEN-GEN-DMD-66	Generic CCF Demand Failure Group Size Of 6, Alpha Factor 6				
#GEN-GEN-DMD-82	Generic CCF Demand Failure Group Size Of 8, Alpha Factor 2				
#GEN-GEN-DMD-83	Generic CCF Demand Failure Group Size Of 8, Alpha Factor 3				
#GEN-GEN-DMD-88	Generic CCF Demand Failure Group Size Of 8, Alpha Factor 8				
#GEN-GEN-DMD-102	Generic CCF Demand Failure Group Size Of 10, Alpha Factor 2				
#GEN-GEN-DMD-103	Generic CCF Demand Failure Group Size Of 10, Alpha Factor 3				
#GEN-GEN-DMD-1010	Generic CCF Demand Failure Group Size Of 10, Alpha Factor 10				
#GEN-GEN-DMD-122	Generic CCF Demand Failure Group Size Of 12, Alpha Factor 2				
#GEN-GEN-DMD-123	Generic CCF Demand Failure Group Size Of 12, Alpha Factor 3				
#GEN-GEN-DMD-1212	Generic CCF Demand Failure Group Size Of 12, Alpha Factor 12				

Table 10-43. Common Cause Alpha And Beta Factor Variables (Reference 10.46) (cont.)

Variable Name	Description	Value	α	β	Variance
#GEN-GEN-DMD-202	Generic CCF Demand Failure Group Size Of 20, Alpha Factor 2				
#GEN-GEN-DMD-203	Generic CCF Demand Failure Group Size Of 20, Alpha Factor 3				
#GEN-GEN-DMD-2020	Generic CCF Demand Failure Group Size Of 20, Alpha Factor 20				
#GEN-GEN-DMD-242	Generic CCF Demand Failure Group Size Of 24, Alpha Factor 2				
#GEN-GEN-DMD-243	Generic CCF Demand Failure Group Size Of 24, Alpha Factor 3				
#GEN-GEN-DMD-2424	Generic CCF Demand Failure Group Size Of 24, Alpha Factor 24				
#GEN-GEN-RF1-22	Generic CCF Fail to Run 1st Hour With Group Size Of 2, Alpha Factor 2				
#GEN-GEN-RF1-32	Generic CCF Fail to Run 1st Hour With Group Size Of 3, Alpha Factor 2				
#GEN-GEN-RF1-33	Generic CCF Fail to Run 1st Hour With Group Size Of 3, Alpha Factor 3				
#GEN-GEN-RF1-42	Generic CCF Fail to Run 1st Hour With Group Size Of 4, Alpha Factor 2				
#GEN-GEN-RF1-43	Generic CCF Fail to Run 1st Hour With Group Size Of 4, Alpha Factor 3				
#GEN-GEN-RF1-44	Generic CCF Fail to Run 1st Hour With Group Size Of 4, Alpha Factor 4				
#GEN-GEN-RF1-52	Generic CCF Fail to Run 1st Hour With Group Size Of 5, Alpha Factor 2				

Table 10-43. Common Cause Alpha And Beta Factor Variables (Reference 10.46) (cont.)

Variable Name	Description	Value	α	β	Variance
#GEN-GEN-RF1-53	Generic CCF Fail to Run 1st Hour With Group Size Of 5, Alpha Factor 3				
#GEN-GEN-RF1-55	Generic CCF Fail to Run 1st Hour With Group Size Of 5, Alpha Factor 5				
#GEN-GEN-RF1-62	Generic CCF Fail to Run 1st Hour With Group Size Of 6, Alpha Factor 2				
#GEN-GEN-RF1-63	Generic CCF Fail to Run 1st Hour With Group Size Of 6, Alpha Factor 3				
#GEN-GEN-RF1-66	Generic CCF Fail to Run 1st Hour With Group Size Of 6, Alpha Factor 6				
#GEN-GEN-RF1-82	Generic CCF Fail to Run 1st Hour With Group Size Of 8, Alpha Factor 2				
#GEN-GEN-RF1-83	Generic CCF Fail to Run 1st Hour With Group Size Of 8, Alpha Factor 3				
#GEN-GEN-RF1-88	Generic CCF Fail to Run 1st Hour With Group Size Of 8, Alpha Factor 8				
#GEN-GEN-RF1-102	Generic CCF Fail to Run 1st Hour With Group Size Of 10, Alpha Factor 2				
#GEN-GEN-RF1-103	Generic CCF Fail to Run 1st Hour With Group Size Of 10, Alpha Factor 3				
#GEN-GEN-RF1-1010	Generic CCF Fail to Run 1st Hour With Group Size Of 10, Alpha Factor 10				
#GEN-GEN-RF1-122	Generic CCF Fail to Run 1st Hour With Group Size Of 12, Alpha Factor 2				
#GEN-GEN-RF1-123	Generic CCF Fail to Run 1st Hour With Group Size Of 12, Alpha Factor 3				

Table 10-43. Common Cause Alpha And Beta Factor Variables (Reference 10.46) (cont.)

Variable Name	Description	Value	α	β	Variance
#GEN-GEN-RF1-1212	Generic CCF Fail to Run 1st Hour With Group Size Of 12, Alpha Factor 12				
#GEN-GEN-RUN-22	Generic CCF Run Failure With Group Size Of 2, Alpha Factor 2				
#GEN-GEN-RUN-32	Generic CCF Run Failure With Group Size Of 3, Alpha Factor 2				
#GEN-GEN-RUN-33	Generic CCF Run Failure With Group Size Of 3, Alpha Factor 3				
#GEN-GEN-RUN-42	Generic CCF Run Failure With Group Size Of 4, Alpha Factor 2				
#GEN-GEN-RUN-43	Generic CCF Run Failure With Group Size Of 4, Alpha Factor 3				
#GEN-GEN-RUN-44	Generic CCF Run Failure With Group Size Of 4, Alpha Factor 4				
#GEN-GEN-RUN-52	Generic CCF Run Failure With Group Size Of 5, Alpha Factor 2				
#GEN-GEN-RUN-53	Generic CCF Run Failure With Group Size Of 5, Alpha Factor 3				
#GEN-GEN-RUN-55	Generic CCF Run Failure With Group Size Of 5, Alpha Factor 5				
#GEN-GEN-RUN-62	Generic CCF Run Failure With Group Size Of 6, Alpha Factor 2				
#GEN-GEN-RUN-63	Generic CCF Run Failure With Group Size Of 6, Alpha Factor 3				
#GEN-GEN-RUN-66	Generic CCF Run Failure With Group Size Of 6, Alpha Factor 6				

Table 10-43. Common Cause Alpha And Beta Factor Variables (Reference 10.46) (cont.)

Variable Name	Description	Value	α	β	Variance
#GEN-GEN-RUN-82	Generic CCF Run Failure With Group Size Of 8, Alpha Factor 2				
#GEN-GEN-RUN-83	Generic CCF Run Failure With Group Size Of 8, Alpha Factor 3				
#GEN-GEN-RUN-88	Generic CCF Run Failure With Group Size Of 8, Alpha Factor 8				
#GEN-GEN-RUN-92	Generic CCF Run Failure With Group Size Of 9, Alpha Factor 2				
#GEN-GEN-RUN-93	Generic CCF Run Failure With Group Size Of 9, Alpha Factor 3				
#GEN-GEN-RUN-99	Generic CCF Run Failure With Group Size Of 9, Alpha Factor 9				
#GEN-GEN-RUN-102	Generic CCF Run Failure With Group Size Of 10, Alpha Factor 2				
#GEN-GEN-RUN-103	Generic CCF Run Failure With Group Size Of 10, Alpha Factor 3				
#GEN-GEN-RUN-1010	Generic CCF Run Failure With Group Size Of 10, Alpha Factor 10				
#GEN-GEN-RUN-122	Generic CCF Run Failure With Group Size Of 12, Alpha Factor 2				
#GEN-GEN-RUN-123	Generic CCF Run Failure With Group Size Of 12, Alpha Factor 3				
#GEN-GEN-RUN-1212	Generic CCF Run Failure With Group Size Of 12, Alpha Factor 12				
#GEN-GEN-RUN-202	Generic CCF Run Failure With Group Size Of 20, Alpha Factor 2				

Table 10-43. Common Cause Alpha And Beta Factor Variables (Reference 10.46) (cont.)

Variable Name	Description	Value	α	β	Variance
#GEN-GEN-RUN-203	Generic CCF Run Failure With Group Size Of 20, Alpha Factor 3				
#GEN-GEN-RUN-2020	Generic CCF Run Failure With Group Size Of 20, Alpha Factor 12				
#GEN-GEN-RUN-242	Generic CCF Run Failure With Group Size Of 24, Alpha Factor 2				
#GEN-GEN-RUN-243	Generic CCF Run Failure With Group Size Of 24, Alpha Factor 3				
#GEN-GEN-RUN-2424	Generic CCF Run Failure With Group Size Of 24, Alpha Factor 24				
#IDS-BCH-FOP-22	CCF Failure IDS BCH Fail to Operate Group Size Of 2, Alpha Factor 2				
#IDS-BCH-FOP-42	CCF Failure IDS BCH Fail to Operate Group Size Of 4, Alpha Factor 2				
#IDS-BCH-FOP-43	CCF Failure IDS BCH Fail to Operate Group Size Of 4, Alpha Factor 3				
#IDS-BCH-FOP-44	CCF Failure IDS BCH Fail to Operate Group Size Of 4, Alpha Factor 4				
#PCS-AOV-FTO-22	CCF Failure PCS AOV Fail to Open, Group Size of 2, Alpha Factor 2				
#PCS-MDP-SF1-22	CCF Failure PCS MDP Fail to Start and Run 1 Hour Group Size of 2, Alpha Factor 2				
#PCS-MDP-SFR-22	CCF Failure PCS MDP Fail to Run Group Size Of 2, Alpha Factor 2				
#PCS-MDP-SFS-22	CCF Failure PCS MDP Fail to Start Group Size Of 2, Alpha Factor 2				

Table 10-43. Common Cause Alpha And Beta Factor Variables (Reference 10.46) (cont.)

Variable Name	Description	Value	α	β	Variance
#PMS-RTB-FOP-82	CCF Failure PMS RTB Fail to Operate Group Size Of 8, Alpha Factor 2				
#PMS-RTB-FOP-83	CCF Failure PMS RTB Fail to Operate Group Size Of 8, Alpha Factor 3				
#PMS-RTB-FOP-88	CCF Failure PMS RTB Fail to Operate Group Size Of 8, Alpha Factor 8				
#RNS-CKV-FTO-22	CCF Failure RNS CKV Fail to Open Group Size Of 2, Alpha Factor 2				
#RNS-MDP-SF1-22	CCF Failure RNS MDP Fail to Start And Run 1 Hour Group Size Of 2, Alpha Factor 2				
#RNS-MDP-SFR-22	CCF Failure RNS MDP Fail to Run Group Size Of 2, Alpha Factor 2				
#RNS-MDP-SFS-22	CCF Failure RNS MDP Fail to Start Group Size Of 2, Alpha Factor 2				
#RNS-MOV-FTO-22	CCF Failure RNS MOV Fail to Open Group Size Of 2, Alpha Factor 2				
#SGS-PRV-FRC-22	CCF Failure SGS PRV Fail to Remain Closed Group Size Of 2, Alpha Factor 2				
#SGS-PRV-FTC-22	CCF Failure SGS PRV Fail to Close Group Size Of 2, Alpha Factor 2				
#SGS-PRV-FTO-22	CCF Failure SGS PRV Fail to Open Group Size Of 2, Alpha Factor 2				
#SGS-PRV-SOX-22	CCF Failure SGS PRV Spurious Operation Group Size Of 2, Alpha Factor 2				
#SGS-SVV-FRC-122	CCF Failure SGS SVV Fail to Remain Closed Group Size Of 12, Alpha Factor 2				

Table 10-43. Common Cause Alpha And Beta Factor Variables (Reference 10.46) (cont.)

Variable Name	Description	Value	α	β	Variance
#SGS-SVV-FRC-123	CCF Failure SGS SVV Fail to Remain Closed Group Size Of 12, Alpha Factor 3				
#SGS-SVV-FRC-1212	CCF Failure SGS SVV Fail to Remain Closed Group Size Of 12, Alpha Factor 12				
#SGS-SVV-FTO-122	CCF Failure SGS SVV Fail to Open Group Size Of 12, Alpha Factor 2				
#SGS-SVV-FTO-123	CCF Failure SGS SVV Fail to Open Group Size Of 12, Alpha Factor 3				
#SGS-SVV-FTO-1212	CCF Failure SGS SVV Fail to Open Group Size Of 12, Alpha Factor 12				
#SGS-SVV-FTO-62	CCF Failure SGS SVV Fail to Open Group Size Of 6, Alpha Factor 2				
#SGS-SVV-FTO-63	CCF Failure SGS SVV Fail to Open Group Size Of 6, Alpha Factor 3				
#SGS-SVV-FTO-66	CCF Failure SGS SVV Fail to Open Group Size Of 6, Alpha Factor 6				
#SWS-MDP-RFR-22	CCF Failure SWS MDP Fail to Run Group Size Of 2, Alpha Factor 2				
#SWS-MDP-RFS-22	CCF Failure SWS MDP Fail to Start Group Size Of 2, Alpha Factor 2				
#SWS-MOV-FTO-22	CCF Failure SWS MOV Fail to Open Group Size Of 2, Alpha Factor 2				
#SWS-STR-PLG-22	CCF Failure SWS STR Plugging Group Size Of 2, Alpha Factor 2				
#ZOS-EDG-SLR-22	CCF Failure ZOS EDG (Standby) Fail to Run After First Hour of Operation Group Size Of 2, Alpha Factor 2				

Table 10-43. Common Cause Alpha And Beta Factor Variables (Reference 10.46) (cont.)

Variable Name	Description	Value	α	β	Variance
#ZOS-EDG-SFR-22	CCF Failure ZOS EDG (Standby) Fail to Start Group Size Of 2, Alpha Factor 2				
#ZOS-EDG-SFS-22	CCF Failure ZOS EDG (Standby) Fail to Load and Run During First Hour of Operation Group Size Of 2, Alpha Factor 2				
#ZRS-BKF-FTC-22	CCF Failure ZRS BKF Fail to Close Group Size Of 2, Alpha Factor 2				
#ZRS-BKF-FTO-22	CCF Failure ZRS BKF Fail to Open Group Size Of 2, Alpha Factor 2				
#ZRS-BKF-SOX-22	CCF Failure ZRS BKF Spurious Operation Group Size Of 2, Alpha Factor 2				
#ZRS-BKS-SOX-22	CCF Failure ZRS BKS Spurious Operation Group Size Of 2, Alpha Factor 2				
$VLS-ALL-CCF-B[1]	CCF Failure VLS All Fail to Operate, Beta Factor				

Note:
1. Refer to Section 10.5.6.4

Table 10-44. C&I Component Beta Factors

CCF Beta Factor Variable	CCF Beta Factor Value	CCF Beta Factor Variance	Description
$DAS-MSW-FTC-B			CCF FAILURE DAS MSW FAIL TO OPERATE, BETA FACTOR
$DAS-RLY-FOP-B			CCF FAILURE DAS RLY FAIL TO OPERATE, BETA FACTOR
$PLS-AIM-FOP-B			CCF FAILURE PLS AIM FAIL TO OPERATE, BETA FACTOR
$PLS-AOM-FOP-B			CCF FAILURE PLS AOM FAIL TO OPERATE, BETA FACTOR
$PLS-CPS-FOP-B			CCF FAILURE PLS CPS FAIL TO OPERATE, BETA FACTOR
$PLS-CTI-FOP-B			CCF FAILURE PLS CTI FAIL TO OPERATE, BETA FACTOR
$PLS-DIM-FOP-B			CCF FAILURE PLS DIM FAIL TO OPERATE, BETA FACTOR
$PLS-DOM-FOP-B			CCF FAILURE PLS DOM FAIL TO OPERATE, BETA FACTOR
$PLS-IOC-FOP-B			CCF FAILURE PLS IOC FAIL TO OPERATE, BETA FACTOR
$PLS-MAU-FOP-B			CCF FAILURE PLS MAU FAIL TO OPERATE, BETA FACTOR
$PLS-PDM-FOP-B			CCF FAILURE PLS PDM FAIL TO OPERATE, BETA FACTOR
$PLS-PFB-FOP-B			CCF FAILURE PLS PFB FAIL TO OPERATE, BETA FACTOR
$PLS-PRM-FOP-B			CCF FAILURE PLS PRM FAIL TO OPERATE, BETA FACTOR
$PLS-PSA-FOP-B			CCF FAILURE PLS PSA FAIL TO OPERATE, BETA FACTOR
$PLS-PWF-FOP-B			CCF FAILURE PLS PWF FAIL TO OPERATE, BETA FACTOR
$PLS-RNC-FOP-B			CCF FAILURE PLS RNC FAIL TO OPERATE, BETA FACTOR
$PLS-ROM-FOP-B			CCF FAILURE PLS ROM FAIL TO OPERATE, BETA FACTOR
$PLS-RTD-FOP-B			CCF FAILURE PLS RTD FAIL TO OPERATE, BETA FACTOR
$PLS-WST-FOP-B			CCF FAILURE PLS WST FAIL TO OPERATE, BETA FACTOR
$PMS-ABD-SIE-B			CCF FAILURE PMS ADS BLOCKING DEVICE SPURIOUS OPERATION, BETA FACTOR
$PMS-AI1-FOP-B			CCF FAILURE PMS AI1 FAIL TO OPERATE, BETA FACTOR
$PMS-AI2-FOP-B			CCF FAILURE PMS AI2 FAIL TO OPERATE, BETA FACTOR
$PMS-CIM-FOP-B			CCF FAILURE PMS CIM FAIL TO OPERATE, BETA FACTOR

Table 10-44. C&I Component Beta Factors (cont.)

CCF Beta Factor Variable	CCF Beta Factor Value	CCF Beta Factor Variance	Description
$PMS-COM-FOP-B			CCF FAILURE PMS COM FAIL TO OPERATE, BETA FACTOR
$PMS-CTI-FOP-B			CCF FAILURE PMS CTI FAIL TO OPERATE, BETA FACTOR
$PMS-DIM-FOP-B			CCF FAILURE PMS DIM FAIL TO OPERATE, BETA FACTOR
$PMS-DO1-FOP-B			CCF FAILURE PMS DO1 FAIL TO OPERATE, BETA FACTOR
$PMS-DO2-FOP-B			CCF FAILURE PMS DO2 FAIL TO OPERATE, BETA FACTOR
$PMS-HSL-FOP-B			CCF FAILURE PMS ISB FAIL TO OPERATE, BETA FACTOR
$PMS-ISB-FOP-B			CCF FAILURE PMS HSL FAIL TO OPERATE, BETA FACTOR
$PMS-MSW-FTC-B			CCF FAILURE PMS MSW FAIL TO OPERATE, BETA FACTOR
$PMS-PRM-FOP-B			CCF FAILURE PMS PRM FAIL TO OPERATE, BETA FACTOR
$PMS-PS1-FOP-B			CCF FAILURE PMS PS1 FAIL TO OPERATE, BETA FACTOR
$PMS-PS2-FOP-B			CCF FAILURE PMS PS2 FAIL TO OPERATE, BETA FACTOR
$PMS-PWF-FOP-B			CCF FAILURE PMS PWF FAIL TO OPERATE, BETA FACTOR
$PMS-RCT-FOP-B			CCF FAILURE PMS RCT FAIL TO OPERATE, BETA FACTOR
$PMS-RNC-FOP-B			CCF FAILURE PMS RNC FAIL TO OPERATE, BETA FACTOR
$PMS-RST-FOP-B			CCF FAILURE PMS RST FAIL TO OPERATE, BETA FACTOR
$PMS-RUV-FOP-B			CCF FAILURE PMS RUV FAIL TO OPERATE, BETA FACTOR
$PMS-SRD-FOP-B			CCF FAILURE PMS SRD FAIL TO OPERATE, BETA FACTOR
$PMS-SRN-FOP-B			CCF FAILURE PMS SRN FAIL TO OPERATE, BETA FACTOR
$PMS-STU-FOP-B			CCF FAILURE PMS STU FAIL TO OPERATE, BETA FACTOR

Table 10-45. Unique C&I Common Cause Variables

Type Code	Description	Value	α	β	Variance
$GEN-SOF-FOP-MM	Software Common Cause Failure (PMS and PLS)				
$GEN-SOF-FOP-IE	Software Common Cause Failure Results in Spurious IE (PMS)				
$GEN-HWY-FOP-LM	Common Cause Failure of Ovation Data Network (PLS)				

Table 10-46. Loss of Long Term Cooling Common Cause Variables

Type Code	Description	Value	Variance
PXS-SSC-LLI	Loss of Long Term Core Cooling – LLOCA		
PXS-SSC-MLI	Loss of Long Term Core Cooling – MLOCA		
PXS-SSC-SLI	Loss of Long Term Core Cooling – SLOCA		
PXS-SSC-TRN	Loss of Long Term Core Cooling – Transient		

Table 10-47. PDS Naming Convention

RCS Pressure/Condition	Hydrogen Generation	Water Availability
H (high)	N (no ADS actuation)	F (reflood failure)
L (low)	1 (ADS sparging into IRWST)	I (injection failure)
A (ATWS)	2 (ADS sparging into IRWST and discharging into containment)	R (recirculation failure)
BL (large bypass)	C (ADS discharge into containment)	
BS (small bypass)		

Table 10-48. High Pressure Recovery Event Tree Definitions

Associated PDSs	Recovery Event Tree	Recoveries Applied
H1 H1F	HP-1	ADS Stage 4 IRWST Recirculation
H1I	HP-H1I	ADS Stage 4 IRWST Recirculation
H1R	HP-H1R	ADS Stage 4 Recirculation
H2I	HP-H2I	IRWST Recirculation
H2R HCR	HP-H2CR	Recirculation
HCI	HP-HCI	IRWST Recirculation
HNI(1)	HP-HNI	ADS Stages 2-3 ADS Stage 4
AN ANF HN HNF	HP-N	ADS Stages 2-3 ADS Stage 4 IRWST Recirculation

Note:

1. This PDS has no recovery of IRWST because the initiator is spurious IRWST. In this instance, the IRWST is not recoverable.

Table 10-49. Low Pressure Recovery Event Tree Definitions

Associated PDSs	Recovery Event Tree	Recoveries Applied
L1I	LP-LI1	ADS Stage 4 IRWST Recirculation
L1R	LP-L1R	ADS Stage 4 Recirculation
L2I	LP-L2I	IRWST Recirculation
L2R	LP-L2R	Recirculation
LC LCF LCI	LP-LC	ADS Stages 2-3 IRWST Recirculation
LCR	LP-LCR	ADS Stages 2-3 Recirculation
LN LNF LNI	LP-N	ADS Stages 2-3 ADS Stage 4 IRWST Recirculation

Table 10-50. List of Screened Out Buildings from the Internal Flooding Analysis

Building	Reason
SWS Cooling Towers	These towers are isolated structures in an open area
Plant Entrance	The entrance is an isolated structure in an open area which is not expected to host critical equipment and flood sources
Circulating Water Pump Intake Structure	Any flood scenario that can occur is only expected to impact CWS given the fact that the Circulating Water Pump Intake Structure is a completely separate structure
CWS Cooling Tower	This tower is a completely separate structure; any flood scenario is only expected to impact the Circulating Water System and no other equipment is affected
CWS Intake Canal	Any flood scenario that can occur is only expected to impact CWS given the fact that the Circulating Water Pump Intake Structure is a completely separated structure. No other equipment is affected
Fire Water & Clearwell Storage Tank	It is a carbon steel tank located in an open area at the north end of the Turbine Building and is only analysed as a potential flood source
Fire Water Storage Tank	It is a carbon steel tank located in an open area at the northwest end of the Turbine Building and is only analysed as a potential flood source
Transformer Area	It is an isolated structure in an open area immediately adjacent to and north of the Turbine Building which is not expected to host flood sources
Switchyard	It is an isolated structure in an open area which is not expected to host flood sources
Condensate Storage Tank	This structure is only considered in the analysis as a potential flood source
Diesel Generator Fuel Oil Storage Tanks	This structure is located in the yard area and has mitigative features to prevent the outflow of oil to the outside, it can be screened out from the analysis
Demineralized Water Storage Tank	This structure is only considered in the analysis as a potential flood source
Boric Acid Storage Tank	This tank is a free-standing stainless steel cylindrical design, located adjacent to the Annex Building and to the Demineralized Water Storage Tank in an open area This structure is only considered in the analysis as a potential flood source
PGS Bulk Gas Storage Area	This structure is situated in the yard areas and is screened from the internal flooding

Table 10-50. List of Screened Out Buildings from the Internal Flooding Analysis (cont.)

Building	Reason
Turbine Building Laydown Area	This structure is outside the Turbine Building boundary. There is neither vulnerable equipment nor flood sources located in this open structure and it is screened from the internal flooding
Circulating Water Pipe	This Circulating Water piping inside the Turbine Building is only considered in the analysis as a potential flood source
Waste Water Retention Basin	This structure is only considered in the analysis as a potential flood source
Passive Containment Cooling Ancillary Water Storage Tank	This cylindrical steel tank is located at ground level in an open area at the west side of the Auxiliary Building. This structure is only considered in the analysis as a potential flood source
Diesel-driven Fire Pump & Enclosure	The diesel pump enclosure is located in the yard and, therefore, it is screened out from the internal flooding analysis

Table 10-51. List of Fluid Systems Included in the Internal Flooding Analysis

System	Description	Spray	Flood	Major Flood	HELB
Auxiliary Steam Supply	A line break in the steam portion of the ASS is expected to result in a steam release in the Turbine Building, which can impact other PSA equipment and induce administrative shutdown				X
Steam Generator Blowdown	Loss of BDS due to a pipe break would not result in a direct plant shutdown, and indirect flood or major flood concerns are not likely due to the limited capacity of the system	X			
Component Cooling Water	A line break in the CCS system has the potential for inducing a plant shutdown	X	X	X	
Condensate	A line break in the CDS system has the potential for inducing a plant shutdown	X	X	X	
Chemical and Volume Control	A break of the CVS piping system will likely cause a reactor trip since CVS is directly connected to the RCS; however, the flowrate is small enough to screen out a major flooding risk	X	X		X
Circulating Water	Circulating Water piping located inside the Turbine Building cannot be screened out. A pressure boundary failure of this piping would have a significant impact on other PSA equipment located inside the Turbine Building.	X	X	X	
Demineralized Water Treatment	The influent to the DTS for treatment is pumped from the RWS which operates at ambient temperature and pressure. Thus, the HELB risk of the DTS is not a concern. The major flood risk is not considered due to the maximum flowrate being low and, therefore, only the flood and the spray risk should be evaluated.	X	X		
Demineralized Water Transfer	Given the tank's size and flowrate, flood and spray risks are a concern. The tank temperature is monitored; therefore, the DWS does not pose a HELB threat. From the information contained in Table 3-1 of the system SSD, the major flood is not considered credible.	X	X		
Fire Protection	HELB is not considered as a credible risk for the FPS, as its operating temperature is below the cutoff criteria.	X	X	X	
Main and Startup Feedwater	A loss of MFW will cause a reactor trip and degrade the mitigating capability. Due to the FWS header design pressure and temperature the HELB is a risk to be evaluated for FWS.	X	X	X	X

Table 10-51. List of Fluid Systems Included in the Internal Flooding Analysis (cont.)

System	Description	Spray	Flood	Major Flood	HELB
Gland Seal	A loss of GSS is likely to cause a reactor trip due to degraded turbine performance	X	X		X
Heater Drain	The HDS does not perform or support any Category-A function, any other licensing-related function or any defence-in-depth function; however, HDS major equipment is located in Turbine Building where plant trip and mitigative equipment are located	X	X	X	X
Hydrogen Seal Oil	Given the location of HSS equipment and piping in the Turbine Building, it will only affect the turbine generator, and it has a limited inventory in comparison to the large area present in the Turbine Building. The risk of oil spray needs to be evaluated.	X			
Main Steam	The MSS does not perform any Category-A functions or mitigative functions. However a loss of MSS will cause a reactor trip	X	X	X	X
Main Turbine	The MTS performs energy conversion and steam flow control, and a loss of MTS will cause a reactor trip.	X	X	X	X
Primary Sampling	Since sampling activities are not performed continuously and only with manual operation of isolation valves, limited spray effects can be envisioned as a result of line/component leakage during sampling procedures. HELB is considered as a risk due to the number of other HELB defined systems that the PSS interfaces with to provide samples for analysis. The flood and major flood risk is not included due to the limited size of the piping that exists within this system.	X			X
Potable Water	Flood, major flood and HELB risks are not a concern due to the operating flow, temperature, and pressure. The PWS system will only be evaluated in risk significant flood areas were the spray impact on the equipment would lead to a plant IE.	X			
Spent Fuel Pool Cooling	Based on its pressure, temperature, and flowrate parameters, the SFS is retained for spray, flood, and major flood risk evaluation. The HELB risk is screened out.	X	X	X	
Steam Generator	A loss of SGS will cause a reactor trip and degrade accident mitigation.	X	X	X	X

Table 10-51. List of Fluid Systems Included in the Internal Flooding Analysis (cont.)

System	Description	Spray	Flood	Major Flood	HELB
Service Water	SWS does not perform or support any Category-A function or any other licensing-related functions. However, the SWS supplies cooling water for the CCS heat exchangers to support the defence-in-depth functions of the CCS. Loss of SWS will cause a reactor trip and degrade mitigating capability.	X	X	X	
Turbine Building Closed Cooling Water	The TCS does not perform or support any Category-A function or any other licensing-related functions. However, the TCS does support normal power generation and non-Class 1 mitigation system. A loss of TCS will cause a reactor trip and degrade mitigative functions.	X	X	X	
Central Chilled Water	The VWS provides cooling, directly and indirectly, to MCR and various Turbine Building rooms. A loss of VWS will not directly cause a reactor trip. However, with a potential temperature increase in MCR, Class 1 equipment rooms and Turbine Building electrical equipment rooms, a manual shutdown is likely for prolonged loss of VWS.	X	X	X	
Hot Water Heating	VYS supplies heated water to selected non-Class 1 AHUs. The loss of VYS will not cause a reactor trip or degrade mitigating functions.	X	X		
Liquid Radwaste	The WLS flood and major flood risks are screened out based on the maximum flowrate of the system.	X			

Table 10-52. List of Screened Out Fluid Systems From the Internal Flooding Analysis

System	Reason
Compressed and Instrument Air	The CAS only includes air filled lines (CAS SSD). Any condensate liquid from the CAS is expected to be of limited capacity and is not considered a credible flood or spray source.
Condenser Tube Cleaning	The CES is not considered as a fluid system, as its function consists in injecting cleaning balls into the condenser tubes, and by itself the system does not contain its own inventory
Turbine Island Chemical Feed	The CFS is not considered risk due to the lines being sufficiently small, the relative low flowrate of the system, and the small system inventory for each chemical used.
Condenser Air Removal	The CMS is not considered a risk due to the limited water inventory and the system is at a low pressure and temperature
Containment	The CNS is screened out from the analysis due to the fact that any fluid system covered within this system is already explicitly considered
Condensate Polishing	The CPS is screened out from the internal flooding analysis as it is not used above 33% plant power level nor does it support any Category-A function, any licensing-related functions or any defence-in-depth function
Standby Diesel and Auxiliary Boiler Fuel Oil	The system components are to be located outdoors in the yard area and inside the Diesel Generator Building of the plant facility which is located on a separate foundation at a distance from the Nuclear Island structures
Storm Drain	DRS is a passive system which is not normally intended to contain fluid inventory
Generator Hydrogen and CO_2	Since the operating fluids of HCS are hydrogen and carbon dioxide, there is no risk of flood, spray or HELB effects in this system
Main Turbine and Generator Lube Oil	According to Section 1.4.1 of the EPRI guidelines any pressure boundary failure is excluded and should be addressed in an internal fire PSA
Passive Containment Cooling	The PCCWST is normally isolated from its makeup sources, precluding any flooding as PCS piping located in the Auxiliary Building does not normally contain water
Plant Gas	This is not a fluid system that could cause a plant trip through one of the common modes of internal flooding failure
Passive Core Cooling	There is no flooding risk from a PXS pressure boundary break in the unscreened flood areas, and the system can be screened out from the internal flooding analyses
Gravity and Roof Drain Collection	The RDS is a passive system, not normally intended to contain fluid inventory
Normal Residual Heat Removal	The RNS is a normal standby non-Class 1 system. A pressure boundary failure will not cause a system actuation.

Table 10-52. List of Screened Out Fluid Systems From the Internal Flooding Analysis (cont.)

System	Reason
Raw Water	There is no RWS piping inside any building of the plant
Sanitary Drainage	Flood, major flood, and HELB risks are not a concern due to the operating flow, temperature, and pressure. The SDS spray risk is screened out based on the fact spray effects can affect no more than one system.
Secondary Sampling	The SSS does not perform or support any Category-A function, any other licensing-related functions or any defence-in-depth function. The SSS has a limited system inventory.
Turbine Island Vents, Drains and Relief	As TDS is used for venting, drainage, and high energy fluid relieving when needed, it is not considered to normally have water inventory in its piping.
Containment Leak Rate Test	The VUS performs containment isolation as a Category-A function. Containment isolation valves and the portion of piping that maintains the integrity of the containment pressure boundary are discussed in individual systems.
Gaseous Radwaste	The WGS operates with a gaseous fluid, so there is no flood risk to be concerned with.
Radioactive Waste Drain	WRS is not considered to normally have water inventory in its piping, and, therefore, it can be screened out as a potential flood source from the internal flooding analysis.
Solid Radwaste	The WSS in general does not handle fluid.
Waste Water	WWS performs drainage functions and is not considered to have normally water inventory in its piping.
Yard Fire Water	Based on the intended function of the system, yard fire control, the system equipment and piping are located outside areas where reactor trip or mitigating equipment is housed.

Table 10-53. Internal Flood Source List

PPP	System Description
ASS	Auxiliary Steam Supply System
BDS	Steam Generator Blowdown System
CCS	Component Cooling Water System
CDS	Condensate System
CVS	Chemical and Volume Control System
CWS	Circulating Water System
DTS	Demineralized Water Treatment System
DWS	Demineralized Water Transfer and Storage System
FPS	Fire Protection System
FWS	Main and Startup Feedwater System
GSS	Gland Seal System
HDS	Heater Drain System
MSS	Main Steam System
MTS	Main Turbine System
PSS	Primary Sampling System
PWS	Potable Water System
SFS	Spent Fuel Pool Cooling System
SGS	Steam Generator System
SWS	Service Water System
TCS	Turbine Building Closed Cooling Water System
VWS	Central Chilled Water System
VYS	Hot Water Heating System
WLS	Liquid Radwaste System

Table 10-54. Fire Compartments Modeled by AP1000 Internal Fire Analysis

AP1000 Fire Compartment	Building	Fire Compartment Description	Fire Frequency	CDF	% Contribution to Fire CDF	Summary of Fire Scenario
0000AF01	Yard	Yard	[ ]	3.45E-08	5.09%	Full compartment burn
1100AF11105	Containment	Reactor Cavity	[ ]	2.98E-12	0.00%	Full compartment burn
1100AF11204	Containment	Vertical Access and Reactor Coolant Drain Tank	[ ]	2.59E-11	0.00%	Full compartment burn
1100AF11206	Containment	Accumulator Room A	[ ]	4.86E-12	0.00%	Full compartment burn
1100AF11207	Containment	Accumulator Room B	[ ]	5.12E-12	0.00%	Full compartment burn
1100AF11208	Containment	Normal Residual Heat Removal Valve Room	[ ]	3.51E-12	0.00%	Full compartment burn
1100AF11209	Containment	Chemical and Volume Control System Room	[ ]	3.35E-12	0.00%	Full compartment burn
1100AF11300A	Containment	Maintenance floor (southeast quadrant access)	[ ]	1.70E-09	0.25%	Detailed transient fire scenarios
1100AF11300B	Containment	Maintenance floor (north half)	[ ]	1.79E-08	2.64%	Detailed fixed and transient fire scenarios
1100AF11301	Containment	Steam Generator Compartment 1	[ ]	1.82E-08	2.68%	Full compartment burn
1100AF11302	Containment	Steam Generator Compartment 2	[ ]	1.22E-08	1.80%	Full compartment burn
1100AF11303	Containment	Pressuriser Compartment	[ ]	3.42E-10	0.05%	Full compartment burn
1100AF11303A	Containment	ADS Lower Valve Area	[ ]	2.78E-09	0.41%	Full compartment burn

Table 10-54. Fire Compartments Modeled by AP1000 Internal Fire Analysis (cont.)

AP1000 Fire Compartment	Building	Fire Compartment Description	Fire Frequency	CDF	% Contribution to Fire CDF	Summary of Fire Scenario
1100AF11303B	Containment	ADS Upper Valve Area	[ ]	2.48E-09	0.37%	Full compartment burn
1100AF11500	Containment	Refueling Cavity/Operating Deck	[ ]	1.72E-09	0.25%	Detailed fixed and transient fire scenarios
1200AF12241	Containment	Lower annulus east/southeast	[ ]	9.61E-12	0.00%	Full compartment burn
1200AF12341	Containment	Middle annulus	[ ]	3.61E-11	0.01%	Full compartment burn
1200AF12461	Auxiliary Building	Corridor	[ ]	1.23E-11	0.00%	Full compartment burn
1200AF12541	Containment	Upper annulus	[ ]	1.32E-12	0.00%	Full compartment burn
1200AF12562	Auxiliary Building	Cask Loading/Fuel Handling/SFP	[ ]	4.37E-11	0.01%	Full compartment burn
1201AF01	Auxiliary Building	Stairwell-Northwest portion of Aux Bldg	[ ]	5.11E-12	0.00%	Full compartment burn
1201AF06	Auxiliary Building	Lower & Upper Main Steam Isolation Valve Compartment	[ ]	3.09E-08	4.57%	Full compartment burn

Table 10-54. Fire Compartments Modeled by AP1000 Internal Fire Analysis (cont.)

AP1000 Fire Compartment	Building	Fire Compartment Description	Fire Frequency	CDF	% Contribution to Fire CDF	Summary of Fire Scenario
1202AF01	Auxiliary Building	Stairwell- Northeast portion of Aux Bldg	[ ]	5.11E-12	0.00%	Full compartment burn
1202AF02	Auxiliary Building	Elevator Shaft- North Side Aux Bldg	[ ]	3.39E-11	0.01%	Full compartment burn
1202AF05	Auxiliary Building	Stairwell- Emergency egress path from MCR	[ ]	5.11E-12	0.00%	Full compartment burn
1204AF01	Auxiliary Building	Normal Residual Heat Removal Pump Room B	[ ]	9.49E-12	0.00%	Full compartment burn
1204AF02	Auxiliary Building	Stairwell- Shield Building	[ ]	3.37E-11	0.00%	Full compartment burn
1204AF03	Auxiliary Building	Elevator Shaft- South Side Shield Building	[ ]	6.36E-11	0.01%	Full compartment burn
1205AF01	Auxiliary Building	Stairwell- Southeast portion of the Aux Bldg	[ ]	5.11E-12	0.00%	Full compartment burn
1205AF02	Auxiliary Building	Elevator Shaft- Radiologically Controlled Area	[ ]	3.31E-11	0.00%	Full compartment burn
1205AF12362	Auxiliary Building	Normal Residual Heat Removal HX Room	[ ]	9.52E-12	0.00%	Full compartment burn
1205AF12365	Auxiliary Building	Waste Monitor Tank Room B	[ ]	1.21E-11	0.00%	Full compartment burn

Table 10-54. Fire Compartments Modeled by AP1000 Internal Fire Analysis (cont.)

AP1000 Fire Compartment	Building	Fire Compartment Description	Fire Frequency	CDF	% Contribution to Fire CDF	Summary of Fire Scenario
1210AF12111	Auxiliary Building	Corridor	[ ]	2.01E-10	0.03%	Full compartment burn
1210AF12151	Auxiliary Building	Demineralizer/Degasifier Column/Radwaste	[ ]	6.20E-10	0.09%	Full compartment burn
1210AF12171	Auxiliary Building	Effluent Holdup Tank Room A	[ ]	1.03E-11	0.00%	Full compartment burn
1211AF12104	Auxiliary Building	Division B Battery Room 1	[ ]	1.11E-09	0.16%	Full compartment burn
1211AF12105	Auxiliary Building	Division D Battery Room	[ ]	6.47E-10	0.10%	Detailed fixed fire scenarios
1212AF12101	Auxiliary Building	Division A Battery Room	[ ]	4.96E-10	0.07%	Full compartment burn
1212AF12102	Auxiliary Building	Division C Battery Room 1	[ ]	5.39E-10	0.08%	Detailed fixed fire scenarios
1212AF12103	Auxiliary Building	Spare Battery Room	[ ]	3.01E-11	0.00%	Full compartment burn
1212AF12112	Auxiliary Building	Spare Room	[ ]	1.36E-11	0.00%	Full compartment burn
1212AF12113	Auxiliary Building	Spare Battery Charger Room	[ ]	1.37E-11	0.00%	Full compartment burn

Table 10-54. Fire Compartments Modeled by AP1000 Internal Fire Analysis (cont.)

AP1000 Fire Compartment	Building	Fire Compartment Description	Fire Frequency	CDF	% Contribution to Fire CDF	Summary of Fire Scenario
1214AF12152	Auxiliary Building	Primary Sample Room	[ ]	5.46E-11	0.01%	Full compartment burn
1214AF12154	Auxiliary Building	Auxiliary Building Sump Room	[ ]	7.94E-12	0.00%	Full compartment burn
1214AF12354	Auxiliary Building	Mid-annulus Access Room	[ ]	9.57E-12	0.00%	Full compartment burn
1215AF12161	Auxiliary Building	Corridor	[ ]	2.06E-11	0.00%	Full compartment burn
1215AF12162	Auxiliary Building	Normal Residual Heat Removal Pump Room A	[ ]	1.19E-11	0.00%	Full compartment burn
1216AF12166	Auxiliary Building	Waste Holdup Tank Room A	[ ]	9.05E-12	0.00%	Full compartment burn
1216AF12167	Auxiliary Building	Waste Holdup Tank Room B	[ ]	9.23E-12	0.00%	Full compartment burn
1216AF12169	Auxiliary Building	Corridor/Liquid Radwaste Pump Room	[ ]	1.02E-10	0.02%	Full compartment burn
1216AF12172	Auxiliary Building	Effluent Holdup Tank Room B	[ ]	1.05E-11	0.00%	Full compartment burn
1216AF12264	Auxiliary Building	Waste Monitor Tank Room C	[ ]	1.21E-11	0.00%	Full compartment burn

Table 10-54. Fire Compartments Modeled by AP1000 Internal Fire Analysis (cont.)

AP1000 Fire Compartment	Building	Fire Compartment Description	Fire Frequency	CDF	% Contribution to Fire CDF	Summary of Fire Scenario
1220AF02	Auxiliary Building	Lower annulus Valve Area	[ ]	8.67E-11	0.01%	Full compartment burn
1220AF12211	Auxiliary Building	Corridor	[ ]	2.63E-10	0.04%	Detailed fixed and transient fire scenarios
1220AF12251	Auxiliary Building	Demineralizer/CVS Makeup Pump Room	[ ]	3.33E-11	0.00%	Full compartment burn
1220AF12256	Auxiliary Building	Containment Isolation Valve Area/Pipe Chase	[ ]	9.14E-12	0.00%	Full compartment burn
1220AF12259	Auxiliary Building	Pipe chase	[ ]	9.24E-12	0.00%	Full compartment burn
1220AF12269	Auxiliary Building	Pipe chase	[ ]	8.88E-12	0.00%	Full compartment burn
1220AF12272	Auxiliary Building	Spent fuel pool System Rooms	[ ]	1.51E-11	0.00%	Full compartment burn
1221AF12204	Auxiliary Building	Division B Battery Room 2	[ ]	1.77E-09	0.26%	Full compartment burn
1221AF12205	Auxiliary Building	Division D DC Equipment Room	[ ]	2.39E-10	0.04%	Detailed fixed fire scenarios
1222AF12201	Auxiliary Building	Division A DC Equipment Room	[ ]	3.53E-10	0.05%	Full compartment burn

Table 10-54. Fire Compartments Modeled by AP1000 Internal Fire Analysis (cont.)

AP1000 Fire Compartment	Building	Fire Compartment Description	Fire Frequency	CDF	% Contribution to Fire CDF	Summary of Fire Scenario
1222AF12202	Auxiliary Building	Division C Battery Room 2	[ ]	3.11E-10	0.05%	Detailed fixed fire scenarios
1222AF12203	Auxiliary Building	Division C DC Equipment Room	[ ]	1.36E-08	2.01%	Detailed fixed fire scenarios
1222AF12207	Auxiliary Building	Division B DC Equipment Room	[ ]	8.64E-09	1.28%	Full compartment burn
1222AF12212	Auxiliary Building	Division B RCP Trip Switchgear Room	[ ]	5.69E-09	0.84%	Full compartment burn
1222AF12213	Auxiliary Building	Spare Room	[ ]	1.16E-09	0.17%	Full compartment burn
1224AF12252	Auxiliary Building	Radiation Chemistry Laboratory	[ ]	1.24E-11	0.00%	Full compartment burn
1225AF12261	Auxiliary Building	Corridor	[ ]	1.11E-10	0.02%	Full compartment burn
1225AF12262	Auxiliary Building	Piping/valve room	[ ]	9.15E-12	0.00%	Full compartment burn
1230AF01	Auxiliary Building	Corridor	[ ]	1.19E-11	0.00%	Full compartment burn
1230AF02	Auxiliary Building	Non-Class 1E Equipment/Penetration Room	[ ]	7.93E-09	1.17%	Full compartment burn

Table 10-54. Fire Compartments Modeled by AP1000 Internal Fire Analysis (cont.)

AP1000 Fire Compartment	Building	Fire Compartment Description	Fire Frequency	CDF	% Contribution to Fire CDF	Summary of Fire Scenario
1230AF12311	Auxiliary Building	Elevation 100'-0" Corridor	[ ]	9.45E-10	0.14%	Full compartment burn
1230AF12371	Auxiliary Building	Waste disposal container/filter storage area	[ ]	1.81E-11	0.00%	Full compartment burn
1231AF12304	Auxiliary Building	Division B I&C/Penetration Room	[ ]	2.58E-09	0.38%	Detailed fixed fire scenarios
1231AF12305	Auxiliary Building	Division D I&C/Penetration Room	[ ]	2.17E-09	0.32%	Detailed fixed and transient fire scenarios
1231AF12306	Auxiliary Building	Valve/Piping Penetration Room	[ ]	3.31E-10	0.05%	Full compartment burn
1231AF12344	Auxiliary Building	Mid Annulus Penetration Room Division B	[ ]	1.55E-10	0.02%	Full compartment burn
1231AF12345	Auxiliary Building	Division D Mid Annulus Penetration Room	[ ]	1.02E-10	0.02%	Full compartment burn
1232AF01	Auxiliary Building	Remote Shutdown Room	[ ]	6.37E-11	0.01%	Full compartment burn
1232AF12301	Auxiliary Building	Auxiliary Building –Division A I&C Room	[ ]	1.47E-10	0.02%	Detailed fixed and transient fire scenarios

Table 10-54. Fire Compartments Modeled by AP1000 Internal Fire Analysis (cont.)

AP1000 Fire Compartment	Building	Fire Compartment Description	Fire Frequency	CDF	% Contribution to Fire CDF	Summary of Fire Scenario
1232AF12302	Auxiliary Building	Division C I&C Room	[ ]	4.77E-10	0.07%	Detailed fixed and transient fire scenarios
1232AF12312	Auxiliary Building	Division C RCP Trip Switchgear Room	[ ]	1.96E-07	28.91%	Detailed fixed and transient fire scenarios
1232AF12313	Auxiliary Building	I&C/Division C Penetration Room	[ ]	1.11E-09	0.16%	Detailed fixed and transient fire scenarios
1232AF12343	Auxiliary Building	Mid Annulus Penetration Room Division C	[ ]	3.26E-10	0.05%	Full compartment burn
1234AF12351	Auxiliary Building	Auxiliary Building –Maintenance floor staging area	[ ]	3.65E-11	0.01%	Full compartment burn
1234AF12352	Auxiliary Building	Personnel Hatch	[ ]	1.52E-10	0.02%	Full compartment burn
1235AF12361	Auxiliary Building	Corridor	[ ]	6.15E-11	0.01%	Full compartment burn
1235AF12363	Auxiliary Building	Waste monitor Tank Room A	[ ]	1.16E-11	0.00%	Full compartment burn
1236AF12372	Auxiliary Building	Resin transfer pump/valve room	[ ]	8.93E-12	0.00%	Full compartment burn

Table 10-54. Fire Compartments Modeled by AP1000 Internal Fire Analysis (cont.)

AP1000 Fire Compartment	Building	Fire Compartment Description	Fire Frequency	CDF	% Contribution to Fire CDF	Summary of Fire Scenario
1236AF12373	Auxiliary Building	Spent resin tank room	[ ]	7.02E-12	0.00%	Full compartment burn
1240AF01	Auxiliary Building	Non-Class 1E Equipment/Penetration Room	[ ]	2.53E-08	3.74%	Full compartment burn
1241AF12405	Auxiliary Building	Lower NI Nonradioactive Ventilation Div B&D Room	[ ]	6.01E-10	0.09%	Full compartment burn
1241AF12506	Auxiliary Building	Main Steam Isolation Valve Compartment A	[ ]	4.29E-09	0.63%	Full compartment burn
1242AF01	Auxiliary Building	Main Control Area/Tagging Room/Vestibule/Shift	[ ]	3.61E-10	0.05%	Detailed fixed fire scenario analysis and review of abandonment and non-abandonment.
1242AF02	Auxiliary Building	Electrical Penetration Room Division A	[ ]	3.94E-09	0.58%	Full compartment burn
1242AF12411	Auxiliary Building	Elevation 117'-6" Corridor	[ ]	2.34E-10	0.03%	Full compartment burn
1243AF01	Auxiliary Building	Reactor Trip Switchgear 1	[ ]	1.15E-09	0.17%	Full compartment burn
1243AF02	Auxiliary Building	Reactor Trip Switchgear 2	[ ]	1.15E-09	0.17%	Full compartment burn

Table 10-54. Fire Compartments Modeled by AP1000 Internal Fire Analysis (cont.)

AP1000 Fire Compartment	Building	Fire Compartment Description	Fire Frequency	CDF	% Contribution to Fire CDF	Summary of Fire Scenario
1244AF12451	Auxiliary Building	Security Room	[ ]	1.09E-11	0.00%	Full compartment burn
1244AF12452	Auxiliary Building	Containment air filtration system penetration	[ ]	2.72E-09	0.40%	Full compartment burn
1244AF12454	Auxiliary Building	SFP/Containment Air Filtration/Sampling Penetration	[ ]	1.76E-10	0.03%	Full compartment burn
1246AF12471	Auxiliary Building	Solid waste system valve/piping area	[ ]	1.02E-11	0.00%	Full compartment burn
1250AF01	Containment	Nuclear Island Nonradioactive Ventilation System	[ ]	2.63E-10	0.04%	Detailed fixed fire scenarios
1250AF12555	Auxiliary Building	Operating Deck Staging Area	[ ]	7.54E-11	0.01%	Full compartment burn
1250AF12561	Auxiliary Building	CCS Valve Room	[ ]	1.22E-11	0.00%	Full compartment burn
1251AF12505	Auxiliary Building	Upper NI Nonradioactive Ventilation Division B&D Room	[ ]	2.03E-09	0.30%	Full compartment burn
1254AF12553	Auxiliary Building	Personnel Access Area	[ ]	5.03E-09	0.74%	Detailed fixed fire scenarios
1254AF12554	Auxiliary Building	Security Room	[ ]	7.56E-08	11.17%	Full compartment burn

Table 10-54. Fire Compartments Modeled by AP1000 Internal Fire Analysis (cont.)

AP1000 Fire Compartment	Building	Fire Compartment Description	Fire Frequency	CDF	% Contribution to Fire CDF	Summary of Fire Scenario
1264AF12651	Auxiliary Building	RCA Ventilation Equipment Room	[ ]	1.44E-09	0.21%	Full compartment burn
1270AF12701	Containment	Passive Containment Cooling Valve Room	[ ]	2.63E-12	0.00%	Full compartment burn
2000AF02	Turbine Building	Stairwell- Southwest	[ ]	4.52E-11	0.01%	Full compartment burn
2000AF03	Turbine Building	Stairwell S03- Northwest Turbine 158' to 196'	[ ]	2.68E-11	0.00%	Full compartment burn
2000AF15	Turbine Building	Stairwell- Northwest Turbine 100' to 150'-7"	[ ]	2.68E-11	0.00%	Full compartment burn
2009AF01	Turbine Building	Stairwell- Northeast	[ ]	2.68E-11	0.00%	Full compartment burn
2009AF02	Turbine Building	Elevator Shaft- 100' to 170'	[ ]	1.04E-10	0.02%	Full compartment burn
2030AF20300	Turbine Building	General Floor Area/Control System Cabinet Room	[ ]	4.61E-08	6.80%	Full compartment burn
2031AF21380	Turbine Building	CCS/BDS Equipment Room	[ ]	9.19E-10	0.14%	Full compartment burn
2038AF20300	Turbine Building	Main Feedwater Pump Area	[ ]	4.43E-11	0.01%	Full compartment burn

Table 10-54. Fire Compartments Modeled by AP1000 Internal Fire Analysis (cont.)

AP1000 Fire Compartment	Building	Fire Compartment Description	Fire Frequency	CDF	% Contribution to Fire CDF	Summary of Fire Scenario
2039AF20301	Turbine Building	Chemical storage Area	[ ]	1.32E-10	0.02%	Full compartment burn
2040AF01	Turbine Building	Lube oil storage Room	[ ]	4.85E-11	0.01%	Full compartment burn
2040AF20400	Turbine Building	Elevation 121'-6" General Floor Area	[ ]	1.34E-08	1.98%	Full compartment burn
2041AF21480	Turbine Building	VTS HVAC Equipment Room	[ ]	6.31E-09	0.93%	Full compartment burn
2043AF01	Turbine Building	Secondary Sampling Lab	[ ]	5.64E-10	0.08%	Full compartment burn
2050AF01	Turbine Building	Turbine Lube Oil Reservoir Room	[ ]	1.92E-09	0.28%	Full compartment burn
2050AF20500	Turbine Building	Elevation 141'-3" General Floor Area	[ ]	4.88E-09	0.72%	Full compartment burn except for ignition sources grouped with the 2050AF20500-Partial fire scenario

Table 10-54. Fire Compartments Modeled by AP1000 Internal Fire Analysis (cont.)

AP1000 Fire Compartment	Building	Fire Compartment Description	Fire Frequency	CDF	% Contribution to Fire CDF	Summary of Fire Scenario
2050AF20500 - Partial	Turbine Building	Elevation 141'-3" General Floor Area - Partial burn	[ ]	2.56E-08	3.79%	Full compartment burn except for ignition sources grouped with the 2050AF20500 fire scenario
2050AF20502	Turbine Building	Digital-electrohydraulic skid	[ ]	1.86E-10	0.03%	Full compartment burn
2051AF21583	Turbine Building	RCP switchgear	[ ]	6.99E-09	1.03%	Full compartment burn
2052AF01	Turbine Building	Switchgear Room 1	[ ]	2.64E-09	0.39%	Full compartment burn
2052AF20504	Turbine Building	HVAC Equipment Area	[ ]	3.77E-10	0.06%	Full compartment burn
2053AF01	Turbine Building	Electrical Equipment Room	[ ]	3.30E-09	0.49%	Full compartment burn
2053AF02	Turbine Building	Switchgear Room 2	[ ]	4.31E-09	0.64%	Full compartment burn
2057AF20503	Turbine Building	Generator seal oil unit	[ ]	1.64E-10	0.02%	Full compartment burn
2060AF20600	Turbine Building	Elevation 170'-0" General Floor Area	[ ]	3.76E-09	0.56%	Full compartment burn

Table 10-54. Fire Compartments Modeled by AP1000 Internal Fire Analysis (cont.)

AP1000 Fire Compartment	Building	Fire Compartment Description	Fire Frequency	CDF	% Contribution to Fire CDF	Summary of Fire Scenario
2063AF20601	Turbine Building	Tool room/storage area	[ ]	2.94E-11	0.00%	Full compartment burn
2063AF20602	Turbine Building	Office/Engineering workstation at Elevation 183'-1.	[ ]	2.93E-11	0.00%	Full compartment burn
2070AF20700	Turbine Building	Heater bay	[ ]	5.65E-11	0.01%	Full compartment burn
2070AF20750	Turbine Building	Upper Heater bay	[ ]	2.79E-11	0.00%	Full compartment burn
2151AF21580	Turbine Building	South bay elevation 135'-3" General Area	[ ]	2.10E-08	3.11%	Full compartment burn
2151AF21581	Turbine Building	Battery Room	[ ]	7.55E-11	0.01%	Full compartment burn
2151AF21582	Turbine Building	Battery Charger Room	[ ]	1.76E-10	0.03%	Full compartment burn
4001AF01	Annex Building	Stairwell S01 in Annex building between Turbine	[ ]	1.48E-11	0.00%	Full compartment burn
4001AF02	Annex Building	Elevator Shaft	[ ]	5.88E-10	0.09%	Full compartment burn
4002AF01	Annex Building	Stairwell S02- Annex Building near Yard	[ ]	1.48E-11	0.00%	Full compartment burn

Table 10-54. Fire Compartments Modeled by AP1000 Internal Fire Analysis (cont.)

AP1000 Fire Compartment	Building	Fire Compartment Description	Fire Frequency	CDF	% Contribution to Fire CDF	Summary of Fire Scenario
4002AF02	Annex Building	Stairwell S04- Annex Building near Yard	[ ]	8.50E-11	0.01%	Full compartment burn
4002AF03	Annex Building	Elevator Shaft near Yard	[ ]	3.63E-10	0.05%	Full compartment burn
4003AF02	Annex Building	Stairwell near Boric Acid Storage Tank	[ ]	1.48E-11	0.00%	Full compartment burn
4003AF40340	Annex Building	Demineralized water deoxygenating room	[ ]	2.60E-10	0.04%	Full compartment burn
4003AF40442	Annex Building	Boric Acid Batching Room	[ ]	2.75E-11	0.00%	Full compartment burn
4003AF40503	Annex Building	Lower south air handling equipment room	[ ]	2.53E-10	0.04%	Full compartment burn
4003AF40601	Annex Building	Upper south air handling equipment room	[ ]	6.49E-11	0.01%	Full compartment burn
4031AF06	Annex Building	Corridor/ Security Room	[ ]	2.79E-10	0.04%	Full compartment burn
4031AF40300	Annex Building	Access Corridor/Security Room	[ ]	1.99E-10	0.03%	Full compartment burn
4031AF40303	Annex Building	Corridor/Restroom	[ ]	6.70E-09	0.99%	Full compartment burn

Table 10-54. Fire Compartments Modeled by AP1000 Internal Fire Analysis (cont.)

AP1000 Fire Compartment	Building	Fire Compartment Description	Fire Frequency	CDF	% Contribution to Fire CDF	Summary of Fire Scenario
4031AF40307	Annex Building	Battery Room 1	[ ]	3.09E-10	0.05%	Full compartment burn
4031AF40308	Annex Building	Battery Charger Room 1	[ ]	5.24E-09	0.77%	Full compartment burn
4031AF40309	Annex Building	Battery Room 2	[ ]	3.85E-10	0.06%	Full compartment burn
4031AF40310	Annex Building	Battery Charger Room 2	[ ]	1.03E-08	1.52%	Full compartment burn
4031AF40411	Annex Building	Computer Room B	[ ]	2.87E-10	0.04%	Full compartment burn
4031AF40412	Annex Building	Battery Room	[ ]	4.38E-11	0.01%	Full compartment burn
4032AF01	Annex Building	Radiologically controlled area entry/exit	[ ]	3.19E-09	0.47%	Full compartment burn
4032AF02	Annex Building	Containment Access Corridor 107'-2"/ Radwaste	[ ]	4.29E-10	0.06%	Full compartment burn
4033AF01	Annex Building	Hot Machine Shop/Pump Seal Shop	[ ]	4.36E-11	0.01%	Full compartment burn
4034AF40311	Annex Building	Corridor	[ ]	1.60E-10	0.02%	Full compartment burn

Table 10-54. Fire Compartments Modeled by AP1000 Internal Fire Analysis (cont.)

AP1000 Fire Compartment	Building	Fire Compartment Description	Fire Frequency	CDF	% Contribution to Fire CDF	Summary of Fire Scenario
4034AF40313	Annex Building	Office/Engineering workstation at Elevation 183'-1"	[ ]	1.43E-11	0.00%	Full compartment burn
4034AF40316	Annex Building	Computer Room L1/2	[ ]	2.25E-11	0.00%	Full compartment burn
4034AF40317	Annex Building	Computer Room L3	[ ]	2.69E-11	0.00%	Full compartment burn
4034AF40318	Annex Building	ALARA briefing/HP Monitoring Room	[ ]	2.11E-11	0.00%	Full compartment burn
4034AF40320	Annex Building	Women's Change Room	[ ]	2.05E-11	0.00%	Full compartment burn
4034AF40322	Annex Building	Men's Change Room/Janitor Closet/Water Heater	[ ]	1.66E-11	0.00%	Full compartment burn
4034AF40370	Annex Building	Conference Room/Restroom	[ ]	2.49E-11	0.00%	Full compartment burn
4034AF40378	Annex Building	Office Area West	[ ]	1.47E-11	0.00%	Full compartment burn
4034AF40379	Annex Building	Office Area East	[ ]	1.51E-11	0.00%	Full compartment burn
4035AF01	Annex Building	Ancillary Diesel Generator Room	[ ]	5.42E-10	0.08%	Full compartment burn

Table 10-54. Fire Compartments Modeled by AP1000 Internal Fire Analysis (cont.)

AP1000 Fire Compartment	Building	Fire Compartment Description	Fire Frequency	CDF	% Contribution to Fire CDF	Summary of Fire Scenario
4041AF02	Annex Building	Corridor	[ ]	1.25E-09	0.18%	Full compartment burn
4041AF40403	Annex Building	Conference Room/Kitchen/NRC Room	[ ]	3.99E-11	0.01%	Full compartment burn
4041AF40410	Annex Building	Computer Room/Corridor	[ ]	2.23E-10	0.03%	Full compartment burn
4042AF01	Annex Building	Electrical Switchgear Room 1 including Electri	[ ]	1.27E-09	0.19%	Full compartment burn
4042AF02	Annex Building	Electrical Switchgear Room 2	[ ]	2.95E-09	0.44%	Full compartment burn
4051AF01	Annex Building	North air handling equipment Room/Air Intake	[ ]	4.00E-10	0.06%	Full compartment burn
4052AF40550	Annex Building	Staging and storage area	[ ]	3.39E-11	0.01%	Full compartment burn
4052AF40551	Annex Building	Containment air filtration exhaust room A	[ ]	6.08E-11	0.01%	Full compartment burn
4052AF40552	Annex Building	Containment air filtration exhaust room B	[ ]	2.47E-11	0.00%	Full compartment burn
5031AF50300	Radwaste Building	Electrical/mechanical equipment room	[ ]	3.97E-11	0.01%	Full compartment burn

Table 10-54. Fire Compartments Modeled by AP1000 Internal Fire Analysis (cont.)

AP1000 Fire Compartment	Building	Fire Compartment Description	Fire Frequency	CDF	% Contribution to Fire CDF	Summary of Fire Scenario
5031AF50350	Radwaste Building	Mobile systems facility	[ ]	9.07E-11	0.01%	Full compartment burn
5031AF50351	Radwaste Building	Waste accumulation room	[ ]	3.07E-10	0.05%	Full compartment burn
5031AF50353	Radwaste Building	HVAC Equipment Area	[ ]	3.18E-11	0.00%	Full compartment burn
5031AF50354	Radwaste Building	Truck staging area	[ ]	1.78E-11	0.00%	Full compartment burn
5031AF50355	Radwaste Building	Monitor tank room	[ ]	1.98E-11	0.00%	Full compartment burn
6001AF01	Diesel Generator Building	Stairwell S01	[ ]	1.48E-11	0.00%	Full compartment burn
6030AF03	Diesel Generator Building	Diesel Fuel Day Tank Vault A	[ ]	1.52E-11	0.00%	Full compartment burn
6030AF04	Diesel Generator Building	Diesel Fuel Day Tank Vault B	[ ]	1.56E-11	0.00%	Full compartment burn
6030AF60310	Diesel Generator Building	DG Room A	[ ]	2.19E-10	0.03%	Full compartment burn
6030AF60311	Diesel Generator Building	Service Module A	[ ]	6.17E-11	0.01%	Full compartment burn

Table 10-54. Fire Compartments Modeled by AP1000 Internal Fire Analysis (cont.)

AP1000 Fire Compartment	Building	Fire Compartment Description	Fire Frequency	CDF	% Contribution to Fire CDF	Summary of Fire Scenario
6030AF60313	Diesel Generator Building	Combustion Air Cleaner Area A	[ ]	2.27E-11	0.00%	Full compartment burn
6030AF60320	Diesel Generator Building	DG Room B	[ ]	2.11E-10	0.03%	Full compartment burn
6030AF60321	Diesel Generator Building	Service Module B	[ ]	5.60E-11	0.01%	Full compartment burn
6030AF60323	Diesel Generator Building	Combustion Air Cleaner Area B	[ ]	2.24E-11	0.00%	Full compartment burn
6030AF60324	Diesel Generator Building	Tool storage area	[ ]	1.44E-11	0.00%	Full compartment burn
6030AF60330	Diesel Generator Building	Security Room	[ ]	2.67E-11	0.00%	Full compartment burn
AnnexBldgRoof	Annex Building	Annex Building Roof	[ ]	3.39E-11	0.01%	Full compartment burn
AuxBldgRoof	Auxiliary Building	Auxiliary Building Roof	[ ]	5.56E-12	0.00%	Full compartment burn
DGBldgRoof	Diesel Generator Building	DG Building Roof	[ ]	2.06E-12	0.00%	Full compartment burn
DGMDP-01A	Yard	Diesel Fuel Oil Subsystem Train A	[ ]	2.03E-12	0.00%	Full compartment burn

Table 10-54. Fire Compartments Modeled by AP1000 Internal Fire Analysis (cont.)

AP1000 Fire Compartment	Building	Fire Compartment Description	Fire Frequency	CDF	% Contribution to Fire CDF	Summary of Fire Scenario
DGMDP-01B	Yard	Diesel Fuel Oil Subsystem Train B	[ ]	2.03E-12	0.00%	Full compartment burn
TurbBldgRoof	Turbine Building	Turbine Building Roof	[ ]	1.65E-10	0.02%	Full compartment burn
UNDRGRND	Yard	Underground cable tunnels	[ ]	4.08E-12	0.00%	Full compartment burn

Table 10-55. Internal Fire Sensitivity Studies

Case	CDF	ΔCDF (%)	LRF	ΔLRF (%)
Assumed routing equipment set to "screened"	5.46E-07	-19.4	[ ]	-2.9
All Severity Factors set to 1.0	7.46E-07	10.2	[ ]	8.2
Manual Detection Time = 5 minutes	6.52E-07	-3.7	[ ]	-3.2
Manual Detection Time = 25 minutes	6.77E-07	0.0	[ ]	0.0
All conditional failure probabilities removed and their corresponding basic event set instead to 1.0	1.17E-06	72.8	[ ]	43.8
HRRs updated per NUREG-2178 methodology(1)	6.02E-07	11.1	[ ]	10.4
Removing credit for automatic detection and suppression	8.27E-07	22.2	[ ]	5.9
Screening all Multi-Compartment Analysis scenarios	4.13E-07	-39.0	[ ]	-26.1

Note:
(1) The benefit of applying the two NUREG-2178 heat release rates is suppressed by the fact that many ignition sources go to full compartment burn or detailed sources have very small assumed distances to the nearest target.

Table 10-56: Review of Top Fire Compartments for CDF

Fire Compartment	Fire Compartment Description	CDF	% Contribution to CDF	Description of Risk Contributors
1232AF12312	Division C RCP Switchgear Room	1.96E-07	28.91%	The fire risk is primarily driven by a High Energy Arcing Fault (HEAF) or an electrical fire starting in one of the RCP switchgear cabinets. This fire compartment has many cable trays routed through it and the switchgear fire may ignite these trays, causing the temperature in the fire compartment to exceed the damaging hot gas layer temperature of 330°C. Multi-compartment effects therefore have to be taken into consideration. The risk for these multi-compartment scenarios are driven by common cause failure of automatic and manual PMS signals, combined with the fire failing DAS. If common cause failure of PMS only affects the automatic PMS signal, operators have a relatively high failure probability to manually take action to maintain cooling. These actions include failing to depressurize the RCS, failing to start CMT injection, and failure to actuate PRHR.
1254AF12554	Auxiliary Building Security Room	7.56E-08	11.17%	The fire risk is primarily driven by transient fires and two fixed ignition sources in the fire compartment. A fire in this fire compartment causes a spurious DAS signal that operators fail to prevent, which initiates spurious IRWST recirculation. Operators then fail to isolate the recirculation line. ZRS power supports are assumed to be failed for this fire compartment given the uncertainties in cable routing. Loss of ZRS fails startup feedwater cooling to both steam generators and plant-specific power failures fail makeup water, resulting in loss of main feedwater pump capability to cool the steam generators. Failure to isolate the recirculation line is assumed to fail PRHR decay heat removal and IRWST injection (both passive and active) due to draining of the IRWST tank.

Table 10-56: Review of Top Fire Compartments for CDF (cont.)

Fire Compartment	Fire Compartment Description	CDF	% Contribution to CDF	Description of Risk Contributors
2030AF20300	Turbine Building Elevation 100’	4.61E-08	6.80%	The fire risk is driven by the assumption that the fire damages all targets in the fire compartment. The consequence of a fire in this fire compartment is low but there are hundreds of ignition sources present and the increased frequency increases the risk. Components important to risk in this area include the condenser steam dump valves (can induce steam line break downstream of the MSIVs) and cables linked to the station transformers (can induce a loss of offsite power).
0000AF01	Yard	3.45E-08	5.09%	The fire risk is driven by loss of offsite power sequences caused by fire-induced failure of the station transformers. This area is modeled such that all fire scenarios are assumed to damage all targets in the fire compartment. The consequence of a fire in this fire compartment is low but there are hundreds of ignition sources present and the increased frequency increases the risk. ZRS power supports are assumed to be routed through this fire compartment, which fails startup feedwater from cooling both steam generators. Cables linked to ZRS components can be revisited once the routing has matured.

Table 10-56: Review of Top Fire Compartments for CDF (cont.)

Fire Compartment	Fire Compartment Description	CDF	% Contribution to CDF	Description of Risk Contributors
1201AF06	MSIV Room	3.09E-08	4.57%	The fire risk is driven by transient and oil fires, both of which are assumed to damage all targets in the fire compartment. Transient fires are typically refined based on routing of high value cables; however, given the pre-operational state of the plant, transients should be refined after the cable routing information has matured for this location. Oil scenarios have a very high degree of uncertainty with how the pool will spread and this fuel often produces very high heat release rates due to the large area available for combustion. Given the uncertainty with oil spill behavior, it is common industry practice to fail all targets in a fire compartment for oil fires. Components important to risk in this area include steam line valves whose failure can induce a steam line break upstream of the MSIVs and the air-handling units for the Train B CVS makeup pump train. These fire-induced failures, combined with independent failure of CMT injection, leads to core damage.
2050AF20500-Partial	Turbine Building 141’	2.56E-08	3.79%	Fire compartment 2050AF20500 is elevation 141’ 3” in the turbine building. This floor of the turbine building contains cables linked to the station transformers in one corner of the compartment. Ignition sources that are sufficiently far from these transformer cables are mapped to the fire compartment 2050AF20500 – Partial, which excludes these cables from failing. The consequence of a fire in this fire compartment is low but there are over a hundred ignition sources present and the increased frequency increases the risk. The dominant cutset for this fire compartment is spurious opening of the condenser steam dump valves coincident with the independent failure of the reactor control rods to insert and the turbine failing to trip due to failures in PMS and DAS.

Table 10-56: Review of Top Fire Compartments for CDF (cont.)

Fire Compartment	Fire Compartment Description	CDF	% Contribution to CDF	Description of Risk Contributors
1240AF01	Non-Class 1E Penetration Room	2.53E-08	3.74%	The fire risk is driven by the assumption the fire damages all targets in the fire compartment. Cables/components important to risk in this area include power supplies for DAS. The top cutsets for this fire compartment consist of fire-induced loss of DAS, common cause failure of PMS, and operators failing to respond following automatic failure of PMS.
2151AF21580	South Bay Elevation 135'-3" General Area	2.10E-08	3.11%	The fire risk is driven by the assumption the fire damages all targets in the fire compartment. Transient fires are typically refined based on routing of high value cables; however, given the pre-operational state of the plant, transients should be refined after the cable routing information is more mature for this location. This fire compartment is not as risk-significant as fires propagating from this location and damaging surrounding fire compartments.

Table 10-57: Review of Top Fire Compartments for LRF

Fire Compartment	Fire Compartment Description	LRF	% Contribution to LRF	Description of Risk Contributors
1232AF12312	Division C RCP Switchgear Room	1.01E-08	18.04%	Following the failures leading to core damage identified in Table 10-56, LRF is driven by failure to isolate VFS penetrations when the VFS purge and supply lines are open and the PMS and DAS isolation signals fail.
2030AF20300	Turbine Building Elevation 100’	7.76E-09	13.86%	Following the failures leading to core damage identified in Table 10-56, LRF is driven by fire-induced failure of the power systems supporting the VLS Hydrogen igniters. Independent failure of the diesel generators combined with a fire-induced loss of offsite power fails ac power to the buses that support the dc battery chargers. Loss of the station transformers also fails the diverse ac power source for the Hydrogen igniters.
1240AF01	Non-Class 1E Penetration Room	7.64E-09	13.66%	Following the failures leading to core damage identified in Table 10-56, LRF is driven by fire-induced failure of the VLS Hydrogen igniters.
0000AF01	Yard	3.55E-09	6.35%	Following the failures leading to core damage identified in Table 10-56, LRF is driven by failure of the PCS to provide flow to the containment shell. Primary PCS fails when the automatic PMS and DAS signals independently fail and operators fail to diagnose high containment pressure and manually actuate PMS and DAS. Alternate PCS alignments also fail due to the operator error to diagnose high containment pressure.
4031AF40310	Annex Building Battery Room 2	3.40E-09	6.08%	The fire risk is primarily driven by the assumption the fire damages all targets in the fire compartment and propagates to multi-compartment scenarios. Important mitigating equipment/cables contained in this compartment are the electrical buses powering the DAS signal to close IRWST gutter valves, and the power supply for PLS signalling to support SFW.

Table 10-57: Review of Top Fire Compartments for LRF (cont.)

Fire Compartment	Fire Compartment Description	LRF	% Contribution to LRF	Description of Risk Contributors
2040AF20400	Turbine Building Elevation 121'6" General Floor Area	2.31E-09	4.13%	The fire risk is primarily driven by the assumption the fire damages all targets in the fire compartment. The consequence of a fire in this fire compartment is low but there are hundreds of potential ignition sources present. The increase fire ignition frequency increases the fire risk. Components important to risk in this area include the site transformers, which can induce a loss of offsite power, loss of power to Hydrogen igniters and loss of power to the buses supporting DAS. Independent failure of the diesel generator combined with common cause failure of PMS challenges the signalling capability to actuate essential Class-1 systems.
4031AF40308	Annex Building Battery Room 1	2.28E-09	4.08%	The fire risk is primarily driven by the assumption the fire damages all targets in the fire compartment and propagates to multi-compartment scenarios. Important mitigating equipment/cables contained in this compartment are the Train B SFW pump, and the bus supporting the electrical support to the Train A SFW pump.
4032AF01	Annex Building Radiologically Controlled Area Entry/Exit	2.10E-09	3.75%	The fire risk is primarily driven by the assumption the fire damages all targets in the fire compartment. Core damage is driven by cable failures of the DAS power supply combined with common cause failure of PMS. LRF is driven by cable failures of the diverse power supplies to the Hydrogen igniters, with the EDS transformer failing ac power and the battery charger failing to recharge the batteries to provide dc power.

Table 10-57: Review of Top Fire Compartments for LRF (cont.)

Fire Compartment	Fire Compartment Description	LRF	% Contribution to LRF	Description of Risk Contributors
4031AF40303	Annex Building – Turbine Building Corridor	1.93E-09	3.45%	The fire risk is primarily driven by the assumption the fire damages all targets in the fire compartment. Transient fires are typically refined based on routing of high risk value cables; however, given the pre-operational state of the plant, transients should be refined after the cable routing is more mature for this location. Components important to risk in this area include the redundant and diverse power supplies for the Hydrogen igniters and for DAS control.
1100AF11300B	Containment Floor (North half)	1.66E-09	2.98%	The fire risk is driven by a transient fire scenario. The fire occurs in an area that induces a PMS signal that induces spurious recirculation of the IRWST. Additionally the fire fails the Train B IRWST isolation path from actuating. Independent failure of the SFW control valves cause a loss of cooling to the steam generators and results in core damage. LRF is driven by fire-induced failure of the VLS Hydrogen igniters.

Table 10-58. External Hazards Screening Scenarios

Case	Description	CCDP	Max. IEF
1	Hazard-induced LOOP	3.8E-07	2.6E-02
2	Hazard-induced LOOP coincident with unavailability of the non-Class 1 systems	4.3E-06	2.3E-03
3	Hazard-induced reactor trip (general transient with main feedwater) and failure of all operator actions	9.0E-07	1.1E-02

Table 10-59. Fujita Tornado F Scale Intensity Wind Speed Relationships (From Table 2-1 of Reference 10.64)

Intensity	Description	Original Fujita Scale [Fastest 0.40 km (Quarter Mile), km/hr (mph)]	Fujita Scale [3-Second Gust, km/hr (mph)]	Operational Enhanced Fujita Scale [3-Second Gust, km/hr (mph)
F0	Light Damage	64.37 – 115.87 (40-72)	72.42 – 125.53 (45-78)	104.61 – 136.79 (65-85)
F1	Moderate Damage	117.48 – 180.25 (73-112)	127.14 – 188.29 (79-1170	138.40 – 177.03 (86-110)
F2	Considerable Damage	181.86 – 252.76 (113-157)	189.90 – 259.10 (118-161)	178.64 – 217.26 (111-135)
F3	Severe Damage	254.28 – 331.52 (158-206)	260.71 – 336.35 (162-209)	218.87 – 265.54 (136 – 165)
F4	Devastating Damage	333.13 – 418.43 (207-260)	337.96 – 420.04 (210-261)	267.15 – 321.87 (166-200)
F5	Incredible Damage	420-04 – 511.77 (261-318)	421.65 – 510.16 (262-317)	> 321.87 (>200)

Table 10-60. Description of Saffir-Simpson Scale (Hurricanes) (Reference 10.63)

Category Number	Wind Speed	Category Description
1	119.09 – 152.89 km/hr (74-95 mph)	Storm surge generally 1.22-1.52 m (4-5 ft) above normal. No real damage to building structures. Damage primarily to unanchored mobile homes, shrubbery, and trees. Some damage to poorly constructed signs. Also, some coastal road flooding and minor pier damage.
2	154.50-177.03 km/hr (96-110 mph)	Storm surge generally 1.83 – 2.44 m (6-8 ft) above normal. Some roofing material, door, and window damage of buildings. Considerable damage to shrubbery and trees with some trees blown down. Considerable damage to mobile homes, poorly constructed signs, and piers. Coastal and low-lying escape routes flood 2-4 hours before arrival of the hurricane centre. Small craft in unprotected anchorages break moorings.
3	178.64 – 209.21 km/hr (111-130 mph)	Storm surge generally 2.74-3.66 m (9-12 ft) above normal. Some structural damage to small residences and utility buildings with a minor amount of curtain wall failures. Damage to shrubbery and trees with foliage blown off trees and large trees blown down. Mobile homes and poorly constructed signs are destroyed. Low-lying escape routes are cut by rising water 3-5 hours before arrival of the centre of the hurricane. Flooding near the coast destroys smaller structures with larger structures damaged by battering from floating debris. Terrain continuously lower than 1.52 m (5 ft) above mean sea level may be flooded inland 12.87 km (8 miles) or more. Evacuation of low-lying residences with several blocks of the shoreline may be required.
4	210.82 – 249.45 km/hr (131-155 mph)	Storm surge generally 3.96- 5.49 m (13-18 ft) above normal. More extensive curtain wall failures with some complete roof structure failures on small residences. Shrubs, trees, and all signs are blown down. Complete destruction of mobile homes. Extensive damage to doors and windows. Low-lying escape routes may be cut by rising water 3-5 hours before arrival of the centre of the hurricane. Major damage to lower floors of structures near the shore. Terrain lower than 3.05 m (10 ft) above sea level may be flooded requiring massive evacuation of residential areas as far inland as 9.66 km (6 miles).
5	>249.45 km/hr (>155 mph)	Storm surge generally greater than 5.49 m (18 ft) above normal. Complete roof failure on many residences and industrial buildings. Some complete building failures with small utility buildings blown over or away. All shrubs, trees, and signs blown down. Complete destruction of mobile homes. Severe and extensive window and door damage. Low-lying escape routes are cut by rising water 3-5 hours before arrival of the centre of the hurricane. Major damage to lower floors of all structures located less than 4.57 m (15 ft) above sea level and within 457.20 m (500 yards) of the shoreline. Massive evacuation of residential areas on low ground within 8.05 – 16.09 km (5-10 miles) of the shoreline may be required.

Table 10-61. Contribution Of Initiating Events to Core Damage

Initiator	IEF (Per Reactor Year)	Core Damage Frequency Contribution (Per Reactor Year)	% CDF	Description
%SLOCA	2.80E-03	5.77E-08	33.00%	SMALL LOCA
%RVR	[ ]	2.99E-08	17.10%	REACTOR VESSEL RUPTURE
%SPRECIRC	[ ]	1.40E-08	8.00%	SPURIOUS IRWST RECIRCULATION INJECTION
%LOOP	3.34E-02	1.30E-08	7.40%	TOTAL LOSS OF OFFSITE POWER
%SGTR	3.29E-03	7.68E-09	4.40%	SGTR
%LEAK	1.44E-03	6.28E-09	3.60%	RCS LEAK
%VWS-HCS	[ ]	6.36E-09	3.60%	TOTAL LOSS OF VWS HCS
%SLBD	9.30E-03	5.98E-09	3.40%	SLB DOWNSTREAM OF THE MSIVS
%SWS	1.26E-01	4.31E-09	2.50%	TOTAL LOSS OF SERVICE WATER
%MVAC	1.72E-02	3.89E-09	2.20%	LOSS OF MEDIUM VOLTAGE AC POWER
%GTRAN-WFW	4.23E-01	3.28E-09	1.90%	GENERAL TRANSIENT WITH MAIN FEEDWATER
%GTRAN-WOFW	2.56E-01	2.35E-09	1.30%	GENERAL TRANSIENT WITHOUT MAIN FEEDWATER
%PRHRTR	[ ]	2.31E-09	1.30%	PRHR TUBE RUPTURE
%FWLB	3.19E-03	2.04E-09	1.20%	FEEDWATER LINE BREAK
%SLBU	9.30E-04	2.16E-09	1.20%	SLB UPSTREAM OF THE MSIVS
%CAS	[ ]	1.96E-09	1.10%	TOTAL LOSS OF COMPRESSED AND INSTRUMENT AIR
%GTRAN-WS	2.01E-02	1.57E-09	0.90%	GENERAL TRANSIENT WITH S SIGNAL
%VTS-T2	[ ]	1.24E-09	0.70%	LOSS OF HVAC TO THE CCS PUMPS

Table 10-61. Contribution Of Initiating Events to Core Damage (cont.)

Initiator	IEF (Per Reactor Year)	Core Damage Frequency Contribution (Per Reactor Year)	% CDF	Description
%IDSC-DD-1	[ ]	1.04E-09	0.60%	LOSS OF LOW VOLTAGE POWER – 250V DC DISTRIBUTION PANEL IDSC-DD-1 FAILS
%CCS	[ ]	9.16E-10	0.50%	TOTAL LOSS OF COMPONENT COOLING WATER
%IDSB-DD-1	[ ]	8.68E-10	0.50%	LOSS OF LOW VOLTAGE POWER – 250V DC DISTRIBUTION PANEL IDSB-DD-1 FAILS
%LMFW	8.92E-02	7.99E-10	0.50%	TOTAL LOSS OF MAIN FEEDWATER
%IDSA-DD-1	[ ]	6.43E-10	0.40%	LOSS OF LOW VOLTAGE POWER – 250V DC DISTRIBUTION PANEL IDSA-DD-1 FAILS
%IDSD-DD-1	[ ]	7.19E-10	0.40%	LOSS OF LOW VOLTAGE POWER – 250V DC DISTRIBUTION PANEL IDSD-DD-1 FAILS
%LCOND	7.54E-02	6.73E-10	0.40%	TOTAL LOSS OF CONDENSER HEAT SINK
%PRHRLB	[ ]	7.41E-10	0.40%	PRHR LINE BREAK
%SPCMT	[ ]	4.55E-10	0.30%	SPURIOUS CMT ACTUATION
%LLOCA	7.78E-07	3.44E-10	0.20%	LARGE LOCA
%DVILB-A	[ ]	1.67E-10	0.10%	DVI LINE A BREAK
%DVILB-B	[ ]	2.61E-10	0.10%	DVI LINE B BREAK
%MLOCA	6.79E-06	2.43E-10	0.10%	MEDIUM LOCA
%SPADS13	[ ]	1.70E-10	0.10%	SPURIOUS ADS STAGES 1-3
%SPADS4	[ ]	2.06E-10	0.10%	SPURIOUS ADS STAGE 4
%SPPRHR	[ ]	2.32E-10	0.10%	SPURIOUS PRHR INITIATOR
%CMTLB-A	[ ]	6.31E-11	0.00%	CMT A LINE BREAK
%CMTLB-B	[ ]	5.79E-11	0.00%	CMT B LINE BREAK

Table 10-61. Contribution Of Initiating Events to Core Damage (cont.)

Initiator	IEF (Per Reactor Year)	Core Damage Frequency Contribution (Per Reactor Year)	% CDF	Description
%ISL-P04	[ ]	1.31E-13	0.00%	ISLOCA FROM CCS RCP EXTERNAL HX
%ISL-P07-N	[ ]	8.29E-11	0.00%	ISLOCA FROM CVS NORMAL MAKEUP LINE
%ISL-P08	[ ]	2.88E-14	0.00%	ISLOCA FROM CVS ZINC ADDITION LINE
%ISL-P19	[ ]	2.37E-12	0.00%	ISLOCA FROM RNS SUCTION LINE
%SPIRWST	[ ]	1.51E-12	0.00%	SPURIOUS IRWST INJECTION

Table 10-62. Internal Initiating Events At Power Dominant Core Damage Sequences

CDF Sequence Name	Accident Sequence Description	%Total	% Total Cumulative
SLOCA-008	Small LOCA with failure of ADS Stage 4 depressurization and RNS injection	13.4%	13.4%
SPRECIRC-37	Spurious IRWST Recirculation with failure of MFW and SFW	9.5%	22.9%
SLOCA-002	Small LOCA with failure of gravity recirculation	8.8%	31.7%
SLOCA-005	Small LOCA with failure of gravity injection and RNS injection	8.0%	39.7%
SLOCA-022	Small LOCA with failure of CMT injection, ADS Stage 4 depressurization, and RNS injection	6.8%	46.5%
GTRAN-012	General Transient with failure of MFW, SFW, and PRHR. ADS Stages 1-3 also fail to depressurize.	4.3%	50.8%
SLBD-006	Steam Line Break Downstream with failure of steam generator isolation, CMT injection failure, and CVS failure.	4.3%	55.1%
LTCP-003	Loss of Long Term Containment Cooling during PRHR operation with failure of PCS and SFW	3.2%	58.3%
SGTR-022	Steam Generator Tube Rupture with failure of PRHR, gravity injection from the IRWST, and active injection from RNS.	2.8%	61.0%
ATWS-014	Anticipated Transient Without Scram with secondary side fault.	2.7%	63.8%
GTRAN-WS-007	General Transient with Safeguards	2.5%	66.3%
SLOCA-024	Small LOCA with failure of CMT injection and ADS Stages 1-3 depressurization	2.2%	68.4%
LTCP-006	Loss of Long Term Containment Cooling during PRHR operation with failure of containment isolation, PCS, and SFW.	2.1%	70.5%
LEAK-009	RCS Leak with failure of CVS makeup, failure of ADS Stage 4 depressurization, and failure of RNS injection.	2.1%	72.6%
GTRAN-011	General Transient with failure of MFW, SFW, and PRHR. ADS Stage 4 fails to depressurize and RNS fails to inject.	1.9%	74.4%
LOOP-028	Loss of Offsite Power with a non-SBO event, failure of the operator action to stop the 22 hour timer, and failure of ADS Stage 4 to depressurize.	1.7%	76.1%

Table 10-62. Internal Initiating Events At Power Dominant Core Damage Sequences (cont.)

CDF Sequence Name	Accident Sequence Description	%Total	% Total Cumulative
LEAK-006	RCS Leak with failure of CVS makeup, failure of IRWST injection, and RNS injection.	1.7%	77.8%
GTRAN-008	General Transient with failure of MFW, SFW, and PRHR. IRWST and RNS fail to inject.	1.6%	79.4%
ATWS-008	Anticipated Transient Without Scram with MFW failure and pressuriser safety valve failure to open.	1.4%	80.7%
ATWS-004	Anticipated Transient Without Scram with the pressuriser safety valves failure to open.	1.3%	82.0%
LOOP-007	Loss of Offsite Power with failure of SFW, PRHR and failure of passive and active injection from IRWST and RNS.	1.3%	83.3%
LOOP-010	Loss of Offsite Power with failure of SFW, PRHR, and depressurization from ADS Stage 4, and failure of RNS injection.	1.0%	84.3%
GTRAN-WS-011	General Transient with Safeguards	1.0%	85.4%
LOOP-011	Loss of Offsite Power with failure of SFW, PRHR and depressurization from ADS Stages 1-3.	1.0%	86.4%
SLBU-021	Steam Line Break Upstream with failure of the steam generator to isolate, failure of CMT injection, and failure of CVS.	0.9%	87.3%
SGTR-007	Steam Generator Tube Rupture with failure of steam generator isolation, and IRWST injection, and RNS injection.	0.9%	88.2%
SGTR-008	Steam Generator Tube Rupture with failure of steam generator isolation and failure of ADS Stage 4 depressurization.	0.8%	89.0%
SLOCA-014	Small LOCA with failures of ADS Stages 1-4 depressurization.	0.7%	89.7%

Table 10-63. LRF Release Categories and Contributions

End State	Description	% of LRF
LERF-BYPASS	Severe accident fission product releases to the environment which are greater than nominal containment leakage because a containment bypass initiator has occurred or because a large containment isolation failure has occurred.	32%
LERF-EV2	Severe accident fission product releases to the environment which are greater than nominal containment leakage, occur during relocation, and have an additional fission product contribution from MCCI.	26%
LERF	Severe accident fission product releases to the environment which are greater than nominal containment leakage and occur during relocation.	17%
LERF-EV1	Severe accident fission product releases to the environment which are greater than nominal containment leakage, occur during relocation, and have an additional fission product contribution from spread and quenched MCCI.	11%
LIRF-BMMT	Severe accident fission product releases to the environment which are greater than nominal containment leakage, occur after relocation, are less than 24 hours after CD, and have basemat penetration.	7%
LERF-SE	Severe accident fission product releases to the environment which are greater than nominal containment leakage and occur during relocation. This release considers the containment challenge from an ex-vessel steam explosion.	5%
LVRF	Severe accident fission product releases to the environment from a containment vent path which are greater than nominal containment leakage, core debris is maintained in the RV, and are approximately 24 hours after CD or later.	1%
LVRF-EV1	Severe accident fission product releases to the environment from a containment vent path which are greater than nominal containment leakage and have an additional fission product contribution from spread and quenched MCCI.	0%
LVRF-EV2	Severe accident fission product releases to the environment from containment vent path which are greater than nominal containment leakage and have an additional fission product contribution from MCCI.	0%
LIRF-EV1	Severe accident fission product releases to the environment which are greater than nominal containment leakage, occur after relocation, are less than 24 hours after CD, and have an additional fission product contribution from spread and quenched MCCI.	0%

Table 10-64 LRF Release Categories and Contributions (cont.)

End State	Description	% of LRF
LIRF	Severe accident fission product releases to the environment which are greater than nominal containment leakage, occur after relocation, core debris is maintained in the RV, and are less than 24 hours after CD.	0%
LIRF-EV2	Severe accident fission product releases to the environment which are greater than nominal containment leakage, occur after relocation, are less than 24 hours after CD, and have an additional fission product contribution from MCCI.	0%

Table 10-65. Uncertainty Results for At-Power Internal Events (Per Reactor-Year)

	Mean	5th Percentile	Median	95th Percentile
CDF	1.7E-07	5.4E-08	1.2E-07	4.2E-07
LRF	1.5E-08	2.2E-09	7.1E-09	5.0E-08

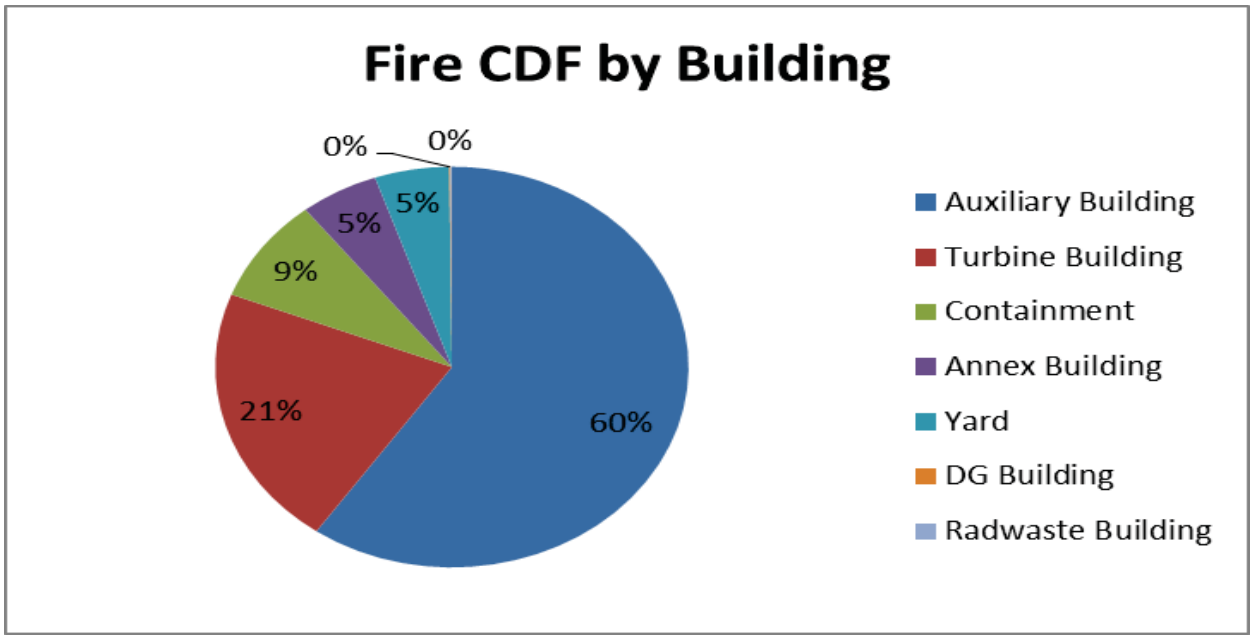


Figure 10-1: Fire CDF by Building or Location

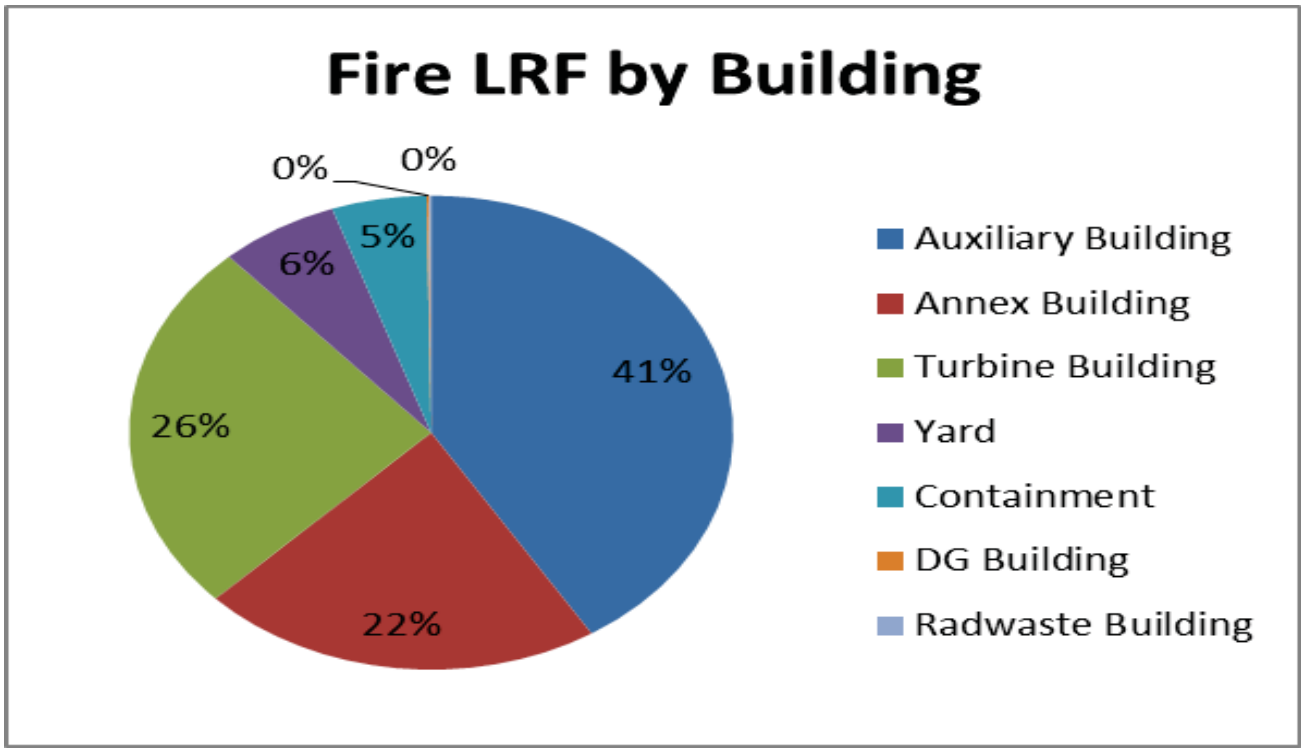


Figure 10-2: Fire LRF by Building or Location

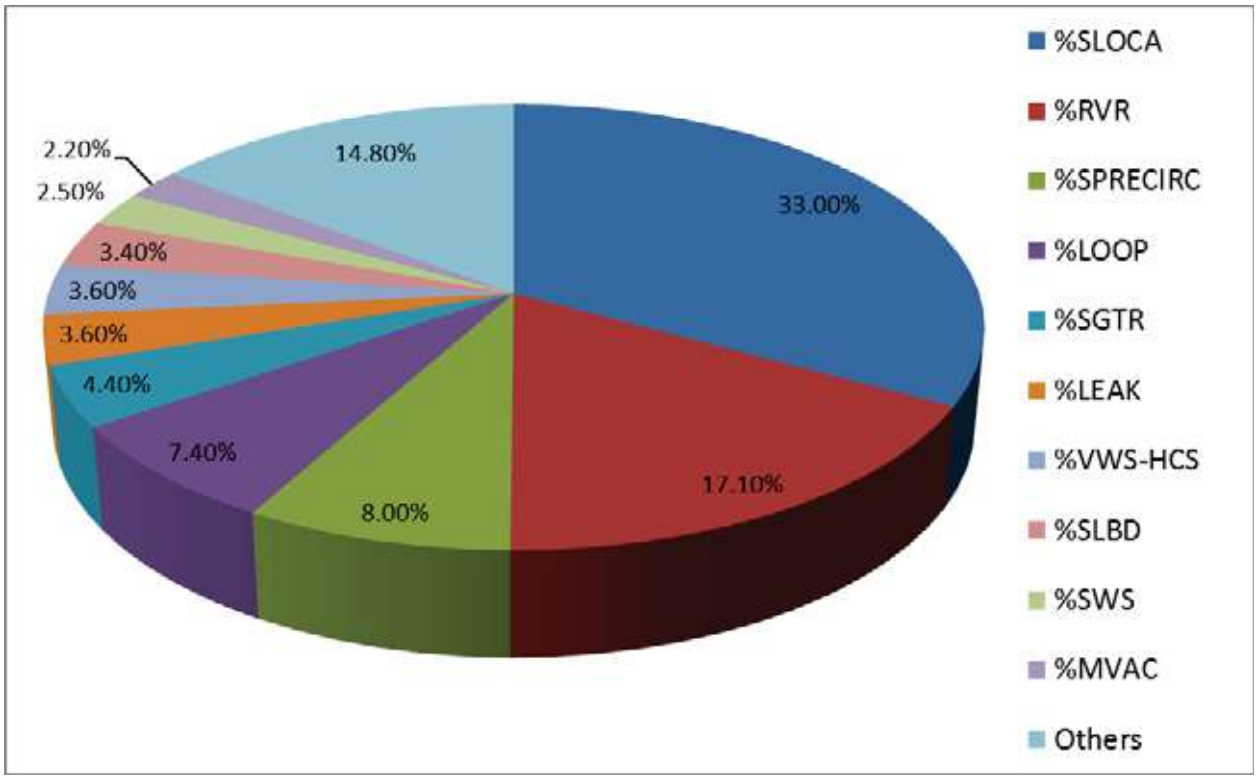


Figure 10-3. Contribution of Initiating Events to Core Damage

APPENDIX 10A
THE USE OF PROBABILISTIC SAFETY ASSESSMENT AND SEVERE ACCIDENT ANALYSIS TO INFORM THE AP1000 DESIGN

10A.1 Introduction

The information presented in this appendix represents historical information on the use of the PSA to inform the AP1000 plant design.

Westinghouse Electric Company has developed the AP1000 design to have a comparable electric power production capability to existing nuclear power stations, but with a level of risk more than an order of magnitude lower than the best reactors currently operating. Current nuclear power stations have achieved an acceptable level of risk by evolving ever-increasing complexity with respect to their engineered safety features, but this complexity is subject to the law of diminishing returns. If taken too far in developing a new design, very low levels of risk might be achievable but at a price so high that it would be uneconomical to build the nuclear power station.

Westinghouse has taken an alternative approach in designing the AP1000; it has reduced complexity by making the engineered safety features passive rather than active to the maximum degree feasible, thereby achieving a very high level of safety and a simplified design. The basic design, based on AP600 design, uses the concepts of inherent safety, fault tolerance, passive safety and defence in depth to produce a design whose risks are significantly lower than earlier designs.

This basic design was subsequently enhanced by using PSA to identify worthwhile improvements, that is, reasonably practicable improvements that would decrease the overall risk from the plant.

This process has two components: a systematic review of the dominant or major cut-sets for CDF and LRF to determine design changes that would have a significant contribution to risk reduction; and using the conclusions of the SAMDA process to identify further risk-reducing measures by evaluating the potential for modifications that might provide significant and practical improvements to the radiological risk profile of the design.

10A.2 Use of Probabilistic Safety Assessment to Inform the Design

10A.2.1 Background

The AP1000 designers chose to use the PSA as a tool to investigate various detailed design solutions and operational strategies to optimise safety. The PSA provides insights on what is contributing to the risk, and it enables potential design improvements to be explored quantitatively. Addressing PSA issues at the design process leads to a low level of risk and results in an ALARP design.

10A.2.2 Design Improvements Introduced as a Result of the AP600 Design Probabilistic Safety Assessment

Design improvements were incorporated in the AP600 design based on the results of the AP600 PSA.

The most significant design changes prompted by the AP600 design PSA are as follows:

- ADS Stages 1, 2, and 3 in-service test frequency was been changed to occur every refuelling. This change had a positive impact on the spurious ADS actuation frequency.

- In the first three stages of the ADS, both series MOVs are closed during normal operation instead of one closed/one open. This reduces the frequency of spurious actuation of the ADS.

- The ADS Stage 4 valves were originally motor operated like the ADS Stage 1/2/3 valves. This led to a low reliability of ADS. The ADS Stage 4 valves were changed to gas piston gate valves, and later changed to squib valves to gain even more reliability.

- The number and size of the fourth-stage ADS valves has been increased. In the event of a SLOCA, this modification provides a redundant and diverse path for depressurisation in case of a CCF of the MOVs in the first three stages of the ADS.

- The DAS is provided to automatically actuate selected systems such as the PRHR, the CMT, the PCS, reactor trip, and containment isolation. In addition, the system provides alarms and information to the MCR for manual actuation of these systems.

- Diversity is provided in the DAS by using components that are diverse from the microprocessor-based components used in the PMS and the PLS. This reduces the importance of potential CCFs (both hardware and software) of microprocessor-based components of the PMS and the PLS that process information and provide for actuation of accident mitigation systems.

- The diversified functions are selected on the basis of PSA insights to reduce the CDF and to reduce the conditional probability of large-release frequency given core damage.

- Manual actuation of the RNS can be accomplished from the MCR. The RNS provides diverse means of coolant injection in case of failure of the check valves of the IRWST. An emergency operating procedure requires aligning the RNS when the ADS is actuated.

- Two parallel paths, each containing a squib valve and a check valve in series, are used for gravity injection from the IRWST. This improves the IRWST reliability for the case of single valve failure during an SI line break event or for the case of a CCF of the two check valves in other events requiring full reactor depressurisation.

- The check valves in the CMT injection lines are designed so that they remain in the open position during the plant normal operation. This design eliminates opening failures and CCFs with the accumulator check valves.

- The ADS is automatically actuated during a transient event with loss of both secondary side heat removal and PRHR capability. This is accomplished by the provision to automatically actuate the CMTs on low SG level and high hot leg temperature signals. CMT injection subsequently causes actuation of the ADS. This improvement reduces the importance of the operator actions.

- Automatic opening of the MOV of the IRWST injection line occurs on a low hot leg water level signal. These valves are closed during shutdown conditions, such as

mid-loop and vessel-flange operation when the RCS is at atmospheric pressure. This also reduces the importance of operator action on these events.

- Alarms are provided in the MCR to inform the operator of mis-positioned isolation valves (IVs) of the PXSs that have remote manual control capability. This reduces the probability of valve mis-positioning.

- Protection system logic is adopted to preclude the SG from overfilling during an SGTR event. This reduces the need for full reactor depressurisation and reduces the frequency of core damage for SGTR events with BP.

- The capability to manually actuate the draining of IRWST water into the reactor cavity is provided. This is incorporated to address a core damage event in which the injection of IRWST water to the RV fails. This drained water cools the core debris inside the RV, removing the heat through the RV wall and avoiding failure of the RV.

10A.2.3 Review of Defence-in-Depth Systems

The International Atomic Energy Agency (IAEA) recognises a number of levels of defence in depth:

- Level 1 – Duty systems
- Level 2 – Systems that are deployed to control abnormal operation and detect failures
- Level 3 – Robust safety measures

These levels correspond to the AP1000 Class 3, Class 2 and Class 1 SSCs, respectively. In the case of the AP1000 design, nuclear safety is less dependent on the Class 3 and Class 2 (Levels 1 and 2) systems then conventional PWRs because of the presence of Class 1 systems. These are robust because they do not require support systems such as ac power, component cooling water and service water.

Nevertheless, sensitivity studies have been performed with the AP1000 risk model to evaluate the significance on risk of the Class 3 and Class 2 (IAEA Level 1 and Level 2) safety measures, to identify those SSCs that are important in providing defence in depth. The following systems have been identified as providing significant additional defence in depth:

- DAS, Class 2 dc and Uninterruptable Power Supply System (EDS)
- Offsite power, main ac power, and onsite standby power systems
- RNS
- CCS
- SWS

Once identified, appropriate functional requirements were incorporated into their design and into the arrangements covering their operation, maintenance and testing, so as to provide reasonable assurance that these SSCs would be operable during the anticipated events. For most of the SSCs involved, a substantial operating history is available, which defines the significant failure modes and their likely causes. The identification and prioritisation of the various possible failure modes for each SSC lead to design improvements for failure prevention or mitigation.

The AP1000 Operating Rules (Reference 10A.1, Section 4) provide control on the availability of some of these SSCs, and on their surveillance and testing frequencies, thereby

providing confidence that the reliability values assumed for them in the PSA will be maintained during plant operations.

These SSCs are also included in the design reliability assurance programme (D-RAP) (Reference 10A.2, Section 17.4) whose purpose is to make sure that the important reliability assumptions made as part of the PSA remain valid throughout plant life (see Section 5.9.3 of this PCSR). The PSA input includes specific values for the reliability of the various SSCs in the plant that provide the defence-in-depth capability.

10A.2.4 AP1000 Design Enhancements Implemented Based on PSA Insights

This section summarises the main design enhancements that are incorporated into the AP1000 plant due to PSA insights and results.

Insights from the AP1000-specific PSA and supporting risk analyses for external and shutdown events, including importance analyses and cut-set screening were used continuously throughout the development of the AP1000 design. The PSA dominant cut-sets and sequences were reviewed to identify the major risk contributors and if feasible risk-reducing alternatives were identified (analysis, procedural, design, and technical specification) and implemented. The total plant risk has been lowered to a point that it has become very difficult to find further cost-effective plant improvements. This design improvement process has been an intimate and natural part of the design and risk evaluation process. This process has resulted in the following plant design modifications:

- Changed the normal position of the two containment motor-operated recirculation valves (in series with squib valves) from closed to open.

  The normal position of the two MOV lines in the two sump recirculation lines have been changed from normally closed to normally open to improve the reliability of opening these paths. These two paths support containment recirculation for core cooling and IRWST draining for IVR. This change reduced the CDF and LRF contribution from the failure modes to open the MOVs.

- Changed IRWST drain procedure so it occurs earlier for IVR support

  Credit is taken for operator action to drain the IRWST into the sump to preserve RV integrity following core melt. The procedure for this severe accident response has been modified so that the operator action associated with IRWST draining is moved to the beginning of the procedure to allow more time for operator success and also to fill the cavity as soon as possible. This improves the probability of success of the operator action.

- Improved IVR heat transfer

  In going from AP600 to AP1000, the heat loads during IVR are increased due to the larger core power level which reduced the margins in the heat removal capability through the RV head during IVR. To compensate for the increase in core power, the critical heat flux (CHF) limit on the outside of the RV has been increased by a reactor vessel insulation design that provides an improved design of the baffle around the lower head to enhance the heat removal.

- Improved IRWST vents

  The larger core in the AP1000 can generate more hydrogen in a severe accident. In the AP1000 hydrogen analysis for Level 2, it was observed that the standing hydrogen diffusion flames at the IRWST vents resulted in a larger thermal loads to the containment steel shell, potentially leading to containment wall failure. The design of the vents has been changed to minimise this potential concern; during a severe accident, the IRWST vents located well away from the containment wall will open and the IRWST vents located next to the containment wall will not open.

- Added third PCS drain valve

  Due to the reduced containment surface area per MW of core power in the AP1000 core, natural air circulation without a PCS water drain may not always be sufficient for long-term (>1 day) containment heat removal in AP1000. For AP600, it was always sufficient for an indefinite time. To reduce the uncertainty in whether air cooling is sufficient to provide adequate long-term containment heat removal, a third path was added to the PCS drain lines to increase PCS reliability. The IV used in the third path is an MOV, which is diverse from the AOVs used in the other two lines. This provides considerable improvement in the PCS water drain reliability.

- Improved reliability of containment recirculation

  An examination of the AP1000 plant CDF cut-sets revealed that the CCF of 4/4 recirculation line squib valves was a dominant contributor to CDF and LRF. This failure mode was reduced by adopting diverse squib valves; two of the IRWST injection paths use high-pressure squib valves, and two use low-pressure (LP) squib valves. The design change reduces the CCF failure contribution of the recirculation squib valves to CDF and LRF. The two types of squib valves are sufficiently different and belong to different CCF groups. The increase in the group size of the high-pressure squib valves from four to six (including the four from the IRWST injection lines) does not add an appreciable contribution to the plant CDF.

10A.3 Conclusions

APPENDIX 10A describes how the basic design of AP600 and, subsequently, AP1000 were reviewed using insights from the PSA and severe accident analysis to identify reasonably practicable design changes that would significantly reduce the risk from the plant.

The risks from AP1000 were already lower than comparable plants of an earlier generation. As a result of these reviews, a number of design improvements have been implemented that reduce the risk further, to levels that can be seen to be ALARP.

10A.4 References

10A.1 Westinghouse Report UKP-GW-GL-500, Rev. 0, "AP1000® UK Limits and Condition Process Description," December 2015.

10A.2 Westinghouse Report APP-GW-GER-005, Rev. 1, "Safe and Simple: The Genesis and Process of the AP1000 Design," August 2008.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS AND ACRONYMS

ac	Alternating Current
ACI	American Concrete Institute
ADS	Automatic Depressurisation System
AFD	Automatic Fire Detection and Alarm System
AHU	Air Handling Unit
AISC	American Institute of Steel Construction
AISI	American Iron and Steel Institute
ALARP	As Low As Reasonably Practicable
ANS	American Nuclear Society
ANSI	American National Standards Institute
AOO	Anticipated Operational Occurrence
AOV	Operated Valve
ASME	American Society of Mechanical Engineers
ASFP	Association of Specialist Fire Protection
AWS	American Welding Society
BDS	Steam Generator Blow Down System
BTP	Branch Technical Position
CCS	Component Cooling Water System
CD	Core Damage
CDF	Core Damage Frequency
CFS	(Turbine Island) Chemical Feed System
C&I	Control and Instrumentation
CMT	Core Make-up Tank
COMAH	Control of Major Accident Hazards
COSHH	Control of Substances Hazardous to Health
CSA	Control Support Area
CVS	Chemical and Volume Control System
CWS	Circulating Water System
DAS	Diverse Actuation System
DBA	Design Basis Accident
dc	Direct Current
DDS	Data Display and Processing System
DECT	Digital Enhanced Cordless Telecommunications
DG	Diesel Generator
DTS	Demineralised Water Treatment System
ECS	Main ac Power System
EDS	Class 2 dc and Uninterruptible Power Supply System
EMC	Electro-Magnetic Compatibility
EMI	Electromagnetic Interference
EMIT	Examination, Maintenance, Inspection and Testing
EPRI	Electric Power Research Institute
FHS	Fuel Handling and Refuelling System
FPS	Fire Protection System
FWS	Start-up Feed Water System
GDA	Generic Design Assessment
HEPA	High Efficiency Particulate Air

LIST OF ABBREVIATIONS AND ACRONYMS (cont.)

HELB	High Energy Line Break
HFL	Higher Flammable Limit
HSE	Health and Safety Executive
HVAC	Heating, Ventilation and Air Conditioning
HX	Heat Exchanger
IAEA	International Atomic Energy Agency
IDS	Class 1E dc and Uninterruptible Power Supply System
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IIS	In-core Instrumentation System
ILW	Intermediate Level Waste
IRWST	In-containment Refuelling Water Storage Tank
LBB	Leak Before Break
LFL	Lower Flammable Limit
LLW	Low Level Waste
LLWR	Low Level Waste Repository
LOCA	Loss of Coolant Accident
MCC	Motor Control Centre
MCR	Main Control Room
MELB	Medium Energy Line Break
MHS	Mechanical Handling System
MSIV	Main Steam Isolation Valve
MSLB	Main Steam Line Break
NCIG	National Construction Issues Group
NEMA	National Electrical Manufacturers Association
NFPA	National Fire Protection Association
NI	Nuclear Island
NRC	Nuclear Regulatory Commission
OCS	Operation and Control Centre System
PCCAWST	Passive Containment Cooling Ancillary Water Storage Tank
PCCWST	Passive Containment Cooling Water Storage Tank
PCS	Passive Containment Cooling System
PCSR	Pre-construction Safety Report
PGS	Plant Gas System
PIE	Potential Initiating Event
PLS	Plant Control System
PMS	Protection and Safety Monitoring System
PORV	Power Operated Relief Valve
PRA	Probabilistic Risk Assessment
PRHR	Passive Residual Heat Removal
PSS	Primary Sampling System
PWR	Pressurised Water Reactor
PXS	Passive Core Cooling System
RCA	Radiological Controlled Area
RCCA	Rod Cluster Control Assembly

LIST OF ABBREVIATIONS AND ACRONYMS (cont.)

RCDT	Reactor Coolant Drain Tank
RCS	Reactor Coolant System
RNS	Normal Residual Heat Removal System
RSR	Remote Shutdown Room
RTS	Reactor Trip System
RZOI	Restrained Zone of Influence
SFS	Spent Fuel Pool Cooling System
SG	Steam Generator
SGS	Steam Generator System
SMS	Special Monitoring System
SQEP	Suitably Qualified and Experienced Personnel
SSC	Systems, Structures and Component
SWS	Service Water System
TSP	Tri-sodium Phosphate
UK	United Kingdom
UL	Underwriters Laboratories
URD	Utility Requirements Document
UZOI	Unrestrained Zone of Influence
VAS	Radiologically Controlled Area Ventilation System
VBS	Nuclear Island Non-Radioactive Ventilation System
VCS	Containment Recirculation Cooling System
VES	Main Control Room Emergency Habitability System
VFS	Containment Air Filtration System
VHS	Health Physics and Hot Machine Shop HVAC System
VLS	Containment Hydrogen Control System
VOIP	Voice Over Internet Protocol
VRS	Radwaste Building HVAC System
VTS	Turbine Building Ventilation System
VWS	Central Chilled Water System
VXS	Annex/Auxiliary Buildings Non-Radioactive HVAC System
VZS	Diesel Generator Building Heating and Ventilation System
WGS	Gaseous Radwaste System
WLS	Liquid Radwaste System
WRS	Radioactive Waste Drain System
WSS	Solid Radwaste System
WWS	Waste Water System
ZOS	On-site Standby Power System

11 INTERNAL HAZARDS

11.1 Introduction

This chapter identifies and assesses the consequences and demonstrates the tolerance of the AP1000 design to a systematically defined set of internally generated safety hazards. Internal Hazards are defined as natural or man-made hazards that originate within the controlled site and its processes as potentially influencing Category A or supporting Category B safety functions. In addition, this chapter considers appropriate consequential hazards arising from the combined influences of both internal and relevant external hazards. External hazards are further addressed in Chapter 12.

The information within this chapter is developed from the fundamental premise of identifying and addressing key safety claims of the AP1000 design. The overarching high level safety claim addressing internal hazard challenges within the AP1000 design basis is summarised as:

Claim IH-0: An internal hazard within the design basis does not prevent delivery of the Category A safety functions and supporting post 72-hour Category B safety functions necessary to respond to the postulated event.

Within the basis for this claim, operation of the AP1000 plant is tolerant to faults as the passive design significantly improves the response of the plant with appreciably reduced risk to the public, workforce, and environment. As a consequence of this design, and as consistent with the high level safety claim, AP1000 operations do not result in:

- Loss of control of core reactivity;
- Loss of control of removal of heat from the core;
- Uncontrolled exposure of plant personnel or the public to radiation, and;
- Uncontrolled dispersion of radioactivity.

The overarching high level nuclear safety claim is supported by more detailed specific claims and Sub-Claims as appropriate to the individual hazards. These claims or Sub-Claims are presented within the following sections of the Chapter as well as identification and discussion of evidentiary substantiation.

Each of these claims or subclaims falls under the general classifications of:

- Prevention of the internal hazard fault. Where claims of this nature are made, minimisation and elimination of hazards so far as is reasonably practicable from the AP1000 design have been used in the prevention of hazard initiation.

- Protection from the internal hazard fault. Where claims of this nature are made, protective measures have been incorporated into the design to safeguard the delivery of Category A safety functions from the effects of an internal hazard.

- Mitigation of the internal hazard fault. Where claims of this nature are made, mitigation of the resulting faulted conditions occurs through crediting the SSC design, selection of materials, limiting inventories, or use of redundant divisions of Class 1 SSCs.

There are a number of important conservative attributes which have been applied universally to all internal hazards assessments within the AP1000 safety case. These attributes are used to

define both the fundamental assessment approach and to establish the degree of safety margin relative to a realistic assessment of the internal hazards fault. In brief, these conservatisms are represented as:

- All internal hazards assessments within the AP1000 safety case are performed from a deterministic perspective. Hazards have not been excluded from consideration based on their hazard curve frequency of exceedance as below once in ten million years per Safety Assessment Principle EHA.19. This attribute conservatively addressed the explicit occurrence of an internal hazard faults without filtering the lower probability faults, thus creating a broader base of initiating events in assessing the internal hazard. In addition to the deterministic assessment, internal hazards have also been assessed from a realistic probabilistically perspective within the AP1000 PRA as discussed within chapter 10, "Reactor Faults Probabilistic Safety Assessment and Severe Accident Analysis".

- Each of the internal hazards assessments focus on the use of unmitigated consequences as a basis for the analyses acceptance. In this manner, use of conservative assumptions as applicable to these consequences is used consistently throughout the internal hazards assessments in determining an acceptable result.

- Operator actions have been minimized in so far as possible as mitigation responses in all internal hazard assessments. In the few areas where such actions are required, cross cutting inputs and reviews from the Human Factors area (Chapter 13), including consideration of human errors, have been used to assess viability of the action and suitability of the time required.

- Analysis of internal hazard faults assume the event occurs simultaneously with the facility's most adverse permitted operating state.

- Single failure has been applied throughout the internal hazards assessments.

Further fundamental safety elements relevant to the AP1000 design and as included within the internal hazards evaluations are identified in Section 1.5, "Key Safety Attributes", including identification of passive safety systems and use of separation, segregation, redundancy, and diversity provided by the design to minimise the effects of internal and external hazards and human errors.

The internal hazards applicable to the AP1000 plant have been derived from a process of assessment and review of the internal hazards lists from the International Atomic Energy Agency (IAEA), Health and Safety Executive (HSE), a plant safety case, and in-house Westinghouse work. This process has been systematic and robust. It has produced a comprehensive list of internal hazards (Reference 11.1) against which the AP1000 plant can be assessed.

Through this structured technical review, the following list of internal hazards has been determined applicable for assessment against the overarching safety claim, supporting claims and Sub-Claims:

- Section 11.2 Internal Fires
- Section 11.3 Internal Flooding
- Section 11.4 Pressure Part Failure
- Section 11.5 Internal Explosion

- Section 11.6 Internal Missiles
- Section 11.7 Releases of Toxic, Corrosive, and Flammable Material
- Section 11.8 Dropped Loads
- Section 11.9 Biological Agents
- Section 11.10 Onsite Transport Accidents
- Section 11.11 Electromagnetic Interference

Further, the combinations of hazards, including relevant externally generated hazards, have also been assessed within the overall internal hazards scope. In doing so, Section 11.12, Combination of Hazards, is also presented.

Internal hazards may initiate internal reactor faults or other non-reactor faults (for example in the fuel and waste handling routes); together these are termed 'internally initiated faults'. The fault identification and analysis of these faults is presented in Chapter 9. This analysis has shown that there are no faults that are unique to internal hazards.

Assessments of the internal hazards relative to the AP1000 design conclude that appropriate safety measures are in place and that there is no reasoned potential for common-cause failure of a claimed safety measure due to internal hazards.

Satisfaction of the claims and Sub-Claims identified throughout this chapter demonstrates that the generic design has incorporated adequate and sufficient defences to ensure the AP1000 design is robustly secured from vulnerabilities associated with internal hazards.

11.1.1 AP1000 Site, Buildings and Plant Description

The relevant AP1000 site and buildings applicable to the internal hazards assessments in this chapter are composed of the five principal buildings of the AP1000 plant:

- Nuclear Island, comprising the Containment/Shield building and Auxiliary Building;
- Turbine building;
- Annex building;
- Diesel Generator building; and
- Radwaste building.

These structures, as well as pertinent information and technical characteristics of the AP1000 design and SSCs may be found in Chapter 6. Detailed information pertinent to assessment of individual internal hazards or combinations of hazards may be found in the relevant section.

11.1.2 AP1000 Approach to Safety

Passive safety systems are the principal means of providing Category A safety functions, i.e., any function that plays a primary role in ensuring nuclear safety (see Chapter 5). These passive SSCs alone are designed to mitigate Design Basis Accidents (DBAs) and meet safety goals for the initial 72 hours following an initiating event; this capability is demonstrated in Chapter 9. The Class 1 SSCs are the principal means of delivering the Category A safety functions.

In so far as internal hazards are concerned, the safety case demonstrates that an internal hazard within the design basis cannot initiate a fault and also prevent delivery of the safety functions that mitigate the fault. Failure of the safety system as a result of an internal hazard, where the hazard does not also initiate a reactor fault, would simply require the reactor to be manually shut down using the duty systems. Should the initiating hazard event cause failure of the duty systems but not the safety systems, then the safety systems will respond to the fault as intended and as described in Chapter 9.

Systems containing Class 1 SSCs that function to mitigate DBAs have component redundancy to satisfy the single failure criterion, such that their Category A safety functions will be performed, even in the unlikely event of the most limiting single failure occurring coincident with the postulated DBA. Additionally, all Class 1 safe shutdown SSCs are located within the Nuclear Island (NI) and, therefore, for hazards originating outside the NI, it only needs to be demonstrated that the outer structures of the NI provide sufficient protection to prevent propagation of the hazard to areas within the NI.

Within the Containment, the segregation of Class 1 SSCs is considered. For each hazard that can arise in the Containment, it is shown that safe shutdown capacity is maintained.

Since the passive Class 1 SSCs used for DBA mitigation are not used in normal operation and on their own can mitigate DBAs, the safety case can be made by demonstrating protection of Class 1 SSCs from internal hazards such that they can still deliver their safety function as shown in Table 8A-2.

11.1.2.1 Safety Functions

Presentation of the categorisation and classification methodology, in addition to a discussion of the Category A, B and C safety functions and SSC Classifications 1, 2, and 3 may be found in Chapter 5, Section 2. Further discussion on categorization and classification may be found in Chapter 15 and in References 11.26 and 11.59. SSCs that are claimed to mitigate hazard faults are listed in Table 8A-2.

11.1.2.2 Additional Defence in Depth

The AP1000 provides multiple levels of defence for most faults, especially the more frequent faults. As shown in Chapter 8, Table 8A-2, frequent faults have two diverse sets of systems that provide mitigation. For example, a typical intact circuit frequent fault, the primary reactor heat removal system is by use of the Class 1 PRHR heat exchanger. The diverse backup is a passive feed and bleed capability that uses Class 1 ADS, Accumulators, IRWST injection and Containment recirculation.

In addition, to these credited Class 1 SSCs, the AP1000 plant has another level of defence for more frequent faults that provides improved investment protection. These Class 2 defence in depth (DiD) systems use active components, such as pumps, with power from onsite AC power supplies. Redundancy for more likely failures is provided to improve system and response reliability. Examples of these systems include the SFW, RNS, SFS, CCS and SWS. These Class 2 DiD systems are not credited in the AP1000 deterministic safety case and, as a result, are not further assessed for internal hazards.

11.2 Internal Fire

11.2.1 Introduction

In demonstrating that a postulated fire within the design basis does not prevent delivery of the Category A safety functions, an assessment within each area of the AP1000 plant as based on a set of criteria and assumptions is undertaken in light of both international and national guidance (References 11.4, 11.21, 11.22, 11.23, and 11.24). The detailed analysis which underpins this assessment is presented in full in Table 11.2-2. This fire analysis follows the guidance of Branch Technical Position (BTP) CMEB 9.5-1 (Reference 11.22) to evaluate the consequence of fires within the plant, document the capabilities of the passive and active fire protection features and evaluate the impact of fire on the delivery of Category A safety functions. The analysis was an integral part of the process of selecting passive fire protection methods, ventilation and smoke control, fire detection, alarm and suppression systems, and provides a design basis for the FPS. Chapter 8, Table 8A-2, lists the Class 1 SSCs claimed to mitigate design basis fires.

11.2.2 Internal Fire Claims, Arguments and Evidence

11.2.2.1 Claims Overview

This section presents the claims, arguments and underlying evidence made in relation to internal fire hazards with the potential to impact safe shutdown.

11.2.2.2 High Level Claim

An internal fire could cause a transient from normal operation of the reactor power plant with the potential to result in a hazard on or off site being realised. In response to such a transient, it may be necessary to shut down the reactor and return it to a safe state. Depending on the exact nature of the transient, there are a number of courses of action to take to shut the reactor down. Ensuring the availability of the Class 1 SSCs required to deliver the Category A safety functions will ensure that the reactor can be shut down and maintained in a safe state, and is the basis of the following high level claim.

Claim IH-1.0 **Postulated fire events within the design basis do not prevent the delivery of the Category A safety functions and the supporting post-72 hour Category B safety functions necessary to respond to postulated events.**

Within the design of the AP1000 plant, this has been achieved by:

- Minimising the fire hazard so far as reasonably practicable;
- Protecting redundant divisions of Class 1 SSC by segregation with the use of fire barriers where practicable;
- Protecting redundant divisions of Class 1 SSC by separation within the Containment ;
- The use of fail-safe equipment.

11.2.2.3 Prevention Claims

For the purposes of the design basis fire assessment, an internal fire is assumed to occur wherever combustible material is present; no claim is made on the absence of an ignition source. Therefore, the fire safety case does not utilise specific prevention claims to minimise the potential for postulated fire events.

Although it is not possible to preclude the possibility of a fire where combustible material is present, it is possible to minimise the severity of the fire by minimising the quantity and type of combustible material present.

Claim IH-1.1: **The internal fire hazard has been minimised so far as is reasonably practicable**

11.2.2.4 Protection Claims

Whilst it is not possible to protect the SSC present in the fire compartment, fire compartmentalisation has been used to protect redundant SSC.

Claim IH-1.2: **Class 1 SSCs will be protected from the direct or indirect effects of a fire by isolating the source of the fire**

Sub-Claim IH-1.2.1: **A postulated fire outside containment will not propagate beyond the fire area of inception; therefore, redundant Class 1 SSCs will not be disabled by a postulated fire event.**

Sub-Claim IH-1.2.2: **A postulated fire within containment will not propagate to the extent that it damages redundant safe shutdown components.**

Sub-Claim IH-1.2.3: **Penetrations through barriers do not degrade the fire withstand capability of the barrier itself.**

11.2.2.5 Mitigation Claims

The AP1000 fire safety case does not utilise mitigation claims by use of SSCs or operator actions.

11.2.2.6 Arguments and Evidence

Prevention Arguments and Evidence

Claim IH-1.1: The internal fire hazard has been minimised so far as is reasonably practicable

In the AP1000 design, the potential for a fire to affect Class 1 SSCs that are not located in the zone of the fire has been reduced by minimising the quantities, controlling the use, and providing appropriate storage of combustible materials. Significant quantities of combustible or flammable materials are not stored in the NI, and areas with high fire loads are segregated from areas containing Class 1 SSCs by appropriately classed fire barriers. Within the AP1000 design, the fire hazard has therefore been minimised by:

- Selecting materials for construction which are non-combustible, fire-retardant and fire resistant wherever possible (see Chapter 6);
- Minimising the fire loading;
- Segregating significant fire loads from areas containing Class 1 SSCs (i.e., the Nuclear Island).

11.2.2.7 Protection Arguments and Evidence

Claim IH-1.2: Redundant divisions of SSC will be protected from the direct or indirect effects of a fire by isolating the source of the fire

The AP1000 design utilises two principles to inhibit the spread of fire during a design basis event:

- In areas outside Containment, the plant is segregated into fire compartments, composed of one or more rooms within a plant area, separated by suitably rated fire barriers. The fire barriers are capable of withstanding a total burn of all combustible material within the fire area;
- Within the Containment, fire spread is prevented by providing adequate separation of equipment by distance or height (particularly for redundant Class 1 SSCs), and by the use of passive fire-protection features to partially segregate redundant SSCs.

Sub-Claim IH-1.2.1: A postulated fire outside containment will not propagate beyond the fire area of inception; therefore, except for the main control room, redundant Class 1 SSCs will not be disabled by a postulated fire event

Argument: The barriers which physically segregate fire areas are capable of withstanding, without failure, the complete burnout of all combustible material within the fire area

Based on a review of the layout of Class 1 SSC delivering Category A safe shutdown safety functions, the AP1000 NI has been sub-divided into a series of fire areas. To prevent the spread of fires, each fire area is enclosed by fire-resistant barriers which provide passive fire protection of the Class 1 SSCs located in other fire areas.Fire compartmentalisation is used extensively throughout AP1000 plant. The fire compartments are detailed in Table 11.2-1.

The Hazard Barrier Matrix (Reference 11.9) identifies the walls, floors, and ceilings forming the fire barriers in the NI, which together make up the fire compartments. The fire barriers separating safe shutdown equipment are constructed to withstand the complete combustion of the fire load within the fire compartment (full-room burnout) as determined in Reference 11.8, thereby preventing the fire from propagating across to, or otherwise causing direct or indirect damage to, materials or items on the sides of the fire barrier that are not directly exposed to the fire. This prevents the effects of a fire in one fire area from damaging redundant SSCs located in adjacent fire areas. Although, in the majority of cases, the walls, floors and ceilings of individual rooms are able to are to withstand the complete combustion of fire load within the room, no claim is made on the fire resistance rating of these internal walls, floors and ceilings.Substantiation (Reference 11.69) that the fire barriers are able to withstand the complete combustion of fire loading within the fire area has been undertaken, using the methodology described in EN 1991-1-2 (Reference 11.43), to confirm, by way of quantitative uncertainty analysis, that the fire loading is less than the claimed withstand of the fire barriers in all cases.

The effects of realistic fires have also been considered (Reference 11.69) and a comparison was made to the standard fire test time/temperature curve, as described in ASTM E119. The review concludes that, with the exception of an oil fire, the maximum hot gas layer temperatures are significantly below the ASTM E119 curve. Although the oil fire does initially exceed the ASTM E119 curve, suche a fire within the NI would self-extinguish due to a lack of combustible material before the peak temperature of the ASTM E119 curve is reached. Furthermore, the ASTM E119 curve is characterised by the ramp up rate of the furnace used for the test, rather than the properties of the test material and the initial exceedance is therefore not considered to be significant in terms of the barrier's ability to withstand the fire.

The sensitivity of the AP1000 plant to localised fires has been assessed (Reference 11.69). Although a number of instances were identified where adjacent fire areas contain redundant divisions of Class 1 SSC, the fire load in the adjacent rooms was determined to pose an insignificant challenge to the integrity of the fire barrier.

The fire barriers protecting Class 1 SSCs are themselves Class 1 structures and are rated for load-bearing capacity, integrity, and insulation as appropriate. A review (Reference 11.10) of the fire resistance rating for NI reinforced concrete (RC) structures demonstrates that the AP1000 design meets or exceeds the requirements of BS EN 1992-1-2 (Reference 11.11). For the composite steel-concrete (SC) walls, floors and ceilings, detailed heat transfer analysis (Reference 11.12) has been performed which demonstrates that their structural integrity is maintained following a three hour standard fire.

Detailed analysis of the fire segregation and separation approaches adopted in the AP1000 design has been undertaken. This demonstrates that the consequences of credible fires are shown to be acceptable.

Sub-Claim IH-1.2.2: A postulated fire within Containment will not propagate to the extent that it damages redundant safe shutdown components

It is assumed that, wherever combustible material is present, an internal fire may. Within containment, the only requirement is that the fire does not subsequently spread sufficient to damage the claimed redundant Class 1SSC.

For the effects of a fire to be communicated to adjacent fire zones, absent the cross-boundary influences of cabling to be examined on a site specific basis, the source fire needs to initiate a fire in the adjacent fire zone. As the in-Containment combustible loadings are low (in most

cases, integral to SSC designs) and the influence of non-combustible structural walls largely prohibit a direct interface between fire zones except for areas of personnel access, no credible locations for such a fire being transmitted between fire zones have been identified. However, for the purposes of assessing fire spread, it is noted that damaging effects of fire spread may be realised through flame impingement, via thermal radiation or due to exposure to smoke. These potential mechanisms are discussed below. It is noted that the mechanisms of flame impingement and thermal radiation require a direct line of sight between the source flame and the target combustible material.

If the combustible material in the adjacent fire zone is sufficiently close to the source flame, and in a suitable configuration, it may be possible for the fire to spread by flame impingement. Where this is not the case, fire spread may occur through radiative heat transfer. In order to ignite a target comprising combustible material by thermal radiation, it is necessary to raise the temperature of the target to at least its flash point[1]; otherwise it is necessary to raise its temperature to the auto-ignition temperature. It is recognised that the functionality of Class 1 SSC may be lost at a temperature below the auto-ignition temperature. However, the sensitivity of the design to this depends upon detailed analysis and final plant layout which will not be confirmed until detailed design. Should it be required, Class 1 SSC will be qualified to operate in elevated temperatures or protected by insulation.

Although smoke could damage Class 1 SSC, particularly sensitive electronic equipment, the vast majority of combustible material within containment is associated with the cable insulation and jacketing material. The cable insulation and jacketing materials have been selected to meet the fire and flame requirements of IEEE 1202 (Reference 11.37) or IEEE 383 (Reference 11.38) and as such are low smoke. Smoke is therefore not expected to be a significant hazard following a fire within Containment.

Argument: The physical segregation by partition between fire zones precludes surface ignition of combustible material

For surface ignition of combustible materials to occur, it is necessary for:

- A flame to impinge on the target; and,
- The thermal flux received to be greater than the target's critical flux or the target's temperature to be raised above its auto-ignition temperature.

Where present, the majority of fire zones in Containment are separated by a combination of non-combustible walls and ceilings/floors as well as spaces devoid of combustible material with recognition that there are some locations where cable trays cross zone boundaries; see the discussion below.

Flames spread by entraining sufficient air to burn the evolved volatiles; however, the exact behaviour of flames depends on a number of factors, many of which are the subject of detailed design (e.g. proximity of combustible material to the surrounding structures). The

[1] The flash point is the temperature at which flammable vapours are released in sufficient quantities to generate a flammable atmosphere. The combustible material will only continue to burn if either the flux imparted on the combustible material remains present or combustion of the flammable vapour/air mix imparts sufficient energy to maintain the process.

walls and ceilings/floors between fire zones will act to completely or partially confine the flame, and thus prevent fire spreading to combustible material located in adjacent fire zones.

The walls/floors which make up the rooms within the Containment are SC structures formed as pre-fabricated modules. As part of the demonstration of the structural integrity of the CA20 module for example, analysis has been undertaken (Reference 11.12) to determine the point at which the walls would fail. The theoretical fire necessary to compromise the CA20 module is significantly more onerous and requires significantly more combustible loading than that present in any of the individual Fire Zones (Reference 11.8). As such, it is not considered credible that an internal fire could degrade the structural partitions to the extent that they are no longer able to perform as required to separate combustible material between fire zones. In addition, the division B & D cabling is routed from the electrical penetration room (11306) to Fire Zone 1100 AF 11500 in a fully enclosed steel-composite chase, which will be tested in accordance with the requirements of BS EN 13501-3 (Reference 11.139) to confirm that the insulation provides a 3 hour resistance to a standard fire.

In areas where the flame is not confined (i.e. not touching a boundary wall/floor/ceiling), the horizontal spread will not be significantly different to the actual size of the combustible material itself. While flames can lean when exposed to air movement, the Containment is an enclosed structure and this phenomena is not considered to be a significant factor.

It is recognised that cables and cable trays may pass between fire zones and, as such, it is possible for fires to spread along cable insulation. In general, fire zones contain cabling associated with either Divisions A and C or B and D, and therefore a fire in one fire zone will not affect all 4 Divisions of Class 1 SSC. However, there are limited fire zones where all four divisions of PMS cabling may by routed together. In these instances, redundancy is provided by an alternative SSC. Management and design specifics of cable routing are the subjects of site specific licensing as per findings AF AP1000 IH 02 through IH 04 (Reference 11.137). In addressing these Assessment Findings, the exact routing of cables and the potential for cabling to detrimentally affect the internal fire safety case will be determined. At such time, assessments are expected which confirm this argument. Where required, design changes may be considered such as cabling routing to minimise the potential for fire spread or specifications of fire wrapped / stopped cable designs used to preclude the propagation of fire or cable trays fitted with fire blocking along the exposed cable route.

Hence, absent the detailed assessment of cable routing as the mechanism for flame spread, the physical segregation by partition between fire zones precludes surface ignition of combustible material in an adjoining fire zone.

Argument: **The separation distance between the heat source(s) and target combustible materials are sufficiently large, and the duration of the fires sufficiently short, that insufficient energy would be imparted to raise their temperature to the flash point; necessary for piloted ignition.**

An evaluation of combustible material (Reference 11.8) has identified that trash, paper, volatiles, lubricating oil and cable insulation may be present variously within Containment. Some of the identified combustible materials (trash, paper and volatiles) would be transient and subject to site specific management arrangements. It is likely that these arrangements would restrict their presence within Containment to plant modes 5 & 6 only (at a time when Containment is occupied), therefore in plant modes 1 to 4 the combustible inventory will be less than that quoted.

In the absence of direct flame impingement, where the target combustible material is a liquid (e.g. lube oil), the bulk temperature of material must be raised to the flash point for piloted ignition to occur, or the temperature increased to the auto-ignition temperature for spontaneous combustion. For solid combustibles (paper, trash & cable insulation), volatiles will only be released once the surface of the material starts to decompose.

Heat transfer between a heat source and the target is possible through a combination of conduction, convection and radiation. Where the heat source and the target are not connected, heat transfer by conduction is not possible. While convection will contribute to heat transfer, the greater proportion of heat received by the target will be through thermal radiation, provided the heat source and target are not physically obscured by a medium which absorbs the thermal radiation. The amount of heat transferred to the target by radiation will depend on the:

- Emissive power of the heat source;
- Spatial relationship of the heat source to the target (view or configuration factor);
- Length of time the source continues to emit radiation.

Flame temperatures in room fires generally have zones of 900 °C but wide spatial variations may be seen and the maximum value which is regularly found is approximately 1200 °C (see Chapter 10 of Reference 11.138). At this temperature, the emissive power at the surface of the flame would be approximately 290 $kW.m^{-2}$; the emissive power is proportional to the 4th power of flame temperature and would therefore be significantly less at lower temperatures.

The radiative energy transferred between the flame source and the combustible target will depend on the geometry and orientation of the two surfaces (Reference 11.138), as well as the presence of any intermediate barriers (either full or partial). Generally speaking, thermal radiation intensity follows an inverse square law with distance, so the greater the separation distance between the source and the target, the less radiative energy will be transferred to the target.

While the geometry of the source could be approximated based on the physical constraints of a fire zone, the geometry of the target and its relationship to the source (both in terms of distance and angle) would not be fully known until detailed design.

The source will continue to emit radiation until all combustible material has been consumed. By reducing the quantity of combustible material present within each fire zone, the duration for which radiation is emitted is also minimised. Based on the fire protection analysis (Reference 11.8), the majority of fire zones within Containment have an equivalent fire duration of less than 10 minutes, with a maximum duration of 24 minutes[2].

Given this, the potential for a fire to propagate from one fire zone to another by means of heat transfer is likely to be minimal due to the short duration for which the effects of a fire in one

[2] It is recognised that the equivalent fire durations have been determined using the methodology described in the NFPA handbook, and that in some respects this may not be conservative. However a comparison (Reference 11.69) using the method described in EN 1991-1-2 (Reference 11.43) has been performed for Fire Areas outside of containment, which shows that for rooms containing just cable insulation the Eurocode derives a fire duration which is approximately 50% longer.

fire zone will exist and the extent to which those effects will have diminished before they are transmitted to the target combustible material in an adjacent fire zone.

Sub-Claim IH-1.2.3: Penetrations through barriers do not degrade the fire withstanding capability of the barrier itself.

Argument: Penetrations through fire barriers are fire-stopped to the same qualifications as the barrier through which they pass.

The number of penetrations (e.g. cabling, ventilation, pipework and doorways) through fire barriers (see Reference 11.9) have been minimised so far as is reasonably practicable. Where possible, penetrations through Class 1 barriers adjoining rooms containing redundant divisions of Class 1 SSC have been avoided.

The penetration seal schedule (Reference 11.13) provides details of all penetrations passing through walls and floors. In accordance with the AP1000 fire protection design criteria and guidelines (Reference 11.64):

- Penetrations through fire barriers will be qualified in accordance with Reference 11.15 to meet the requirements of BS EN 1366 Part 3 (Reference 11.16);
- The number of openings and penetrations in exterior fire barrier walls of safety-related buildings will be minimised.

In order to minimise the number of openings, the AP600 architectural design criteria[3] (Reference 11.140) stipulates that, where possible, multiple commodities should be grouped into a single opening to minimise the number of barrier penetration. Furthermore, the AP1000 plant design criteria (Reference 11.141) set out the requirements to develop a design that:

- Uses the minimum number of SSCs
- Requires the minimum amount of instrumentation, control functions and control loops.

In satisfying these design criteria, the AP1000 plant has minimised the number, and combined size of penetrations through barriers, including fire barriers.

In addition to penetrations, the AP1000 HVAC system passes through fire barriers. As such the HVAC system incorporates fire, smoke and combination fire/smoke dampers to prevent the propagation of fire and/or smoke to adjacent fire areas (Note: the containment shield building is a single fire compartment and ventilation dampers do not restrict the movement of air). Based on a review of ventilation dampers (Reference 11.17), all Class 1 barriers are fitted with redundant combination fire/smoke dampers. The combination fire/ smoke dampers, and associated ductwork up to the fire barrier, will be tested in accordance with BS EN 13501-3 (Reference 11.139) to demonstrate that they have a fire rating at least equivalent to the barrier through which they pass (e.g. 3 hours). The dampers will comply with the relevant parts of BS ISO 10294 (Reference 11.18), and shall be tested in accordance with the requirements of BS EN 1366-Part 2 (Reference 11.19).

[3] The AP600 is the predecessor to the AP1000 and as such the design philosophy was carrier forwards into the AP1000.

Fire doors are fitted with self-closing mechanisms to ensure that they return to the closed position when not in use. The fire doors themselves, including surround, will be qualified in accordance with BS 476: Part 24 (Reference 11.20) to provide the same fire resistance as the barrier through which they pass. In all but the following five instances, a fire would have to pass through two fire doors in order to affect redundant Class 1 SSC in a given fire area. In these five instances, the fire doors are fitted with Portal Access Controllers which monitor the door. In the event that the door is opened, and remains open for a prolonged period[4], an alarm is generated in the MCR. The Portal Access Controllers and associated alarms are Class 2 on the basis that they support the Category A safety function which is principally delivered by the fire barriers and doors. The following doors are fitted with Portal Access Controllers:

- APP-12303-AD-D01;
- APP-12304-AD-D01;
- APP-12305-AD-D01;
- APP-12423-AD-D01;
- APP-12422-AD-D01.

11.2.3 Internal Fire Safety Case Summary

11.2.3.1 Introduction and Overview

The safety design approach adopted for internal fire consists of a range of complementary design features. These are applied as appropriate to individual items of equipment or systems to prevent a fire from occurring, contain a fire to its area of origin or prevent it from propagating to protect Class 1 SSC from the effects of fire. Suitable and sufficient design features and measures are identified such that a postulated fire within the design basis, does not prevent delivery of the Category A safety functions. An assessment within each area of the AP1000 plant based on a set of criteria and assumptions is undertaken in light of both international and national guidance (References 11.4, 11.21, 11.22, 11.23, and 11.24) and the detailed analysis which underpins this assessment is presented in full in Table 11.2-2.

11.2.3.2 Applicable Codes and Standards

The internal fire hazard analysis has been undertaken in accordance with NFPA guidance (Reference 11.33), to determine the fire loading and equivalent fire duration of those combustible materials present within the plant. A comparative review has been undertaken (Reference 11.69) in accordance with BS EN 1991-1-2 (Reference 11.43), which is considered relevant good practice, the results of which form the basis of the safety assessment.

The Equivalence/Maturity Study of U.S. Codes and Standards (Reference 11.25), identifies applicable codes and standards. It also provides a clear and auditable demonstration that all

[4] The prolonged period is set by the utility, although it is intended that the 'grace period' corresponds to the length of time required for an operator to traverse the boundary of the room.

codes and standards to support the design substantiation of UK Class 1 and 2 SSCs have been identified.

To evaluate the AP1000 design's codes and standards against the UK expectations, the codes and standards applicable to the AP1000 design have been organised by the relative safety significance of the SSCs to which they have been applied. To support this organisation, the UK Safety Categorisation and Classification Methodology (Reference 11.26) describes the process for categorisation of safety functions and classification of SSCs, which indicate the significance of an SSC to deliver the relevant safety function.

Fire Barriers

The fire resistance rating of claimed fire barriers constructed from reinforced concrete have been determined in accordance with ACI 216.1 (Reference 11.45). A comparison (Reference 11.10) to BS EN 1992-1-2 (Eurocode 2) (Reference 11.11) has been undertaken to confirm that the fire resistance rating of claimed fire barriers remains valid when compared to UK codes and standards.

For SC structures, there are no codes and standards against which comparison can be made. Instead, detailed heat transfer analysis has been performed (Reference 11.12) to demonstrate the suitability of these structures when exposed to a 3 hour fire.

The UK AP1000 plant fire barriers are designed in accordance with BSI and IAEA guidance (References 11.4 and 11.23).

Fire Compartment Penetrations

Fire dampers and doors penetrating fire barriers are also fire rated for integrity and will comply with the relevant parts of the appropriate standards (References 11.44 and 11.46). UKP-GW-AF-001, "AP1000 Fire Protection Dampers – UK Compliance Report" (Reference 11.17) demonstrates that the AP1000 design conforms to appropriate BS EN codes and standards.

All penetrations within barriers will be fire stopped in accordance with relevant and appropriate BS EN standards such as BS9999 (Reference 11.4) and relevant industrial standards as described in the Association of Specialist Fire Protection (ASFP) Grey and Red Books (References 11.48 and 11.49).

Provision of Redundant Systems

The detailed fire assessment included as part of this report identifies the Category A, Class 1 components used for safe shutdown and the safety functions that they deliver (Tables 11.2-2 and 11.2-3). Where there is the potential for the Class 1 safe shutdown SSCs to be compromised by fire, redundant Class 1 safety equipment has been identified such that all Category A safety functions continue to be supported. This redundancy has been incorporated into the design taking into account the following:

- IAEA-NS-G-1.7 "Protection against Internal Fires and Explosions in the Design of Nuclear Power Plants" (Reference 11.23).
- IAEA NS-R-1, "Safety of Nuclear Power Plants: Design" (Reference 11.21).
- BTP CMEB 9.5-1, "Guidelines for Fire Protection for Nuclear Power Plants" (Reference 11.22).

- NFPA 804, "Standard for Fire Protection for Advanced Light Water Reactor (ALWR) Electric Generating Plants," 2010 (Reference 11.33).

Automatic Fire Protection System

The design philosophy for the FPS is in accordance with the guidance provided in IAEA-NS-G-1.7 (Reference 11.23) and as a minimum the FPS system is designed in accordance with the appropriate standards, such as BS 5839-1 (Reference 11.54), to provide comprehensive coverage and appropriate protection for the fire hazards identified. No safety case claim is made on the FPS.

11.2.3.3 Redundancy, Segregation, and Separation

Redundancy

In the event of a fire within any fire compartment forming part of the AP1000 plant (fire area within the Auxiliary Building and fire zone within the Containment), it is pessimistically assumed that all SSCs fail within that area. In general, this might result in the safety function(s) supported by the equipment within that fire compartment no longer being delivered and/or spurious actuations that may have a negative impact on plant safety. Therefore, in order that no safety functionality is lost, the AP1000 plant is designed such that:

- No single SSC failure can result in the failure to deliver the Category A safety functions.
- No spurious activation can cause erroneous actions that may have a negative impact on plant safety.

These two areas of design are discussed in the following subsections.

Provision of Redundant Systems

The detailed fire assessment (Reference 11.73) identifies the Class 1 safe shutdown SSCs and the safety functions that they deliver (Tables 11.2-2 and 11.2-3). Where there is the potential for the Class 1 safe shutdown components to be compromised by fire, redundant Class 1 safety equipment have been identified such that all Category A safety functions continue to be supported.

The availability of redundant equipment during a design basis fire is ensured either through use of SSCs that are qualified to withstand the effects of the fire hazard or by the controlling the spread of fire hazards through segregation and separation (e.g. by Class 1 fire barriers). These approaches ensure that no other redundant train of equipment is susceptible to the same fire.

Defence in Depth

The internal hazards nuclear fire assessment has taken no credit for the Class 2 systems that provide defence in depth for Category A safety functions, The assessment pessimistically assumes that all Class 2 systems providing Category A safety functions are unavailable, and therefore, the assessment identifies redundant Class 1 equipment in order to fulfil the safety function.

However, in practice, duty systems and Class 2 defence in depth systems are used to control abnormal conditions, should they be available, to reduce the demand on the high integrity Class 1 systems.

Prevention of Spurious Actuations of Equipment

An assessment of multiple/simultaneous spurious actuations or signals resulting from the fire leading to electrical power supply failure faults and spurious component actuations was undertaken in the AP1000 Fire Induced Multiple Spurious Actuation Report (Reference 11.56), in which components were assumed to be energised or de-energised by one or more circuit faults.

The assessment concludes that either spurious actuations do not occur, or the consequences are such that they do not prevent delivery of the Category A safety function and the Category B support functions. Principal spurious actuations are discussed below.

High-Low Pressure Interfaces

High-low pressure interfaces between the RCS and interfacing systems, such as the RNS, typically contain two redundant and independent motor-operated valves in series. On a typical PWR plant, these two valves and their control and power cables may be subject to a single fire and therefore warrant specific identification; this is considered below for the AP1000 design. Potential high-low pressure system interfaces of particular interest are discussed below. Additional discussion is contained in UKP-GW-GLR-111, "UK AP1000 Internal Hazards Topic Report – Fire Protection" (Reference 11.73).

- RCS Valve Actuation:

  Nuclear Regulatory Commission (NRC) Generic Letter 81-12 (Reference 11.57) specifically addresses the reactor coolant/residual heat removal system interface on PWRs. For the AP1000 design, the RCS to RNS interface is similar to the typical PWR configuration. However, the RNS is not a Class 1 system and is not required for safe shutdown. To preclude the spurious opening of the interface valves as a result of a fire, the power to the valves is locked out during power operations. Thus, spurious actuation of the RCS to RNS interface valves does not occur and the safe shutdown capability is not affected. In addition, the RCS to RNS interface contains a third isolation valve whose power is locked out during power operations and which is segregated from the first two valves. Finally, the RNS design pressure has been upgraded so that RCS pressure would not rupture the RNS if the two systems were connected inadvertently or as the result of a spurious valve actuation.

- ADS Valve Actuation:

  The ADS valves are not considered to be high-low pressure interface valves when postulating spurious actuations following a fire. The concern is that the spurious opening of two or more isolation valves forming the boundary between the RCS and a low pressure system could lead to damage to the low pressure system and a loss of coolant outside the Containment. Since the ADS valve actuation cannot damage a low pressure system, and since the system is entirely within Containment, the ADS valves do not represent a high-low pressure interface.

  Spurious actuation of the ADS stage 4 squib valves, as a result of fire, is prevented by the use of a squib valve controller circuit controlled by the AP1000 PMS which requires multiple simultaneous hot shorts for actuation. In the event of a fire affecting one of the PMS interface cabinets the operator is able to remove the power from that electrical division, although failure to do so does not lead to spurious actuations in other PMS interface cabinets.

ADS stages 1, 2, and 3 consist of parallel paths, each path having two motor-operated valves in series. Spurious actuation of stages 1, 2, or 3 is prevented by the use of physical separation of control circuits for the two series valves and provisions for operator action to remove power from the affected fire zone. No fire was identified which could spread to both sets of ADS stage 1, 2 and 3 valves or both sets of the ADS stage 4 squib and block valves. In addition the ADS 4 squib valve initiation charge and propellant have been shown to not initiate due to a localised fire (Reference 11.147).

- RCS Reactor Vessel Head Vent Valve Actuation:

  The reactor vessel head vent valves are connected to the reactor vessel head and discharge to the IRWST. The head vent valves are not required to operate following a fire. There are four head vent valves arranged in two flow paths with two series valves in each path. The head vent valves are fail-closed dc powered solenoid valves, and each valve is powered by a separate, Class 1 power supply. In the unlikely event that a spurious signal was to open a head vent valve, the flow path is blocked by the closed series head vent valve.

  The head vent valves are controlled from switches mounted on the primary and secondary dedicated safety panels in the control room. Each safety panel contains a switch for controlling each head vent valve.

- Other Spurious Actuations

  Principal spurious actuations not involving high-low pressure interfaces are discussed below.

  – PXS PRHR HX Valve Actuation:

    One normally open valve is provided to isolate the inlet line to the PRHR HX. To preclude the spurious closing of the inlet valve as a result of a fire, the power to the valve is locked out during power operations. Therefore, spurious closing of the passive core cooling PRHR HX inlet valve does not occur and the safe shutdown capability is not affected.

    Two normally closed air operated globe valves, in parallel, are provided to isolate the outlet line from the PRHR HX. Spurious actuation of either of these valves could result in reactivity insertion (see Chapter 8). However, the Class 1 SSC required to achieve a safe shutdown are not affected by the same fire, and therefore the safe shutdown capability is not affected (see Table 11.2-2).

  – PCS Valve Actuation:

    Two valves in series isolate each of the three discharge flow paths from the PCS storage tank. For the purposes of system reliability, one valve in each flow path is normally open and the other is normally closed.

    Spurious actuation of one of these valves is assumed to occur where a fire affects its electrical circuitry. Such a fire can occur in the MCR, an electrical equipment fire area, in the PCS valve room, or in fire areas or fire zones through which the applicable electrical cables are routed.

    Spurious actuation of one of these valves causes a PCS flow path to be disabled or inadvertently opened, depending on which valve is affected. If a normally closed

valve spuriously opens, PCS water delivery from that flow path will be initiated which does not adversely affect the capability to achieve and maintain safe shutdown. If one of the normally open valves were spuriously closed to prevent PCS water delivery through that flow path when called upon during the safe shutdown process, the redundant PCS water delivery flow paths would be sufficient to achieve and maintain safe shutdown.

Segregation

Within the AP1000 design, redundant divisions of Class 1 SSC are segregated from one another such that a fire cannot result in the loss of all divisions.

The AP1000 design utilises two principles to inhibit the spread of fire during a design basis event:

- In areas outside of Containment, the plant is segregated into fire areas composed of one or more rooms. Fire areas are segregated from one another by credited fire barriers, capable of withstand the complete burn of all combustible material present within the given fire area.

- Due to limitations on equipment positioning and routing, and the requirements of the PCS to maintain the free movement of gases and liquids, the Containment represents just one fire area. The Containment is instead divided into fire zones determined by a zone of influence. The potential for fire to spread from one fire zone to another is minimised by maximising the separation, horizontal distance or height (particularly for redundant trains of safety systems), and by the use of partial structural barriers to separate redundant divisions of Class 1 SSC, so far as is reasonably practicable.

An assessment of the adequacy of the segregation and separation design philosophy for AP1000 design forms part of the detailed assessment of individual fire areas presented within the topic report (Reference 11.73).

The location and fire resistance rating of the fire barriers is identified in the Hazard Barrier Matrix (Reference 11.9). Of note regarding these barriers:

- The walls, floors, and ceilings of fire compartments in the NI are surrounded by fire-resistant barriers. The fire barriers are constructed to withstand the complete combustion of the fire load within the enclosure (full-room burnout), thereby preventing the fire from propagating across to, or otherwise causing direct or indirect damage to, materials or items on the sides of the fire barrier that are not exposed to the fire. This prevents the effects of a fire in one compartment from damaging redundant SSCs located in adjacent fire compartments.

- Primary fire area barriers protecting Class 1 SSCs are themselves Class 1 structures and are rated for load bearing capacity, integrity, and insulation. Other fire barriers are fire rated for integrity and insulation only. In all other fire areas, the fire resistance of fire barriers is specified based on the fire load and the calculated fire severity of the fire area.

- With the exception of stairwells and elevator shafts, which are rated for 2 hours, all fire areas within the NI are all 3-hour fire compartments, except for the MCR room, where the ceiling is only credited as a fire barrier in one direction; instead, which provides adequate 3 hour fire barrier protection against for the MCR from a fire originating in the room above. These barriers are Class 1 SSCs. This is discussed in detail in the relevant

part of the non-radiologically controlled Auxiliary Building assessment within this report and assessed as adequate. Although there are no Class 1 SSCs located outside of the NI, many of the fire areas in these other buildings also form fire –resistant compartments, but these are not nuclear Class 1 barriers.

- In instances where fire severity is estimated to be greater than three hours (such as locations with a significant oil inventory), 3-hour barriers are specified, and additional active fire protection systems are installed so that the barrier are not compromised. Such barriers occur within the turbine, annex, and DG buildings, and do not occur within the NI. A fuel oil pool fire in these areas does not threaten the Category A safety function, even in the event that the active fire protection systems fail to operate (Reference 11.69). The adequacy of the fire barriers to withstand full-room burn out is presented as part of the AP1000 design assessment discussed in the topic report (Reference 11.73).

- Penetrations in fire compartment barriers including ventilation ductwork, cables and pipework, are minimised in barriers separating redundant divisions of Class 1 SSC, and fire stopped to the same fire resistance as the barrier they penetrate to reduce the potential for the spread of fire. Additionally, where vent ductwork passes between fire areas containing redundant divisions of Class 1 SSC, dual redundant combination fire/smoke dampers are provided in accordance with the requirements of the single failure criterion (Reference 11.17).

Separation

Where the segregation of fire areas by a fire-rated full enclosure is not practicable for functional reasons, Class 1 SSCs are separated by distance (horizontal and vertical) to the maximum extent practicable.

Within the Containment, the segregation and separation of Class 1 safety systems is considered. For each postulated fire hazard that can arise in the Containment, it is shown that design basis events cannot affect more than one train of redundant Class 1 SSC and that these SSC remain unaffected and are therefore available to deliver the required Category A safety function to safely shut down the reactor. There are a few specific instances where all Divisions of Class 1 SSC could be affected, however the assessment has shown that alternative means of delivering the Category A safety functions remain unaffected (Reference 11.73).

Inside the Containment, fire compartmentalisation cannot be provided because of the need to maintain the free exchange of gases and liquids for purposes such as passive Containment cooling. Instead, the Containment is a single fire area encompassing the entire building and is a 3 hour fire compartment. Within this fire area, fire zones are identified that establish each zone of influence; i.e., the extent to which a fire originating within any given location can spread and cause damage to equipment. Fire resistant barriers are incorporated where practicable to minimise fire spread beyond the fire zone via radiated and conducted heat. Detailed analysis of each arrangement is discussed in the topic report (Reference 11.73), which demonstrates that the consequences of fires are shown to be acceptable.

11.2.4 Internal Fire Assessment Approach

11.2.4.1 Identification of Fire Sources

The fire protection analysis presented in the topic report (Reference 11.73) details, on a fire area by fire area basis, the type and quantity of combustible material inherent in the AP1000

design. In accordance with relevant international guidance (Reference 11.23), a single fire is assumed to occur at any one time wherever there is combustible material present (i.e., no credit is taken for the apparent absence of ignition sources).

Assumptions

The fire-related assumptions used in the assessment of the design are of three types:

- Design basis fire assumptions.
- Design assessment assumptions.
- Initiating event and fault progression assumptions.

Design Basis Fire Assumptions

- Only a single, independent fire is assumed to occur in any plant location.

- An independent fire is not assumed to occur simultaneously with the most severe natural phenomena, e.g., tornadoes, flooding or earthquakes or during other internal initiating events such as Loss of Coolant Accidents (LOCA) or loss of off-site power. Combined hazard evaluations are presented in Section 11.12.

- The fire is assumed to occur under worst case normal plant conditions for the initiating fire which may include such states as loss of a redundant train for maintenance purposes or under early shutdown conditions when the systems are pressurised.

- Fire spread to adjacent fire areas is only discounted where adequate fire resistant barriers (and their penetrations) appropriate to the fire hazard are provided.

- Fire spread to adjacent fire zones within Containment is only discounted where adequate fire separation and or passive fire protection features are provided.

- A design basis fire is a credible initiating event for other internal hazards such as internal explosions, internal floods or loss of off-site power (the combined consequential effects of which are discussed in Section 11.12).

- Consequential fires, generated as a result of other internal initiating events, such as explosions are discussed in Section 11.12.

Design Assessment Assumptions

- Only Class 1 SSCs are assumed to be available to deliver Category A functions with no benefit claimed for available duty systems unaffected by the fire.

- A concurrent single active component failure (independent of the fire) is considered within the design assessment.

- FPS is available to detect fire and extinguish fires but no credit is taken for active systems to control or extinguish fire (no safety case claim made).

Initiating Event Assumptions

- Only a single, independent fire is assumed to occur in any plant location whether or not the area contains in situ combustible materials or any credible ignition sources are present.

- The fire leads to full room burn out damaging all equipment immediately within the fire area (or fire zone within Containment) even where normal operation of equipment (e.g., fire suppression systems) or movement of valves within the fire area would mitigate potential consequences.

- Re-entry into the affected fire area for repairs and operator actions is not considered when assessing consequences of plant safety.

- Where 3 hour fire resistant (integrity and insulation) passive fire protection features are used to protect electrical cables or ducts that only pass through the affected fire area, these are not included in the consequence assessment.

- Inside Containment, only SSCs beyond the zone of influence of the fire are assumed to be unaffected by smoke.

11.2.4.2 Fire Assessment

Each fire compartment has been assessed to determine:

- The potential for fire, and the fire severity, based on the fire loading.
- The segregation or separation between redundant divisions of Class 1
- Adequacy of redundant Class 1 SSCs required in delivering the Category A function.
- Ventilation system design to minimise fire spread.

This assessment is undertaken in the light of both international and national guidance as discussed above, reported in full in the topic report (Reference 11.73), and is achieved through the following:

- Deterministic assessment of fire within each individual fire compartment for each of the plant areas:

  – Containment.
  – Shield building.
  – Non-Radiologically Controlled Area of the Auxiliary Building.
  – Radiologically Controlled Area of the Auxiliary Building.
  – Turbine building.
  – Annex building.
  – Diesel Generator building.

- Identification of the combustible load within each fire area and, where appropriate, analysis of concentrated fire loads and the locations of these in relation to Class 1 SSCs within that area. For fire in areas containing radioactive materials, the capability to minimise and control a potential release of radioactivity is specifically addressed.

- Identification of Class 1 SSCs located within the fire area.

- Identification of the provision of segregation of Class 1 SSCs by fire compartmentalisation, other passive fire protection features or the separation by distance within each fire area (or fire zone within Containment) so as to demonstrate that a fire cannot spread to more than one train of Class 1 SSCs.

- Assessment of the provision of redundancy in the event of the postulated fire, demonstrating that alternative means of providing the Category A safety functions is maintained during and after this event so far as is reasonably practicable. This analysis also seeks to demonstrate that no design basis fire can result in the failure of multiple redundant trains of safety equipment. The potential for consequential loss as a result of fire spread is also considered.

Because of the roles the ventilation plays in preventing fire spread and maintaining plant habitability, control of fire and smoke spread via the ventilation system is specifically assessed to demonstrate that no design basis fire can result in the failure of multiple redundant trains of safety equipment.

The potential for a postulated fire to impact upon the plant control room areas is assessed due to the importance of these areas in ensuring the safety of plant operators and controlling the plant during design basis and beyond design basis faults.

11.2.4.3 Interface with Other Internal Hazards

The internal fire hazards assessment (Reference 11.73) considers, on a deterministic basis, a single fire event and the consequential impact on SSC in the affected plant areas.

The consideration of credible combinations of internal fire with other postulated internal hazards likely to occur independently of fire is considered in Reference 11.75. This reference provides a coherent approach across all internal hazard types (e.g., fire, explosion, missiles, dropped loads, pressure part failure). This is discussed in Section 11.12.

Combinations of independent internal and external hazards are considered to be Beyond Design Basis events and as such have not been explicitly considered in this section. However, compliance with relevant equipment and structural design codes ensure that combinations of internal hazards with the relevant abnormal operating occurrences (including environmental hazards) are addressed.

11.2.4.4 Conclusions

The assessment of internal fire hazards for the AP1000 plant has been completed and documented in the internal hazards fire protection internal hazards topic report (Reference 11.73) and the hazard schedule (see Tables 11.2-2 and 11.2-3). The assessment was an integral part of the process of selecting fire protection barriers, equipment and systems and provides a design basis for the FPS. The internal fire assessment demonstrates that a postulated fire does not prevent delivery of the Category A safety functions.

11.2.5 Internal Fire Analysis and Assessment

11.2.5.1 Introduction

This section presents a summary of the results of the fire hazard analysis of the AP1000 design.

11.2.5.2 Identification of Fires

A fire protection analysis (Reference 11.58) has been prepared detailing, on a room by room basis, the type and quantity of combustible material present as part of the AP1000 design. In accordance with relevant international guidance (Reference 11.23), a single fire is assumed to occur at any one time wherever there is combustible material present (i.e., no credit is taken for the apparent absence of ignition sources). The fire areas or zones are detailed in Table 11.2-1

11.2.5.3 Assessment of Fires

The fire protection analysis (Reference 11.58) provides a detailed assessment of fire hazards.

Outside of the Containment building, the AP1000 plant is broken down into a series of fire areas as defined in the Hazard Barrier Matrix (Reference 11.9). A fire is not considered to propagate beyond the confines of the fire area in which it initiates, based on the substantiation of fire barriers (References 11.10, 11.12, and 11.69). Inside the Containment Building, it is not possible to provide complete segregation of fire zones owing to the need to maintain the free exchange of gases for purposes such as passive containment cooling. Instead, the fire zones are separated by distance or passive structures which will limit the zone of influence of the fire to the fire zone in which it initiates.

The basis of the fire hazard analysis is that all SSC within a fire area (or fire zone within the Containment Building) are damaged sufficient to inhibit further operation.

11.2.5.4 Hazard Schedule

The internal fire hazard schedule (see Tables 11.2-2 and 11.2-3) has been prepared based on the fire hazard analysis.

The internal fire hazard schedule presents, for each fire area (or fire zone), the:

- SSCs affected by the fire along with the Category A safety function at risk
- Potential unmitigated consequences should the plant be unable to effect safe shutdown
- Details of any protected redundancy
- Fault conditions (see Chapter 8) for which the fire has been identified as a potential initiator.

The schedule is presented in tabular form providing a concise and comprehensive summary of the postulated fires, their significance and how the AP1000 plant is designed to cope with the hazard.

11.2.5.5 Discussion of Results

A detailed fire hazard analysis has been undertaken. The analysis details, by fire compartment, those Class 1 SSC which would be affected and the adequacy of redundant SSC to deliver Category A Safety Functions in support of safe shutdown. The following sections present a summary of the analysis.

11.2.5.5.1 Containment/Shield Building

The Shield Building, part of the NI, is a Class 1, 3-hour credited fire barrier which separates it from the Auxiliary Building. Within the Shield Building is the steel containment which is the containment vessel. The structure and the construction of both of these are discussed in detail in Chapter 16.

For fire segregation purposes the Containment and Shield Building comprises one fire area (designated 1000 AF 01) and includes the spaces inside Containment as well as the valve room for the PCS, the middle annulus, the upper annulus, and the operating deck staging area outside Containment.

The Containment/Shield Building comprises a series of fire zones separated from one another using a combination of distance and physical structures, which inhibit fire propagation. Many of the fire zones (e.g., each of the SG rooms) form significant physical barriers from other fire zones for much of their height. However, complete segregation cannot be achieved inside Containment given the need to maintain the free exchange of gases for purposes such as passive Containment cooling.

Within the detailed fire hazard analysis (Reference 11.73), it is assumed that a fire within a fire compartment affects all equipment within it (including the Class 1 SSCs) and the impact to delivery of the Category A safety functions is assessed. A review of in Containment fires has been undertaken (Reference 11.14), which identified the following eight instances where redundant divisions of Class 1 SSC are located in adjacent fire zones:

- The core exit thermocouples located in 1100 AF 11500 are redundant to the excore detectors in 1100 AF 11105.
- Divisions A and C of the Hot Leg 1 & 2 flow instrumentation are located in 1100 AF 11204 with the redundant Divisions B & D located in 1100 AF 11301 and 1100 AF 11302 respectively.
- Divisions A and C of the IRWST level instrumentation are located in 1100 AF 11300B with the redundant Divisions B & D located in 1100 AF 11300A.
- Divisions A and C of the Steam Generator 2 wide range level instrumentation are located in 1100 AF 11300B with the redundant Divisions B & D located in 1100 AF 11300A.
- Divisions A and C of the pressuriser pressure and level instrumentation are located in 1100 AF 11300B with the redundant Divisions B and D located in 1100 AF 11500.
- The reference leg temperature instrumentation located in 1100 AF 11300B and the Reactor Coolant System (RCS) temperature instrumentation located in 1100 AF 11301 and 1100 AF 11302 are redundant.
- Division A of Automatic Depressurisation System (ADS) valve stages 1, 2 and 3 are located at 1100 AF 11303A with the redundant Division B ADS valve stages 1, 2 and 3 located in 1100 AF 11303B.
- Divisions A and C of the IDS electrical cable penetrations are located in 1100 AF 11300B with the redundant Divisions B and D located in 1100 AF 11500.

The analysis concludes that, in all eight instances, the separation between the adjacent fire zones minimises the potential for fire to spread to the extent that redundant divisions of Class 1 SSC are affected by a single fire. Given this, the Category A safety functions necessary for achieving a safe shutdown can be delivered following a design basis fire within Containment.

In addition to the potential impact on the delivery of Category A safety functions, fire has been identified as an initiator to a number of faults (see Table 11.2-2). In all instances, the fire zone in which the fault is potentially initiated is separate from the fire zone containing the Class 1 SSC necessary to safeguard against the unmitigated consequences of the fault (see Chapter 8).

11.2.5.5.2 Auxiliary Building – Non-Radiologically Controlled Areas

The non-radiological area of the Auxiliary Building comprises the portion of the NI to the north of the Containment. The building houses SSCs associated with the auxiliary functions that do not directly involve radioactive material but have been designed to meet their nuclear safety functions.

For fire segregation purposes, the Auxiliary Building is segregated into a series of fire areas each of which is enclosed by a 3 hour fire barrier(s). The fire barriers are designed to inhibit the propagation of fire from one fire area to another. Ventilation ductwork which passes through a Class 1 barrier separating redundant divisions of Class 1 SSC are fitted with dual redundant combination fire/smoke dampers. These damper arrangements ensure that the ventilation penetration is not a potential source of single failure leading to the loss of redundant divisions of Class 1 SSC.

In the detailed fire hazard analysis (Reference 11.73) it is assumed that a fire within a given fire area affects all equipment within it (including the Class 1 SSCs) and the potential impact to the delivery of the Category A safety functions is assessed. Given the physical segregation, and the redundancy provided, the Category A safety functions can be delivered following a fire.

11.2.5.5.3 Auxiliary Building – Radiologically Controlled Areas

The radiologically controlled part of the Auxiliary Building, located to the south side of the Containment, is designed to handle and store nuclear fuel outside of Containment as well as holding the intermediate level radioactive waste, in the form of filters and spent ion exchange resin, and containing elements of the liquid and gaseous radwaste systems.

In the detailed fire hazard analysis (Reference 11.73) it is assumed that a fire within a given fire area affects all equipment within it (including the Class 1 SSCs) and the impact on delivering the Category A safety functions is assessed. Given the physical segregation, and the redundancy provided, the Category A safety functions can be delivered following a fire.

The radiologically controlled areas of the Auxiliary Building contain radioactive material which may be exposed to the effects of an internal fire hazard, and therefore there is the potential to release radioactive material. From the fire hazards analysis, it is concluded that, for there to be a release of radiological material, the fire would have to breach vessels/ pipework, which is considered to be unlikely. A release of radiological material from the radiologically controlled areas of the Auxiliary Building is therefore considered unlikely.

Additionally, the ventilation fire or combination fire/smoke dampers on the exhaust ductwork are located externally to the wall. This arrangement minimises the maintenance burden and potential radiological risk to the workers.

Therefore a fire initiating in an individual fire area within the radiologically controlled area of the Auxiliary Building will not prevent delivery of the Category A safety functions required to effect and maintain safe shutdown or present a significant direct radiological hazard.

11.2.5.5.4 Areas outside the Nuclear Island

There are no Class 1 SSCs located in buildings outside of the NI. The fire hazard analysis shows that a fire initiating in a fire area outside of the NI will have no impact on Class 1 SSC. Therefore a fire initiating in an individual fire area outside of the NI will not prevent delivery of any Category A safety functions required to effect and maintain safe shutdown.

11.2.6 Sensitivity of Results and Cliff Edge Effects

The fire hazard analysis assumes that a single fire will occur wherever combustible material is present. That is to say that no account is taken for the probability of whether or not a fire will occur. The results are therefore not sensitive to event frequency.

Further, the analysis assumes that all SSC present in the affected fire compartment are unable to perform their Category A safety functions but that the fire will not propagate between fire compartments due to the respective segregation and separation. The following sensitivity considers the potential for a fire to propagate between fire compartments and the significance of this.

Within the Containment/Shield Building, it is not possible to provide discrete fire areas separated by fire barriers owing to the need to maintain the free exchange of gases and liquids for purposes such as passive Containment cooling. Given that the Containment/Shield Building houses the reactor vessel and associated primary circuit, it is inevitable that all divisions of Class 1 SSC providing some Category A safety functions are present in some locations and therefore potentially at risk of fire damage. It is not considered reasonably practicable to further reduce the risk of a fire propagating between the fire zones. On this basis, a sensitivity analysis within the Containment has not been carried out as it is considered to offer no benefit.

Propagation of Fire between Fire Areas

The fire load in each Fire Area has been calculated (Reference 11.8) based on the estimated quantity and type of combustible material present in similar plant areas for commercial nuclear power plants and these values adjusted to account for the design of the AP1000 plant. In addition, an amount of ‘transient material’ has been allowed for during outage and refuelling operations.

The fire load assumes that the combustible material is evenly spread over the floor area of the Fire Area/Zone. Where a Fire Area comprises more than one Fire Zone, the severity of fire from the combustible material within one Fire Zone may be higher than the average contribution to the whole Fire Area. The fire loading and duration for each individual fire zone has been calculated as well to ensure that fire zones with higher loads than that averaged over the entire fire area does not exceed the fire resistant rating of the fire area barriers. The potential of these ‘hot spots’ to challenge the integrity of the fire barrier, potentially resulting in propagation of the fire to adjacent Fire Areas has been further evaluated (Reference 11.69) and described in the section below.

Equivalent Fire Load Methodology

The correlation of fire loading and fire severity are used to determine equivalent fire durations as described in the Fire Analysis Combustible Loading and Fire Severity calculation (Reference 11.8). Those durations are compared to the ASTM E119 curve to justify that the fire barrier rating for the compartment provides adequate protection for the calculated combustible fire loading/duration.

A complementary analysis of equivalent fire duration has been performed (Reference 11.69) in accordance with the methodology described in the European structural fire protection standard EN 1991-1-2 (Reference 11.43). While this complementary technique has derived longer equivalent fire durations, than those determined using the methodology described in the NFPA Fire Protection Handbook, in all instances, within the NI, the equivalent fire duration remains within the prescribed fire duration rating of the Class 1 fire barriers.

A quantitative uncertainty analysis has also been performed (Reference 11.69) which indicated that there is a very high probability (99.7%) that the barriers will confine the fire to the fire area of inception.

Consideration of Realistic Fires

The adequacy of the fire barriers is based on a comparison of the equivalent fire duration, calculated in accordance with EN 1991-1-2 (Reference 11.43), against the fire rating of the exposed wall/ floor/ ceiling (Reference 11.9). The equivalent fire duration assumes that the time/temperature profile of the fire follows the curve given in ASTM E119 against which the barrier's performance is tested. However, 'realistic fires' may lead to localised conditions that for a period could exceed the predictions which support the ASTM E119 curve.

In order to demonstrate that the use of equivalent fire durations is conservative and bounding, a number of realistic fires have also been modelled (Reference 11.69). The results of this review are summarised below:

- With the exception of the oil, the hot gas layer temperature following a fire in RNS pump room 'A' (room 12162) would be significantly lower than the ASTM E119 curve. Although the oil fire initially exceeds the curve, the fire would self-extinguish due to a lack of combustible material and, as such, quickly returns below the curve. The hot gas layer temperature in the room would return to ambient after approximately 37 minutes, which is less than the 45 minute equivalent fire duration for fire area 1200 AF 01.

- The hot gas layer temperature in the Division C I&C penetration room (room 12313) would reach a peak of approximately 200 °C after 18 minutes before returning to ambient temperature after approximately 25 minutes. The equivalent fire duration for fire area 1202 AF 03 is 85 minutes.

- The hot gas layer temperature in the lower pressuriser compartment (room 12303) reaches a peak of 250 °C around the actual fire, with temperatures of 100 °C to 200 °C in the area above the pressuriser. The open ceiling of this compartment allows the hot gases to escape into the larger containment space without significantly increasing the temperature in the affected fire zone.

In addition, an assessment of the structural integrity of the SC structures (Reference 11.12) has been performed to determine the required fire hazard necessary to cause structural collapse. The assessment concluded that the required fire hazard would be significantly in excess of the combustible loading, irrespective of the location of the combustible material

relative to the structural element (i.e. the wall was exposed to the adiabatic flame temperature).

Therefore, the use of equivalent fire durations in assessing the adequacy of the fire barriers is shown to be conservative and bounding.

Heat Transfer Analysis – Nuclear Island Fire Barriers

Heat transfer calculations were performed for the module fire barriers (Reference 11.12). Thermal gradients (temperatures through the barrier) were developed for a three hour fire load on the barriers, even though the actual combustible loading are substantially less than three hour fire loading in all cases in the nuclear island. The analysis shows that even with a three hour fire assumed the thermal gradient only increases the wall temperature to a point halfway through the wall thickness with no effects on the unexposed side of the wall. Margin is demonstrated in both the wall thickness along with the estimated combustible loading used in the analysis.

11.2.7 Combined Hazards Discussion

The fire hazard analysis considers on a deterministic basis, a single fire in each of the fire areas/zones and the consequential spread of that fire to adjacent fire areas.

The consideration of credible combinations of fire with other internal hazards, either consequentially or due to a common cause, is discussed in Section 11.12.

However, compliance with relevant equipment and structural design codes as expressed in Chapter 5 ensure that combinations of internal hazards discussed in Section 11.12 with the relevant abnormal operating occurrences (including environmental hazards per References 11.60 and 11.61) are addressed.

11.2.8 ALARP Assessment and Discussion

Deterministic analysis of postulated, design basis, internal fire events shows that all Class 1 SSCs will continue to provide their Category A safety functions following the worst case postulated internal fire, even in the presence of an unrelated single failure elsewhere in the plant design. In the unlikely event that the Class 1 SSCs fail for some unrelated reason, the Category A safety function would be maintained by other, additional and redundant, Class 2 SSCs. SSC design classification and categorisations are discussed in Chapter 5 and References 11.26 and 11.59.

Further Mitigation Measures

In addition, other measures have been taken within the AP1000 design that, although not claimed in the deterministic analysis, will further reduce the consequences of postulated internal fires such as the provision of active fire suppression systems in some areas.

The AP1000 fire safety design has been achieved by:

- Minimising combustible loads and ensuring that no significant concentrations exist that could cause failure of Class 1 SSCs.

- Ensuring that a fire is prevented from spreading between redundant trains of equipment utilising appropriate combinations of physical separation, partial fire resistant barriers and fire barriers, including Class 1 nuclear fire barriers.

- Providing sufficient redundancy in the design such that if one train of protection fails as a result of fire, coincidental with an unrelated single active failure elsewhere, the safety functions continue to be provided by the equipment that remains unaffected.

- Providing a ventilation system that minimises the spread of fire between fire compartments and the damage to electrical systems from smoke.

- Ensuring a suitable and adequate early warning system of fire and the provision of fire-fighting equipment to extinguish fires.

- Maintaining the habitability of control room areas.

While combustible loads have been minimised the use of combustible materials in the AP1000 design cannot practically be avoided. In particular, for cable insulation organic compounds provide the best combination of flexibility, electrical insulation and resistance against ageing. Oils are also required for most rotating and sliding machinery in order for them to operate effectively. The arguments presented in the above subsections, together with the Hazard Schedule (Table 11.2-2) indicate how the combustible materials are distributed within the plant, and demonstrates that the design intent is met.

High concentrations of combustible material (typically oil tanks) are required to ensure the safe and reliable operation of items of machinery such as diesel generators, which are required for operations. The volume stored within the buildings is limited to minimum 'day' amounts and is within robust and reliable systems to minimise leaks. In mitigation these areas are adequately segregated from areas containing Class 1 SSCs by fire barriers and distance and are further protected by reliable active automatic suppression systems. This meets the design intent of containing fires involving large quantities of combustible material and relevant good practice.

The prevention of fire spread between redundant trains of SSCs using segregation by compartmentalisation within Containment is not possible because of the requirements of the Passive Containment Cooling System. However, of those walls and floors present most are either of substantial concrete construction or proprietary passive fire protection systems and provide some protection (insulation and integrity) from the effects of fire. However, the principal fire safety design philosophy for the protection of Class 1 SSCs within Containment has been achieved by separating redundant trains of Class 1 SSCs by distance, with some use of passive fire protection measures to segregate electrical supplies of different divisions. This approach has been shown to provide adequate protection.

Additional Features to Detect and Mitigate Internal Fire

No claim is made on the firefighting system within the AP1000 design. Instead, these systems and the fire detection and alarm system are provided to minimise the consequences of fire and to limit fire spread. In addition, the firefighting systems are used to protect Class 2 and 3 equipment; keeping the Class 2 and 3 systems operational minimises the demand placed on Class 1 systems.

Firefighting Systems

The FPS provides defence in depth functions and comprises automatic fire detection, an alarm system, and firefighting equipment, and meets the requirements of IAEA NS-R-1 (Reference 11.21) to:

- Detect fires early;

- Extinguish fires quickly;
- Minimise fire spread;

As a result, the damage to SSCs and the spread of radiological contamination is minimised. In order to achieve this, the AP1000 plant FPS is designed to perform the following functions:

- Detect and locate fires and provide the operator with an indication of the location.
- Provide the capability to extinguish fires in any plant area, protect site personnel, limit fire damage, and enhance safe shutdown capabilities.
- Supply fire suppression water at a flow rate and pressure sufficient to satisfy the demand of any automatic sprinkler system, plus adequate capacity for fire hoses, for a minimum of 2 hours.
- Maintain 100 percent of fire-pump design capacity, assuming failure of the largest fire pump or the loss of offsite power.
- Following a safe shutdown earthquake, provide water to hose stations for manual firefighting in areas outside of Containment containing Class 1 SSCs.
- Satisfy the requirements of the PCS as an alternate source of water to wet the Containment dome or to refill the PCCWST after a Loss-of-Coolant accident, if the FPS is available, as discussed in detail in Chapter 6.
- Provide an alternate supply of cooling water to the RNS or SFS HX for decay heat removal after a loss of normal CCS function, as discussed in detail in Chapter 6.
- Provide additional Containment spray capability for severe accident management, if available.

The FPS piping and instrumentation drawings covering the FPS are shown in Reference 11.71. The fire protection provision for each room within the plant containing automatic fire suppression systems is discussed in detail within the topic report (Reference 11.73), summarised below, and where appropriate, assessed as to its suitability to control the identified fire hazards. Although not relied upon in the deterministic assessment, the consequences of failures are also discussed. The system comprises the following:

- Automatic fire detection and alarm system;
- Manual firefighting equipment, i.e., portable fire extinguishers and hose stations;
- Automatic fire suppression systems, i.e., fixed firefighting systems such as sprinklers in specific locations outside Containment.

The fixed firefighting system has seismic design requirements applied to portions of the standpipe system located in areas containing equipment required for safe shutdown following a safe shutdown earthquake so that water is available to manual hose stations. However, there are no identified operator actions required to protect Category A safety functions via use of the manual hose stations. The standpipe system serving areas containing equipment required for safe shutdown following a safe shutdown earthquake is designed and supported so that it remains functional. In addition, the Containment isolation valves and associated penetration piping for the FPS are Class 1 and C-I.

Automatic Fire Detection System

The design philosophy for the automatic fire alarm and detection system is in accordance with the guidance provided in IAEA NS G 1.7 (Reference 11.23), and as a minimum, the defence in depth system provided throughout the AP1000 plant is designed in accordance with the appropriate standards (such as BS 5839 1:2002 (Reference 11.54) to provide comprehensive coverage and appropriate protection for the fire hazards identified.

Exact locations and types of detectors will be reviewed as part of the site-specific licensing process to take account of relevant good practice and operating conditions to ensure that factors such as obstructions to gas flow, crane movements, and concealed spaces have been considered. The installation of the system will be in accordance with BS 5839-1 (Reference 11.54) and manufacturers' recommendations. The installer will be approved according to LPS 1014 (Reference 11.55) or the equivalent.

Additional Means of Providing Safety Functions

Since the Category A safety functions can be maintained despite internal fires, the safety of the plant is ensured. As such, it is judged that there would be no benefit in providing additional means of delivering the Category A safety functions, or enhancing the existing SSCs. On this basis, the risk of internal fire on the ability of the AP1000 plant to deliver the Category A safety functions required to safely shutdown the reactor has been shown to be broadly acceptable and ALARP.

11.3 Internal Flooding

11.3.1 Introduction

The AP1000 Internal Flooding Hazard Analysis is performed in order to assess the bounding effects to Structures, Systems and Components (SSCs) resulting from an internal flood within the AP1000 plant. The AP1000 plant has been designed such that flooding events within the design basis will not compromise the ability of the plant to safely shutdown. The Category A safety functions required for safe shutdown following flooding and the supporting post 72 hour Category B safety functions are shown to be maintained through a combination of claims made on compartment barriers and the segregation of Class 1 SSCs.

Flooding within the AP1000 plant which has the potential to damage SSCs required to deliver Category A safety functions or supporting Category B safety functions is addressed in more detail within the Flooding Topic Report (Reference 11.76). Detailed flooding assessments have been carried out for the AP1000 design. The demonstration of the plant response to internal flooding has been performed on a deterministic basis making the following conservative assumptions:

- Gross failure (e.g., circumferential double ended guillotine fracture) of pipework and vessels (except those qualified as Highest Safety Significance [HSS]);
- Total release of system inventory; for systems with an inexhaustible supply the release is assumed to continue for at least 7 hours before isolation is effected;
- Flood heights based on effective room volume where components are present (except where the flood height does not exceed the bottom of the vessels/components);

- No credit taken for mitigation of flood height by building drains which cannot readily be inspected along their full length;

- Failure will occur during the most restrictive plant operating state.

The overall scope of the analysis considers sources of flooding within the Nuclear Island (NI), those in adjacent buildings and those originating in the yard area, for potential impact on Class 1 SSC delivering Category A safe shutdown safety functions. Although flooding will ensue following a pressure part failure[5], the mechanical effects of pressure part failure (e.g., pipe whip, jet impingement) on Class 1 SSC are not considered in this section and are instead addressed separately in Section 11.4 and Reference 11.77.

The internal flooding assessment concludes that Category A safety functions can continue to be delivered by Class 1 passive SSCs following a design basis flood through a combination of claims made on structural barriers, equipment qualification, passive flood relief systems and, where necessary, minimal operator actions to isolate inexhaustible sources of flooding following identification by a level sensor (i.e., no claim has been made on the prevention or limitation of fault occurrence).

11.3.2 Internal Flooding Claims, Arguments and Evidence

11.3.2.1 Claims Overview

This section presents the claims, arguments and underlying evidence made in relation to internal flooding hazards with the potential to impact safe shutdown.

11.3.2.2 High Level Claim

Internal flooding could cause a transient from normal operation of the reactor power plant with the potential to result in a hazard on or off site being realised. In response to such a transient, it may be necessary to shut down the reactor and return it to a safe state. Depending on the exact nature of the transient, there are a number of courses of action available to safely and reliably shut the reactor down. Availability of the Class 1 SSCs required to deliver the Category A safety functions will ensure that the reactor can be safely shutdown, and is the basis of the following high level claim.

Claim IH-2.0: **Postulated internal flooding events within the design basis will not prevent the delivery of the Category A safety functions by Class 1 SSCs and supporting post 72 hour Category B safety functions necessary to respond to the postulated event.**

This has been achieved by:

- Protecting delivery of Category A safety functions by Class 1 SSCs with structural barriers (i.e., walls, ceilings, floors) to prevent flood propagation;

- Protecting Class 1 SSC through appropriate qualification for the environment (e.g., submergence);

5. Within the PCSR, the term pressure part failure has been used interchangeably with the term Pipe Rupture Hazard to better reflect the hazard assessed within the Flooding Topic Report.

- Protecting Class 1 SSC by positioning above the maximum flood height;
- Protection through segregating Class 1 SSC delivering Category A safety functions from flooding sources, when physical barriers cannot be provided;
- Minimising the severity of flooding by limiting the number of sources of flooding and their volumes.
- Providing engineered discharge routes to alleviate the effects of flooding.
- The SSCs claimed to provide post-72 hour support functions include only offsite procured SSCs and their associated Class 1 connections.

11.3.2.3 Prevention Claims

Flooding is deterministically assumed to occur as a result of gross failure of pipework, vessels and components handling fluid, except those justified by the Structural Integrity Classification as HSS. There are therefore no specific claims made on the prevention of internal flooding hazards.

11.3.2.4 Protection Claims

Protective measures have been incorporated into the design to protect the delivery of Category A safety functions from the effects of flooding. These claims are based on protecting Class 1 SSC from being exposed to a flooded environment or, as required, ensuring that Class 1 SSC can continue to operate in a flooded environment. The following protective claims and Sub-Claims are therefore made in support of the overall high level claim:

Claim IH-2.1: **Class 1 SSCs required for delivery of Category A Safety Functions are protected from sources of internal flooding by civil/structural barriers**

Sub-Claim IH-2.1.1: **PXS Room A and PXS Room B will not flood concurrently**

Sub-Claim IH-2.1.2: **Flooding in the non-RCA Auxiliary Building mechanical areas will not spread to the electrical areas of the Auxiliary Building**

Claim IH-2.2: **Where Class 1 SSCs are not qualified to operate in a submerged state, sources of flooding will be isolated prior to exposing Class 1 SSC to a flooded environment**

Claim IH-2.3: **Where required, Class 1 SSC will be capable of delivering the Category A safety function when submerged**

11.3.2.5 Mitigation Claims

The extent to which flooding impacts Class 1 SSC has been minimised by limiting the maximum flood height in rooms/areas by reducing the available inventory of the leaking system and through the use of passive measures.

Claim IH-2.4: **The available inventory of flood sources has been minimised so far as is reasonably practicable.**

Claim IH-2.5: **Flooding will be alleviated by passive flood relief measures.**

Sub-Claim IH-2.5.1: **Flood heights in Division A, B, C & D I&C Rooms, 12301, 12302, 12304 & 12305, will not exceed 0.076 m**

Sub-Claim IH-2.5.2: **Flood height in the Valve/Pipe Penetration Room, 12306, will not exceed 0.533 m**

Sub-Claim IH-2.5.3: **Flood height in Middle Annulus, 12341, will not exceed 2.36 m**

Sub-Claim IH-2.5.4: **Flood heights in the Main Steam Isolation Rooms, 12404 and 12406, will not exceed 0.91 m**

Sub-Claim IH-2.5.5: **Flood heights in the Truck Bay/Filter Storage Area and RNS HXs Rooms, 12371, 12372 and 12362, will not exceed 1.22 m**

Sub-Claim IH-2.5.6: **Flood heights in the VBS MCR/A&C Equipment Room, 12501, will not exceed 0.152 m**

Sub-Claim IH-2.5.7: **Internal doors, will not retain the full volume of fluid within the affected room**[6]

11.3.2.6 Arguments and Evidence

Prevention Arguments and Evidence

There are no specific claims made on the prevention of flooding. Flooding is assumed to occur as a result of gross failure of pipes, vessels and components containing fluids.

Claim IH-2.1: **SSCs required for delivery of Category A Safety Functions are protected from sources of internal flooding by civil/structural barriers**

Passive structural barriers are used to limit the spread of internal flooding throughout the NI and as such the extent to which Class 1 SSC are exposed to a flooded environment. The application of the design criteria for protection from flooding ensures that:

- Structural barriers are identified to limit the extent of flooding;
- Maximum flood levels, and therefore loading, on the structural barriers are derived.

6. It is recognised that watertight doors are present in the design; however these are present to limit the loss of water from the spent fuel pools and not to protect against a flooding event.

The Hazard Barrier Matrix (Reference 11.9) identifies those walls, floors and doors which are required to prevent the propagation of flooding to adjacent areas of the nuclear island. The identified barriers have been designed to withstand the loading associated with the maximum flood-up height (Reference 11.76), as determined by the relevant Pipe Rupture Hazards Analysis (PRHA), present on either side of the barrier. The principal flood areas segregated by flood retaining barriers are the:

- Steel Containment
- Containment Shield Building
- Radiologically controlled area (RCA) of the Auxiliary Building
- Non-Radiologically controlled area (non-RCA) of the Auxiliary Building

The Auxiliary Building is sub-divided into the RCA and non-RCA, separated from one another by 0.61 m (2 ft) and 0.91 m (3 ft) thick walls and floors (References 11.9 and 11.78).

The number of penetrations in the flood retaining barriers have been minimised below the maximum flood height, or will be sealed to eliminate flow paths (Reference 11.76).

Sub-Claim IH-2.1.1: PXS Room A and PXS Room B will not flood concurrently

Partitions between rooms or areas below the 100 m (100'-00") level, rising to different elevations, require the affected room to flood completely before the next lowest room/area becomes affected. Based on the bounding flood source (in terms of volume) within Containment, it is not possible to flood both PXS room A and PXS room B from a single event.

In order to maintain the free exchange of air, and therefore cooling, the Containment has a largely open internal structure with no full height walls. Furthermore, for certain design basis events (e.g., Loss of Coolant Accident), as well as refuelling purposes, it is necessary to flood portions of the Containment in order to ensure that the fuel remains submerged.

Below the maintenance floor, 100 m (100'-0") elevation, the Containment is divided into four compartments: PXS room A; PXS room B; CVS room; General Containment (including the vertical access tunnel, Steam Generator A and B areas and the refuelling cavity), which are separated by partition walls. During a design basis accident, it is necessary to prevent premature flooding of the PXS compartment and the CVS compartment. The drain line from each of these compartments to the sump has two check valves in series. These check valves prevent reverse flow through the drain lines which could cause premature cross flooding. These check valves (back flow preventers) are included in the design and are UK Category A and Class 1. Extending above the maintenance floor, each of the compartments (PXS room A, PXS room B and CVS room) has an elevated curb around the perimeter (Reference 11.76). The curbs prevent water from passing into the enclosed compartment until the flood level in the general Containment proceeds beyond the height of the curb. The curb elevations are as follows:

- PXS room A: 103.1 m (110.17 ft)
- PXS room B: 103.07 m (110.08 ft)
- CVS room: 103.05 m (110 ft)

- Refuelling Cavity: 102.8 m (109.28 ft)[7]

The PRHA of Containment (Reference 11.77) concludes that:

- The bounding source in the general Containment would be wholly retained without over-spilling the curbs into the CVS room, PXS room A or PXS room B;
- The bounding source in the CVS room, assuming ADS actuation, would flood the general Containment and CVS rooms with some over-spill into PXS room B;
- The bounding source in PXS room B, assuming ADS actuation, would flood the general Containment space and PXS room B with some over-spill into the CVS room;
- The bounding source in PXS room A, assuming ADS actuation, would flood the general Containment space and PXS room A with some over-spill into the CVS room.

On this basis, there is no scenario where both the PXS room A and PXS room B become submerged concurrently. Note that this Sub-Claim applies to the initial post fault flood. In longer term plant recovery scenarios, it is assumed that all of the Containment rooms that do not flood initially do eventually flood due to leakage.

Sub-Claim IH-2.1.2: Flooding in the non-RCA Auxiliary Building mechanical areas will not spread to the electrical areas

Within the non-RCA side of the Auxiliary Building, rooms containing electrical equipment are segregated from those containing mechanical equipment. The rooms containing mechanical equipment are:

- 12306: Valve/piping penetration room;
- 12404: Lower Main Steam Isolation Valve (MSIV) compartment B;
- 12405: Lower VBS B&D Equipment room;
- 12406: Lower MSIV compartment A.

The Hazard Barrier Matrix (Reference 11.9) identifies those walls, floors and ceilings which are required to prevent the propagation of flooding to adjacent rooms within the non-RCA side of the Auxiliary Building. The identified barriers have been designed to withstand the loading associated with the maximum flood-up height (Reference 11.76), as determined by the relevant PRHA, present on either side of the barrier. Penetrations in the flood retaining barriers have been minimised below the maximum flood height, or will be sealed to eliminate flow paths (Reference 11.76).

Claim IH-2.2: Where Class 1 SSCs are not qualified to operate in a submerged state, sources of flooding will be isolated prior to exposing Class 1 SSC to a flooded environment

7. This is the elevation of the refuelling canal connecting line, and the elevation above which the refuelling cavity will flood.

Differential pressure level sensors located in the Auxiliary Building RCA and Auxiliary Building non-RCA will alert operators, via the PMS, to flooding in the respective areas and the need to effect isolation of the affected system.

There are two redundant differential pressure level sensors (WLS-LT-400A and WLS-LT-400B) within the Auxiliary Building RCA sump room (12154), located at 0.30 m (1 ft.) above the 89.8 m (66'-6") level. These differential pressure level sensors are provided to ensure that all sources of flooding can be isolated prior to the 95.58 m (85'-6") criteria flood-up level being exceeded; the criteria flood-up level is the point at which Class 1 SSC would become submerged and therefore cease to function. Each differential pressure level sensor has two set-points. Exceeding each set-point annunciates an alarm in the MCR via the PMS, these sensors will be designed to meet UK Category A and Class 1 criteria.

The bounding flooding event in the Auxiliary Building RCA to be a HELB of the CVS in room 12255 leading to cascade failure of CCS, FPS and Central Chilled Water System (VWS) pipework present in the vicinity.

Similarly, there are two redundant differential pressure level sensors (WWS-LT-030 and WWS-LT-031) within rooms 12104 and 12105. Both sensors are located at 0.1 m (4 inches) above the 89.8 m (66'-6") level. The differential pressure sensors are provided to ensure that all sources of flooding can be isolated prior to the level reaching 0.19 m (7.5 inches) above the basemat, at which point the bottom of the batteries in rooms 12101, 12102, 12104 and 12105 would come into contact with the liquid. These sensors will be designed to meet UK Category A, Class 1.

The bounding flooding event in the Auxiliary Building non-RCA is a MELB of the Potable Water System (PWS) line in room 12111. It should be noted that flood water contacting the bottom of the batteries does not render the batteries inoperable but potentially reduces their capacity depending upon the temperature of the fluid. The rooms must flood up to the top of the terminals to short out the batteries, which is another 0.60 m (23.5 inches), providing additional margin to the total loss of battery function.

The only sources of flooding with the potential to trigger the differential pressure sensors originate from the FPS and the PWS, however the FPS has insufficient inventory to exceed the criteria flood height. The operators will therefore be required to isolate the PWS only.

Claim IH-2.3: Where required, Class 1 SSC will be capable of delivering the Category A safety function when submerged

Class 1 SSCs credited to operate when located below the maximum flood height will be qualified for operation in a submerged environment.

Environmental qualification tests and methods are detailed in Reference 11.61 based on the guidelines provided in IEEE 323-1974 (Reference 11.124) and IEEE 344-1987 (Reference 11.79), and include:

- Type testing: Testing of equipment in the environment, normal and abnormal, under which it will be required to perform its function;
- Analysis: Review of relevant data for similar components;
- On-going qualification: Maintenance and surveillance of in service equipment.
- Equipment qualification program documentation consists principally of:

- Methodology for Qualifying Safety-Related Electrical and Mechanical Equipment (Reference 11.60): Over-arching document detailing the strategy for equipment qualification.

- Equipment Qualification Data Packages: Details the qualification program objectives, methods performance specification and qualification plan for each SSC subject to qualification.

- Equipment Qualification Test Reports: Details of the specific methods used during qualification and the results of the process.

The criterion for equipment qualification depends upon the environment, during normal and abnormal conditions, under which the SSC is required to operate. The AP1000 plant has been broken down into 11 environmental zones and a number of associated sub-zones. The normal and abnormal environmental conditions for equipment qualification in each zone/sub-zone have been established (Reference 11.61).

11.3.2.7 Mitigation Arguments and Evidence

Claim IH-2.4: The available inventory of flood sources has been minimised so far as is reasonably practicable

The principal areas comprising the NI (Containment/Shield Building; Auxiliary Building RCA; Auxiliary Building non-RCA, which itself is sub-divided into mechanical and electrical compartments) are separated by structural partitions (see Chapter 6) such that flooding in one area will be retained without affecting another area. So far as is reasonably practicable the pipework comprising each of the systems has been routed to minimise the number of rooms through which they pass. Furthermore, where practicable, significant accumulations of water have been located outside of the Nuclear Island.

Within the Auxiliary Building non-RCA side, the FPS draws water from the PCCWST via a standpipe during all plant modes. The standpipe has been elevated such that the maximum flood height on level 1 of the Auxiliary Building RCA is limited to 19 cm (7.5 inches).

Within Containment, the FPS is isolated during plant modes 1-4 and only available during plant modes 5 & 6. The FPS cannot therefore contribute an additional source of flooding within Containment, except when the reactor is already shut down.

Claim IH-2.5: Flooding will be alleviated by passive flood relief measures

Where it is not possible to either limit the maximum flood height in a room or area, or to qualify the SSC for operation in a submerged environment, it is necessary to credit passive flood relief design attributes such that the flood height does not affect Class 1 SSC. Situations where this may be the case include flooding sources where:

- Isolation cannot be provided for operational reliability reasons;
- Isolation cannot be effected sufficiently quickly.

Sub-Claim IH-2.5.1: Flood heights in Division A, B, C & D I&C Rooms, 12301, 12302, 12304 & 12305, will not exceed 0.076 m

The bounding pipe rupture in 12300 is a MELB of FPS, which would result in water being discharged into the room. There exist five drains (WWS-D212 through WWS-216) in room

12300 which feed into a common header; these drains are UK Category A, Class 1.. The drain discharges, from 12300, to the Auxiliary Building north sump.

The MELB of FPS discharge into the Auxiliary Building sump; accumulation of FPS water on level 1 is insufficient to challenge Class 1 SSC present on this level.

Sub-Claim IH-2.5.2: Flood height in the Valve/Pipe Penetration Room, 12306, will not exceed 0.533 m

The bounding pipe rupture in 12306 is a MELB of FPS. There exists two floor drains (WWS-D104 and WWS-D235) in room 12306, both drains feed into a common header; these drains are UK Category A, Class 1. The drain discharges into the Turbine Building sump. The sump tanks each have sufficient capacity to accommodate the total discharge from the FPS. Should the sump tanks become full; as a defence-in-depth measure, four sump pumps will automatically discharge to the oil separator tank located outside of the Turbine Building.

Sub-Claim IH-2.5.3: Flood height in Middle Annulus, 12341, will not exceed 2.36 m

The bounding flood height in 12341 is a result of a MELB of FPS in room 12351. Four floor drains are present in room 12351 (WRS-D313 to WRS-D316 and seven floor drains in room 12341 (WRS-D318, D319, D321, D324, D328, D330 and D333). These drains will be designed as UK Category A, Class 1.. The four drains from 12351 feed into a common header. The seven drains from 12341 feed into a separate common header. Floor drains present in 12341 and 12351 will discharge into the Auxiliary Building south sump.

The drain discharges to the Auxiliary Building south sump in 12154. The sump has a limited capacity and once full would overflow throughout the 89.79 m (66'-6") level; this overflow is bounded by a cascade failure in 12255 initiated by failure of the CVS which is shown to have no impact on Class 1 SSC.

Sub-Claim IH-2.5.4: Flood heights in the Main Steam Isolation Rooms, 12404 and 12406, will not exceed 0.91 m

Pressure relief panels (12404-AY-P01 and 12406-AY-P01, UK Category A and Class 1), located at floor level in each of 12404 and 12406, provide an engineered discharge route into the Turbine Building 1st Bay. In accordance with the design specification (Reference 11.80) the pressure relief panel will actuate when a pressure head acts on the panels' surface.

The bounding pipe rupture in the MSIV compartments is a gross failure (full guillotine break of 0.508 m [20 in] diameter pipe) of the SGS main feedwater pipe upstream of the check valve. The analysis demonstrates that the flood heights in 12404 and 12406 are below the criteria flood height.

Sub-Claim IH-2.5.5: Flood heights in the Truck Bay/Filter Storage Area and RNS HXs Rooms, 12371, 12372 and 12362, will not exceed 1.22 m

Pressure relief door located within 12362-AD-D02 door, UK Category A and Class 1, located on the floor level of room 12362, provides and engineered discharge route into the lower levels of the RCA side of the Auxiliary Building. In accordance with DCP (APP-GW-GW-4568) which is part of the Design Reference Point (Reference 11.3) the pressure relief device will actuate when a pressure head acts on the panel surface equivalent to 0.61 m (2 feet).

The bounding pipe rupture in the Truck Bay/Filter Storage Area is a gross failure of the FPS pipe. The analysis demonstrates that the flood heights ini 12371, 12372 and 12362 are below the criteria flood height.

Sub-Claim IH-2.5.6: Flood heights in the VBS MCR/A&C Equipment Room, 12501, will not exceed 0.152 m

The flow orifice plate (DWS-PY-R002) limits the DWS supply flow rate to less than the Room 12501 floor drains (WWS-D251, D229 and D230) capacity to ensure flood waters are directed out the Auxiliary Building and into the Turbine Building floor sump. These UK Category A and Class 2 components will be designed in accordance with the design specification,

The bounding pipe rupture in the VBS MCR/A&C Equipment Room is a gross failure of the DWS pipe. The analysis demonstrates that the flood height in Room 12501 is below the criteria flood height.

Sub-Claim IH-2.5.7: Internal doors will provide a means of discharge from the flood affected room

Divisional barriers separating rooms will allow a flow of water to pass into the adjacent room(s).

A range of divisional barriers (e.g., wire mesh door, safety chain & standard door) are utilised throughout the AP1000 plant. Wire mesh doors and safety chains offer little or no resistance to flows out of the room and are not considered explicitly. Standard doors are fitted with a 1.6 cm (5/8") door gap at the bottom of the door. The door gap allows liquid to pass to adjacent compartments; the rate at which liquid passes through the door gap depends upon the pressure head generated by liquid in the flooded compartment.

11.3.3 Internal Flooding Safety Case Summary

11.3.3.1 Introduction and Overview

The safety design approach adopted for internal flooding hazards consists of a range of complementary approaches. These are applied as appropriate to reduce the potential disruption to the passive safe shutdown Class 1 SSC. Flooding events within the design basis do not prevent the delivery of the Category A safety functions necessary to respond to a postulated event. Preservation of required safety functions ensures alignment with fault studies (see Chapter 8) and structural integrity analysis (see Chapter 20).

Flooding is assumed to occur as a result of an initiating event leading to the gross failure of piping or equipment, except that which is justified by the Structural Integrity Classification (Reference 11.72) as HSS (see Chapter 20). Passive protective measures have been incorporated into the design to protect SSCs that deliver Category A safety functions from the effects of internal flooding. The consequences of flooding hazards are contained through the use of passive barriers to limit the impact to and loss of a safety function and by the qualification of SSC to operate in a flood affected environment.

In summary, the safety case approaches adopted are as follows:

- Protection of SSC, whose availability is required to deliver Category A safety function, from the effects of flooding;

- Qualification of SSC in a submerged environment;
- Provision of redundant SSC, capable of delivering the Category A safety function, in segregated locations which cannot be affected by a single flood hazard.

The AP1000 design employs a mixture of the approaches stated above to form levels of defence in depth which, together, reduce the risk of internal flooding to a level which is As Low As Reasonably Practical (ALARP).

11.3.3.2 Applicable Codes and Standards

The PRHAs have been undertaken in accordance with the following codes and standards, as specified by the pipe rupture protection design criteria (Reference 11.81):

- ACI 349-01, 'Code Requirements for the Design, Fabrication and Erection of Steel Safety-Related Structures for Nuclear Facilities';
- ANS-58.2, 'Design Basis for Protection of Light Water Nuclear Power Plants against the Effects of Postulated Pipe Rupture';
- ASME Boiler and Pressure Vessel Code, Section III, 'Rules for Construction of Nuclear Power Plants';
- ASME B31.1, 'Power Piping';
- ASME Boiler and Pressure Vessel Code, Section XI, 'Rules for Inservice Inspection of Nuclear Power Plant Components'.

In addition, the PRHAs of internal flooding have been undertaken in accordance with the following codes and standards, as specified by the design criteria for protection from flooding (Reference 11.78):

- ANSI/ANS-56.10, 'Subcompartment Pressure and Temperature Transient Analysis in Light Water Reactors';
- ANSI/ANS-56.11, 'Design Criteria for Protection against the Effects of Compartment Flooding in Light Water Reactor Plants';
- ANS-58.2, 'Design Basis for Protection of Light Water Nuclear Power Plants against the Effects of Postulated Pipe Rupture';
- ANSI/ANS-58.8, 'Time Response Criteria for Safety-Related Operator Actions'.

The AP1000 Equivalence/Maturity Study of US Codes and Standards (Reference 11.25) determines, based on their importance to safety, the applicability, adequacy and sufficiency of those standards when compared with relevant UK and international good practice. It also provides a clear and auditable demonstration that all codes and standards to support the design substantiation of UK safety related or safety significant SSCs have been identified.

To evaluate the AP1000 design codes and standards against the UK expectations, the codes and standards have been organised by the relative safety significance of the SSCs to which they have been applied. The safety significance has been determined in accordance with the

AP1000 UK Safety Categorisation and Classification Methodology (Reference 11.26), which describes the process for categorisation of safety functions and classification of SSCs.

11.3.3.3 Redundancy and Segregation

The design of the AP1000 plant incorporates redundant Class 1 SSCs, each of which is capable of delivering the Category A safety function. Where there is the potential for Class 1 SSCs to be compromised by flooding, the redundant Class 1 SSC delivering the Category A safety function have been identified. The provision of redundancy takes into account the following:

- IAEA-NS-G-1.11 "Protection against Internal Hazards other than Fires and Explosions in the Design of Nuclear Power Plants" (Reference 11.82).
- IAEA NS-R-1, "Safety of Nuclear Power Plants: Design" (Reference 11.21).
- APP-GW-J1R-008, April 2002, "Safety Criteria for the AP1000 Instrumentation and Control Systems" (Reference 11.51).
- APP-GW-J1R-004, April 2002, "AP1000 Instrumentation and Control Defence in Depth and Diversity Report" (Reference 11.52).
- NS-TAST-GD-011 Technical Assessment Guide, "The Single Failure Criterion" (Reference 11.83).

Within the Containment/Shield Building, redundant divisions of Class 1 SSC have been separated, so far as is reasonably practicable, by distance. While the Containment/Shield Building is a largely open space to maintain the free movement of gases, some compartments have been segregated by walls and floors. Curbs around the top of each compartment determine the sequence in which each one floods.

Outside the Containment/Shield Building, the Auxiliary Building comprises RCA and non RCA, which are physically segregated from one another by walls, floors and ceilings. Adjoining buildings are also physically segregated from the Auxiliary Building by walls, floors and ceilings. Access to either the RCA or non-RCA portions of the Auxiliary Building is from the adjoining buildings, which are themselves sub-divided into RCA and non-RCA sections (as appropriate) by walls, floors and ceilings. A flooding hazard which initiates on the RCA side cannot therefore propagate to the non-RCA side of the NI, and vice-versa.

11.3.3.4 Internal Flooding Assessment Approach

The internal flooding assessment has been carried out in accordance with the pipe rupture protection design criteria (Reference 11.81) and the design criteria for protection from flooding (Reference 11.78), with the following exceptions:

- Systems which during normal operation may be considered high energy, regardless of duration, will be assessed for HELBs.
- One inch, and below, Nominal Pipe Size (NPS) piping will be considered for the effects of flooding;
- Seismically-supported piping is not exempt from postulated MELBs.

- For areas or rooms where drains are available as a discharge flow path, flood levels are evaluated based on a range of drain blockages.

For each system where an initiating event leading to equipment failure could result in flooding of the surrounding room/area, the flooding hazard analyses have determined:

- The maximum inventory of the affected system;
- The path, and therefore affected areas, of flooding;
- The maximum flood height in affected rooms/areas.

The output of the flooding hazard analyses has been compared against the location of Class 1 SSC to determine those which could be affected by flooding in order to demonstrate that Category A and supporting post-72 hour Category B safety functions will continue to be delivered.

11.3.3.5 Interface with Other Internal Hazards

The AP1000 has been evaluated for internal hazards to confirm that SSCs delivering Category A functions will perform as required for the identified internal hazards listed in Section 11.1.

It is recognised that internal flooding may occur, due to a common initiator, coincidentally with other internal hazards or selected external hazards. In such instances, the combined effects of both hazards constitute the full extent of the internal hazard.

An assessment of the consequences of combined hazards has been completed and documented in Section 11.12 based on the combined hazards analysis (Reference 11.75). Section 11.12 demonstrates that for credible combinations of flooding with other potential internal hazards, the Category A and/or supporting Category B safety functions can continue to be delivered, as consistent with the individual internal hazard assessments.

11.3.3.6 Conclusions

Sufficient evidence has been shown throughout this section that the risk of loss of Class 1 SSCs as a result of internal flooding is low and controlled. Internal flooding has been shown to not prevent the delivery of the Category A safety functions and the post 72-hour Category B safety functions. This is due to the combination of inherent design features, routine and non-routine early detection regimes, and the application of routine and non-routine remediation actions, respectively preventing, detecting and controlling the risk to the AP1000 plant from such flooding.

11.3.4 Internal Flooding Analysis and Assessment

11.3.4.1 Introduction

The internal flooding assessments have been prepared according to the following general assumptions:

- With the exception of SSC qualified as HSS, any pipe, vessel or component could fail;
- Any PIE will result in the most limiting equipment failure (e.g., gross failure of the pipe, vessel or component);

- The entire system inventory will be released following failure; for systems with an inexhaustible supply, the release will continue for a further reasonable human response time before isolation is effected with a total of 7 hours as the maximum allowable operator response time following the alarm;

- Secondary effects may be induced following the PIE;

- Dynamic effects of a HELB induced pipe whip resulting in cascade failure of piping with a smaller diameter (regardless of wall thickness) and piping of an equal or greater diameter (with the same or smaller wall thickness);

- Only passive flood mitigation features are credited; active features are assumed failed except where the system is appropriately classified and qualified for the fault induced environment;

- Floor drains are assumed to be blocked, except where the drain may lead to flooding in downstream rooms;

- The PIE will occur during the most limiting plant state (e.g., full power operation);

- A single active component failure is assumed to pre-exist prior to the PIE, or a single active failure occurs post fault, but not both;

- Penetrations through fire barriers (see internal fire assessment in Section 11.2) are leak tight. Flood levels are used to create design pressure loading conditions and/or specification requirements;

- The volume occupied by equipment in a room is accounted for in determining the flood height.

This internal flooding safety case does not consider the effects of:

- Seismically induced internal flooding, where such an event is assumed to result in multiple system failures from non-seismically qualified SSC (see Section 11.12);

- Internal flooding on civil structural integrity (see Chapter 16).

11.3.4.2 Internal Flooding Sources

The piping rupture protection design criterion establishes the guidelines for determining the location and configuration of pipe ruptures in accordance with Section 11.4. Such pipework falls into one of the two following categories:

- High-energy piping: systems or portions of systems in which the maximum normal operating temperature exceeds 93 °C (200 °F) or the maximum normal operating pressure exceeds 2.0 MPa (275 psig).

- Moderate-energy piping: systems or portions of systems pressurised above atmospheric pressure during normal plant conditions that are not classified as high energy.

Due to the potential of pipe whip resultant from a HELB, cascading ruptures may occur in pipework present in the vicinity except where the high energy line is fitted with pipe whip restraints. Systems subject to cascade rupture will add additional fluid inventory to that of the

HELB. In accordance with the design criteria for protection from flooding (Reference 11.78), such cascade ruptures will initiate as follows:

- Gross failure of pipework with a smaller nominal pipe diameter, regardless of pipe wall thickness;
- Through Wall Crack (TWC) of pipework with an equal or larger nominal pipe diameter with an equal or thinner wall thickness;
- No failure in pipework with an equal or larger nominal pipe diameter with a thicker wall thickness.

All pipe ruptures, except those cascade ruptures leading to a TWC as defined above, are taken to be a gross failure of the pipe.

Based on the approach outlined in subsection 11.3.3.4, internal flooding sources have been identified as applicable to the various PRHA calculations. A brief summary is presented in the following discussion:

Containment Building

The Containment is a sealed environment designed to contain the primary circuit in the event of a LOCA, along with any radioactive discharges. The only systems with the potential to flood the Containment are therefore those which are wholly contained within or pass through the Containment structure.

The PRHA evaluation of flooding in Containment (Reference 11.76) identifies the SGS, RCS, PXS, RNS, SFS, CCS, VWS, DWS and CVS systems as potential flood sources during plant modes 1-4. During plant modes 5 & 6, the reactor is in a shutdown state and the impact of flooding to safe shutdown is bounded. Table 11.3.2 details in which rooms each of the various systems are present.

The DWS and FPS are both normally isolated from the Containment by locked closed manual valves. These valves are only opened during shutdown and maintenance activities and therefore the DWS and FPS are not considered to comprise flood sources during normal operation; the coincident failure to isolate these systems and a pipework failure/spurious operation of the FPS is considered to be beyond the design basis.

The WLS pumps liquid effluent from the Containment sump to storage tanks in the Auxiliary Building. It is not possible to siphon effluent from these tanks and therefore the WLS is not considered to be a potential flood source in Containment.

Auxiliary Building

The following sections provide a brief description of each of the systems present within the Auxiliary Building. Table 11.3.1 details in which rooms each of the various systems are present. Details of tank volumes and refill capability are presented in (Reference 11.76).

CCS – Component Cooling Water System

The CCS includes three system tanks, two 20.4 m3 (5400 US gallon) CCS surge tanks and the 82 litre (21.6 US gallon) CCS chemical addition tank. In addition to this, the CCS system has a total volume of 160 m3 (42,406 US gallons), giving a total system inventory of 182.6 m3 (48228.6 US gallons).

During normal operation, parts of the CCS will operate at temperatures in excess of 79.4 °C (175 °F) Makeup to the CCS is provided by the DWS from the Demineralised Waster Storage Tank (DWST), which is itself made-up by the Demineralised Water Treatment System (DTS).

CVS – Chemical and Volume Control System

The CVS comprises the Boric Acid Storage Tank (BAST), Boric Acid Batching Tank (BABT) and associated pipework. The maximum capacities of the BAST and BABT are 300 m3 (79,315 US gallons) and 3.03 m3 (800 US gallons) respectively.

In general terms, there are three sections of the CVS makeup lines which have different flow rates. The three sections are:

1. Upstream of the Makeup Pump (CVS-MP-01A/B);
2. Between the Makeup Pump (CVS-MP-01A/B) and the Cavitating Venturi (N01);
3. Downstream of the Cavitating Venturi (N01).

In section 1, the flow rate is driven by the static head of pressure from the BAST. In section 2, the flow rate would be limited by the run out flow from one of the CVS makeup pumps. Section 2 is wholly contained within room 12255. In section 3, the flow rate is limited by the cavitating Venturi.

Makeup to the CVS is provided from the DWST, which is itself made-up by the DTS (see Chapter 6), at a rate of 1.1E-02 m3 s-1 (175 gpm).

Section 1 of the CVS is Moderate Energy, while sections 2 and 3 are High Energy.

DWS – Demineralised Water Transfer and Storage System

The DWST has a maximum capacity of 477 m3 (126,000 US gallons). Demineralised water is distributed throughout the DWS by two motor driven pumps each of which has a run out flow rate of 2.52E-02 m3 s-1 (400 gpm) giving a maximum system flow of 5.05E-02 m3 s-1 (800 gpm).

Within the Annex Building, the DWS pipework incorporates an orifice plate (DWS-PY-R002, UK Category A, Class 2) to limit flow within the DWS in room 12501 to no greater than 1.89E-02 m3 s-1 (300 gpm). The flow rate is therefore less than the capacity of the floor drain within the room, and as such it is not possible for there to be significant accumulations arising from a pipe rupture in the DWS.

Makeup to the DWS is provided by the DTS direct to the DWST on low level in the DWST. The DTS pumps have a maximum flow rate of 2.3E-02 m3 s-1 (360 gpm), and feed from an unlimited source.

FPS – Fire Protection System

The FPS is present in both the Auxiliary Building RCA and non-RCA, as well as elsewhere outside of the nuclear island. The FPS is also present within Containment; however, it is isolated external to Containment during plant modes 1-4.

The FPS has a 30.5 cm (12 inch) diameter distribution header, feeding a network of branch lines the smallest of which has a 1.27 cm (0.5 inch) diameter. The system is designed as a

loop such that gross failure of any pipe comprising the FPS would see a flow from both ends of the rupture location.

The FPS is served by two 1910 m3 (504,000 US gallon) yard tanks operating in duty and standby modes. A make-up source, provided by the Raw Water System (RWS), supplies both FPS yard tanks independently. The 15.24 cm (6 inch) lines provide an 8 hour refill of each yard tank. Each 15.24 cm (6 inch) line is fitted with a butterfly valve which is normally locked closed, isolating the main refill line. A smaller, 5.08 cm (2 inch), line provides automatic makeup to either yard tank. The automatic makeup lines are fitted with motor operated valves and an orifice plate to limit the automatic makeup flow to no more than 3.16E-03 m3 s-1 (50 gpm).

The FPS has a normal operating pressure of 1.27 MPa to 1.34 MPa (185 psig to 195 psig), which is maintained by a jockey pump. Should the system pressure drop below 1.24 MPa (180 psig), an electric pump will begin to supply flow at 1.26E-01 m3 s-1 (2000 gpm). If, as for a pipe rupture, the system pressure continues to drop, a diesel pump will also begin to supply flow at an additional 1.26E-01 m3 s-1 (2000 gpm). The affected room(s) will therefore flood at a combined flow, from both the electric and diesel pumps, of 2.52E-01 m3 s-1 (4000 gpm) until the duty tank is depleted or system isolation is affected.

During all plant modes, the Auxiliary Building non-RCA portion of the FPS is isolated from the two yard tanks by a normally closed and locked valve and is instead gravity fed, via a standpipe, in the PCCWST. The elevation of the standpipe is such that the maximum system inventory is limited to 99 m3 (3500 ft3).

As well as being a source of flooding following a pipe rupture, the FPS may be actuated in rooms where there are sprinklers and a pipe ruptures in a system with a temperature which exceeds 79.4 °C (175 °F), contributing an additional 2.27E-02 m3 s-1 (360 gpm) of water. Such systems are only present in the Auxiliary Building RCA and therefore the FPS will not contribute to flooding in the Auxiliary Building non-RCA (note: systems satisfying this criteria are also present within Containment, however the FPS is isolated within Containment during plant modes 1-4.

PCS – Passive Containment Cooling System

The PCCWST has a capacity of at least 2,864 m3 (756,700 US gallons). When full, each of the flow paths from the PCCWST delivers a flow rate of 3.0E-02 m3 s-1 (469 gpm) to the outside of the Containment structure.

The Passive Containment Cooling Auxiliary Water Storage Tank (PCCAWST) has a capacity of at least 2,952 m3 (780,000 US gallons). Two recirculation pumps each provide 6.3E-03 m3 s-1 (100 gpm) of makeup water from the PCCAWST to the PCCWST.

Gross failure of the pipework on one of the three flow paths would result in an unrestricted, gravity fed, flow from the PCCWST into the upper annulus. During normal operation of the PCS, water discharged from the PCCWST would flow, via two floor drains to the building exterior where it is removed by storm drains. In order to prevent the upper annulus becoming flooded, the floor drains are claimed in support of the internal flooding hazard analysis.

During all plant modes, the PCCWST provides the supply of water for the FPS within the non-RCA side of the Auxiliary Building. The elevation of the standpipe within the PCCWST is such that the supply of water is limited to 99 m3 (3500 ft3). PCS pipework within the non-RCA of the Auxiliary Building is restricted to that supplying the FPS.

PWS – Potable Water System

The PWS is an unlimited water supply distributed throughout the Auxiliary Building. The PWS incorporates regulating valves to reduce system pressure as appropriate. The design flow rate for the PWS is 1.1E-02 m3 s-1 (172 gpm); however, adherence to international plumbing code in both the RCA and the Non-RCA will restrict the flooding flow rate to 2.8E-03 m3 s-1 (44 gpm) as PWS lines are limited to 0.55 MPa (80 psig), equating to 0.03 m (1 inch) diameter piping.

RNS – Normal Residual Heat Removal System

The RNS is essentially a closed loop system with a limited volume which removes heat from the core and RCS and provides RCS low temperature over-pressure protection at reduced RCS pressure and temperature conditions after shutdown. The RNS also provides a means for cooling the IRWST during normal plant operation.

SFS – Spent Fuel Pool Cooling System

The Spent Fuel Pool (SFP) (including Cask Loading Pit (CLP), Cask Washdown Pit (CWP), spent fuel storage pit and Fuel Transfer Canal) has a surface area of 141 m2 (1516 ft2). The volume of liquid which could be released is 254 m3 (67,131 US gallons). For the same reduction in height of the refuelling cavity, the volume of liquid discharged would be 241 m3 (63,677 US gallons). The combined volume is therefore 495 m3 (130,808 US gallons).

If the pipe rupture is in the discharge side of the SFS pump, the release would be limited by the pump runout flow rate. If the rupture occurs in the suction side, the release rate would be limited by the gravity feed through the piping. For a pressure head of 13.5 m (44.36 ft) through a 0.2 m (8 inch) NPS pipe, the flow rate would be 5.29E-01 m3 s-1 (8384.6 gpm). Makeup to the SFP is from the DWST and DTS at 6.31E-03 m3 s-1 (100 gpm).

A second scenario exists where the SFS piping is aligned to the IRWST. A drop in the IRWST level by 4% will automatically isolate all valves. The IRWST has a design capacity of 2140 m3 (75,626 ft3), the maximum leak is therefore 85.7 m3 (3025 ft3). In this scenario, the flow rate would be limited by the gravity feed through the pipe at 5.5E-01 m3 s-1 (8684.9 gpm).

VWS – Central Chilled Water System

The VWS comprises a 0.07 m3 (18.3 US gallon) chemical feed tank, 1.2 m3 (318 US gallon) expansion tank and the volume of the connecting pipework at 60 m3 (15,813 US gallons), giving a total system inventory of 61.1 m3 (16,149 US gallons). The flow rate within the system is 0.5 m3 s-1 (7947 gpm).

Automatic makeup to the VWS is from the DWS on low-low level within the expansion tank. The makeup flow from the DWS is 3.1E-04 m3 s-1 (5 gpm), which is considered to be negligible for the purpose of the internal flooding analysis.

VYS – Hot Water Heating System

The Hot Water Heating System (VYS) comprises a 3.2 m3 (855 US gallon) surge tank and an 82 litre (21.6 US gallon) chemical addition tank. During normal power operations , hot water is circulated throughout the VYS by a single pump rated to a total flow of 5.0E-02 m3 s-1 (788 gpm). During operation, the VYS operates at temperatures in excess of 79.4 °C (175 °F).

A low level within the VYS surge tank will initiate a makeup flow, of 1.58E-03 m3 s-1 (25 gpm), from the DWS, which is considered to be negligible for the purpose of the internal flooding analysis.

WLS – Liquid Radwaste System

The WLS comprises the following tanks:

- Reactor Coolant Drain Tank – 3.4 m3 (900 US gallons)
- Containment Sump – 0.4 m3 (99 US gallons);
- Effluent Holdup Tanks (2) – 106 m3 (28,000 US gallons) each;
- Waste Holdup Tanks (2) – 56.8 m3 (15,000 US gallons) each;
- Monitor Tanks (3) – 56.8 m3 (15,000 US gallons) each;
- Chemical Waste Tank – 33.7 m3 (8,900 US gallons).

The total system inventory for the WLS is therefore 533 m3 (140,899 US gallons). The maximum flow rate of the WLS is 7.19E-03 m3 s-1 (114 gpm).

Makeup to the WLS is provided from the DWST, which is itself made-up by the DTS at a rate of 4.73E-03 m3 s-1 (75 gpm).

WSS – Solid Radwaste System

The WSS comprises two resin basin tanks, each of which has a capacity of 8.6 m3 (2,274 US gallons). The WSS can also be aligned with the SFS, which has a total system inventory of 495 m3 (130,808 US gallons), at a maximum flow rate of 4.73E-03 m3 s-1 (75 gpm).

Makeup flow to the WSS is provided from the DWST, which is itself made-up by the DTS, at a rate of 4.73E-03 m3 s-1 (75 gpm).

11.3.4.3 Flood Paths

Flooding is expected to propagate both horizontally throughout the level on which the pipe rupture occurs as well as vertically between levels. While it is typical for flooding to proceed to lower levels, it is also possible for flooding to affect higher levels through back flow processes when all available space on the lower level(s) has become flooded. In accordance with the guidance provided in ANS/ANSI 56.11 (Reference 11.85), flood propagation from the room of inception considers the following paths:

- Door gaps;
- Pipe chases which are not sealed;
- Stairwells/elevator sumps;
- Radioactive Waste Drain System (WRS) and Waste Water System (WWS) drains;
- Penetrations (e.g., cable tray or piping) which are not sealed;
- Floor gratings, weirs and unsealed ladder and hatch openings.

Various door types are present throughout the NI and connected buildings. Depending on which type of door separates two rooms, dictates the flow between the rooms. The door types and their influence on flow are as follows:

- Physical barriers which obstruct flow between adjacent divisions (e.g., standard door, steel door). Where present, the flow to an adjacent compartment is assumed to be through a door gap present at the base of the door.

- Adjacent rooms or compartments which are not segregated by physical barriers (e.g., safety rope, wire mesh doors). Flow to an adjacent compartment is assumed to be unobstructed and would proceed as a flow through a contracted rectangular weir.

- The watertight doors in rooms 12166 and 12167 are assumed to be conservatively closed in which increases the water heights in adjacent areas for flooding originating outside these rooms.

Stairwells and elevators provide an opportunity for flooding to proceed vertically between different levels. Although the room itself may flood, stairwells and elevators are treated as conduits through which flooding propagates to other areas of the plant.

The drains provide a means for flood mitigation within affected rooms, but in doing so communicate the flood to downstream rooms (typically only the rate at which the downstream room is flooded will be affected, with the flood height largely unchanged). In accordance with the guidance provided in section 5.2.2 of ANS 56.11-1988 (Reference 11.85), the efficacy of flood mitigation by the drains is subject to the following conditions:

- Drains in rooms subject to a HELB are assumed to be 100% clogged by debris;

- Drains in rooms subject to a MELB are assumed to be 25% clogged by debris;

- Drains in rooms other than that in which the pipe rupture occurred are assumed to be 25% clogged;

- A 10.16 cm (4 inch) drain can extract up to 1.58E-02 m3 s-1 (250 gpm) (Reference 11.76). Where multiple drains combine into a single 10.16 cm (4 inch) header, the combined rate of extraction from all drains is limited to 1.58E-02 m3 s-1 (250 gpm).

- A 15.24 cm (6 inch) drain can extract up to 1.97E-02 m3 s-1 (312 gpm) (Reference 11.76). Where multiple drains combine into a single 15.24 cm (6 inch) header, the combined rate of extraction from all drains is limited to 1.97E-02 m3 s-1 (312 gpm).

Broadly speaking, the Containment area comprises of four areas separated from one another by walls and floors such that flooding in one area would not propagate to another area unless the height of the flood exceeds the height of the separating wall. The four areas are:

- CVS room (11209);
- PXS room B (11207 and 11208);
- PXS room A (11206);
- General Containment Area (including refuelling cavity).

Curbs around the PXS and CVS rooms ensure that, during postulated flooding scenarios, the refuelling cavity is flooded from the Containment sump before flood water overflows into the PXS or CVS rooms. The curbs for each area are designed such that the CVS room will flood prior to both PXS rooms, and that PXS room B will flood prior to PXS room A. This arrangement is shown diagrammatically in Reference 11.76.

The RCA and non-RCA portions of the Auxiliary Building are separated from one another by thick concrete walls and floors (Reference 11.76). Flooding within the RCA will therefore not propagate to the non-RCA and vice-versa.

The connections, for flood propagation, between the rooms/areas which together constitute the Auxiliary Building RCA and non-RCA are shown in Figures 10-2 to 10-11 in Reference 11.76. The rooms which may be affected by flooding are shown in Figures 10-12 to 10-23 in Reference 11.76. Where the flood height in a room/area reaches the full height of the room, flooding progresses upwards via stairwells or migrates through drains and pipe chases, etc.

The ground elevation of the Turbine Building, Annex Building and Radwaste Building are all graded such that significant flooding would flow away from the nuclear island. However, doorways between the nuclear island and each of these buildings provide potential pathways through which flooding could migrate.

11.3.4.4 Hazard Schedule

The internal flooding hazard schedule (see Table 11.3-3) has been prepared based on the results of the PRHA. In accordance with relevant international guidance (Reference 11.82), the flooding hazard analysis has considered single pipework failures, secondary effects and cascade events in determining the bounding case. The flooding hazard analysis has been prepared on the basis that:

- Flooding will not propagate from one flood area to another; i.e., a flood in Containment may not find its way to the RCA or non-RCA areas;
- All SSC below the maximum flood height for that room will be lost, except where the SSC is qualified for a submerged environment;
- The unmitigated flood height comprises exhaustible sources and 7 hour of inexhaustible supply; significant flooding would not go undetected for longer than 7 hours without operator intervention.

The internal flooding hazard schedule presents, for each room (or group of rooms), the:

- The Fault ID (listed in Chapter 8) associated with the listed flooding event;
- Divisions of each SSC affected[8] by the flood;

8. Only those SSC located below the maximum flood height, which are not qualified for operation in a submerged environment, are reported in the hazard schedule. All SSC not reported in the hazard schedule, but otherwise present in the room, are assumed to be unaffected by flooding and therefore capable of delivering their Category A safety function as required.

- Category A safety function at risk;
- Unmitigated consequences should the plant be unable to effect safe shutdown;
- Redundant SSC available to deliver the Category A safety function, which have not been exposed to the same internal hazard.

The hazard schedule is presented in tabular form providing a concise and comprehensive summary of the postulated flood events, their significance and how the AP1000 plant is designed to cope with the hazard.

11.3.4.5 Discussion of Results

The PRHA have shown the flood heights as a result of pipe rupture in each of the rooms comprising the NI (Reference 11.76).

The analysis has produced the bounding flood height, and the associated bounding flood height. The bounding flood heights have been compared against the elevation of SSC to determine the Class 1 SSC which may become submerged. The results of this analysis are summarised in the following subsections.

Containment Building

The Containment is, in order to maintain the free movement of gases, an open space. The majority of rooms are separated by open grate structures which would not inhibit the movement of fluid; however, the CVS room (11209), PXS valve room B (11207/11208) and PXS valve room A (11206) have substantial concrete partitions/curbs rising to the 103.05 m (110.00 ft), 103.7 m (110.08 ft) and 103.1 m (110.17 ft) levels respectively. Flooding in the general Containment space would therefore only impact the CVS room, PXS valve room B and subsequently PXS valve room A once the partition/curb height has been exceeded (Reference 11.76). The rupture/failure of the RCS or PXS pipework represents the worst case bounding flooding event due to the impacts to floodup levels, environmental conditions, submergence pressure, submergence temperature conditions, containment pressure and external containment cooling environment. Similarly, pipework failure in one of these compartments would initially result in the affected compartment flooding, before cascading into separate compartments. The VWS pipework break coupled with ADS actuation will provide higher flood levels however the related environmental impacts are significantly lower.

During refuelling operations, the refuelling cavity is flooded and, as such, the SSC present in these areas are qualified to operate in a submerged environment.

The CVS room doesn't contain any Class 1 SSCs. PXS valve room A and PXS valve room B contain redundant divisions of the PXS IRWST injection isolation valves. It is not postulated that both PXS valve room A and PXS valve room B flood from a single design basis event, therefore the redundant division remains available to deliver the Category A safety function of coolant make-up following a LOCA.

That PXS room A and PXS room B do not both become flooded from a single design basis internal flooding event is a result of the curb height elevations ensuring preferential flooding of non-sensitive areas of the Containment and the back flow preventers between each of these rooms and the general Containment space.

Auxiliary Building – Radiologically Controlled Area

The Auxiliary Building RCA is physically segregated from the non-RCA by 2 ft (0.61 m) thick (at least) concrete walls and floors. The only systems with the potential to flood the Auxiliary Building RCA are therefore those which originate in or pass through the Auxiliary Building RCA.

In the majority of rooms from 94.7 m (82'-6") level upwards, a rupture of the FPS produces the bounding case flood height for that specific room; given that the FPS is the subject of cascade failure following rupture of the CVS in room 12255, the flood height in communicated rooms is bounded by the HELB of the CVS in room 12255. In all instances, the bounding flood height for the affected room is below the level at which Class 1 SSC would be affected.

The analysis of internal flooding within the RCA has identified the bounding flood source to be a failure of the high energy CVS line in room 12255. This fault is assumed to result in the cascade failure of all other piping systems in the room, namely the CCS, FPS and VWS.

There are no Class 1 SSCs located on Level 1 of the Auxiliary Building RCA; however, Class 1 SSCs would become submerged once flooding progresses to level 2.

At the onset of flooding in the RCA, two redundant Class 1 differential pressure sensors located in the Auxiliary Building RCA sump, located on level 1, will alert operators present in the MCR via the PMS. On receipt of the alarm, operators are required to identify and isolate the sources of flooding. There are several hours to effect isolation of the systems prior to Class 1 SSC becoming submerged.

Auxiliary Building – Non-Radiologically Controlled Area

The Auxiliary Building non-RCA is physically segregated from the RCA by 2 ft (0.61 m) thick (at least) concrete walls and floors. The only systems with the potential to flood the Auxiliary Building non-RCA are therefore those which originate in or pass through the Auxiliary Building non-RCA. The non-RCA is further segregated into electrical and mechanical areas, which are physically segregated from one another by concrete walls and floors such that flooding in the mechanical areas cannot propagate into the electrical areas and vice-versa.

Within the mechanical area, the bounding flood is presented by a failure of the SGS in rooms 12404 or 12406 which is a high energy line. The flood height is limited by pressure relief panels, in each of the rooms, the function of which is to discharge flooding to the Turbine Building 1st bay.

The flood relief panels and floor drains protect Class 1 SSC from the effects of flooding by ensuring that the maximum flood heights in these rooms remains below the elevation at which they would become submerged.

Within the electrical area, all sources of flooding would eventually migrate to level 1 where the batteries are located. With the exception of the PWS, all flood sources are exhaustible and the inventory of individual systems is insufficient to submerge the battery banks which are the lowest elevated Class 1 SSC. The PWS is inexhaustible and would eventually submerge the batteries.

Two differential pressure sensors, located in 12104 and 12105, will alert operators in the MCR of the presence of flooding in this area. The alarm, actuated via the PMS, will prompt

an operator to effect isolation of the PWS (or other flood source) before the level reaches the base of the batteries.

A failure of the PWS located in the operator break room within 12401, will initially flood rooms 12400 and 12401 before spreading, via stairwell S05 to the remote shutdown room, 12303. The door between 12400 and 12411 is watertight. The analysis of flooding in this area (Reference 11.76) shows that it is not credible that flooding progresses to the extent that Class 1 SSC becomes submerged.

Areas Outside the Nuclear Island

Areas outside of the Nuclear Island do not contain any Class 1 SSC and therefore flooding of these areas cannot directly result in a loss of Category A safety functions. However, it is possible that flooding originating in these areas, including that originating from yard tanks, could migrate to the Auxiliary Building. Detailed discussions of the flooding origination and consequences are provided in Reference 11.76. The following subsections consider the implications of flooding in the buildings directly abutting the Nuclear Island (radwaste, annex and turbine) for impact on the Nuclear Island.

Turbine Building

The Turbine Building 1st bay communicates with rooms 12306, 12405, 12504, 12505 and 12506 in the Auxiliary Building non-RCA. The flooring within the Turbine Building 1st bay, at elevations other than the 100 m (100'-0") level, comprises grating with a largely open structure; flooding originating in the Turbine Building 1st bay will flow down to the 100 m (100'-0") level without significant accumulation at higher elevations. Flooding of the Turbine Building 1st bay could therefore only migrate into room 12306.

The MSS is a HE line, failure of which could cause a cascade rupture of the BDS; CCS; CDS; CFS; DWS; FPS; FWS; LOS; MSS; PWS; SSS; SWS; TCS; TDS; TOS; VWS and the VYS. The maximum flood height in the Turbine Building 1st bay is conservatively assumed to exist in room 12306, however this flood height is bounded by a MELB of the SGS. All other communicated areas of the Auxiliary Building non-RCA become wetted only and as such pose no hazard to Class 1 SSC.

Annex Building

There are no sources of flooding present in the Annex Building which are not also present in the Auxiliary Building. Given that there are additional discharge routes, away from the Auxiliary Building, for flooding initiated in the Annex Building, the flood heights as a result of pipe failure are bounded by those which originate in the Auxiliary Building.

Radwaste Building

There are no sources of flooding present in the Radwaste Building which are not also present in the Auxiliary Building. Given that there are additional discharge routes, away from the Auxiliary Building, for flooding initiated in the Radwaste Building, the flood heights as a result of pipe failure are bounded by those which originate in the Auxiliary Building.

11.3.5 Sensitivity of Results and Cliff Edge Effects

The three bounding flooding cases determined for the Containment, RCA portion of Auxiliary Building and the Non-RCA side of the Auxiliary Building demonstrate that the Category A and post-72 hour Category B safety functions can be delivered. Each of the flood

bounding cases are based on large volumes and will require several hours to reach their full flood up heights but these flood heights are not that sensitive not are there any cliff edge effects.

Containment

The Containment flooding is based on all the available flooding volumes possible within the Containment vessel. Flood levels have been reviewed and applicable weirs have been designed and installed to preferentially flood key compartments and not flood others. There is as significant margin and appropriate passive overflow mechanisms to ensure flooding of the PXS-A and PXS-B, is prevented or minimized. The redundancy of trains and barriers between compartments also ensures the boundary flooding event can be accommodated while still delivering the required Category A safety functions to place the plant in a safe shutdown mode.

RCA Side of Auxiliary Building

The PRHA calculations have shown that the cascading break in room 12255 delivers the enveloping flooding condition and still allows the Category A safety functions to occur as necessary. This flooding event occurs over a long duration with sufficient time for operators to react to the event and to isolate the failed pipework before challenging the Containment isolation valves. The flooding event assumes the conservative flood volumes and assumes the water volume spreads over a large portion of the RCA side of the Auxiliary Building undetected. The safety grade sensors identify the break event only after 12 inches of water which provides early indication of this flooding event. There are no cliff edge effects since the time durations are well understood flood volumes are also limited.

Non-RCA Side of Auxiliary Building

The enveloping event on the non-RCA side is related to the possible flooding of the 4 divisions of the Class 1 batteries at the basemat elevation. The worst case enveloping event is the break of the PWS with unlimited water volume. The installation of the Class 1 sensors provides early warning to the MCR operators of the possible flooding event. These sensors provide warnings at the 0.1 m (4 inches) level prior to water making contract with the bottom of the batteries at 0.19 m (7.5 inches). The low flooding rate provides adequate time for operators to isolate the flood sources which are within one floor of the MCR. In addition, the batteries can still deliver the safety function once the bottom of the batteries are contact by water which may reduce their capability, but the flood level can rise another 0.60 m (23.5 inches) before batteries become shorted out. Therefore based on the early warning to the MCR, low flooding rate and extra margin to shorting out batteries eliminates any cliff edge effects. Furthermore, AP1000 can mitigate the consequences of shorting out batteries using self-actuating Class 1 SSCs or by the use of Class 2 SSCs.

11.3.6 Combined Hazards Discussion

The PRHA calculations (Reference 11.77) consider, on a deterministic basis, a single flooding event[9] and the consequential impact on SSC in the affected plant areas.

9. A single flooding event could be a HELB, MELB or cascade failure following HELB.

The consideration of credible combinations of flooding with other postulated internal hazards likely to occur independently of flooding is discussed in Section 11.12. Reference 11.75 provides a coherent approach across all internal hazard types (e.g., fire, explosion, missiles, dropped loads, pressure part failure).

Combinations of independent internal and external hazards (e.g., internal flooding and extreme low ambient air temperatures) are considered to be Beyond Design Basis events and as such have not been explicitly considered in this section. However, compliance with relevant equipment and structural design codes ensure that combinations of internal hazards with the relevant abnormal operating occurrences (including environmental hazards) are addressed.

11.3.7 ALARP Assessment and Discussion

Deterministic analysis of postulated, design basis, internal flooding events shows that the Category A safety functions will be available to provide a safe shutdown following the worst case postulated internal flood.

The AP1000 plant, by its very nature, makes extensive use of water and water based systems to operate normally. It is therefore not possible to remove the hazard of internal flooding from the design of the plant. However, the use of structural barriers has made it possible to protect sensitive areas of the plant from significant sources of liquid, primarily the non-RCA side of the Auxiliary Building.

Where it has not been possible to remove or isolate sources of flooding, Class 1 SSC have been located above the maximum flood height or qualified for operation in a submerged environment. In order to ensure that the maximum flood height does not exceed that of the Class 1 SSC, passive discharge routes have been incorporated into the design (e.g., door gaps, floor drains & flood relief panels).

Further Mitigation Measures

The analysis supporting this assessment of internal flooding has, wherever possible, made claims on passive features to mitigate the effects of flooding. These features include flood relief panels, door gaps and internal floor drains; for the majority of pipe ruptures, the maximum flood level takes no credit of floor drains and the flood height would therefore be considerably lower than that which is presented.

Sump pumps are located in all areas of the Nuclear Island. In the event that a pipe ruptures, as fluid percolates down, the sump pumps would automatically start to displace the liquid as it builds up.

The majority of systems which present a source of flooding require a minimum inventory in order to function correctly. Should the water level drop in the delay/storage tanks as a result of a leak, a number of process level alarms would alert operators in the MCR to the event and corrective action would be taken in significantly shorter times than those credited. For a number of systems, the hazard potential presented by a loss of fluid is such that the reactor would trip, initiating a safe shutdown, long before the hazard to Class 1 SSC was realised.

Additional Means of Providing Safety Functions

The primary Class 1 SSC used to mitigate internal flooding identified in Chapter 8 self-actuate on loss of Class 1 dc power or on loss of the instrument air pressure. This reduces the vulnerability to flooding.

Furthermore, the AP1000 design provides several additional levels of defence that are separate and diverse from the primary Class 1 SSC. As shown in Chapter 8 for frequent faults such as loss of main feedwater, there are separate and diverse Class 1 SSCs that can provide the necessary safety functions. These SSCs provide a passive feed and bleed capability using ADS, Accumulators, IRWST injection and Containment recirculation.

Another level of defence is provided by active Class 2 SSC. These SSCs are separate and diverse from the Class 1 SSC, and are powered by the standby DGs when off-site electrical power and house power are not available. Note that these Class 2 features are not claimed / credited in the deterministic UK safety case.

The active Class 2 SSC includes the following:

- Make-up of borated water to the RCS using the CVS
- Heat removal from the SGs using SG Power Operated Relief Valves and the SGs using start-up feedwater pumps
- Heat removal from the RCS (at reduced pressure) using the RNS
- Supporting functions include:
    - CCS and SWS
    - AC power from the Standby DGs
    - VWS air cooled chillers
    - HVAC by the VBS
    - I&C by the PLS

Internal floods within the NI are anticipated to occur at frequencies <1E-3 per year as shown in Chapter 8 and as a result are classified as infrequent faults. As such, diverse mitigation is not required in the UK. Even so, there are self-actuation and diverse Class 1 passive features of the AP1000 design in providing additional mitigation capability.

Nonetheless, the design of these active, Class 2 SSC has taken into account the potential effects of internal floods in accordance with the American Light Water Reactor Utility Requirements Document (Reference 11.87).

As such, measures have been taken to protect the above listed equipment from postulated internal floods:

- Separating Class 2 equipment from possible flood sources, where practicable.
- Locating equipment above the postulated flood height.
- Separating the redundant of Class 2 equipment

Furthermore, failure of the Class 2 equipment, whether due to an inherent fault or an internal flood, will not prevent the Class 1 SSC from fulfilling their Category A safety functions.

On the basis of the above discussion, and given that Category A safety functions can be maintained in the event of internal flooding, it is judged that there would be minimal safety benefit from introducing additional measures to protect or mitigate the effects of flooding; the risk from internal flooding hazards is therefore considered to be broadly acceptable and

ALARP.

The assessment concludes that Category A safety functions can continue to be delivered following a design basis flood through a combination of claims made on structural barriers, equipment qualification, passive flood relief systems and, where necessary, minimal operator actions to isolate inexhaustible sources of flooding following identification by a level sensor.

11.4 Pressure Part Failure

11.4.1 Introduction

The AP1000 plant Pressure Part Failure assessment (Reference 11.77) has been performed to determine the effects to Class 1 SSC, delivering Category A safety functions and the supporting post-72 hour Category B safety functions necessary to achieve and maintain a safe shutdown plant, resulting from the failure of pressure retaining fluid systems.

The assessment has been based on the deterministic assumption of gross failure of applicable fluid systems. The exception to this is those systems with a structural integrity classification of Highest Safety Significance (HSS) (see Chapter 20). The following conservative assumptions have formed the basis of the assessment of PPF:

- All fluid systems without an Incredibility of Failure (IoF) claim are candidates for gross failure.
- Gross failures are instantaneous circumferential break events.
- Longitudinal breaks are also considered as a function of pipe size and failure location.
- Calculation of the maximum thrust load for pipe whips and jet impingement.
- No operator action will be taken to control or mitigate a failure.
- All SSCs within the zone of influence (ZOI) of a postulated pressure part failure are unavailable, unless the SSCs are designed for the associated loads.
- All SSCs designed for the resulting environmental conditions following a pressure part failure are available.
- A single active failure is present in the plant response to a pressure part failure event.

The assessment concludes that SSCs delivering Category A and supporting post 72-hour Category B are protected from the effects of pressure part failure through a combination of claims made on the location of failures, the protection of SSCs by means of restraints, shield, and barriers, and the engineering qualification of SSCs for post-failure environmental conditions.

11.4.2 Pressure Part Failure Claims, Arguments and Evidence

This section presents the claims, arguments and underlying evidence made in relation to pressure part failure hazards with the potential to inhibit safe shutdown of the reactor plant.

11.4.2.1 Claims Overview

This section presents the claims, arguments and underlying evidence made in relation to pressure part failure hazards with the potential to inhibit safe shutdown of the reactor plant

11.4.2.2 High Level Claim

A pressure part failure event could cause a transient from normal full power operation of the reactor power plant with the potential to result in a hazard on or off site being realised. In response to such a transient, it may be necessary to shut down the reactor and return it to a safe state. Depending on the exact nature of the transient, there are a number of courses of action to shut the reactor down. Ensuring the availability of the Class 1 SSCs required to deliver the Category A safety functions will ensure that the reactor can be shut down, and is the basis of the following high level claim:

Claim IH-3.0: **Postulated pressure part failure events within the Design Basis do not prevent the delivery of the Category A safety functions and the supporting post-72 hour Category B safety functions necessary to respond to the postulated event.**

Within the design of the AP1000 plant, this has been achieved by:

- No claim is made on the prevention of gross failure of systems and components without an incredibility of failure (IoF) argument
- Protecting redundant divisions of Class 1 structures, systems, and component (SSCs) by separation using barriers or physical distance
- Protecting redundant divisions of Class 1 SSCs by restricting the hazard impact through use of restraints, shields, or physical separation
- The use of passively-designed fail-safe equipment
- Where required, SSCs required to implement Category A safety functions are designed for failure conditions
- The SSCs claimed to provide post-72 hour support functions include only offsite procured SSCs and their associated Class 1 connections.

11.4.2.3 Prevention Claims

The AP1000 plant pressure part failure safety case utilises prevention claims to preclude postulated pressure part failure events, as well as to provide a method for combining postulated events for consequence evaluation.

In conjunction with the structural integrity classification process (Chapter 20), it is possible to preclude the possibility of the gross failure of a pressure retaining system or component through the application of an IoF argument. The AP1000 plant structural integrity classification denotes those components with an IoF argument as highest safety significance (HSS).

Claim IH-3.1: **Pressure part failures are deterministically assumed to occur as a gross failure initiating event, except those justified by the**

Structural Integrity Classification as Highest Safety Significance

Sub-Claim IH-3.1.1: **Piping equal to or less than DN25 is considered bounded by failure of larger piping systems when they are present within the same room or compartment.**

Sub-Claim IH-3.1.2: **Failure of fluid systems of moderate-energy cannot result in pipe whip, jet impingement, compartment pressurisation, or decompression transients.**

11.4.2.4 Protection Claims

While it is not always possible to protect the SSCs present in the room/compartment of a postulated pressure part failure event, separation and segregation have primarily been used to protect redundant SSCs throughout the nuclear island (NI).

Claim IH-3.2: **Passive protective measures have been incorporated in the AP1000 design to protect SSCs that deliver Category A and post-72 hour Category B safety functions from pressure part failures.**

Sub-Claim IH-3.2.1: **Consequences of pressure part failure will be contained through the design of barriers or physical separation as to not cause the loss of a Category A or post-72 hour Category B safety function.**

Sub-Claim IH-3.2.1.1: **Class 1 civil/structural relief devices are used to control subcompartment pressure where unmitigated effects may challenge the integrity of claimed Class 1 barriers.**

Sub-Claim IH-3.2.2: **Consequences of pressure part failure will be restricted through the design of shields, restraints, barriers, or physical separation so as to not cause the loss of a Category A or post-72 hour Category B safety function.**

11.4.2.5 Mitigation Claims

Whereas protection of SSCs in rooms/compartments of origin is limited, mitigation of the resulting conditions is possible through the proper design of SSCs and selection of materials.

Claim IH-3.3: **SSCs that deliver required Category A and post-72 hour Category B safety functions will operate following a pressure part failure in the resulting environmental conditions.**

11.4.2.6 Arguments and Evidence

Prevention Arguments and Evidence

Claim: IH-3.1: **Pressure part failures are deterministically assumed to occur as a gross failure initiating event, except those justified by the Structural Integrity Classification as Highest Safety Significance**

The structural integrity assessment, and classification, of systems and components for the AP1000 plant are documented in Chapter 20. Discounting the failure of a component based on an IoF argument removes the postulated failure from the plant design basis; therefore, interfacing design criteria and assessments need not consider these events as initiating failures.

Sub-Claim IH-3.1.1: Piping equal to or less than DN25 is considered bounded by failure of larger piping systems when they are present within the same room or compartment.

Assuming similar process conditions, a larger pipe failure will result in more significant direct effects as well as the associated dynamic consequences. Environmental consequences have been deterministically developed to consider the failure of all applicable piping in a defined room to support equipment qualification as describe in Chapter 5. Further discussion and substantiation of this argument is contained in the pressure part failure topic report (Reference 11.77).

Elevations of the Non-RCA Auxiliary Building located below grade (El. 100.00m (100'-0")) which are not in the vicinity of an enveloping fluid system are limited to DN 1" (1" NPS) piping failures; however, this piping is low temperature moderate-energy piping and is evaluated for unmitigated effects as part of internal flooding in Section 11.3.

Sub-Claim IH-3.1.2: Failure of fluid systems of moderate-energy cannot result in pipe whip, jet impingement, compartment pressurisation, or decompression transients.

The AP1000 plant design applies a piping classification scheme based on the fluid energy levels. This classification system identifies those systems and components with the potential for dynamic effects, e.g., pipe whip and jet impingement, this piping is referred to as high-energy.

Two parameters used to identify high-energy piping and they are applied independently, either parameter is sufficient to consider piping as high-energy.

- Temperature – Normal operating fluid temperature of greater than 93 °C (200 °F) to identify conditions that may result in steam release upon failure.

- Pressure – Normal operating fluid pressure of 1.896 MPa(g) (275 psig) or greater to identify systems with sufficient energy to propel a pipe and create a dynamic response.

In addition to these service conditions, consideration of the frequency of use of the fluid system is also included in the AP1000 plant pressure part failure assessment. Systems or portions of systems that do not exceed the high-energy threshold for either 98% of the system total operating time or 99% of the plant operating life are considered as moderate-energy. As failure probability of these systems is not expected during plant life, additional restriction on high-energy availability adds further confidence that postulated pressure part failure will be a moderate energy event.

The fluid energy classification scheme has been reviewed and adopted internationally as relevant good practice as evidenced by applications in the United States (Reference 11.84), adoption into consensus standards applied in European applications, recognition in international safety standards (Reference 11.89), and application precedent in the UK.

Protection Arguments and Evidence

Claim IH-3.2: Passive protective measures have been incorporated in the AP1000 design to protect SSCs that deliver Category A and post-72 hour Category B safety functions from pressure part failures.

Sub-Claim IH-3.2.1: Consequences of pressure part failure will be contained through the design of barriers or physical separation as to not cause the loss of a Category A or post-72 hour Category B safety functions.

The AP1000 plant is segregated into rooms, or compartments composed of one or more rooms; these rooms/compartments are separated from one another by suitably designed civil/structural barriers constructed of reinforced concrete or composite steel construction. These barriers are identified in the AP1000 plant Hazard Barrier Matrix (Reference 11.9). The principal protection features to protect essential SSCs from the dynamic effects of a pressure part failure event are barriers. The pressure part failure assessment claims barriers consistent with the resulting mitigated consequences; i.e., flood, ventilation, pressure, radiological, missile. Environmental effects are not assumed to be constrained by barriers unless they are specifically designed for the resulting conditions.

Barriers protecting Class 1 SSCs are themselves Class 1 structures and are rated for load-bearing capacity and integrity. Specific to high-energy pipe failures in the main steam and main feedwater systems located in the Turbine Building, seismically-designed Class 2 barriers are acknowledged in the protection of SSCs inside the nuclear island. Where acceptable load conditions are not practicable, the addition of restraints or the design of essential SSCs for the resulting conditions are permissible means to address the consequences of a pressure part failure event.

If there are no barriers available, zones of influence determine the scope of consequences. These zones of influence are discussed in the pressure part failure topic report (Reference 11.77) and defined consistent with recognised consensus standards and good practice (Reference 11.89).

Sub-Claim IH-3.2.1.1: Class 1 civil/structural relief devices are used to control subcompartment pressure where unmitigated effects may challenge the integrity of claimed Class 1 barriers.

Subcompartment pressurisation is a dynamic effect of a pressure part failure in associated rooms and results in distributed loads upon the associated barriers. The magnitude of pressurisation is a function of the rate of mass and energy release, the volume of the room or compartment, and the venting capability of the room or compartment.

The Containment Vessel is claimed for retention of pressurisation effects from all postulated pressure part failures located within its pressure boundary consistent with the vessel's function as a fission product barrier. The Auxiliary Building is a reinforced concrete structure that provides structural support and protection of Class 1 SSCs outside of the Containment Vessel. Postulated failure of large diameter high-energy piping has to potential to over-pressurise rooms in the Auxiliary Building with an unmitigated consequence of damage to claimed Class 1 barriers.

Pressure relief panels are designed for those rooms that require additional venting capability to protect the integrity of a claimed Class 1 barrier. These pressure relief panels are Class 1

SSCs and designed to be self-actuating (e.g., they require no power or C&I interface to operate). These devices are controlled by passive means such as the panel mass or shear pins. Due to the inherent reliability of the control device and its passive nature of actuation, the pressure relief panels are not subject to an assumption of single active failure. Relief panels are identified in the hazard schedule.

Sub-Claim IH-3.2.2: Consequences of pressure part failure will be restricted through the design of shields, restraints, barriers, or physical separation so as to not cause the loss of a Category A or post-72 hour Category B safety function.

Where separation or the design of intervening barriers is not adequate to protect essential SSCs, the dynamic effects of the postulated pressure part failure event may be restricted through the design of restraints or shields. The application of these protective measures results in a restrained zone of influence, which decreases the extent of the dynamic effects of pipe movement.

Restraints and shields are limited to the restrictions and modifications of dynamic pipe movement and do not affect the environmental responses in affected regions of the plant.

Pipe restraints and shields protecting Class 1 SSCs are themselves Class 1 structures and are rated for load-bearing capacity and integrity. Restraints and shields are designed with structural attachment points and their corresponding faulted load conditions are analysed for acceptability.

Mitigation Arguments and Evidence

Claim IH-3.3: SSCs that deliver required Category A and post-72 hour Category B safety functions will operate in conditions following a pressure part failure event.

As described in Chapter 5, Class 1 SSCs are designed to operate in differing environmental conditions which include consideration of:

- Temperature
- Pressure
- Radiation
- Humidity
- Spray Wetting
- Submergence
- Chemical Effects

The limiting environmental conditions within the AP1000 plant are defined by room and reflect the full spectrum of pressure part failure events. Components within rooms are qualified for the resulting conditions through application of the AP1000 plant equipment qualification methodology as described in Chapter 5.

Design requirements are applied in addition to qualification testing to reduce the exposure of sensitive materials to harsh environments; these include the use of passive components with metallic parts and enclosure within an IEC IP66 or NEMA 4/4X rated enclosures for mitigation of spray effects.

For the evaluation of plant response to a postulated pressure part failure, it is assumed that all SSCs affected by the environmental consequences of a pressure part failure event that are not qualified for the conditions are not available.

11.4.3 Pressure Part Failure Safety Case Summary

11.4.3.1 Introduction and Overview

Pressurised components within the AP1000 design comprise pipes, pipe components (such as valves and sensors), vessels, tanks and HXs. Failure of such components may result in direct effects, such as the failure of a train of the system associated with the pressurised component. Such pressure part failures are considered within the AP1000 design as internal plant faults and are listed in the fault schedule (Chapter 8, Appendix 8A).

In addition, pressure part failures also have the potential to cause damage to other plant items due to indirect effects such as:

- Pipe whip
- Jet impingement
- Jet spray
- Subcompartment pressurisation
- Asymmetric pressurisation of large equipment
- Fluid Decompression (e.g., water hammer)
- Environmental effects
- Missiles
- Flooding
- Blast effects

Pipe whip, jet impingement, jet spray, subcompartment pressurisation, asymmetric pressurisation of large components, fluid decompression, and environmental conditions are discussed in this section. Missiles, flooding, and blast effects (i.e., explosions) are contained within their respective sections of this PCSR chapter.

Consideration of the pressure part failure analysis is focused on those areas containing the Class 1 SSCs, namely the AP1000 plant nuclear island. Consideration of pressure part failures in locations outside of the nuclear island is limited to a demonstration that the NI is adequately protected from postulated pressure part failures from these sources by physical barriers.

The scope of the AP1000 plant pressure part failure assessment includes pressurised systems and components, including in line components; e.g., valves, sensors, vessels, and heat exchangers. The gross failure of these inline components is evaluated as part of the pressure part failure assessment in the form of the connections to the associated piping. This approach is applied for hazard evaluation based on the following considerations:

- Components such as valves are more robust that the connecting piping as required by the ASME Code (References 11.91 and 11.3) and associated supporting standards.

- The failure of an inline component is limited to the energy and inventory of the connecting system; therefore, failure of the connecting piping envelops the consequential effects.

- Components such as valves and instruments represent constrictions in flow paths that are bounded by the assumption of flow area of the connecting pipe.

- Failure of in-line components that create missiles are discussed in Section 11.6.

- Rupture of tanks and vessels are considered inputs to the internal flooding assessment and discussed in Section 11.3.

11.4.3.2 Applicable Codes and Standards

Pressure part failure assessments have been undertaken in accordance with the following principal codes and standards, as discussed in the topic report (Reference 11.77):

- ASME Boiler and Pressure Vessel Code, Section III, 'Rules for Construction of Nuclear Power Plants' (Reference 11.90);

- ASME B31.1, 'Power Piping' (Reference 11.3);

- ANS-58.2, 'Design Basis for Protection of Light Water Nuclear Power Plants against the Effects of Postulated Pipe Rupture' (Reference 11.84);

The AP1000 Equivalence/Maturity Study of US Codes and Standards (Reference 11.25) determines, based on their importance to safety, the applicability, adequacy and sufficiency of those standards when compared with relevant UK and international good practice. It also provides a clear and auditable demonstration that all codes and standards to support the design substantiation of UK safety related or safety significant SSCs have been identified.

To evaluate the AP1000 design codes and standards against the UK expectations, the codes and standards have been organised by the relative safety significance of the SSCs to which they have been applied. The safety significance has been determined in accordance with the AP1000 UK Safety Categorisation and Classification Methodology (Reference 11.26), which describes the process for categorisation of safety functions and classification of SSCs.

11.4.3.3 Redundancy and Segregation

Measures have been applied to ensure that postulated pressure part failures cannot prevent Class 1 systems from delivering their Category A safety functions. The measures are set out in the safety design approach adopted for the control and mitigation of the pressure part failure hazard. The measures related to redundancy, separation, and segregation are described below:

- The design of the AP1000 plant ensures multiple means of delivering the Category A safety functions, such that a pressure part failure cannot prevent delivery of the Category A safety function.

- Within the Containment, segregation of Class 1 systems is provided by a combination of barriers formed by the walls/floors of compartments and the distance between systems providing redundant means of delivering Category A safety functions.

- Outside Containment, only a limited portion of the CVS and SGS have been identified as a location for high-energy breaks based on the pipe rupture design criteria. There is sufficient equipment redundancy, segregation, and protection such that all of the equipment in a single room can be lost without preventing delivery of the Category A safety functions.

- The Class 2 systems are an additional defence in depth means of delivering Category A safety functions. The Class 2 system design also features redundancy.

11.4.3.4 Pressure Part Failure Assessment Approach

Analysis of postulated pressure part failure events has been performed in accordance with the AP1000 plant pipe rupture design criteria in Reference 11.77 on a room-by-room basis. The assessment criteria provides the methodology for determining the locations of pressurised failures, the effects of such failures, and the approach to be adopted to assess the impact of such failures on Class 1 SSCs.

Each fluid system is initially analysed for gross failure, regardless of pipe size or system energy. The resulting plant-level initiating event is compared to the fault schedule in Appendix 8A to ascertain the design basis classification of the event. Design basis classification is assigned to plant faults to determine the limits for the assessment of tolerability and acceptable means and methods for evaluation. Tolerability of the resulting plant response is confirmed consistent with the plant fault study and transient analysis in Chapter 9.

Whereas the evaluation of the gross failure of pressure parts cannot be eliminated through an argument of low initiating event frequency the probability of occurrence is a consideration in the selection of the design basis classification as described in Chapter 8. In general, pressure part failure events are treated as DB1 Class (Infrequent Faults) for evaluation purposes, specific event and design basis classification assignments are contained in the hazard schedule (Tables 11.4-1 and 11.4-2)

The assessment approach has been applied in the following manner, as presented in Figure 11.4-2.

1. Identification of hazard sources, including consideration of:

    a. Pressurised system energy level
    b. Postulated rupture location

2. Evaluation of the indirect effects of the pipe break, including:

    a. Dynamic effects including hydraulic transients, pipe whip, jet effects and subcompartment pressurisation

    b. Environmental effects

    c. Flooding/Submergence (Section 11.3)

3. Evaluation of the consequence of the indirect effects on essential Class 1 equipment, namely functionality of Category A safety functions consistent with the transient and accident analysis.

4. Identification of response measures required to ensure plant response to the failure is ALARP:

    a. Prevention
    b. Protection

        i. Barriers/Arrangement of equipment
        ii. Restraints and Shields

    c. Mitigation

11.4.3.5 Implementation and Management of the Pressure Part Failure Assessment Process

The initial assessment of pressure part failure effects has been performed and includes postulated pressure part failures in high and moderate-energy systems. This assessment was supplemented by the inclusion of additional postulated events shown to not present (Reference 11.77):

1. Significant challenges to the tolerability of the AP1000 safety case,

2. Substantial design changes with high complexity affecting multiple existing designed systems, structures or components, and

3. An increased potential for lower complexity design changes.

11.4.3.6 Interface with Other Internal Hazards

With consideration of the propagation of a failure and the assessment of the plant response, the evaluation of internal pressure part hazards is an input to several other internal hazard evaluations, a summary diagram of internal hazards interfaces in included in Figure 11.4-1. Internal flooding is addressed in Section 11.3, internal explosions resulting from pressure part failures are addressed in Section 11.5, and internal missiles are addressed in Section 11.6.

11.4.3.7 Conclusions

Assessment of pressure part failures for the AP1000 plant has been completed and documented in the pressure part failure topic report (Reference 11.77) and the hazard schedule (Tables 11.4-1 and 11.4-2).

The pressure part failure assessment demonstrates that necessary Category A safety functions can be appropriately maintained following postulated pressure part failure events with AP1000 plant Class 1 SSCs. As the design criteria guiding the detailed pipe rupture assessment methodology has been clearly defined in Reference 11.77 for consideration during the development of design changes or assessment of as-installed deviations, it is concluded that future AP1000 plant pipework design activities will not invalidate the conclusions of this safety case.

11.4.4 Pressure Part Failure Analysis

11.4.4.1 Identification of Potential Sources of Pressure Part Failure

A review of the AP1000 plant design has been performed in accordance with the AP1000 plant pipe rupture design criteria in Reference 11.77. This process included consideration of:

- High-energy piping
- Moderate-energy piping
- Piping components, such as valves and sensors
- High-pressure vessels, tanks, and heat exchangers

The approach applied for high-energy piping is summarised below and can be referenced in Appendix A of the pressure part failure topic report (Reference 11.77); moderate-energy piping is not specifically discussed here as the failure of this piping is limited to environmental effects and is therefore less dependent of failure location considerations.

- DN 100 (4" NPS) and larger: Circumferential and longitudinal failures are evaluated at terminations and at intermediate locations where the pipe stress or fatigue duty is significant. Branch connections are regarded as terminations and, at terminations, only circumferential breaks are assumed.

- Larger than DN 25 (1" NPS) but less than DN 100 (4" NPS): Circumferential breaks are postulated considering the pipe stress or fatigue duty.

- DN 25 (1" NPS) and smaller: No breaks are explicitly postulated as the effects are bounded by larger piping.

Piping will be of high quality, designed as ASME Section III for Class 1 piping systems or ANSI/ASME B31.1 Power Piping Code for non-Class 1 systems.

11.4.4.2 Consequences of Postulated Pressure Part Failures

The consequences of the breaks are analysed for dynamic effects (pipe whip, hydraulic transients, jet impingement, and compartment pressurisation), environmental effects on Class 1 SSCs, and operability of essential Class 1 SSCs.

Due to reduced flow area of small diameter piping and the resulting low failure energy, effects due to breaks of pipes DN 25 (1" NPS) and smaller are assessed considering the following attributes:

- Indirect effects of pipe whip and jet impingement on small diameter pipework, tubing, and sensitive instruments.

- Indirect effects on Class 1 equipment due to the resulting environmental conditions, including flooding.

An operability review was undertaken with the objective to provide assurance that Class 1 SSCs are not adversely affected by jet impingement or pipe whip by identifying:

- SSCs that are within the unrestrained zone of influence of circumferential and longitudinal pipe breaks.

- SSCs inside of a unrestrained zone of influence that are essential to the mitigation of the effects of the postulated break

  – Consideration of protection of these Class 1 SSCs through the use of barriers or restraining the failure.

- Essential in-line components that are required to function to mitigate the postulated break and qualify them for the effects of the transients.

The evaluation of the post-rupture environmental effects made appropriately conservative assumptions about the environment that would exist following a postulated pressure part failure in order to determine the impact on exposed equipment. The assessment reviews for the potential impact of:

- Spray wetting effects

- Environmental effects such as rupture-induced pressure, steam, corrosiveness, combustibility, radiation, and chemical spills.

- Temperature and humidity effects.

Dynamic pipe effects are evaluated for high-energy piping as moderate-energy piping is not considered to have the potential to propagate the free end of a broken pipe as described in Sub-Claim 1.2.

Each of these environmental effects is addressed, with specific applications discussed below.

Spray Wetting Effects

In accordance with ANSI/ANS 58.2, "Design Basis for the Protection of Light Water Nuclear Power Plants against the Effects of Postulated Pipe Rupture" (Reference 11.84), a thin film of liquid at the jet temperature (by high-energy circumferential or longitudinal breaks) is assumed to cover the target. Class 1 systems and components are evaluated for the potential effects of spray from high-energy and moderate-energy failures. The following other key evaluation assumptions are noted:

- Spray effects are assumed to be limited to the compartment in which the pipe failure occurs.

- Spray effects are assumed to wet all systems and/or components in a compartment.

- Spray effects are not assumed to damage non-electrical passive metallic components (piping, ducts, valve bodies, mechanical components of valve operators).

- Spray effects are assumed to cause failure of electrical components and cables not designed to withstand the wetting.

- Spray effects are not assumed to affect components protected by IEC IP66 or NEMA 4/4X enclosures.

Environmental Effects

Class 1 systems and components have been evaluated for environmental effects through comparison of the calculated post-rupture environment to the environmental qualification requirements for the system or component consistent with the requirements of Chapter 5.

The escape of steam, water, combustible, or corrosive fluids, gases, and/or heat in the event of pipe rupture are ensured to not preclude:

- Habitability of the control room
- Capability of Class 1 instrumentation, electrical power supplies, electrical and mechanical components, and controls to perform their post-rupture safety function(s)

The effect of corrosive fluids is considered through the evaluation of the environmental qualification chemistry parameters. The evaluation of combustible fluids or liquid is contained within Section 11.5.

Temperature and Humidity Effects

The temperature increases resulting from a pipe rupture in compartments and sub-compartments containing Class 1 SSCs have been evaluated to verify that they bound the temperature and humidity conditions used in the environmental qualification of those SSCs and that the module frames and supporting (or overhead) structures/embedments can withstand the differential expansion between steel and concrete.

11.4.4.3 Propagation of Pressure Part Failure

Pipe rupture can result in dynamic effects, such as pipe whips and jets, which can result in damage to adjacent pipe lines and their associated functions. Testing, analysis, and a review of international design practices is summarised in the pressure part failure topic report (Reference 11.77). The evaluation of a pipe whip shall be considered to propagate:

- Gross failure to impacted pipes of smaller nominal pipe size, irrespective of pipe wall thickness.
- Gross failure is not considered for interactions between a faulted pipe and an equal or larger pipe, based on nominal size.
- Leakage cracks are considered for environmental effects where the pipe wall thickness of the impacted pipe is equal to or less than that of the pipe with a postulated gross failure.

External loads applied to pipe systems from jet spray are calculated using generally accepted methods (Reference 11.89) and applied as inputs into the pipe stress analysis.

11.4.5 Design and Construction Considerations

General

All safety-significant SSCs within the AP1000 plant have been categorised and classified in accordance with Reference 11.26. This process, which also includes fluid-retaining structures, ensures that the quality requirements placed on SSCs, in terms of their design, manufacture, testing, and operation, reflects their importance to safety and hence minimises,

so far as is reasonably practicable, the likelihood that they may fail to provide their safety function.

Section 16.5 details the relevant design standards, primarily Section III of the ASME Code, including the loading and loading combinations for the Containment and associated penetrations, which includes loads from postulated pipe breaks, jet impingement, missile impact, pressure and temperature loads.

Protection

The plant arrangement is based on maximising the physical separation of redundant Class 1 components and systems from each other and from other SSCs as appropriate. Therefore, in the event a pressure part failure occurs, there would be a minimal effect on other Class 1 systems or components required for safe shutdown of the plant or to mitigate the consequences of the failure.

The effects associated with a particular pipe failure are mechanistically consistent with the failure. Thus, pipe dimensions, piping layouts, material properties, and equipment arrangements are considered in defining the specific measures for protection against the consequences of postulated failures.

Protection against the dynamic effects of pipe failures is provided by physical separation of systems and components, barriers, equipment shields, pipe whip restraints, and qualification or analysis of failure loads. The precise method chosen depends upon considerations such as accessibility and maintenance.

The preferred method of providing protection is through separation. When separation is not practical, pipe whip restraints are used. Barriers or shields are used when neither separation nor pipe whip restraints are practical.

Separation

The plant arrangement provides separation, to the extent practicable, between redundant safety systems (including their appurtenances) to prevent loss of safety function as a result of events for which the system is required to be functional. Separation between redundant safety systems, with their related appurtenances, therefore, is the basis protective measure incorporated in the design to protect against the dynamic effects of postulated pipe failures.

In general, separation is achieved by:

- Class 1 and 2 SSCs located remotely from high-energy piping, where practicable
- Redundant safety systems located in separate compartments, where practicable

Where separation by distance is not possible, the pressure part failure assessment includes an evaluation to determine the systems and components that require a structure for separation from the effects of a break in a high-energy line. For these structures, the evaluation assumes that the break may be at the closest point in the line to the separating structure.

Design of Pipe Whip Restraints

When protection of Class 1 SSCs in the unrestrained zone of influence cannot be achieved through separation, a pipe whip restraint may be used to reduce the zone of influence down to a narrow, restrained zone of influence which may then exclude the Class 1 SSCs. Detailed

design requirements for pipe whip restraints can be referenced in the pressure part failure topic report (Reference 11.77).

Location of Pipe Whip Restraints

Pipe whip restraints are located as close to the axis of the reaction thrust force as practicable. Pipe whip restraints are generally located so that a plastic hinge does not form in the pipe. If, because of physical limitations, pipe whip restraints are located so that a plastic hinge can form, the consequences of the whipping pipe and the jet impingement effect are further investigated. Lateral guides are provided where necessary to predict and control pipe motion.

Pipe whip restraints are designed and located with sufficient clearances between the pipe and the restraint in such a way that they do not interact and cause additional piping stresses. A designed hot position gap is provided that allows maximum predicted thermal, seismic, and seismic anchor movement displacements to occur without interaction between the pipe and the pipe whip restraint.

The pipe whip restraints do not prevent the access required to conduct in-service inspection examination of piping welds. When the location of the restraint makes the piping welds inaccessible for in-service inspection, a portion of the restraint is designed to be removable to provide accessibility.

Analysis and Design of Pipe Whip Restraints

The criteria for the analysis and design of pipe whip restraints for postulated pipe break effects are provided in the pressure part failure topic report (Reference 11.77). The criteria are consistent with the guidelines in ANS-58.2-1988 (Reference 11.84).

Barriers and Shields

In addition to pipe whip restraints, other protective devices are designed to protect against the effects of postulated pipe ruptures. Barriers and shields are designed to protect against jet impingement. Guard pipes in the Containment penetration regions provide confidence that fluid discharge due to a pipe rupture will not enter the annulus between the Containment vessel and the Shield Building.

Jet Impingement Barriers and Shields

Barriers and shields, constructed of either steel or concrete, are provided to protect Class 1 equipment from the effects of jet impingement resulting from postulated pipe breaks. Barriers differ from shields in that barriers may also accept the impact of whipping pipes. Protection requirements are met through the protection afforded by walls, floors, columns, abutments, and foundations.

Barriers and shields include walls, floors, and structures specifically designed to provide protection from postulated pipe breaks. Design criteria and loading combinations are according to Chapter 16. Barriers and shield that are added to the plant design for the specific purpose of the pressure part failure assessment are designed for loads from a break in the line at the closest location to the structure.

Auxiliary Guard Pipes

Guard pipes are specialised shields applied to protect against the effects of postulated gross failures within or onto Containment penetration assemblies; guard pipes are Class 1 SSCs.

The use of guard pipes has been minimised by plant arrangement and routing of high-energy piping. Guard pipes in the Containment annulus area are designed according to the rules of Class MC, subsection NE, of the ASME Code. The guard pipe assemblies are subjected to a pressure test performed at the maximum operating pressure of the enclosed process pipe.

11.4.5.1 Discussion of Results

The following subsections briefly describe the principal conclusions of the pressure part failure assessment. Areas reviewed in this section include:

- Containment
- The Non-RCA Auxiliary Building
- The RCA Auxiliary and Shield Buildings
- Building adjacent to the NI
- Areas outside of the NI

Postulated pressure part failures are summarised in detail in the hazard schedule (Tables 11.4-1 and 11.4-2); the summary of effects provided in this section are a narrative of significant observations and conclusions from the evaluation of these events.

Although the primary issues addressed in this subsection are the potential hazards posed by pressure part failures to Class 1 equipment, consideration is also given to Class 2 equipment delivering the supporting post-72 hour Category B safety functions:

- **Long-term power supply**: Supply of long-term power to the Class 1 voltage regulating transformers (PMS divisions B and C) provided by two electrical connections in the Annex Building.

- **Post-accident monitoring**: The equipment with the Category B safety function of post-accident monitoring is located in various areas of the non-RCA Auxiliary Building, including the main control room (MCR) (room 12401), the remote shutdown room (room 12303), and control and instrumentation equipment rooms (rooms 12301, 12302, 12304, and 12305).

- **MCR lighting**: Equipment associated with this function is located in room 12401.

- **MCR and C&I room ventilation**: Equipment associated with this function is located in the MCR (room 12501) and C&I ventilation compartments (rooms 12302 and 12304).

- **Makeup to the passive containment cooling water storage tank and spent fuel storage pool**: Equipment associated this Category B safety function is located external to the NI and in room 12306, this includes the passive containment cooling system valves for alignment of post-72 hour water sources.

Additionally, the AP1000 plant design incorporates several other SSCs that are provided to minimise the severity of postulated pressure part failures or the demand rate on the passive, Class 1 safety features. The plant design also incorporates appropriate monitoring features for the detection of pressure part failures in the vicinity of the WLS sump (level detector) and RCS (inventory monitoring).

Containment

The analysis of pressure part failures indicates that all but a small number of potential break sites occur on systems entirely or principally located within the Containment vessel. These systems are:

- Reactor Coolant System (RCS)
- Steam Generator System (SGS)
- Passive Core Cooling System (PXS)
- Chemical and Volume Control System (CVS)
- Normal Residual Heat Removal System (RNS)

Postulated pressure part failures within the Containment could result in one or all of the following effects: pipe whip, jet impingement, and pressure effects. Pressure part failure evaluations have been completed and have demonstrated that the delivery of Category A safety functions is not inhibited by the indirect effects of these postulated failure events. The potential sources of such effects are further summarised below.

A number of rooms in Containment contain inboard Containment isolation valves. These Containment isolation valves are provided with redundant valves outside Containment in the RCA Auxiliary and Non-RCA Auxiliary Buildings, which will remain unaffected by the possible pipe whip, steam release and water spray events. Furthermore, Class 1 Containment isolation valves are protected and qualified for the dynamic and environmental effects of postulated gross failure events to ensure their function is not adversely affected.

Pipe Whip

Pipe whip has been evaluated in several rooms in the plant as summarised in the pressure part failure topic report (Reference 11.77) and hence safety Class 1 SSCs contained in them are protected against pipe whip. Where the potential for pipe whip cannot be precluded then protection for affected essential Class 1 SSCs is provided in the form of pipe whip restraints or barriers or shields. Chapter 16 addresses the requirements on the civil structures to protect against pipe whip.

Jet Impingement

The following systems are potential sources of jet impingement inside the Containment:

- RCS, including the:
  - Reactor vessel.
  - Pressurizer.
  - Reactor coolant pumps.
  - Steam generator channel heads.
  - ADS.
  - Associated piping and valves including automatic depressurisation features.
- The SGS, including the
  - Steam generator shell.
  - Main steam lines inside Containment.
  - Feedwater lines inside Containment.

- The PXS, including:
  - Accumulator tanks.
  - The CMTs.
  - PRHR heat exchanger.
  - RNS.
  - CVS.

The structural integrity of the reactor vessel, pressuriser, SGs, reactor coolant loop piping, RCPs, PRHR HX, CMT, and accumulator are substantiated in Chapter 20. Failure of these components within the scope of pressure part failure is not deemed credible because the pressuriser is fitted with safety valves. Rupture of the PRHR system HX is also not a credible jet impingement hazard, because the HX is normally submerged and located within the IRWST.

Safety Class 1 SSCs are protected from jet effects through separation as a result of their physical location and the function of barriers, or through the restriction of failure consequences by the application of restraints or shields.

Safety Class 1 equipment within the areas listed below is redundant and has been qualified to withstand the faulted environment without loss of operability consistent with Chapter 5. The areas are:

- Operating deck and refuelling cavity, which contain the following safety Class 1 equipment. The safety-related equipment in this location is:
  - Class 1E cable trays.
  - Class 1E electrical penetrations.
- ADS valve areas.
- SG compartments.
- Vertical access and RCDT room.
- General access and maintenance areas (includes maintenance floor, maintenance mezzanine, and portions of the operating deck away from the refuelling cavity) which contain the following safety Class 1 equipment.
- Main steam lines.
- Main feed water lines.
- SG blowdown lines.
- Start-up feed water lines.
- Passive core cooling system compartments. Under specific conditions, the following components within the PXS compartments could be exposed to indirect effects if a pressure part failure is postulated:
- Accumulators and isolation valves for the accumulators.

- CMTs and isolation valves for the CMTs.
- IRWST isolation valves.
- Containment recirculation piping and valves
- One normally closed spent fuel pit cooling system Containment isolation valve and one normally closed RNS Containment isolation valve.
- Automatically actuated Containment isolation valves.
- RCS to RNS pump suction isolation valves.

Pressurisation Effects

Where a postulated pressure part failure event may occur in the SG compartment, the structure is designed to prevent this failure from affecting the redundant SSCs in the other SG compartment or SSCs in the adjoining RCS loop compartment. The DN 80 (3" NPS) CVS purification pipe, the DN 100 (4" NPS) SG blowdown line, the DN 500 (20" NPS) main feed water line and the DN 150 (6" NPS) start-up feed water line all have postulated failures that may lead to pressurization effects within the SG compartments.

The SG compartments are provided with composite concrete-steel walls and are separated from each other by the reactor cavity and the refuelling compartment. The SSCs in the SG compartments have redundant trains, which are segregated between the two SG compartments. Segregation of these areas is such that an overpressure in the SG compartments would not affect the redundant train.

The DN 80 (3" NPS) CVS regenerative HX return line and the DN 80 (3" NPS) CVS purification supply line from the cold leg have postulated failures within the vertical access (room 11204) and RCDT room (room 11104). The boundaries of the room are designed to prevent this affecting the redundant SSCs in segregated areas.

The DN 100 (4" NPS) ADS pipe in the ADS valve area is open to the main volume of Containment, and hence, compartment differential pressures would be negligible following rupture of this pipe. Therefore, no damage to SSCs is expected to occur from the effects of postulated pressure part failures.

The DN 150 (6" NPS) start-up feedwater line within the maintenance area has such a large free volume that it is judged that the effects from a rupture of this pipe would be dissipated before it could damage the SSCs in its vicinity.

The failure of the DN 100 (4" NPS) SG blowdown or DN 80 (3" NPS) CVS purification piping in the CVS room and pipe tunnel (room 11209) will result in pressure effects. Additional mass and energy released evaluated to support the AP1000 design include the failure of the DN 100 (4" NPS) pressuriser spray line in pressuriser spray valve room (room 11403). The postulated failure of these lines all have been analysed to result in pressurisation effects (Reference 11.77).

Non-RCA Auxiliary Building

High-energy break locations within the Non-RCA Auxiliary Building are limited to the Main Steam Isolation Valve (MSIV) Compartments (rooms 12204/12505 and rooms 12406/12506) and the valve/piping penetration room (room 12306), which are separated from the balance of

the structure by suitable barriers. This piping from the high-energy systems passes through the Non-RCA Auxiliary Building between the Containment/Shield Building and the Turbine Building. Pressure part failure evaluations have been completed and have demonstrated that the delivery of Category A safety functions is not inhibited by the indirect effects of postulated failure events in the Non-RCA Auxiliary Building.

This piping is designed to ASME Section III requirements; additionally, due to the function of the piping as Containment pressure boundary and the close proximity of the Class 1 C&I equipment and facilities, this piping is designed with additional supplemental deterministic requirements to provide added confidence that the gross failure of the piping will be a very unlikely event.

The areas within the Non-RCA Auxiliary Building that contain these hazard sources are summarised in turn in the following text.

Main Steam Isolation Valve Compartments

Each compartment comprises:

- A main feedwater line.
- A startup feedwater line.
- A main steam line.
- Steam isolation valves.
- A power-operated atmospheric relief valve.
- Six safety valves.
- Heating and cooling equipment.

Failure of the feedwater and steam lines within the MSIV compartments are very low probability faults in the hazard schedule. Pipe restraints are used to prevent pipework impact with the compartment walls by limiting movement of the pipe in the event of a break for those failures that may directly impact the Class 1 C&I spaces and the integrity of the main control room. The compartment walls will also prevent the spread of steam or water from steam releases or water spray incidents from affecting the rest of the clean Auxiliary Building.

The MSIV A Compartment and MSIV B Compartment are protected from excess pressure through use of self-actuated pressure relief devices consistent with Claim IH-3.2.2.1. Devices claimed to protect the affected Class 1 barriers are identified in the hazard schedule.

Assessment of the gross failure of a main steam line in the MSIV B Compartment (rooms 12404/12504) is summarised in the pressure part failure topic report (Reference 11.77).

Valve and Piping Penetrations

The valve and piping penetration room at elevation 100 m (100' 0") contains automatically actuated Containment isolation valves for the VWS, SGS, PCS, DWS, as well as PCS recirculation equipment, piping and valves. A pipe whip from the PCS is not expected since the PCS is a moderate-energy system. Dynamic effects from the gross failure of piping in these areas are limited to the SGS blowdown piping in room 12306.

The valve and piping penetration room communicates with the MSIV A compartment through openings in the interfacing barrier. This room is protected from excess pressure

through use of self-actuated pressure relief devices consistent with Claim IH-3.2.2.1. Devices claimed to protect the affected Class 1 barriers are identified in the hazard schedule.

RCA Auxiliary and Shield Buildings

High-energy break locations have been identified in CVS pipework located in rooms 12156, 12255, 12258, and 12259. A break in these rooms does not adversely impact Class 1 SSCs. Pressure part failure evaluations have been completed and have demonstrated that the delivery of Category A safety functions is not inhibited by the indirect effects of postulated failure events in the RCA Auxiliary and Shield Buildings.

Beyond the high-energy systems for which detailed assessments have been carried out, the radiological Auxiliary Building is potentially subject to indirect, environmental effects from a variety of potential sources, including:

- Component Cooling Water System (CCS)
- Central Chilled Water System (VWS)
- Hot Water Heating System (VYS)
- Spent Fuel Pool Cooling System (SFS)
- Normal Residual Heat Removal System (RNS)
- Main Control Room Emergency Habitability System (VES)

The areas within the RCA Auxiliary and Shield Buildings that contain these hazard sources are addressed in turn in the following text.

Normal Residual Heat Removal System Pumps, Heat Exchangers and Containment Isolation Valves

The RNS pumps are located at elevation 89.79 m (66' 6") with each pump train provided in a separate room (room 12162 [RNS A] and room 12163 [RNS B]).

The RNS suction line from the RCS branches inside the Containment into two parallel trains. Each train has two RCS isolation valves inside Containment, one of which is a Containment isolation valve. The two RNS suction lines are separated and have separate Containment penetrations, separate outside Containment isolation valves, and separate piping to their corresponding RNS pump. Therefore, no potential exists for a postulated pressure part failure in one train to impact the other when the RNS is in use.

The RNS pumps, heat exchangers and their associated piping and valves are not located in the vicinity of high-energy piping, therefore there are no postulated pressure part failure that could result in dynamic effects upon this equipment. Class 1 RNS SSCs in the Auxiliary Building are qualified for their associated environmental conditions, including postulated gross failure events.

Containment Isolation Valves

A number of rooms in the RCA Auxiliary Building contain Containment isolation valves. These Containment isolation valves are provided with redundant valves inside the Containment, which will remain unaffected by the possible pipe whip, steam release and water spray events. Furthermore, Class 1 Containment isolation valves are protected and qualified for the dynamic and environmental effects of postulated gross failure events to ensure their function is not adversely affected.

Habitability System Compressed Air Tanks

Compressed air tanks for the VES are located within a structural steel frame in the VES air storage area at elevation 110.74 m (135' 3"). However, there are no other Class 1 SSCs in close proximity, piping is limited to small diameters (DN 25 (1" NPS) or less), and concrete walls segregate the compressed air tank storage area from other rooms at elevation 110.74 m (135' 3") with Class 1 SSCs.

The VES air tanks are constructed of forged, seamless pipe and conform to Section VIII and Appendix 22 of the ASME Code. Failure of the tanks is evaluated as part of the internal missile evaluation in Section 11.5. Postulated failure of the VES does not result in a plant-level fault as the system does not support normal operations; failure of the VES is controlled through the plant Operating Rules (Reference 11.92).

Buildings Adjacent to the Nuclear Island

Buildings adjacent to the NI have been reviewed to identify significant sources of pressure part failure and to define protective measures that may be deemed appropriate. The application of high-energy systems has been limited to the Turbine Building in the plant arrangement to reduce external challenges to the NI.

Turbine Building

There are no Class 1 SSCs in the Turbine Building; therefore the only hazards requiring assessment are credible pressure part failures originating in the Turbine Building that could affect the Class 1 SSCs in the NI. The First Bay of the Turbine Building contains Class 2 defence-in-depth SSCs and is a Class 2 structure with a Category A safety function (Ref. 11.59).

The high-energy fluid systems within the Turbine Building that can result in indirect effects on the NI are the main steam system (MSS), main and startup feedwater system (FWS), and steam generator blowdown system (BDS). Other high-energy power generation systems are not potential sources of interaction due to the design of the Turbine Building for defence in depth.

The barrier between the Turbine Building and the Auxiliary Building (Wall 11) is a Class 1 structure and provides a rigid anchor for the NI piping and is designed for faulted pipe loads in the First Bay of the Turbine Building; this barrier provides the principal means of protecting Class 1 SSCs from an internal hazard that would directly result in loss of a Category A safety function. The barrier between the First Bay of the Turbine Building and the balance of the Turbine Building structure (Wall 11.2) is a seismically-designed Class 2 barrier that is a significant contributor to fulfilment of the Wall 11 Category A safety function.

Hydrodynamic forces resulting from the fluid decompression transient within the faulted piping is analysed for interfacing piping and structural commodities within the NI. In summary, the NI is sufficiently designed to prevent a dynamic impact on essential SSCs in the NI.

Other Buildings and Structures Adjacent to the NI

The remaining buildings and structures adjacent to the NI are the Annex Building and the Radwaste Building; these structures contain moderate-energy systems only. None of these

buildings and structures contains, nor can they therefore be subject to, the adverse dynamic effects of high-energy pipe rupture.

There are pressure part failure locations within these buildings that can result in environmental consequences; however, there are no Class 1 SSCs in these buildings. Furthermore, water sources for consideration in submergence evaluations are quantified for all access points through exterior NI barriers as part of the internal flooding assessment in Section 11.3.

Areas Away from the Nuclear Island

None of the areas/buildings away from the NI contain Class 1 SSCs, or have the potential for a pressure part failure hazard to impinge upon the NI. Failure in these areas is treated as a hazard external to the NI and essential Class 1 SSCs are afforded protections from these events by adequate barriers (Reference 11.9). Therefore, there are no pressure part failure events of concern applicable to these areas; this conclusion includes:

- DG building
- DG fuel oil storage tanks
- Bulk gas storage area
- Diesel-driven and electric motor-driven fire pumps and fire water storage tanks
- PCCAWST
- Transformer compound
- Boric acid storage tank
- Service water cooling towers (where applicable)
- Condensate storage tank
- Demineralised water storage tank

11.4.6 Sensitivity of Results and Cliff Edge Effects

The evaluation of the AP1000 plant for postulated pressure part failure is not sensitive to cliff edge effects since:

- The design basis classification of the resulting plant-level event is consistent with the fault schedule and has been reviewed for cliff-edge effects as discussed in Chapter 8.

- Gross failure events are deterministically assumed for all components without an IoF claim documented in Chapter 20; therefore, the population of failures is not affected by cliff edge effects.

- A sensitivity analysis of the high energy classification parameters was performed in the pressure part topic report and concluded that the population of high-energy fluid systems in the AP1000 plant was not sensitive to the temperature or pressure limit.

11.4.7 Combined Hazards Discussion

The pressure part failure assessments (Reference 11.77) consider, on a deterministic basis, a single failure event and the consequential impact on SSCs in the affected plant areas. Consequential hazards are recognised between pressure part failure, flooding, explosions, and missiles as depicted in Figure 11.4-1 and described in Section 11.12.

The consideration of credible combinations of a pressure part failure with other postulated internal hazards likely to occur independently of the postulated pressure part failure is

considered in a separate document. Reference 11.75 provides a coherent approach across all internal hazard types (e.g., fire, explosion, missiles, dropped loads, pressure part failure).

Combinations of independent internal and external hazards (e.g., internal flooding and extreme low ambient air temperatures) are considered to be Beyond Design Basis events and as such have not been explicitly considered in this section. However, compliance with relevant equipment and structural design codes ensure that combinations of internal hazards with the relevant abnormal operating occurrences (including environmental hazards) are addressed.

11.4.8 ALARP Assessment and Discussion

Deterministic analysis of the effects of postulated pressure part failures demonstrate that the Class 1 SSCs would continue to provide their Category A safety function following a DBA, even in the presence of an unrelated single active failure elsewhere in the plant design. In the unlikely event that the Class 1 SSCs fail for some unrelated reason, the Category A safety function would, for the less severe events, be maintained by other, additional and redundant, Class 2 SSCs. The AP1000 plant probabilistic safety assessment (PSA, refer to Chapter 10) demonstrates that the risks associated with the secondary effects of postulated pressure part failures are not significant.

The AP1000 plant, by its very nature, makes extensive use of pressurised fluid systems to operate normally; therefore it is not possible to remove the internal hazard of pressure part failure from the design of the plant while complying with safety assessment principles for the integrity of SSCs.

The safety design of the AP1000 plant for pressure part failure has been achieved by:

- Removing pressure part failure events that challenge the tolerability of the plant safety case through the assessment of structural integrity (Chapter 20).
- Ensuring redundant essential Class 1 SSCs are protected from postulated pressure part failure events through:
- A combination of physical separation and passive barriers.
- Restraint of dynamic effects through Class 1 supports, restraints, and shields.
- Providing sufficient redundancy in the design such that the consequences of postulated pressure part failures, coincident with an unrelated single active failure, do not adversely affect the delivery of Category A and post-72 hour Category B safety functions.

11.4.8.1 Approach to Safety

Within the overall design of the AP1000 plant methods are applied to assess and apply design provisions to minimising risk. Westinghouse assessment has been performed consistent with the pressure part failure high level claims.

Prevention

Where tolerability cannot be demonstrated, pressure part failures may be prevented using a claim of incredibility of failure. This option is subject to structural integrity review and

should be minimised in the safety case to be consistent with the safety assessment principles (SAPs).

Incredibility of failure claims are currently made for the reactor vessel, steam generator, and pressuriser as documented in the Chapter 20.

Protection

Protection from postulated pressure part failure events is achieved through the use of separation, segregation, and restraint methods. Separation and segregation are primarily achieved through use of barriers and physical separation in the plant layout. Restraint is achieved through the use of pipe whip restraints or jet shields.

The application of protective SSCs is subject to location and application-specific assessment of benefits and detriments. The addition of barriers and restraints has the beneficial effect of reducing the indirect consequences of pressure part failure on the plant by means of decreasing the number of Class 1 SSCs that are affected by the dynamic and environmental effects. Other effects considered in the assessment of detriments of the addition of barriers and restraints are summarised below.

- Effects on Radiological Exposure

  Protective SSCs may require increased access for inspections and maintenance. Improvements in offsite radiological doses may be realised through improvement in overall plant safety; however, occupational radiological dose will also increase appreciably due to increased accessibility requirements.

- Effects on Piping Stresses

  Restraints may have adverse effects on piping system stress behaviour; namely, the addition of restraints introduces restrictions to piping system movement and increases the probability of restrictions on systems with large thermal expansion and dynamic response displacements.

- Other Generic Risk Considerations

  The inclusion of barriers and restraints can give rise to additional influences on the overall plant safety case, some of which are interrelated:

  – Increase in the loadings on structures and supports.
  – More complex in-service inspection requirements
  – Increased complexity of system layout and design.

Mitigation

Mitigation of the indirect effects of postulated pressure part failures is achieved through the selection of adequate design requirements for the resulting gross failure conditions. Class 1 SSCs are subject to qualification consistent with Chapter 5 of the PCSR for these conditions.

11.4.8.2 Further Mitigation Measures

In addition to the design of Class 1 SSCs, the AP1000 plant design incorporates a number of other features to minimise the demand rate on the passive Class 1 SSC. These features are designed to function following Anticipated Operational Occurrences which result in plant

trip; i.e., events that are anticipated to occur at least once in the plant lifetime. These SSCs are active and independent from the Class 1 SSCs, and are powered by the standby DGs when off-site electrical power and house power are not available.

The functions provided by these additional features include (but are not limited to):

- Make-up of borated water to the RCS using the CVS makeup pumps, boric acid tank and associated valves and pipework.
- Heat removal from the secondary side of the SGs using SG Power Operated Relief Valves.
- Feed water makeup to secondary side of the SGs using start-up feedwater pumps, condensate storage tank, and associated valves and pipework.
- Decay heat removal from the RCS (at reduced pressure).
- RNS and associated valves and pipework.
- Decay heat removal from spent fuel pool.
- SFS and associated valves and pipework.
- RNS and associated valves and pipework.
- Supporting functions include
- CCS.
- SWS.
- Standby DGs and associated ECS sets.
- VWS air cooled chillers and associated valves and pipework.
- VBS.
- I&C (PLS).

Pressure part failures within the NI are anticipated to occur at frequencies <1E-03 per year, with limited exceptions as presented in the hazard schedule; i.e., most postulated pressure part failure events are not expected to occur within the life time of the plant. Nonetheless, the design of these active, Class 2 SSC has taken into account the potential effects of pressure part failure consistent with considerations for the assessment of non-Class 1 SSCs with importance to safety (Reference 11.26) and the plant reliability assurance programme (Chapter 5).

As such, similar design measures have been taken to provide assurance that these Class 2 functions will be available, i.e.:

- Class 2 equipment is segregated from its Class 1 counterpart and typically located in a separate structure, for example

- Class 1 RCS make up with borated water is performed by the CMTs through the DVI lines. The Class 2 counterpart of CVS makeup uses a separate connection to the RCS, located in a SG compartment, and the active pumps are physically located outside of the Containment.

- Class 1 decay heat removal is performed by the PRHR Heat Exchanger within the Containment. The Class 2 counterpart at high temperature is the startup feedwater function. The active pumps, control valves, and water inventory for this function is located in the Auxiliary Building, the Turbine Building, and in the yard.

- Class 2 equipment has been separated, where practicable and demonstrated to be ALARP, through the application of design changes in the plant design reference point (Reference 11.3), for example:

- Separation of CCS, RNS, SFS, and SWS piping for protection from environmental effects and other internal hazards (e.g., fire).

Furthermore, failure of the Class 2 equipment, whether due to an inherent fault or the effects of a pressure part failure, will not prevent the Class 1 SSC from fulfilling their Category A safety function(s).

On the basis of the above discussion, and given that Category A safety functions can be maintained in the event of a pressure part failure event, it is judged that there would be minimal safety benefit from introducing additional measures to protect or mitigate the effects of pressure part failure; the risk from pressure part failure hazards is therefore considered to be broadly acceptable and ALARP.

11.4.8.3 Process Implementation

The AP1000 plant pressure part failure assessment process is developed as an on-going live process to be continuously implemented and managed throughout the life of the plant. The purpose of this process is to ensure essential Class 1 SSCs required to delivery Category A and post-72 hour Category B safety functions remain available in performing their safety function as consistent with the plant safety case, thereby ensuring the plant response to postulated failures is ALARP (see the assessment of plant transients and accidents in Chapter 8 and Chapter 9).

The assessment of pressure part failure effects includes postulated failures in high and moderate-energy systems. This population has been (or will be) supplemented by inclusion of additional deterministic gross failure events; assessment of these discrete postulated pressure part failure events will be completed to support nuclear site licensing.

In order to address the potential risk gap in the generic design assessment of the AP1000 plant, the scope of new failures added to the AP1000 plant design was reviewed to ensure that these postulated failures did not represent a risk of a major design change. Major design changes are those changes representing a potentially significant adverse radiological or safety impacts to the AP1000 plant. As consistent with safety assessment principle EHA.7, such adverse impacts are those that affect the potential performance of a Category A safety function in creating a disproportionate increase in radiological consequences.

The conclusion reached is that the remaining population of postulated failure events does not pose a risk of major design change, and therefore will not challenge the safety case bases of the GDA. This conclusion has been corroborated through the performance of supplemental

analyses in Appendix C, Appendix D, and Appendix E of the pressure part failure topic report (Reference 11.77). The identification of these supplemental analyses is documented in Appendix B of the topic report (Reference 11.77) and consists of a risk assessment of piping subject to gross failure.

11.4.8.4 Relevant Good Practice

The AP1000 plant has been designed and assessed for the incidence of gross failure of pressure retaining fluid systems consistent with relevant good practice including NUREG-0800 (Reference 11.88), ANS 58.2 (Reference 11.84), and IAEA Safety Guide NS-G-1.11 (Reference 11.82).

The location of pipe supports, restraints, and shields are determined through the application of mechanistic considerations as defined in Reference 11.77. Sensitivity to intermediate break locations is assessed using more realistic means and methods to confirm the complete population of affected Class 1 SSCs is identified; this action is consistent with current relevant good practice.

11.4.8.5 Conclusion

This layered approach to safety is seen to reduce the hazard from a postulated pressure part failure to ALARP. Additional redundancy and separation has been added to the AP1000 design reference point (Reference 11.3) to further protect plant Class 2 SSCs from the effects of pressure part failure.

Since the Category A and supporting post 72-hour Category B safety functions can be adequately maintained despite postulated pressure part failure, the safety of the plant is ensured. It is judged that the risk is broadly acceptable and ALARP.

11.5 Internal Explosions

11.5.1 Introduction

This section presents the key claims, arguments and underlying evidence made in relation to internal explosion hazards with the potential to impair safe shutdown. It aims to provide sufficient evidence to show that the delivery of Category A safety functions or supporting post 72 hour Category B safety functions will not be impaired by the effect of internal explosions. Claims, arguments and underlying evidence are presented in Section 11.5.2, whilst the internal external explosions safety case is described in Section 11.5.3.

11.5.2 Internal Explosion Claims, Arguments and Evidence

Those SSCs which deliver a Category A safety function are the principal means of ensuring nuclear safety in response to Design Basis Accident (DBA) plant faults (see Chapter 8). Whether the internal hazard initiates a plant state fault or not, by ensuring that the ability to deliver Category A safety functions is maintained following an internal hazard, the internal hazards safety case aligns with the fault studies in demonstrating that the plant risk is broadly acceptable.

This section presents the claims, arguments and underlying evidence made in relation to internal explosion hazards with the potential to impact safe shutdown.

11.5.2.1 High Level Claim

SSCs important for nuclear safety must be protected from dynamic effects within the plant, including those of internally generated explosions. An internal explosion could result in a transient from the normal operating state of the reactor and potentially lead to an uncontrolled radiological release. In response to such a transient, it may be necessary to shutdown the reactor and return it to a safe shutdown state. Depending on the exact nature of the transient, there are a number of courses of action to take to shutdown the reactor. Availability of the Class 1 SSCs required to deliver the Category A safety functions will ensure that the reactor can be safely shutdown, and is the basis of the following high level claim:

Claim IH-4.0: **Postulated internal explosions within the design basis do not prevent the delivery of the Category A safety functions and the supporting post-72 hour Category B safety functions necessary to respond to the postulated event.**

The above high level claim has been divided into claims associated with preventing explosions and, where this is not possible, protecting Class 1 SSC from the effects of an explosion. As appropriate, these divisions are further broken down into Sub-Claims. Arguments and evidence for each Sub-Claim are presented in subsection 11.5.2.5.

The SSCs claimed to provide post-72 hour support functions include only offsite procured SSCs and their associated Class 1 connections.

11.5.2.2 Prevention Claims

Preventative measures have been incorporated into the design to ensure that Class 1 SSC delivering Category A safety functions are not exposed to an explosion hazard. These claims are based on preventing the formation of an explosive atmosphere.

Claim IH-4.1: **Internal explosions which could compromise delivery of Category A safety functions are prevented by controlling flammable substances such that an explosive atmosphere does not form.**

The following Sub-Claims are defined to deliver the above higher level prevention claim:

Sub-Claim IH-4.1.1: **The risk of explosion on-site from flammable materials that have the potential to generate explosive atmospheres is minimised by inventory control.**

Sub-Claim IH-4.1.2: **Under normal conditions, flammable substances which if released could form an explosive atmosphere will be adequately contained.**

Sub-Claim IH-4.1.3: **Under fault conditions a guillotine break or leak of the CVS hydrogen injection line in the Auxiliary Building will not result in the formation of an explosive atmosphere.**

Sub-Claim IH-4.1.4: **Under normal conditions, an explosive atmosphere is prevented from forming in the Auxiliary Building battery rooms by appropriate ventilation design.**

Sub-Claim IH-4.1.5: Under fault conditions, an explosive atmosphere is prevented from forming in the Auxiliary Building battery rooms by operator action.

Sub-Claim IH-4.1.6: Under the faulted condition of a Loss of Offsite Power (LOOP), an explosive atmosphere is prevented from forming in the Auxiliary Building battery rooms by the inherent safety characteristics of the battery charging system.

Sub-Claim IH-4.1.7: Under fault conditions a guillotine break or leak of the CVS hydrogen injection line in the Containment Building will not result in the formation of an explosive atmosphere.

Sub-Claim IH-4.1.8: Explosive atmospheres will be prevented from forming in tanks/vessels by maintaining the atmosphere outside of the flammable range.

Sub-Claim IH-4.1.9: Hydrogen will not be present within the WLS in significant concentrations downstream of the degasifier.

11.5.2.3 Protection Claims

Protective measures have been incorporated into the design to ensure that Class 1 SSC delivering Category A safety functions are not affected by an explosion hazard. These claims are based on protecting Class 1 SSC form the effects of an explosion.

Claim IH-4.2: Passive protective measures have been incorporated in the AP1000 design to protect SSCs that deliver Category A safety functions from internal explosions.

The following Sub-Claim is defined to deliver the above higher level protection claim:

Sub-Claim IH-4.2.1: Safe shutdown SSCs located within the NI would not be affected by internal explosions generated in areas outside the NI.

Sub-Claim IH-4.2.2: Redundant Safe shutdown SSCs located within the NI would not be affected by a hydrogen deflagration event in the NI battery rooms.

11.5.2.4 Mitigation Claims

Explosions are deterministically assumed to result in the loss, or loss of functionality, of Class 1 SSC exposed to the effects of an explosion. Therefore, no specific claims are made on mitigation of internal explosion hazards.

11.5.2.5 Arguments and Evidence

Prevention Arguments and Evidence

Claim IH-4.1: Internal explosions which could compromise delivery of Category A safety functions are prevented by controlling flammable substances such that an explosive atmosphere does not form.

The following arguments demonstrate how the prevention claims made in subsection 11.5.2.2 are delivered:

Argument: **Only those flammable substances required to support plant operation are located in or routed through the Nuclear Island.**

Small quantities of chemicals are required to support the correct operation of a number of systems including, but not limited to, reactor and balance of plant chemistry control. These chemicals are stored in the CFS which is located outside of the NI in the yard area. Based on the results of continuous or periodic sampling, chemicals are introduced to batching tanks.

The exception to this is the hydrogen addition to the RCS via the CVS. Bottled hydrogen is piped directly into Containment from the hydrogen injection package located in the Turbine Building. A direct route for the piping, from the hydrogen injection package, into Containment is taken which minimises the number of rooms within the NI through which the pipework passes and therefore in which an explosive atmosphere could form.

Further, hydrogen is evolved during the charging of lead acid batteries. Only those batteries providing an essential power supply are housed in the NI, with all other batteries located outside the NI. The battery banks themselves have been sized to provide an uninterruptible supply for between 24 and 72 hours following a LOOP, depending on division. By this time it is postulated that emergency arrangements will be enacted and the sole reliance upon the batteries is no longer required. Minimising the size of the batteries correspondingly minimises the hydrogen generation rate and therefore the time taken to achieve an explosive atmosphere increases.

Argument: **In the short term (or the near field effects), detonation of a hydrogen plume in the Auxiliary or Containment Building during a break or leak of the CVS hydrogen injection line or WLS lines will have no influence on the broader compartment integrity.**

It is acknowledged that the local hydrogen source plume does have flammability potential near the source origin at the injection line break. Since the plume begins as a pure hydrogen plume at the source point, this plume must attain a flammable condition at some axial region in the plume rise prior to becoming sufficiently diluted and non-flammable via entrained air during the formation of the noted non-flammable stratified layer at the ceiling of auxiliary building Room 12306, for example.

As described in Section 7.8 of Reference 11.142, while plume detonation in the presence of an assumed local ignition source is possible, the ultra-small size of this region results in corresponding ultra-rapid decay of the shock wave such that it does not represent any hazard to the broader room itself. In fact, in the highly unlikely event that an ignition source is present at the precise location, the resulting detonation event is best characterized as a mere auditory nuisance, not a structural hazard. Although the analysis in Reference 11.142 is based on the CVS hydrogen injection line which contains pure hydrogen, degassing during a WLS line leak or break may develop into a hydrogen plume, though the hazard would be bounded by the pure hydrogen plume from the CVS hydrogen injection line.

Argument: **Systems within the NI containing materials that have the potential to generate explosive atmospheres are designed to prevent leakage through use of welded pipe joints and leak-tight (hermetically sealed) valves compliant with the appropriate**

codes and standards. Such systems will be pressure-tested during commissioning to ensure leak-tight integrity.

Within the NI, the only systems which contain materials with the potential to generate explosive atmospheres are specific components within the CVS, PSS, WGS and WLS.

The high pressure hydrogen gas line routed through room 12306 is seamless. All connections to the pipework, including the vent line end cap, are formed by welded joints. The section of pipework incorporates a single, air operated, Containment isolation valve and two manually operated valves all of which are hermetically sealed butt weld globe valves. During normal operation this line will therefore adequately contain the enclosed hydrogen gas without any leakage into the valve/piping penetration room. The hydrogen gas line then passes through the short section of the middle annulus to enter the Containment.

The PSS and WLS are fluid based systems. The hydrogen component in both systems is dissolved in the liquid and would not readily off-gas whilst contained within the systems. These systems use flanged bolted joints which are pressure tested and rated for the anticipated process conditions.

The WGS is operated at a slight positive pressure in order to preclude the ingress of air. All connections on the WGS are formed by welded joints.

Argument: **Under fault conditions a guillotine break of the CVS injection line in the Auxiliary building will not result in the formation of an explosive atmosphere sufficient to challenge redundant divisions of Class 1 SSC.**

Assessments of a break of the CVS hydrogen injection line in the Auxiliary building (References 11.105 and 11.142) have been performed. These assessments have determined that a worst case gross failure of the CVS hydrogen line would not lead to an explosive atmosphere in rooms 12306, 12406, and 12506, even if the break leak would continue for multiple days without mechanical ventilation active in the rooms. The results of Reference 11.142 show that even after 14 days of continuous leakage, the upper portion of room 12306 will not reach 1 v/v % hydrogen in air. Hydrogen concentrations in rooms 12406, and 12506 (specifically the upper area of room 12506 as the anticipated area of highest concentration) remain below the concentration of the upper area of room 12306 throughout the transient. This auxiliary building condition corresponds to a very benign circumstance with regard to hydrogen hazard for even this most conservative configuration of no ventilation flow. Thus in the long term, the inventory control (Claim 4.1.1) in combination with the volume of the room(s) in the Auxiliary building means that the hydrogen concentration does not exceed 1 v/v %.

In the short term (or the near field effects), during a break of the CVS injection line in the Auxiliary building, hydrogen would initially be at 100 v/v % , but would rapidly dilute due to the entrainment of air. Further, an assessment of any potential limiting localized plume was confirmed to not result in failure of the room barrier (walls, ceiling floor) (Reference 11.142); therefore, deterministically assuming loss of safety functions within the impacted room, the redundant safety function systems remain unaffected.

Argument: **The Auxiliary Building battery rooms are mechanically ventilated to maintain the concentration of evolved hydrogen below the lower flammability limit, including under the most onerous normally anticipated conditions.**

The only continuous release of hydrogen is presented by the batteries which, during charging, evolve hydrogen due to the disassociation of electrolyte at the electrodes when fully charged.

Within the NI, battery banks are located in rooms 12101, 12102, 12103, 12104, 12105, 12202 and 12205, each of which comprises 60 lead-acid cells (Reference 11.97). During normal operation the batteries revert to float charge when fully charged. Under these conditions the battery bank would generate 3.4E-06 $m^3 s^{-1}$ (7.2E-03 cfm) of hydrogen (Reference 11.97). The smallest battery room, 12101, has approximately 200 m^3 (7063 ft^3) of free space into which the hydrogen gas could accumulate. At a generation rate of 3.4E-06 $m^3 s^{-1}$ (7.2E-03 cfm) it would take approximately 163 hours before the 1 v/v % hydrogen concentration is reached, without crediting ventilation. Each of the battery rooms is ventilated at a design exhaust flow rate of 0.156 $m^3 s^{-1}$ (330 cfm). In accordance with the guidance in BS EN 60079-10 (Reference 11.98), the background concentration of hydrogen, X_b (vol/vol) can be calculated using the following equation:

$$X_b = \frac{f \times Q_g}{Q_2}$$

Where: f is a measure of the degree of mixing, 1 for good mixing; Q_g volumetric release rate of flammable gas ($m^3 s^{-1}$); Q_2 is the volumetric flow rate of air leaving the room ($m^3 s^{-1}$). Within the battery room, the background concentration would therefore be 2E-03 v/v %. This is significantly lower than the Lower Flammability Limit (LFL) for hydrogen in air and therefore a flammable atmosphere is prevented from accumulating.

Argument: **The ventilation exhaust systems servicing the Auxiliary Building battery rooms contain flow detection which provides an alarm in the MCR when the extract flow-rate drops below 75% of its design value.**

Each of the IDS battery divisions (including spare) is serviced by a VBS exhaust fan with flow detection on the outlet. At 75% of the design flow setting, an alarm is triggered which displays in the MCR.

Argument: **Battery rooms contain dual-redundant hydrogen detectors which provide an alarm in the MCR when the relevant hydrogen-in-air concentration set point is reached.**

Each of the Auxiliary Building battery rooms contains 2 hydrogen detectors which are installed as shown in Reference 11.97. Hydrogen pocketing cannot occur in the battery rooms between the I-beams, which run east-west, because the ribs of the corrugated metal deck which forms the battery room ceiling run north-south. Furthermore, hydrogen will be evolved from each of the 60 cells, rather than a single location, which are spread throughout the room. Hydrogen would therefore accumulate evenly across the battery room ceiling and within the sampling space of one (or both) of the detectors.

The hydrogen detectors provide an alarm in the main control room alerting operators to the build-up of hydrogen.

Argument: **On actuation of either the ventilation low flow alarm or the high hydrogen alarm, operators will reinstate normal conditions or isolate charging to the batteries.**

On receipt of the low exhaust flow alarm, operators will reinstate the extract flow, either by repairing the affected unit or by swapping in the redundant back-up unit.

During normal operation, the ventilation system is designed to maintain the concentration of hydrogen below 1 v/v % in air. Assuming the hydrogen concentration is being maintained at 1 v/v %, and that an equalising charge is being applied to the batteries in the affected room, it would take approximately 28.8 hours before the hydrogen concentration reached the LFL at 4 v/v % in air. This is more than sufficient time to either reinstate the ventilation extract, or isolate charging to the affected battery division.

On receipt of the high hydrogen concentration alarm, operators will undertake the following actions (Reference 11.99):

- Sampling of hydrogen levels in the room;
- Reinstate the HVAC
- In the event that the HVAC cannot be reinstated:
  - Cease charging of the batteries;
  - Heaters in the air supply lines are disabled;
  - Activities which might present an ignition source are stopped;
  - Temporary local ventilation is installed.
- Maintenance of the HVAC initiated.

From the point at which the alarm is triggered until the LFL is reached, there is sufficient time to either reinstate the ventilation extract, or isolate charging to the affected battery division.

Argument: **During a LOOP event (which would lead to loss of ventilation), batteries cease charging due to loss of AC power. As a result, hydrogen generation ceases, thereby providing an inherently safe arrangement for the battery charging system and associated compartments.**

During normal operation, the VBS is designed to maintain the concentration of hydrogen below 1 v/v % in air. The VBS is powered by the site mains supply, and as such in the event of a LOOP would cease operation. However, the IDS batteries are also charged by the site mains supply and therefore hydrogen would also cease to be generated.

On reinstatement of power, the HVAC will automatically return to normal service, as would the battery chargers. It is therefore not possible for the batteries to evolve hydrogen, in the absence of ventilation, following a LOOP. During normal operation, the ventilation system is designed to maintain the concentration of hydrogen below 1 v/v % in air. Following a LOOP the concentration of hydrogen would therefore remain at or below 1 v/v % in air, which is below the LFL.

Argument: **Under fault conditions a guillotine break of the CVS injection line in the Containment building will not result in the formation of an explosive atmosphere sufficient to challenge redundant divisions of Class 1 SSC.**

Assessments of a break of the CVS hydrogen injection line in the Containment building (Reference 11.106 and 11.142) have been performed. These assessments have determined that a worst case gross failure of the CVS hydrogen line would not lead to an explosive atmosphere in rooms 11209 and 11300, even if the break leak would continue for multiple days without mechanical ventilation active in the rooms. The results of Reference 11.142

show that even after 14 days of continuous leakage, the upper portion of room 11209 will not reach 1v/v % % hydrogen in air. Hydrogen concentrations in rooms 11300 (specifically the upper area of room 11300 as the anticipated area of highest concentration) remain below the concentration of the upper area of room 11209 throughout the transient. This containment building condition corresponds to a very benign circumstance with regard to hydrogen hazard for even this most conservative configuration of no ventilation flow.

In the short term (or the near field effects), during a break of the CVS injection line in the Containment building, hydrogen would initially be at 100 v/v % , but would rapidly dilute due to the entrainment of air. Further, an assessment of any potential limiting localized plume was confirmed to not result in failure of the room barrier (walls, ceiling floor) (Reference 11.142); therefore, deterministically assuming loss of safety functions within the impacted room, the redundant safety function systems remain unaffected.

Argument: **Air (oxygen) will be purged from the RCDT and WGS prior to processing of WLS effluent by the WGS.**

Both the WGS and RCDT are purged with nitrogen gas to expel any residual oxygen before the start of influent processing. When the WGS is purged, nitrogen gas is continually added until the effluent indicates a low oxygen concentration.

Argument: **The atmosphere of systems handling flammable materials is monitored for concentrations of oxygen (and/or) combustible material.**

The WGS sample stream oxygen concentration monitors monitor the concentration of oxygen in the gas stream discharged by the WGS vacuum pumps. Should the oxygen concentration reach a High-2 set-point of 2.4 v/v %, the WGS vacuum pumps are automatically stopped to isolate a potential source of air ingress. Furthermore, the nitrogen purge valve is opened to purge the system with nitrogen.

Hydrogen concentration monitors are installed within the gas space of the WLS effluent hold-up tanks. These monitors provide an alarm to the MCR at 1 v/v % of hydrogen in air, prompting the operator to initiate an air purge through the tank(s) using the CAS.

Argument: **The degasification process, undertaken in the degasifier, boils off dissolved hydrogen from the WLS influents and discharges into the WGS. Any dissolved hydrogen remaining in the WLS would not readily result in additional off-gas of hydrogen.**

The degasifier receives influent from the CVS letdown and RCDT at a maximum dissolved hydrogen concentration of 4.5E-05 $m^3 kg^{-1}$. Based on the maximum dissolved hydrogen concentration and the CVS letdown flowrate of 6.3E-03 $m^3 s^{-1}$ (100 gpm), the hydrogen content of the influent is approximately 2.84E-04 $m^3 s^{-1}$ (0.6 scfm). The degasifier is a vacuum type which can discharge up to 2.7E-04 $m^3 s^{-1}$ (0.58 scfm) to the WGS. The effluent discharged to the WLS hold-up tanks could therefore contain 1.4E-05 $m^3 kg^{-1}$ of hydrogen.

The hydrogen which remains dissolved in the effluent represents 3% of the initial content. The conditions within the WLS effluent hold-up tank would not promote boiling of the effluent and therefore significant quantities of dissolved hydrogen are unlikely to off-gas.

Protection Arguments and Evidence

Claim IH-4.2: Passive protective measures have been incorporated in the AP1000 design to protect SSCs that deliver Category A safety functions from internal explosions

The following arguments demonstrate how the protection claims made in subsection 11.5.2.3 are delivered:

Argument: Areas that accommodate sources of hydrogen or other materials that have the potential to generate explosive atmospheres outside the NI are located at safe distances from the NI (where the 'safe distance' is defined as that at which the maximum explosive overpressure resulting from an explosion will not damage the NI structure, and hence, the SSCs protected by the structure). Implicit to this safety argument is the ability of the external walls of the Containment Shield Building and AB to provide an external overpressure resistance capable of withstanding the explosive overpressure applicable to the defined safe distance.

The design has been developed in accordance with USNRC Regulatory Guide 1.91, which defines the safe distance from an explosion as the point at which the blast wave overpressure is limited to approximately 7 kPa (1 psi); below this no significant damage would be expected. This value is broadly similar to the hazard criteria for blast effects as used by Health & Safety Laboratory (HSL) (Reference 11.103), which are as follows:

- >60 kPa (8.7 psi) likely to cause total demolition of buildings, near certainty of fatality;
- 14-60 kPa (2-8.7 psi) likely to cause some structural damage, some fatalities of building occupants;
- 7-14 kPa (1-2 psi) structural damage unlikely, window damage, fatalities unlikely.

For those sources of flammable material, present outside the NI, which can form an explosive atmosphere, analysis has been performed (References 11.95 and 11.96) to determine the distance from the centre of the Vapour Cloud Explosion (VCE) by which point the blast overpressure would have dropped to 7 kPa.

The Civil/Structural Design Criteria (Reference 11.107) defines the overpressure resistance requirement for the external walls of the NI (including the Shield Building) as 34 kPa (5 psi). The external walls of the Auxiliary Building are composed of nominally 0.6 m (2 ft) thick reinforced concrete walls (Reference 11.104). Similarly, the Containment Shield Building (which envelopes the Containment Building) is constructed from two external 19 mm thick steel plates infilled with concrete, giving an overall thickness of 0.91 m (3 ft) (See Chapter 6). It is reasonable to assume that the construction of the NI walls is at least as strong as a similar thickness of brick panels given that concrete is homogeneous and not subject to the discontinuities inherent in brick and mortar joints. The NI overpressure resistance requirement for the external walls represents a factor of 4.8 compared to the blast overpressure experienced at a safe distance from an explosion.

Based on the standard plant layout, the assessments of explosions originating from the bulk hydrogen storage and other chemicals concludes that the blast overpressure would not exceed the 7 kPa (1 psi) threshold at the NI exterior walls. The Class 1 SSC within the NI would

therefore be unaffected by the postulated explosions and would continue to deliver their Category A safety functions.

Failure of the HVAC system servicing the Annex Building battery rooms would result in the build-up of hydrogen in the battery rooms during charging. The assessment of hydrogen explosions within the battery rooms (Reference 11.94) concludes that the blast overpressure would exceed 7 kPa at the nearest external wall of the NI.

Argument: **A deflagration event in the NI battery rooms will not prevent the delivery of redundant Category A safety functions, due to the assurance of room barrier integrity.**

Battery Room 12104 has been analysed for the scenario of unmitigated hydrogen release and accumulation using a release rate for sustained equalizing charge at maximum temperature 48.9 °C (120 °F) (Reference 11.143).

The hydrogen release in the NI battery rooms is in the form of a slow release of buoyancy-driven plumes that entrain the surrounding quiescent air, yielding a stratified layer at the ceiling that is below the LFL. This layer must grow downward and encompass the entire room. Only then can further hydrogen release increase the hydrogen concentration to the LFL at 4.5 - 4.7 v/v % of hydrogen in air. This process takes roughly 1.6 days for the smallest battery room, Room 12101 (Room volume 200 m^3 per Reference 11.97).

As the release of hydrogen from the batteries continues, the concentration of hydrogen in the room must cross the LFL to achieve flammability. If stray ignition sources in the battery rooms are postulated as an intermittent, but persistent, source that is responsible for deflagration, then the low hydrogen concentration range of 4.5 – 6.0 v/v % is the most likely candidate for deflagration. Such deflagrations can be readily handled via passive venting through HVAC ducts, remaining below the withstand of the battery room walls (5 psi).

Per Reference 11.143, elevated hydrogen concentration in the range of 8 - 12 v/v % is less likely since it requires the initial absence of an ignition source for the additional hydrogen accumulation followed by the latter-stage. If the less likely deflagration at elevated hydrogen concentrations in the range 8 - 12 v/v % must be considered for conservatism, 8 – 12 v/v % hydrogen concentration in air will exceed withstand of the battery room walls (5 psi) and remain above the limit for 45 - 60 seconds if passive venting is not credited. If passive venting through HVAC ducts is credited, then the peak pressure ratio is mitigated, and the duration above the administrative limit is reduced substantially to 5 - 6 seconds. Finally, if pressure relief via over-pressure catastrophic failure of the main access door is credited, then the peak pressure ratio remains below the administrative limit for the entirety of the deflagration duration. Note, there are no safe shut down SSCs serving Category A functions in the Corridors, Rooms 12111 and 12211, into which the battery room doors will relieve to. Further discussion of the mechanisms of the door over-pressure failure is provided in Section 3.1.4 of Reference 11.143.

While the deflagrations occurring in the concentration range 8 – 12 v/v % can be accommodated, deflagration-to-detonation (DDT) remains a concern for 10 v/v % and larger. Per Reference 11.143, detonation tolerance is not established, so a successful outcome is not assured. 8 v/v % is the highest concentration analysed that can both tolerate a deflagration and avoid a detonation. It yields a successful outcome in all respects. Furthermore, the roughly 3.3 day timeframe for development of 8 v/v % (Smallest battery room, Room 12101) provides ample time for operators to recognize an unmitigated hydrogen release scenario and take action to counteract this circumstance far in advance.

Mitigation Arguments and Evidence

There are no specific claims made on mitigating the effects of an explosion. Explosions are assumed to result in gross failure of exposed SSC.

11.5.3 Internal Explosions Safety Case Summary

11.5.3.1 Introduction and Overview

The safety design approach adopted for internal explosion hazards consists of a range of complementary design and operation measures. These are applied as appropriate to individual items of equipment or systems to prevent an internal explosion occurring or to protect Class 1 SSC from the effects of an explosion. Suitable and sufficient design basis measures are identified such that an internal hazard, which may give rise to an explosion, does not prevent the delivery of the Category A safety functions necessary to respond to a postulated event. Preservation of required safety functions ensures alignment with fault studies and structural integrity analysis. In accordance with relevant international good practice (Reference 11.23), the following approaches have been applied:

- Prevent explosions from occurring;
- Minimise the risk of an explosion, if an explosive atmosphere cannot be avoided;
- Minimise the consequences of an explosion.

Internal explosions typically occur because of occurrences that result in the build-up of concentrations of volatile or unstable materials coupled with an ignition source. Such explosive combinations could, in theory, arise from the following types of contributory events:

- Inappropriate location or storage of flammable/explosive materials;
- Accidental release of flammable/explosive material during normal operations;
- Failure to control normal accumulation of flammable/explosive materials generated during operations;
- Accidental introduction of an ignition source when a flammable/explosive concentration of material is normally present.

Explosions are assumed to occur, as a result of Postulated Initiating Events (PIEs), wherever an explosive atmosphere may be present, except where equipment is qualified to not present a source of ignition. Passive protective measures have been incorporated in the design to protect SSCs that deliver Category A safety functions from internal explosions. The consequences of an explosion will be contained through the use of passive barriers to limit the impact to and loss of a safety function. In summary, the safety case approach adopted is as follows:

- Control of flammable material inventories;
- Incorporation of component design features that prevent explosive atmospheres from forming;
- Safe routing of systems containing flammable materials;

- Location of Safety Class 1 SSCs outside the zone of influence of a postulated explosion;
- Protection where practicable using segregation and/or separation by structural barriers.

The AP1000 design employs a mixture of the approaches stated above to form levels of defence which reduce the likelihood of an internal explosion generated from equipment and also reduces the risk of internally generated explosions to ALARP. It is argued that all SSC exposed to an overpressure in excess of 7 kPa are assumed to fail. Where an explosion overpressure has not been explicitly determined (e.g., because the explosion is prevented) the failure of equipment within a segregated area because of an explosion is bounded by other hazard analyses (i.e., internal fire), which assumes that all equipment in such an area is lost as a result of the hazard.

The focus of the explosion hazard analysis is on those areas containing Class 1 SSCs; i.e., those within the NI (Shield/Containment Building and AB). Consideration of internal explosion hazards in other locations is limited to the demonstration that the NI is adequately protected from an internal explosion from these sources by appropriate separation distance and/or physical barriers.

11.5.3.2 Applicable Codes and Standards

The internal explosion assessments have been undertaken in accordance with the following codes and standards:

- BS EN 60079-10, 'Explosive Atmospheres Part 10-1: Classification of Areas – Explosive Gas Atmospheres';
- NRC Regulatory Guide 1.91, 'Evaluations of Explosions Postulated to Occur at Nearby Facilities and on Transportation Routes Near Nuclear Power Plants';
- HSL/2001/04, "Explosion Hazard Assessment: A Study of the Feasibility and Benefits of Extending Current HSE Methodology to Take Account of Blast Sheltering';
- Multi-Energy Method (MEM);
- TNT-equivalence method

Protective structures are designed to withstand and absorb peak positive incident over-pressures generated by explosions in order to prevent damage to Class 1 SSCs. Appropriate safe separation distances from explosion sources also forms an implicit part of the design process for protection against explosions.

SSC claimed in support of this assessment are designed in accordance with the relevant US codes and standards. To evaluate the codes and standards against the UK expectations, the codes and standards have been organised by the relative safety significance of the SSCs to which they have been applied. To support this organisation the AP1000 UK Safety Categorisation and Classification Methodology (Reference 11.26) describes the process for categorisation of safety functions and classification of SSCs.

The AP1000 Equivalence/Maturity Study of U.S. Codes and Standards (Reference 11.25), determines, based on their importance to safety, the applicability, adequacy and sufficiency of those standards when compared with relevant UK and international good practice. It also

provides a clear and auditable demonstration that all codes and standards to support the design substantiation of UK Class 1 or safety significant SSCs have been identified.

11.5.3.3 Redundancy and Segregation

An internal disruption within a building can lead to plant damage. In such cases, the measures for ensuring continuing delivery of safety functions up to and after 72 hours are exactly the same as for any other causes of damage to the potentially affected plant. The location and level of redundancy of Class 1 SSC within the plant is such that complete loss of operability of the SSCs within a room or compartment because of disruption resulting from an internally generated explosion would not result in loss of the Category A safety function.

Measures applied with respect to redundancy, separation, and segregation consist of the following:

- There are multiple divisions of Class 1 SSC each of which is wholly capable of delivering the Category A safety functions;
- Within the Containment Vessel there is segregation and separation of Class 1 equipment. This is provided by a combination of barriers formed by the walls and floors of compartments and the distance between systems providing redundant means of delivering the Category A functions.
- Outside the Containment Vessel there is sufficient equipment redundancy, segregation, and protection such that all of the equipment in a single room can be lost without preventing delivery of the Category A safety functions.
- The Class 2 systems are an additional means of delivering Category A safety functions. They provide a level of defence in depth. The Class 2 system designs also feature redundancy. The Category A functions provided by these systems are summarised in Chapter 6.

The plant is designed such that it can be operated with sufficient levels of protection in place to ensure that internally generated explosions will not prevent delivery of Category A safety functions. This defence in depth is provided by:

- The conservative design, manufacture, maintenance and operation of equipment in accordance with safety margins (through compliance with recognised design codes) appropriate engineering practices and monitoring of the quality of these aspects.
- The use of structural barriers to limit the impact of any explosion generated to areas where damage will not prevent the delivery of Category A safety functions.

Sufficient redundancy and defence in depth is provided to ensure that even if there is the loss of any SSC as a result of an internally generated explosion the Category A safety function can still be delivered.

11.5.3.4 Explosions Assessment Approach

The approach to assessing potential internal explosions is in accordance with the following basic steps:

1. Identify all known chemicals stored in the AP1000 plant.

2. Determine whether these chemicals present an explosion hazard.
3. Determine the location of the chemicals with potential to cause an explosion hazard.
4. Calculate the minimum safe distance for SSCs if the conditions are met for an explosion to occur[10].

In accordance with the Dangerous Substances and Explosive Atmospheres Regulations 2002 (DSEAR) (Reference 11.109), an explosive atmosphere exists where a substance(s) mixed with air, in the form of gases, vapours, mists or dust, which when ignited, combustion spreads throughout the entire unburned mixture. Explosive atmospheres will therefore form wherever flammable gases, vapours mists or dusts mix with air at concentrations which are flammable.

An explosion will result in an increase in temperature or pressure, or both simultaneously. SSC exposed to the effects of an explosion will be damaged where the temperature or pressure exceeds the capacity of the SSC to withstand the effect. In general the effect of temperature increase will be short lived and the thermal radiation dose will be low. However, the peak pressure will have a deterministic effect. On this basis, it is reasonable to assume that the effects of pressure will bound those of temperature.

The blast overpressure from a VCE has been determined using the Multi-Energy Method (MEM) developed by the Netherlands Organisation for Applied Research (TNO) (Reference 11.96).

11.5.3.5 Interface with Other Internal Hazards

The AP1000 design has been evaluated for internal hazards to confirm that SSCs delivering Category A or supporting Post-72 hours Category B safety functions will perform as required for the identified internal hazards listed in Section 11.1.

It is recognised that internal explosions may occur, due to a common initiator, coincidentally with other internal hazards or selected external hazards. In such instances, the combined effects of both hazards constitute the full extent of the internal hazard.

An assessment of the consequences of combined hazards has been completed and documented in Section 11.12 based on the combined hazards analysis (Reference 11.75). Section 11.12 demonstrates that for credible combinations of flooding with other potential internal hazards, the Category A and/or supporting Category B safety functions can continue to be delivered, as consistent with the individual internal hazard assessments.

11.5.3.6 Conclusions

Sufficient evidence has been shown throughout this section that the risk of loss of a nuclear safety-significant system as a result of internal explosions is low and controlled. Internal explosions have been shown to not prevent the delivery of the Category A safety functions and the post 72-hour Category B safety functions. This is due to the combination of inherent design features (Safe Distances), routine and non-routine early detection regimes (Hydrogen Detectors), prevention devices (mechanical HVAC), and the application of routine and non-

10. Within the NI, the approach adopted is to prevent an explosion from occurring through the provision of suitable and sufficient SSC. Explosion overpressures, and minimum safe distances, have therefore not been calculated for explosive atmospheres originating from within the NI.

routine remediation actions (Operator response to high hydrogen concentration or loss of HVAC), respectively preventing, detecting, protecting and controlling the risk to the AP1000 plant from internal explosions.

11.5.4 Internal Explosions Analysis

11.5.4.1 Flammable Substances

A detailed review of the chemical inventory has been performed (Reference 11.95) to identify those chemicals which could form an explosive atmosphere when mixed with air. An additional review has been performed to identify systems which handle or generate hydrogen. The chemicals, considered capable of developing a flammable atmosphere are listed in Table 11.5-1 of this document.

11.5.4.2 Sources of Release

For those systems which contain flammable substances, reviews have been undertaken to identify possible locations where a leak could form a flammable atmosphere. The rooms in which a flammable atmosphere could form are detailed in the Hazard Schedule, Table 11.5-2. The Containment building is, in order to maintain the free movement of gases, an open space. The majority of rooms are separated by open grate structures which would not inhibit the movement of gases. Irrespective of location, a release within Containment is therefore assumed to permeate all rooms.

11.5.4.3 Assessment of Internal Explosions

To support the claims and arguments made as part of the internal explosions hazard analyses, a number of assessments have been carried out. The following sections provide a summary of the analyses and the assessment findings.

Containment Building

Failure of the WLS pipework and/or the CVS hydrogen injection line could result in a build-up of hydrogen in Containment. The assessments of leakage from the hydrogen injection line in Containment (Reference 11.106 and 11.142) evaluate the potential for an explosion within Containment, while the WLS and WGS hydrogen leakage assessment (Reference 11.100) considers a loss of effluent from the WLS.

The hydrogen injection package is supplied from 4 high pressure hydrogen bottles located in the PGS. The high pressure hydrogen switchover station automatically switches the supply from the 2 duty bottles to the 2 standby bottles once they become depleted. Each of the high pressure hydrogen bottles has a nominal capacity of 15.6 m^3 (550 scf), giving a total available hydrogen volume of 62.3 m^3 (2200 ft^3).

The hydrogen injection package has two modes of operation, continuous and batch, depending on the plant mode, supplied via two parallel lines. The maximum flow rate during either continuous or batch mode is limited, by orifice plates, to 5 E-04 $m^3 s^{-1}$ (1.05 scfm) or 9.3 E-05 $m^3 s^{-1}$ (0.2 scfm) respectively (Reference 11.106).

The hydrogen injection package originates in the Turbine Building and passes, via rooms 12306 and 12341, into Containment. Within Containment, the hydrogen injection line is present in rooms 11209 and 11300. The pipework, valves and fittings for the CVS are butt

welded and hermetically sealed. During normal operation, there would be no leak of hydrogen within Containment.

However, should the pipework, valves or fittings fail (e.g., double guillotine failure), hydrogen would leak from the pipework into rooms 11209 or 11300.

The RCDT, located in room 11104, contains borated effluent which is potentially hydrogen bearing. As required, the RCDT is pumped out to the WLS, passing via 11300. A leak from the RCDT or associated pipework within Containment therefore has the potential to generate hydrogen off-gas from the effluent.

Rooms 11104 and 11300 have an open grate ceiling, such that any hydrogen would pass directly into the general Containment space.

The assessment of the CVS hydrogen injection line in Containment has identified that it may be possible for an explosive atmosphere to form in Room 11209 (Reference 11.106). As a result of this scenario, a detailed assessment of a break of the CVS hydrogen injection line in the Containment building was completed (Reference 11.142). This assessment has determined that a worst case gross failure of the CVS hydrogen line would not lead to an explosive atmosphere in rooms 11209 and/or 11300, even if the break leak would continue for multiple days without mechanical ventilation active in the rooms. The results of the assessment show that even after 14 days of continuous leakage, the upper portion of room 11209 will not reach 1 v/v % hydrogen in air. It would take approximately 38 days to reach 1 v/v % of hydrogen in the most limiting room, Room 11209. A continuous leak of 31 days or more is not considered credible as it would exceed the quantity of hydrogen available (4 high pressure hydrogen bottles, each containing 15.6 m^3 (550 scf) of hydrogen). Hydrogen concentrations in rooms 11300 remain below the concentration of the upper area of room 11209 throughout the transient. This containment building condition corresponds to a very benign circumstance with regard to hydrogen hazard for even this most conservative configuration of no ventilation flow.

As described in Reference 11.142 of CVS hydrogen line break assessment, while plume detonation in the presence of an assumed local ignition source is possible during a guillotine break or long term leak of the hydrogen injection line in the Containment Building, the ultra-small size of this region results in corresponding ultra-rapid decay of the shock wave such that it does not represent any hazard to the broader room itself. In the highly unlikely event that an ignition source is present at the precise location, the resulting detonation event is best characterized as a mere auditory nuisance, not a structural hazard.

In addition, the VCS system (Reference 11.144) can be credited as defence-in-depth. The VCS promotes mixing of the containment atmosphere and can reduce the likelihood of a flammable mixture of hydrogen from forming.

Auxiliary Building – Radiologically Controlled Area

Gaseous Radwaste System

The WGS receives processes and discharges the radioactive waste gases during all modes of plant operation. The primary feeds to the WGS are from the Reactor Coolant Drain Tank and the WLS system degasifier. The degasifier receives a feed from the CVS letdown and RCDT which incorporates dissolved hydrogen (Reference 11.100). The degasifier is operated under vacuum conditions to remove the dissolved hydrogen from the CVS letdown feed for onward processing by the WGS.

During normal operation of the plant, the degasifier is able to process 6.3E-03 $m^3 s^{-1}$ (100 gpm) with a dissolved H_2 concentration of 4.5E-05 $m^3 kg^{-1}$ (Reference 11.101). After processing through the degasifier, the H_2 concentration in the liquid stream drops to 1.4E-05 $m^3 kg^{-1}$, with the majority of the dissolved hydrogen off-gassing into the WGS. The WGS pipework, valves and fitting contain the gaseous stream prior to discharge via the VFS plant vent.

A leak from the WGS pipework could result in an accumulation of hydrogen in the affected room. The WGS is present in rooms 12153 and 12155. Based on the generation rate from the degasifier, hydrogen would be released into the room at a rate of 2.8E-04 $m^3 s^{-1}$ (0.6 scfm) at standard temperature and pressure. Both rooms are mechanically ventilated by the VAS. In accordance with the guidance in BS EN 60079 Part 10-1 (Reference 11.98), the background concentration of hydrogen, X_b (vol/vol) can be calculated using the following equation:

$$X_b = \frac{f \times Q_g}{Q_2}$$

Where: f is a measure of the degree of mixing, 5 for poor mixing; Q_g volumetric release rate of flammable gas ($m^3 s^{-1}$); Q_2 is the volumetric flow rate of air leaving the room ($m^3 s^{-1}$). Within room 12155, the background concentration would therefore be 0.8 v/v %. This is lower than the LFL for hydrogen in air (4 v/v %) and therefore a flammable atmosphere is prevented from accumulating by the VAS.

Liquid Radwaste System

The WLS receives borated and hydrogen bearing water from the PSS, RCDT and CVS. The liquid waste is passed through a degasifier to remove dissolved hydrogen (and other radiogases). The degasifier receives a feed from the CVS letdown and RCDT which incorporates dissolved hydrogen. The degasifier is operated under vacuum conditions to remove the dissolved hydrogen from the CVS letdown feed for onward processing by the WGS.

During normal operation of the plant, the degasifier is able to process 6.3E-03 $m^3 s^{-1}$ (100 gpm) with a dissolved H_2 concentration of 4.5E-05 $m^3 kg^{-1}$ (Reference 11.101). After processing through the degasifier, the H_2 concentration in the liquid stream drops to 1.4E-05 $m^3 kg^{-1}$, with the majority of the hydrogen passing into the WGS. The liquid is then passed to one of two effluent hold-up tanks. During hold-up in the effluent tank, some of the dissolved hydrogen may off-gas into the airspace above the effluent. The vent line from each of the effluent tanks incorporates a hydrogen monitor to detect the build-up of hydrogen. At 1 v/v % hydrogen in air, an alarm is triggered in the MCR. On receipt of the alarm an operator is required to initiate an air purge through the tank using the CAS to maintain the concentration below the flammable limit.

Auxiliary Building – Non-Radiologically Controlled Area

Auxiliary Building Battery Rooms

The hydrogen assessments of the Auxiliary Building battery rooms (References 11.97 and 11.143) evaluated the hazard presented by an explosive atmosphere and identifies those SSC necessary to prevent or protect Class 1 SSC from the effects of an explosion.

Each of the battery rooms contains 60 lead calcium cells. During charging the batteries generate hydrogen, which is released into the surrounding room. During normal operation, the VBS extracts sufficient air from the battery rooms to ensure that the hydrogen

concentration, including under the most onerous conditions, remains below 25% of the LFL. However, should the ventilation system fail, the hydrogen concentration will increase in the affected room(s).

The following table details the hydrogen generation rates under a range of conditions and the time to reach the LFL, assuming no ventilation extract, in the smallest room (Room 12101) which has a volume of 200 m^3.

Condition	Hydrogen Generation Rate (m3 s-1)	Time to LFL (4 v/v %) Days
Normal float charge at normal temperature (22.8 °C)	3.39×10^{-5}	27.3
Normal float charge at maximum temperature (48.9 °C)	2.6×10^{-5}	3.6
Equalising charge at maximum temperature (48.9 °C)	5.67×10^{-5}	1.6

The Auxiliary Building battery rooms are serviced by the VBS which when operating maintains the hydrogen concentration below 1 v/v % hydrogen in air. The exhaust of each fan (both duty and standby) incorporates a flow element to detect low, or no, exhaust flow. At 75% of normal exhaust design flow[11], the flow element will trigger an alarm in the MCR (Reference 11.99).

On low ventilation exhaust flow operators will preferentially undertake the following tasks:

1. Attempt to reinstate correct functionality of the duty fan;
2. Manually initiate the standby fan;
3. Isolate charging to the affected battery rooms.

Each of the AB battery rooms has two off hydrogen detectors. At 25% of the LFL, the hydrogen detector will trigger an alarm in the MCR alerting operators to the build-up of hydrogen (Reference 11.99).

On high hydrogen operators will:

- Isolate charging to the batteries in the affected rooms;
- Disable heaters in the ventilation supply lines;
- Halt activities which have the potential to cause a spark;
- Effect temporary ventilation of the affected rooms.

11. The VBS normally extracts 0.15 m3 s-1 (330 scfm) from each of the battery rooms. Assuming the worst case hydrogen evolution rate of 5.67 x 10-5 m3 s-1 (0.12 cfm), and poor HVAC performance, the VBS would need to extract at least 19% of its normal exhaust flow in order to maintain the hydrogen in air concentration below 1 v/v %.

During normal operation, any hydrogen evolved by the batteries during charging is removed from the room by the ventilation system. The vent system has been designed to maintain the concentration of hydrogen below 1v/v % in air. The formation of an explosive atmosphere within one of the battery rooms is postulated to arise as a result of either failure of the HVAC or a LOOP. The power to the ventilation system and the batteries is such that in the event of a LOOP, the batteries would stop charging. On reinstatement of power, the HVAC will automatically return to normal service, as would the batteries. It is therefore not possible for the batteries to evolve hydrogen, in the absence of ventilation, following a LOOP.

In the event of failure of the HVAC system and charging of the batteries continues, for the smallest battery room, it would take 28.8 hours at equalizing charge at maximum temperature before a flammable atmosphere (4 v/v % hydrogen/air) is formed. This assumes that the hydrogen concentration in the battery room was 1 v/v % prior to cessation of the HVAC although during normal operation it will be significantly lower than this.

The batteries are normally float charged to maintain their power and would only undergo equalising charge periodically. Furthermore, once charged, the batteries would revert to trickle charge. The assumed hydrogen evolution rate is based on the equalising charge being applied even after the batteries are fully charged. Given the length of time before an explosive atmosphere is formed in the battery room, it is not considered necessary to interlock the charging of the battery with the vent system.

Given the length of time, on loss of ventilation extract, to reach the LFL and the multiple warnings provided by the low ventilation extract flow alarm and the high hydrogen concentration alarm, it is considered unlikely that an explosive atmosphere would form in the battery rooms. Further, the battery rooms themselves are not claimed to be hermetically sealed and it would be expected that, either due to natural ventilation or the buoyancy of hydrogen, concentrations would not increase at the rates calculated.

In the highly unlikely event of redundant VBS fan failure and no action from operators to a high hydrogen alarm in the MCR, the hydrogen concentration in the battery rooms may increase to explosive levels. An unmitigated release of hydrogen in the battery rooms will lead to severe consequences, including structural barrier failure and ultimately the loss of redundant Class 1, Category A SSCs. The consequences of a detonation in one or more battery rooms have not been quantified, rather it is assumed that all IDS batteries and chargers are destroyed, leading to a loss of Category A safety function, including that of redundant division. In the event of unmitigated hydrogen build-up in one or more of the battery rooms, Reference 11.143 analysed the conservative scenario of unmitigated hydrogen release and accumulation using a release rate for sustained equalizing charge at maximum temperature 48.9 °C (120 °F). It would take roughly 1.6 days to reach the hydrogen LFL of 4 v/v % at equalizing charge at maximum temperature 48.9 °C (120 °F) for the smallest battery room, 12101. Using a normal float charge at normal temperature 22.8 °C (73 °F), that time period would get extended 27.3 days for Room 12101.

As the release of hydrogen from the batteries continues, the concentration of hydrogen in the room must cross the LFL to achieve flammability. If stray ignition sources in the battery rooms are postulated as an intermittent, but persistent, source that is responsible for deflagration, then the low hydrogen concentration range of 4.5 – 6.0 v/v % is the most likely candidate for deflagration. Such deflagrations can be readily handled via passive venting through HVAC ducts, remaining below the withstand of the battery room walls (5 psi). The pressure pulse will be relieved through the HVAC penetrations in the concrete room structure. It would take roughly 2.5 days to reach a hydrogen concentration of 6 v/v % at equalizing charge at maximum temperature 48.9 °C (120 °F) for the smallest battery room,

Room 12101. Using a normal float charge at normal temperature 22.8 °C (73 °F), that time period would get extended to 41 days for Room 12101.

Per the battery room hydrogen explosion analysis (Reference 11.143), elevated hydrogen concentration in the range of 8 - 12 v/v % is less likely since it requires the initial absence of an ignition source for the additional hydrogen accumulation followed by the latter-stage. If the less likely deflagration at elevated hydrogen concentrations in the range 8 - 12 v/v % must be considered for conservatism, 8 – 12 v/v % hydrogen concentration in air will exceed withstand of the battery room walls (5 psi) and remain above the limit for 45 - 60 seconds if passive venting is not credited. If passive venting through HVAC ducts is credited, then the peak pressure ratio is mitigated, and the duration above the administrative limit is reduced substantially to 5 - 6 seconds. Finally, if pressure relief via over-pressure catastrophic failure of the main access door is credited, then the peak pressure ratio remains below the administrative limit for the entirety of the deflagration duration. Note, there are no safe shut down SSCs serving Category A functions in the Corridors, Rooms 12111 and 12211, into which the battery room doors will relieve to. Further discussion of the mechanisms of the door over-pressure failure is provided in Section 3.1.4 of Reference 11.143.

While the deflagrations occurring in the concentration range 8 - 12 v/v % can be accommodated, deflagration-to-detonation (DDT) remains a concern for 10 v/v % and larger. Per the battery room hydrogen explosion analysis, Reference 11.142, detonation tolerance is not established, so a successful outcome is not assured. 8 v/v % is the highest concentration analysed that can both tolerate a deflagration and avoid a detonation. It yields a successful outcome in all respects. Furthermore, the roughly 3.3 day (Room 12101) timeframe for development of 8 v/v % provides ample time for operators to recognize an unmitigated hydrogen release scenario and take action to counteract this circumstance far in advance. Using a normal float charge at normal temperature 22.8 °C (73 °F), that time period would get extended to 54.6 days for Room 12101, giving even more time to take action.

As described in the details of this section, the Westinghouse safety case approach to the battery rooms is a multilayer approach, consisting of VBS ventilation, VBS low flow detection, hydrogen detection, operator action, and room barriers. Thus to summarize the auxiliary building battery room safety case (Timeframes based on smallest battery Room 12101):

1. Under normal conditions an explosive atmosphere is prevented by the VBS.

2. Under fault conditions of loss of VBS extract an explosive atmosphere will form. However the effects of an explosion will be confined to the room in question provided the hydrogen concentration remains below 8 v/v % (most limiting). Battery room walls can withstand a deflagration up to 12 v/v % or detonation up to 8 v/v %. As an example, at the maximum hydrogen generation rate, it would take around 3.3 days to reach 8 v/v % for Room 12101. Assuming a float charge at normal operating temperature, that time period would get extended to 54.6 days giving even more time to take action.

3. It is not considered credible that hydrogen will accumulate for 3.3 days because:

- The vent low flow alarm will sound in the MCR at 75% of the design exhaust flow (giving 3.3 days prior warning to operators);

- The hydrogen detection in the room will alarm at 1 v/v % (giving 2.9 days prior warning to operators);

- Operators perform rounds and would identify issues in the battery rooms, as an example if there is an absence of exhaust flow due to a low flow alarm, high temperatures in the room, or an alarm from the hydrogen detectors.

A host of process and equipment failures need occur before an explosive atmosphere large enough to impact multiple divisions of IDS battery rooms or other Class 1, Category A SSCs. The timeframe for the event to occur also provides ample time for operators to recognize an unmitigated hydrogen release scenario and take action to counteract this circumstance far in advance.

Valve/Piping Penetration Room (12306)

The assessment of leakages associated with the hydrogen injection package (Reference 11.105) evaluates the potential for an explosive atmosphere to form in the valve/pipe penetration room.

The hydrogen injection package is supplied from 4 high pressure hydrogen bottles located in the PGS. The high pressure hydrogen switchover station automatically switches the supply from the 2 duty bottles to the 2 standby bottles once they become depleted. Each of the high pressure hydrogen bottles has a nominal capacity of 15.6 m^3 (550 scf), giving a total available hydrogen volume of 62.3 m^3 (2200 ft^3) (Reference 11.105).

The hydrogen injection package has two modes of operation, continuous and batch, depending on the plant mode, supplied via two parallel lines. The maximum flow rate during either continuous or batch mode is limited, by orifice plates, to 5 E-04 $m^3 s^{-1}$ (1.05 scfm) or 9.3 E-05 $m^3 s^{-1}$ (0.2 scfm) respectively.

The hydrogen injection package originates in the Turbine Building and passes, via 12306, into Containment. The pipework, valves and fittings for the CVS within 12306 are butt welded and hermetically sealed. During normal operation, there would be no leak of hydrogen from the CVS into room 12306 or any room communicated to 12306.

However, should the pipework, valves or fittings fail (e.g., double guillotine failure), hydrogen would leak from the pipework into room 12306 which communicates directly with rooms 12406 and 12506 above, via pipe penetrations.

The assessment of a leak from the hydrogen injection line, Reference 11.105, has identified that it may be possible for an explosive atmosphere to form in 12306, 12406 and 12506. As a result, an assessment of a hydrogen injection line break in the Auxiliary building, Reference 11.142 was completed. This assessment has determined that a worst case gross failure of the CVS hydrogen line would not lead to an explosive atmosphere in rooms 12306, 12406, and 12506, even if the break leak would continue for multiple days without mechanical ventilation active in the rooms. The results of Reference 11.142 show that even after 14 days of continuous leakage, the upper portion of room 12306 will not reach 1% hydrogen. Hydrogen concentrations in rooms 12406, and 12506 (specifically the upper area of room 12506 as the anticipated area of highest concentration) remain below the concentration of the upper area of room 12306 throughout the transient. This auxiliary building condition corresponds to a very benign circumstance with regard to hydrogen hazard for even this most conservative configuration of no ventilation flow. It was determined that 1 v/v % of hydrogen in Room 12306 would be reached in approximately 54 days. A continuous leak of 31 days or more is not considered credible as it would exceed the quantity of hydrogen available (4 high pressure hydrogen bottles, each containing 15.6 m^3 (550 scf) of hydrogen)

Further, an assessment of any potential limiting localized plume was confirmed to not result in failure of the room barrier (walls, ceiling floor (Reference 11.142); therefore, deterministically assuming loss of safety functions within the impacted room, the redundant safety function systems remain unaffected. As described in Section 7.8 of CVS hydrogen line break assessment (Reference 11.142), while plume detonation in the presence of an assumed local ignition source is possible during a guillotine break or long term leak of the hydrogen injection line in the Auxiliary Building, the ultra-small size of this region results in corresponding ultra-rapid decay of the shock wave such that it does not represent any hazard to the broader room itself. In the highly unlikely event that an ignition source is present at the precise location, the resulting detonation event is best characterized as a mere auditory nuisance, not a structural hazard.

Areas Outside of the Nuclear Island

Areas outside of the NI include the Annex Building, Turbine Building, Radwaste Building and those buildings/structures/installation not directly abutting the NI in the wider yard area. There are no Class 1 SSCs located in areas outside of the NI and therefore the significance of any explosion is instead focussed on the overpressure experienced by the NI and Shield Building outer walls.

The following sections present the results of the analyses for the various flammable substances which have the potential to generate an explosive atmosphere.

Annex Building Battery Rooms

The explosive hazard presented by the Annex battery rooms has been evaluated (Reference 11.94), based on a series of conservative assumptions, to determine if an explosive atmosphere can be generated. For exclusion purposes, it is noted that there are no batteries used or stored within the Radwaste Building. In addition, it is also noted that, as the batteries and ventilation system will be powered from the same power source a loss of power will cease ventilation and charging, and thus, hydrogen generation.

For the battery rooms, an acceptable method for establishing safe separation distances (beyond which no adverse effect would occur following a hydrogen explosion) is based on a level of peak positive incident over-pressure (Reference 11.94). In accordance with industry guidance, the maximum peak positive incident over-pressure relevant to the SSCs of concern has been conservatively determined by the USNRC to be 1 psi (6.9 kPa) (Reference 11.102).

Each battery room contains 120 battery cells. The hydrogen generation rate for 120 battery cells operating (i.e., the amount generated in one room) is estimated to be 4.63E-02 $m^3 hr^{-1}$ (1.63 cf hr^{-1}) for an equalising charge. At an elevated temperature of 50°C the hydrogen generation rate is increased to 3.24E-01 $m^3 hr^{-1}$ (11.4 cf hr^{-1}) for an equalising charge.

The volume of battery rooms have been assessed, with battery room 40412 forming the bounding case (smallest room) with a total volume of 150 m^3 (5300 ft^3). Of the total volume, 30% is assumed to be occupied by internal structures and equipment, giving a net 'free-space' volume of 105 m^3 (3710 ft^3).

Averaging the volume of hydrogen generated during a 12-hour battery charging period (4.2E-02 m^3) over the entire free-space volume of battery room 40412 results in a concentration of less than 1 v/v % hydrogen. At the elevated temperature the LFL is reached in 12 hours if ventilation is not present.

The LFL and Lower Explosive Limit (LEL) for hydrogen in air are 4% and 18% by volume, respectively. For an equalisation charge it would take 3.8 days to reach the LFL and 17 days to reach the LEL at STP and 12 hours and 2.4 days at the elevated temperature. This would be under fault conditions as the ventilation would have had to fail.

For a float charge the hydrogen generation rate is significantly reduced (2.1E-02 $m^3 hr^{-1}$ (0.75 cf hr^{-1}) at STP, such that the time to reach the LFL and LEL is 8.2 and 37.1 days respectively. Thus, the times to LFL and LEL for the elevated temperature are 1.2 days and 5.3 days.

In the event of a loss of ventilation to the Annex battery rooms and a build-up of hydrogen, operator action is required to restore ventilation or cease battery equalisation charge. Battery rooms 40307 and 40309 contain exhaust airflow monitors that monitor VXS exhaust flow. At 75% of normal exhaust flow, the flow element will trigger an alarm in the MCR. Room 40412 contains air temperature monitors to provide temperature indication and alarm when the room air temperature is either too high or too low to support operation of the batteries. A temperature alarm in room 40412 may be used to indicate if the VXS HVAC system is working correctly.

The battery rooms also contain hydrogen detectors which trigger an alarm in the MCR at 1 v/v % hydrogen in air. Thus, the time within which operator action is required is a minimum of 9 hours assuming an equalisation charge at elevated temperature. This is the bounding case. At standard temperature and pressure conditions, the time available is 68 hours. The conditions for a float charge (the normal operation of the batteries) produces much longer times to reach the LFL. Thus, detection of a hydrogen atmosphere and sufficient response time is available for the operator to either restore ventilation or cease charging of the batteries.

Chemical Feed System – Chemical Explosion & Pool Fire Assessment

Numerous chemicals are stored and used to support normal plant operations. The main system used to manage these operations is the Chemical Feed System (CFS), which stores chemicals needed for the operation of the Condensate System (CDS), FWS, Auxiliary Steam Supply System (ASS), Steam Generator Blowdown System (BDS), SWS and Demineralised Water Treatment System (DTS). Reference 11.95 identifies the chemicals handled by the CFS that present an explosive hazard along with the relevant storage vessel identifier, each of which is vented to the outside of its associated building.

In addition to the explosively hazardous chemicals handled by the CFS, a number of other flammable and explosively hazardous chemicals are stored and used on site, including liquid hydrocarbons (e.g., bulk diesel fuel oil supplies for the DG Building) and liquefied/gaseous hydrogen supplies (Reference 11.95).

It is noted that, although a release of diesel oil at ambient temperature does not necessarily produce a potentially explosive atmosphere, however, if the tank contents were to be heated by an external source, a potentially explosive atmosphere could be formed.

As an on-site explosion involving any of the above chemicals has been assessed on the potential to affect the function of safety-related SSCs, (Reference 11.95), in accordance with the following methodologies:

- TNT-equivalence method (described in NUREG Guide 1.91 [Reference 11.102])

- Multi-Energy Method (MEM) (described in the report on 'Methods for the Calculation of Physical Effects' produced by the Committee for the Prevention of Disasters).

Although not a prescribed requirement of Reference 11.102, a 30% margin is added to the required minimum safe separation distance between the postulated explosion and Class 1 SSCs to account for the potential under-prediction of the blast radius by the TNT equivalence method (due to several factors including explosive material type, form and shape).

In addition to explosion analysis, thermal radiation effects on SSCs from a chemical pool fire have been examined where appropriate (i.e., for diesel fuel oil and waste oil spillages) using the US NRC Fire Dynamic Tool, which allows comparison of incident heat fluxes resulting from a pool fire with critical heat fluxes (associated with thermal radiation effects on structures) for the purposes of determining minimum safe separation distances between postulated pool fires and Class 1 SSCs.

The results of the chemical explosion and thermal radiation analyses (Reference 11.95) demonstrate that, in all cases (and with significant safety margins), the required safe separation distances between Class 1 SSCs and explosively hazardous chemicals, or those chemicals that have the potential to form pool fires in the event of loss of containment is satisfied.

Plant Gas System Hydrogen Assessment

Hydrogen is used in the Turbine Building for cooling the generator and in the AB for de-oxygenation of water stored in the Condensate Storage Tank (CST) and water discharged from the Demineralised Water Storage Tank (DWST).

Hydrogen is sourced from the liquid hydrogen storage tank located in the PGS storage area, which is to be located outside and away from the west-side of the Turbine Building.

The hydrogen bulk storage vessel will be charged with liquid hydrogen from bulk delivery via a transport trailer. The details of the transport trailer, consignment sizes and local management arrangements to maintain liquid hydrogen to minimum quantities are site-specific and, hence, these will be addressed during the site specific licensing process.

The hydrogen bulk storage facility is comprised of:

- One liquefied hydrogen cryogenic storage vessel and cylinder filled with liquefied hydrogen per power generating unit;
- Vapouriser;
- Interconnecting piping, fittings, valves and gauges.

The cryogenic storage vessel will be double-skinned and comprise of both an inner and outer vessel with insulation in between.

As it is postulated that a hydrogen release could occur from the PGS, an assessment of the relevant mechanisms for and consequences of hydrogen release has been undertaken (Reference 11.96) to determine the minimum safe separation distance required between the PGS (and associated storage plant) and safety-related SSCs. Credible release mechanisms include:

- Catastrophic vessel failure;
- Catastrophic pipework failure (such as a guillotine break);
- Loss of hose connection (during filling operations);
- Small leaks (at valves and glands, or from holes in the filling hose).

The hydrogen release assessment has been undertaken using the MEM. It is noted that the consequences of small leaks are bounded by catastrophic vessel and pipework failures and, as filling operations are considered site-specific (i.e., covered during the site licensing process), the scope of the hydrogen release assessment is focused on catastrophic failures of the vessel and pipework only.

The hazard to SSCs from a hydrogen flash fire is judged not to be significant compared to the potential damage caused by the blast overpressure.

The PGS is located in the yard area outside of the Nuclear Island. Class 1 SSC are only located inside of the Nuclear Island; in order for Class 1 SSC to be damaged by an explosion originating external to the NI, the resultant overpressure must exceed the withstand of the NI exterior walls.

The hydrogen gas explosion evaluation (Reference 11.96) has determined a safe separation distance, from the centre of the cloud, of 187 m (614 ft). Locating the cryogenic hydrogen storage vessel at an approach no less than this distance will ensure that the NI walls resist the overpressure.

11.5.4.4 Hazard Schedule

The internal explosion hazard schedule (see Table 11.5-2) has been prepared based on the results of the analyses of explosive atmospheres. In accordance with relevant international guidance (Reference 11.23), the explosion hazard analyses have considered an explosion wherever the possibility exists for a flammable atmosphere to form.

The hazard schedule is presented in tabular form providing a concise and comprehensive summary of the postulated explosion events, their significance and how the AP1000 plant is designed to cope with the hazard.

11.5.4.5 Discussion of Results

The analysis concluded that there are no internal explosion hazards which could result in the loss of all divisions of Class 1 SSC delivering a Category A safety function. Further, the potential hazard to operators required to undertake actions in support of Category A safety functions is low.

11.5.5 Sensitivity of Results and Cliff Edge Effects

The approach to internal explosions does not lend itself to the consideration for cliff edge effects. The inherent design features respectively prevent, detect, protect and control the risk

of an internal explosion. Design features such as conservative safe distance, or redundant detection equipment contain enough margins to keep the internal hazard in-line with analysed scenarios. It is therefore determined that cliff edge effects are not a concern for internal explosion hazards.

11.5.6 Combined Hazards Discussion

The internal explosion hazard analyses consider, on a deterministic basis, an explosion occurring in each of the rooms with a potential source for generating an explosive atmosphere.

The consideration of credible combinations of internal explosion with other postulated initiating events likely to occur independently of an explosion is considered in section 11.12. A separate document, Reference 11.75, provides a coherent approach across all internal hazard types e.g., fire, missiles, dropped loads, flooding.

Combinations of independent internal and external hazards (e.g., internal explosion and extreme low temperatures) are considered to be outside of the design basis and have not been explicitly considered in this report. However, compliance with relevant equipment and structural design codes ensure that combinations of internal hazards with the relevant abnormal operating occurrences (including environmental hazards) are addressed.

Discussion of combined and consequential hazards is presented within the Combination of Hazards section (see Section 11.12).

11.5.7 ALARP Assessment and Discussion

Deterministic analysis of postulated, design basis, internal explosions shows that the Category A safety functions will be available to provide a safe shutdown following the worst case postulated initiating event.

A number of hazardous substances are required to operate the reactor and maintain a safe state. Wherever possible, these hazardous substances are located outside the Nuclear Island and therefore are remote from the Class 1 SSC delivering Category A safety functions. Where it has not been possible to locate the bulk chemical supplies outside of the NI, the quantity has been minimised so far as is reasonably practicable.

The approach to managing hazardous substances within the Nuclear Island has been to prevent the formation of flammable atmospheres. This has been achieved through the use of containment (e.g., piping), mechanical ventilation and alarms set at a level below the LFL for the relevant substance.

With the exception of the battery rooms, which would continue to evolve hydrogen, faults leading to the release of hydrogen would result in a hydrogen concentration above the LFL but below the LEL. At a concentration of less than 8 v/v % in air, hydrogen burns in a single direction with little or no overpressure. At concentrations of 8 v/v % and above, hydrogen will burn in all directions but the flame speed is low. Only where there is congestion or a concentration of 18 v/v % or more would the ignition result in significant overpressures. Within this assessment, it has conservatively been assumed that any release above the LFL would result in significant overpressure.

Outside of the Nuclear Island, the same, preventative, approach has been adopted. However the reliance is instead placed on the structural integrity of the Nuclear Island external walls to resist the effects of an explosion.

It is further anticipated that, during site licensing, a DSEAR (Reference 11.109) assessment will be undertaken and hazardous areas classified in accordance with BS-EN-60079 (Reference 11.98). Where a hazardous area is classified, equipment will be categorised according to the hazardous area and the nature of the flammable substance (e.g., ignition temperature and energy) such that the potential for a flammable atmosphere to form and subsequently be ignited is minimised.

Since the Category A and supporting post 72-hour Category B safety functions can be adequately maintained despite the hazard posed from internal explosions, the safety of the plant is ensured. It is judged that only minimal safety benefit may result from the introduction of further design measures to reduce the risks further and on this basis the risk from internal explosions is considered to be broadly acceptable and ALARP.

11.6 Internal Missiles

11.6.1 Introduction

The Internal Missiles Hazards Analysis (Reference 11.110) has being performed in order to define the safety case in determining the effects to Systems, Structures, and Components (SSCs) as resulting from an internally generated missile arising within the AP1000 plant. Internally generated missiles are considered arising from postulated initiating events such as the failure of pressure vessels, the failure of valves, and the failure of high speed rotating equipment. AP1000 has been designed such that an internal missile within the design basis will not compromise the ability of the plant to safely shutdown the reactor. The Category A safety functions and supporting post 72-hour Category B safety functions required for safe shutdown following an internal missile scenario are shown to be maintained through a combination of claims made on equipment design, room barriers and the separation and segregation of safe shutdown SSCs.

Potential missile sources that have the potential to directly damage equipment containing SSCs required to deliver Category A or supporting Category B safety functions have been identified on a deterministic basis. The barriers that protect the Category A and supporting post 72-hour Category B safety functions are identified. These are then evaluated to confirm that they will provide protection against the identified missiles. The following credible postulated sources of internally generated missiles having sufficient energy to create a hazard to Class 1 SSCs considered are:

- Turbine disintegration
- Rotating components
- Pressurised components
- Valves
- Tanks

Additionally, rooms assessed for internal missiles are identified to demonstrate separation of sources from SSCs required as delivering diverse or redundant functions. The demonstration of the response to an internal missile hazard is performed using the following conservative assumptions:

- SSCs protection within a compartment with a potential missile source is not credited,

- SSCs within a compartment are assumed to fail (gross failure) as a result of missile strike,

- Generating an internal missile is credible in any compartment with a potential missile source,

- Hazard assessments evaluate the operating plant state applicable to each missile as appropriate defined by the missile source. Structural barriers assessed as missile barriers are claimed to prevent a missile exiting its originating compartment.

The overall scope of the internal missile analysis requires evaluation of missile sources within the Nuclear Island (NI), and in adjacent buildings for potential impact on the NI. The assessment concludes that the function of essential SSCs are protected from the effects of an internally generated missile through a combination of claims made on equipment design, structural barriers and, where necessary, separation of SSCs required to deliver safe shutdown.

11.6.2 Internal Missiles Claims, Arguments and Evidence

This section presents the key claims, arguments and evidence made in relation to internal missile hazards on the AP1000 design.

SSCs important for nuclear safety must be protected from dynamic effects within the plant, including those of internally generated missiles. An internal missile hazard has as a potential result the development of a transient from the normal operating state of the reactor which may potentially contribute to an uncontrolled radiological release. In response to such a transient, it may be necessary to shutdown the reactor and return it to a safe shutdown state. Depending on the nature of the transient, there are a number of courses of action using Category A or supporting Category B SSCs in placing the reactor into a safe state. Availability of the SSCs required to deliver the Category A or Category B post 72-hour safety functions ensures that the reactor can be safely shutdown in accordance with the design intent.

Therefore, protecting SSCs important to safety from the adverse effects of a hazard, such as an internally generated missile, prevents both failure of systems required for safe shutdown of the reactor and hence potentially significant uncontrolled release of radioactivity. This forms the basis of the high level claim as stated below.

11.6.2.1 Claims Overview

The high level claim has been divided into claims for Prevention and Protection and is broken down into Sub-Claims within these divisions. Detailed arguments and evidence for each Sub-Claim are presented in (Reference 11.110).

11.6.2.2 High Level Claim

Claim IH-5.0: **An internal missile event within the design basis does not prevent delivery of the Category A safety functions and supporting post 72-hour Category B safety functions necessary to respond to the postulated event.**

Within the AP1000 design, this has been achieved through:

- Prevention: Missiles are deterministically assumed to occur as a result of a gross failure of SSCs, except those justified as Highest Safety Significance (Reference 11.9) and those where valves are qualified to prevent missile generation.

- Protection: Passive protective measures are incorporated in the AP1000 to protect SSCs that deliver Category A and post 72-hour Category B safety functions from internal missiles.

The SSCs claimed to provide post-72 hour support functions include only offsite procured SSCs and their associated Class 1 connections.

11.6.2.3 Prevention Claims and Arguments

Missiles are deterministically assumed to occur as a result of a gross failure of SSCs, except those justified as Highest Safety Significance (Reference 11.9) and those where valves are qualified to prevent missile generation. The following claims and Sub-Claims and arguments are defined in support of the overall high level claim:

Claim IH-5.1: **Internal missiles have been eliminated from the design so far as reasonably practicable.**

Sub-Claim IH-5.1.1: **Internal missiles generated from failure of rotating equipment are eliminated by design so far as reasonably practicable.**

Argument IH-5.1.1: **To prevent abnormal operation and failures by design, the material selection, design, build and verification requirements for a selection of SSCs ensure that the total energy contained in the rotating elements of the SSC is insufficient to move the mass of rotating parts so that it breaches the equipment housing. Therefore a potential missile is retained within the SSCs equipment housing and does not result in a missile external to the SSC.**

Within containment, catastrophic failure of rotating equipment, such as pumps, fans, and compressors, but excluding the reactor coolant pumps, leading to the generation of an internal missile impacting Class 1 SSCs, is not considered credible. These components are designed to preclude having sufficient energy to move the masses of their rotating parts through the housings in which they are contained. In addition, the Design Criteria for the Protection from Internally Generated Missiles, Reference [11.145] states that the material characteristics, inspections, quality control during fabrication and erection, and prudent operation as applied to the particular component will enhance prevention.

The maintenance and inspection program for the turbine assembly and valves is based on turbine missile probability calculations, operating experience of similar equipment and inspection results. The methodology for analysis of generating missiles from fully integral rotors identifies that stress corrosion cracking is the dominant mechanism for determining missile generation from the turbine. The probability of rotor burst by

this mechanism does not exceed 1 x 10-5 per year, based on conservative analysis, Reference [11.113].

Sub-Claim IH-5.1.2: **Internal missiles will not be created from SSCs which are classified as HSS.**

Argument IH-5.1.2: **Internal missiles will not be created from SSCs which are classified as HSS. The most demanding of these, HSS, is broadly equivalent in definition to the term Incredibility of Failure (IoF), used within the UK structural integrity community to describe components where the claim is that the likelihood of gross failure is so low it can be discounted.**

The basis for the component classifications determined using the process are detailed in Appendix A of Reference [11.72]. Based on the results of this evaluation, the following AP1000 plant components are to be treated as HSS components include the Reactor Vessel, Pressuriser, Steam Generator Secondary Shell, Tube Sheet and Channel Head.

Sub-Claim IH-5.1.3: **The failure of valve stems, bonnets and thermowells in SSCs where the stored energy is high will not lead to internal missiles.**

Argument IH-5.1.3: **For the AP1000, valves will be constructed with missile retention and preventative measures in order to prevent internally generated missiles. The material selection, design, build and verification requirements for valve stems, bonnets and thermowells incorporate measures to prevent them from becoming credible missiles. Threaded connections in high-energy systems are avoided wherever possible.**

The AP1000 Valve Missile Protection report, APP-GW-M3C-013, Reference [11.146], defines how valves in high energy systems are designed to prevent missiles, as required by the AP1000 Design Criteria for the Protection from Internally Generated Missiles, Reference [11.145]. A detailed discussion of the criteria applied to valves is presented in Section 5.4.2.1 of Reference [11.110].

Sub-Claim IH-5.1.4: **Nuts, bolts and nut bolt combinations have only a small amount of stored energy and are not considered credible missiles.**

Argument IH-5.1.4: **Potential missiles are not considered a credible hazard to Class 1 SSCs when there is insufficient energy available to produce a missile, or if by design the probability of creating a missile is remote. The stored energy in ejected nuts, bolts or nut and bolt combinations is low and will not breach the internal barriers or containment.**

Sub-Claim IH-5.1.5: **Gross failure of control rod drive mechanism housing is not considered a credible missile source.**

Argument IH-5.1.5: **Gross failure of control rod drive mechanism housing is not considered a credible missile source.**

Equipment within the containment is designed to prevent generation of internal missiles as required by the Design Criteria, Reference [11.145]. Prevention of Gross failure of a control rod drive mechanism housing with sufficient energy to allow a control rod to be ejected rapidly from the core is detailed in Section 4.2.1.1 of Reference [11.110].

11.6.2.4 Protection Claims and Arguments

Passive protective measures have been incorporated in the AP1000 design to protect SSCs that protect Category A and post 72-hour Category B safety functions from internal missile.

This claim is based the provision of structural barriers that prevent a missile originating in one area of the AP1000 from impacting the SSCs outside that area, that are required for delivery of the Category A and supporting post 72-hour Category B safety functions. The following Sub-Claims and arguments are made to achieve the overall high level claim:

Claim IH-5.2: **SSCs required for delivery of Category A and supporting Category B safety functions are protected by barriers that will prevent missile penetration.**

Sub-Claim IH-5.2.1: **The consequences of missiles will be protected through the use of passive barriers to limit the impact to and/or loss of a Category A or post 72-hour Category B safety functions.**

Argument IH-5.2.1: **The consequences of missiles will be protected through the use of passive barriers to limit the impact to and/or loss of a Category A or post 72-hour Category B safety functions.**

Missile barriers and protective structures are designed to withstand and absorb missile impact loads to prevent damage to safety-related components as detailed in the AP1000 Civil/Structural Design Criteria, Reference [11.107]. Correct application of these design criteria protect the Category A and post 72-hour Category B safety functions contained within the NI.

Sub-Claim IH-5.2.1.1: **SSCs are protected from missiles through internal barriers such as walls, floors and ceiling structures. Gross failure is assumed for all SSCs within the barriers affected by the missile.**

Argument IH-5.2.1.1: **The locations of the SSCs that provide the Cat A and supporting Cat B safety functions relative to the missile sources have been identified, Reference [11.112]. The barriers that provide protection to the SSCs have been identified and the potential missiles categorised according to mass, shape, size, velocity, orientation and trajectory. The missile impact energy has therefore been assessed and the barrier withstand are therefore known and the protection claimed from the barrier can be determined using the Missile Barrier Design Procedures, Section 4.3.1 of Reference [11.107].**

The frequency of missile generation from all sources has been identified and the resulting consequences of the missiles

assessed. The barriers that will protect the SSCs providing Category A and supporting Category B safety functions are identified in the Hazard Barrier Matrix, Reference [11.9]. It is demonstrated by the missile hazard assessment, Reference [11.112] that these barriers provide adequate protection from an internal missile event.

Sub-Claim IH-5.2.2: **Orientation of equipment will protect delivery of Category A or post 72-hour Category B safety functions in the NI.**

Argument IH-5.2.2: **The turbine is oriented such that its shaft axis is perpendicular to the NI. The orientation of the turbine applies relevant good practice, minimising the possibility of a missile fragment from impacting the NI. Protection of the NI safety functions from internal missiles due to orientation of equipment is further detailed in Section 4.2.2 of Reference [11.110] and Reference [11.112].**

11.6.2.5 Mitigation Claims

Mitigation actions are not directly claimed for Internal Missiles because the passive SSCs are designed to independently mitigate Design Basis Accidents (DBAs) for the initial 72 hours following an initiating event. This capability is presented in Chapter 10.

11.6.3 Internal Missiles Safety Case Summary

11.6.3.1 Introduction and Overview

The UK AP1000 safety design approach adopted for the internal missile hazard is composed of a range of complementary approaches. These are applied as appropriate in order to minimise the frequency of an internal missile occurring and reduce the potential disruption to nearby Class 1 SSC.

Missiles are assumed to occur as a result of a gross failure initiating event for assessment, except those justified by the Structural Integrity Highest Safety Significance (HSS) classification (Reference 11.9) and those where equipment is qualified to prevent missile generation. For instance, use of valves designed and constructed with missile retention and preventative measures which prevent the generation of missiles are not considered missile sources. Such passive protective measures have been incorporated in the AP1000 design to protect SSCs that deliver Category A and post 72-hour Category B safety functions from internal missile faults. In this regard, the consequences of missile hazards are contained through the use of passive barriers, thus limiting impacts to, and loss of, a safety function.

With respect to generation of turbine missiles, the turbine generator is located north of the NI with its shaft oriented north-south according to relevant good practice (11.114). Orientation of the steam turbine provides a level of protection for the delivery of Category A or post 72-hour Category B in the NI, since postulated turbine missiles will be projected essentially perpendicular to the shaft.

The role of gross failure in the internal missiles case pertains to all missile sources, except where prevention claims are made for missile sources. In summary, the safety case accepted such prevention claims as based on the following:

- Incorporation of design features in components to prevent missiles from being generated externally to the component
- Orientation of components, such as the main turbine, to direct any missile away from Safety Class 1 SSCs
- Location of Safety Class 1 SSCs outside the zone of influence of a potential missile
- Protection where practicable using either distance or separation by a structural barrier

Further, the AP1000 design employs a mixture of the approaches stated above to form levels of defence which reduce the likelihood of an internal missile generated from equipment and also reduces the consequences of an internally generated missile to ALARP. It is argued that the gross failure of equipment within a segregated area because of a missile impact, regardless of orientation, is entirely consistent with, and bounded by, other hazard analyses (i.e., internal fire), in assuming that all equipment in such an area is lost as a result of the hazard. In this manner, consistency between other areas of the safety case is maintained.

11.6.3.2 Applicable Codes and Standards

The following guidelines and methods are used in the evaluation of the Turbine Missile Safety Case:

- R3
- Modified NDRC
- Hagg & Sankey (Reference 115)

Missile barriers and protective structures are designed to withstand and absorb missile impact loads in order to prevent damage to Class 1 SSCs.

The appropriate design codes and standards are provided in the AP1000 Civil/Structural Design Criteria (Reference 11.107). To evaluate the AP1000 codes and standards against UK expectations, the AP1000 codes and standards have been organised by the relative safety significance of the SSCs to which they have been applied. To support this organisation (Reference 11.26) describes the process for categorisation of safety functions and classification of SSCs. The classification methodology defines Safety Categories (A, B or C) which are based on how important each safety function is for maintaining nuclear safety. This leads to the Safety Classes (1, 2 or 3) which indicate the significance of an SSC to deliver the relevant safety function.

The AP1000 Equivalence/Maturity Study of US Codes and Standards (Reference 11.25), provides an assessment of the applicability of US-based codes and standards to UK, European and international codes and standards in the present Topical Report. It provides a clear and auditable demonstration that the applicable codes and standards to support the design substantiation of UK Class 1 SSCs have been identified.

Detailed discussion of applicable codes and standards is presented in Chapter 5.

11.6.3.3 Redundancy and Segregation

The location and level of redundancy of Class 1 and 2 safety systems within the plant is such that complete loss of operability of the SSCs within a room or compartment because of

disruption resulting from an internally generated missile would not result in loss of the Category A safety function. Redundant and segregated Class 1 or Class 2 SSCs are located solely within the NI. Inside buildings, the AP1000 compartmentalised design minimises the probability of internally generated missiles affecting SSCs. Should an internal missile occur as affecting Class 1 or Class 2 SSCs, redundant equipment is located elsewhere.

Measures applied with respect to redundancy, separation, and segregation ensure that missiles cannot prevent Class 1 SSCs from delivering their Category A functions. These measures consist of the following:

- The design of the AP1000 plant ensures multiple means of delivering the Category A safety functions, such that a missile cannot prevent delivery of the Category A function.

- Within the Containment there is segregation and separation of Class 1 equipment. This is provided by a combination of barriers formed by the walls and floors of compartments and the distance between systems providing redundant means of delivering the Category A functions.

- Outside the Containment there is sufficient equipment redundancy, segregation, and protection such that all of the equipment in a single room can be lost without preventing delivery of the Category A safety functions.

- The Class 2 systems are an additional means of delivering Category A safety functions. They provide a level of defence in depth. The Class 2 system designs also feature redundancy. The Category A functions provided by these systems are summarised in Section 3.5 of Reference 11.110.

- In the immediate vicinity of a missile, barriers may be employed to limit the zone of influence of the missile such that no Class 1 equipment is impacted. The civil engineering structures provide structural support to the SSCs, but also act as suitable barriers for a number of functions, including preventing accidentally generated missiles from travelling to a location where significant harm could occur.

The plant is designed such that it can be operated with sufficient levels of protection in place to ensure that internally generated missiles will not prevent delivery of Category A safety functions. This defence in depth is provided by:

- The conservative design, manufacture, maintenance and operation of equipment in accordance with safety margins (through compliance with recognised design codes) appropriate engineering practices and monitoring of the quality of these aspects.

- The use of structural barriers to limit the path of any missile generated to areas where damage will not prevent the delivery of Category A safety functions.

- Sufficient redundancy and defence in depth is provided to ensure that even if there is the loss of any SSC as a result of an internally generated missile the Category A safety function can still be delivered.

The plant is designed such that it can be operated with sufficient levels of protection in place to ensure that internally generated missiles will not prevent delivery of Category A safety functions. This defence in depth is provided by:

- The conservative design, manufacture, maintenance and operation of equipment in accordance with safety margins (through compliance with recognised design codes) appropriate engineering practices and monitoring of the quality of these aspects.

- The use of structural barriers to limit the path of any missile generated to areas where damage will not prevent the delivery of Category A safety functions.

- Sufficient redundancy and defence in depth is provided to ensure that even if there is the loss of any SSC as a result of an internally generated missile the Category A safety function can still be delivered.

11.6.4 Internal Missile Assessment Approach

For a detailed description of each missile source refer to Reference 11.110. Missile sources are identified and analysed in subsection 11.6.6.

11.6.4.1 Interface with Other Internal Hazards

The UK AP1000 Nuclear Island Missile Penetration Calculation, (Reference 11.111) consider, on a deterministic basis, a single internal missile event and the consequential impact on SSC in the affected plant areas.

The consideration of credible combinations of internal missiles with other postulated internal hazards likely to occur independently of an internal missile hazard is presented in Section 11.12 and provides a comprehensive approach across all internal hazard types (e.g., fire, explosion, flooding, dropped loads, pressure part failure).

11.6.4.2 Conclusions

No analysis is required for Type I rooms that contain either Safety Class 1 equipment with no potential missiles, or Safety Class 2/3 equipment with no potential missiles.

The Type II and III analysis performed in (Reference 11.114) identifies postulated internal missile penetration depths in all relevant rooms of the Auxiliary and Shield Buildings. The integrity of all barriers within the NI is maintained following an internal missile event. This information is presented in (Reference 11.114). The bounding case for each equipment group (valves, tanks, rotating equipment) has been presented for each room studied along with the minimum thickness of the room barriers (i.e., North, South, East, West Walls, Floor and Ceiling for typical rooms). As demonstrated the minimum barrier thickness is adequately sized to withstand the bounding penetration depths for potential missiles into neighbouring rooms with Class 1 shutdown SSCs.

11.6.5 Internal Missiles Analysis

11.6.5.1 Identification of Missile Sources

This section provides a summary of internal missile hazard analyses, as presented in the AP1000 Nuclear Island Missile Penetration calculation, (Reference 11.111) and the UK AP1000 Turbine Missile Assessment (Reference 11.113). The approach taken followed three aims: to fully understand the consequences of a potential postulated missile, to establish an extent of condition, and to document fulfilment of all relevant safety requirements, licensing claims and design features of an AP1000 Plant. From these references, the

systematic assessment of potential sources of a postulated missile determined the following likely origination sources:

- Turbine disintegration
- Rotating components
- Pressurised components

The effects of missiles originating from these sources depend on their physical characteristics, i.e., mass, shape of the impinging cross-section, and on the constraints acting on the component hit by the missile. The effect of the missile depends heavily on these variables, along with flight path and whether or not the projectile rotates or tumbles. For design purposes, it is more conservative to overestimate the velocity of the missile than to underestimate it. Simple conservative methods for calculating the velocities of postulated missiles, along with potential mass, are presented in References 11.114 and 11.115 to provide insight into the analysis.

Since structural/mechanical components for light-water reactor power plants are constructed of concrete and steel, penetration calculations were conducted to understand how a missile will be contained within its specific housing/room. All penetration formulas for concrete and steel are based on normal impact. When a missile strikes a target at an angle, the penetration depth is naturally reduced. Gross failure is assumed for all SSCs within a room containing a missile source.

11.6.5.2 Assessment of Internal Missiles

Type I Failure Analysis

Analysis is not required in rooms containing Safety Class 1 equipment or Safety Class 2/3 equipment with no potential missile sources.

Type II Failure Analysis

Valve Missiles

In the case of a valve missile, such as a valve stem that is acted upon by a constant force stream of fluid for a certain distance, a modified version of the Bernoulli's Equation can be used to establish a relationship between potential energy and kinetic energy as shown in the below equations :

$$\text{Kinetic Energy} = \text{Potential Energy}$$

$$\frac{1}{2}mv^2 = pAL$$

$$v = \sqrt{\left(\frac{2pAL}{m}\right)}$$

Where v is the initial velocity exerted onto a valve stem (ft/sec), p is the pressure of the fluid (psi), A is the cross-sectional area of the valve stem (in^2)[12], L is the length of the valve stem (ft)[13] and m is the mass of the missile, i.e., valve stem (lb-sec^2/ft, or lbm)[14].

For all valves analysed, failure is deterministically assumed. Utilising the valve stem's initial velocity, and the modified NDRC equations (Reference 11.110), the integrity of all boundaries for a particular room must retain the missile; i.e., the full missile penetration depth is less than the thickness of a given wall. Correspondingly, since the direction of a missile is unknown, gross failure of all SSCs within the originating room containing missile sources is assumed.

The summary table in (Reference 11.111) identifies the minimum boundary thicknesses and the bounding penetration for the components for a given room. From this reference, it can be seen that the integrity of each boundary wall is satisfied in protecting against the propagation of an internal missile generated by a valve failure.

Pressure Vessel Missiles

The rupture of a pressure vessel operating at high pressure can lead to large high velocity missiles as either random fragments of unknown mass and cross-sectional area or entire parts of the vessel. In the case of a cylindrical vessel, these missiles may include such large components as the top head, the bottom head, or longitudinal segments from the side wall(s). Accurate calculation of possible random fragment velocities and masses are necessarily difficult to determine. Therefore, the conservative approach is taken as based on the assumption that all stored energy within the vessel is converted into kinetic energy and applied to the largest missile mass possible, i.e., the entire tank. The change of internal energy into kinetic energy is captured by assuming an isentropic expansion of the fluid from its operating pressure to standard atmosphere, represented by total change in enthalpy. By assuming an isentropic process, no energy will be lost by heat transfer, ensuring a conservative calculation. Kinetic energy equations may then be used to evaluate a tank's initial velocity;

$$\delta H = (Volume\ of\ Tank)(\delta p)$$

$$\delta H = KE = \frac{1}{2}mv^2$$

$$v = \sqrt{\left(\frac{2KE}{m}\right)}$$

Where v is the initial velocity exerted onto a tank (ft/sec), p is the pressure of the fluid (psi), KE represented the kinetic energy (ft-lbs, ft-kips), H is the enthalpy (ft-lbs, ft-kips) and m is the mass of the missile, i.e., tank (lb-sec^2/ft, or or lbm)[15]

12. A conservative assumption of 1.5 times the connecting pipe nominal pipe diameter is used as the cross-section area of the valve stem in this calculation.
13. The internal length of all valve stems is assumed as 1.0 ft. The internal length of the valve stem is used to calculate the total work done during ejection of the valve stem missile.
14. A conservative assumption of using the entire mass of the valve is used as the mass of the missile in this calculation.

For all tanks analysed, a deterministic failure is assumed. Utilising the tank missile initial velocity and the modified NDRC equations (Reference 11.110), the integrity of all boundaries for a particular room must be maintained; i.e., the full penetration depth is less than the thickness of a given wall. Gross failure of all SSCs within rooms containing missile sources is assumed.

Reference 11.111 identifies the minimum barrier thicknesses and the bounding penetration from the pressure vessel missile components in a given room. It is demonstrated that the integrity of each barrier is satisfactory to protect against an internal missile generated by a pressure vessel failure.

Rotating Equipment Missiles

In analysing missiles from rotating machinery, varying assumptions are required in determining the missile characteristics; i.e., the impeller/flywheel/etc. Within the internal missile safety case, the size and mass of the postulated rotating equipment projectile have been conservatively assumed to overpredict both the size and mass. Characteristics of impact, such as shape factors and the percent of mass converted into a missile, have been established with probability density functions and the frequency of occurrences.

To eliminate possible ambiguity, and ensure further conservative results, the potential rotating equipment missile assumes that the full rotor/impeller will construct the postulated missile. The influence of the rotating component housing was not considered, which removes any calculations of steel perforations. The velocity of the missile from rotating equipment can be calculated using;

$$v_{missile\ source} = \left(\frac{\pi}{720}\right)(d)(overspeed\ factor)(\omega)$$

Where $v_{missile\ source}$ is the velocity of the origination point (i.e., max velocity of a rotating impeller), d is the diameter of the missile source, over speed factor defines a factor for all throttling elements (equivalent to 1.2 for the AP1000) and ω is the rotation speed of the missile source.

It is understood these assumption do not adequately depict a realistic outcome, but rather demonstrate the strength of each boundary and purpose of separating dual system paths by means of civil/structural barriers. With the rotating equipment missile velocity known, and utilising the modified NDRC equations defined in Section 6.2.4.1 of Reference 11.110, the integrity of all barriers for a particular room must be satisfactory, i.e., the full penetration depth is less than the thickness of a given wall.

Each summary table in Reference 11.111 identifies the minimum boundary thicknesses and the bounding penetration from the components in a given room. This reference demonstrates that the integrity of each barrier is satisfactory to protect against an internal missile generated by rotating equipment failures.

15. A conservative assumption of using the entire mass of the tanks (dry weight) is used as the mass of the missile in this calculation

Separation of Class 1 Equipment with Redundancy

In cases where a postulated missile eliminates the use of a Class 1 component, AP1000 plant design ensures multiple means of delivering the Category A safety function(s). Therefore, all Type II analysis results provide evidence of redundant paths that adequately separate Class 1 components in the case of single active component failure.

11.6.5.3 Hazard Schedule

The principal purpose of the hazard schedule is to identify the safety-related systems called upon for each internal missile initiating event and the overall protection claims being made for those systems.

The general structure of the hazard schedule presented within this section is as follows.

- Column 1 of the schedule designates all rooms in which the potential for missile generation is postulated to exist.
- Column 2 of the schedule lists the systems contained within each designated room that present a missile generation hazard (i.e., the sources of missiles).
- Columns 3 and 4 of the schedule list and describe the essential safe-shutdown (SSCs) contained within each designated room (i.e., the safety systems that could be impacted by a missile).
- Columns 5 and 6 of the schedule identify the 'at risk' safety functions (including UK categorisation and SSC classification) provided by the essential safe-shutdown systems contained within each designated room and the associated unmitigated consequences of failure to deliver the safety functions.
- Column 7 of the schedule identifies the main passive safety features that provide protection for essential safe-shutdown systems against internal missiles.
- Column 8 of the schedule lists the rooms or divisions that provide redundant SSCs or an explanation of how the Category A safety function is maintained (i.e., by segregation and separation or other safety features of the AP1000 design).
- Column 9 of the schedule lists additional defence-in-depth safe-shutdown SSCs provided to support maintenance of Class 1 essential safe-shutdown safety functions.
- Column 10 provides any extra information deemed relevant to the assessment.

The hazard schedule is presented Table 11.6-1.

11.6.5.4 Discussion of Results

The method of analysing internal missile hazards is detailed in Reference 11.113. Based on the calculations as presented in References 11.111 and 11.112, a detailed analysis of the protection for internal missiles within the NI has been performed. Concrete penetration depths generated by internal missiles from valves, tanks and rotating equipment are provided in these references.

The calculated penetration depths have been used to validate that the barriers within the NI are resistant to failures from a missile strike. Protection from damage to Class 1 SSCs supporting plant safe shutdown in adjacent rooms is adequately provided whilst the barrier integrity is maintained.

The analysis further demonstrates that Class 1 SSCs which are potentially affected during an internal missile scenario have sufficient redundancy elsewhere outside the missile impact range to ensure the delivery of the Category A or supporting post 72-hour Category B safety functions, required for safe shutdown.

The following sections present a summary of the analysis.

Containment/Shield Building

The AP1000 Shield Building, part of the AP1000 NI, is a steel-concrete-steel composite construction and constitutes a Class 1 3 hour fire barrier which separates it from the AB. Within the Shield Building is the steel Shield Building which is the containment for AP1000 and this fabrication is used in structural modules inside the Containment. The structure and the construction of both of these are discussed in detail in Chapter 16.

The Containment/Shield Building comprises a series of areas separated from one another using a combination of distance and physical structures. Many of the rooms (e.g., each of the SG rooms) are modular steel-concrete composite constructions which form significant physical barriers from other rooms for much of their height. However, complete segregation cannot be achieved inside Containment given the need to maintain the free exchange of gases for purposes such as passive Containment cooling.

In the internal missile hazard analysis it is assumed that a missile within a room affects all equipment within it (including the Class 1 SSCs) and the impact on AP1000 to deliver the Category A safety functions is assessed. Given the separation, and the redundancy provided outside the missile impact reach, the Category A and supporting post 72-hour Category B safety functions can be safely delivered following an internal missile event.

Auxiliary Building – Non-radiologically Controlled Areas

The non-radiological area of the Auxiliary Building comprises the portion of the NI to the north of the Shield Building. The building houses SSCs associated with the auxiliary functions that do not directly involve radioactive material but have been designed to meet their nuclear safety functions.

For segregation purposes, this building is segregated into a series of areas, each of which is enclosed by barriers. The barriers are designed to prevent a missile from penetrating from the room of origin into another area. Therefore potential safety equipment located in a neighbouring room is protected from the internal missile.

In the internal missile hazard analysis it is assumed that a missile generated within a given room potentially affects all equipment within it (including the Class 1 SSCs). Given the physical segregation, and the redundancy provided, the Category A and supporting post 72-hour Category B safety functions will be delivered following an internal missile event.

Auxiliary Building – Radiologically Controlled Areas

The radiologically controlled portions of the Auxiliary Building, located to the south side of the Shield Building, is designed to handle and store nuclear fuel outside of Containment as

well as holding the intermediate level radioactive waste, in the form of filters and spent ion exchange resin, and containing elements of the Liquid and Gaseous Radwaste Systems.

In the detailed internal missile hazard analysis it is assumed that a missile generated within a given boundary potentially affects all equipment within it (including the Class 1 SSCs) and, correspondingly, impacts the AP1000 to deliver the Category A safety functions. Based on the Internal Missile evaluations discussed previously, and the physical segregation and the redundancy provided, the Category A and supporting post 72-hour Category B safety functions will be delivered following an internal missile event. Therefore an internal missile initiating in an individual room within the radiologically controlled area of the Auxiliary Building will not prevent safe shutdown of the reactor.

Turbine Building

Within the equipment included within the AP1000 design, missiles originating from a turbine generator disintegration represent a significantly hazardous items due to the size and considerable energy or a potential missile.

The generation of an internal missile as a result of failure of a turbine rotor ('rotor burst') has the potential to impart significant kinetic energy into the turbine casing and, in the event of casing perforation, the missile has the potential to impact SSCs beyond the boundaries of the turbine. Failures of the rotor occur as a result of structural defects (stress corrosion being the dominant mechanism) or from excessive stresses created during over-speed operation.

The missiles from a turbine failure are divided into two groups:

- 'High trajectory' missiles – These are ejected in a predominantly upward direction and may cause damage if the descending missile strikes an SSC;

- 'Low trajectory' missiles (or 'direct' missiles) – These are ejected in a predominantly lateral direction directly towards SSCs.

High trajectory missiles would be directed up through the roof of the Turbine Building and then fall to earth under gravity. These missiles would not have sufficient energy to penetrate the Shield Building and are not considered credible missiles for the other on site buildings that house SSCs that deliver Category A or supporting post 72-hour Category B safety functions. The probability of an impact in the safety-related areas is the product of the probability of missile generation from the turbine, the probability that a high trajectory missile would land within a few hundred feet from the turbine (10^{-7} per square foot); and the area of the safety-related area. In the AP1000, the safety-related area is contained within the exposed roof area of the Containment Shield Building and the Auxiliary Building. Given this, the potential for a high-trajectory missile impacting safety-related areas of the AP1000 is much less than 10^{-7}. Based on this very low probability, the potential damage from a high-trajectory missile is not evaluated.

The turbine casing is designed to provide a level of missile containment capability in the unlikely event of rotor burst and subsequent missile generation. However, as a bounding case, the impact energy of a quarter-disk fragment from the last stage disk of the low pressure turbine has been evaluated using the Hagg and Sankey method (Reference 11.115) and are shown to be capable of turbine casing perforation.

Reference 11.115 evaluated the maximum velocity of a quarter-disk fragment at a 50 Hz turbine normal operating speed, design over-speed, and destructive over-speed, whilst noting that ductile burst of the rotor does not occur until 185% of normal speed

(Reference 11.113). At normal operating speed, a quarter-disk fragment is predicted to penetrate the turbine primary casing. For both the design and destructive over-speed conditions, the disk fragment will have sufficient energy to breach the turbine's protective outer casing. As stated previously, the casing would offer a significant degree of mitigation (i.e., absorption of kinetic energy) if impacted by a missile that possessed the minimum initial energy required to perforate the protective outer casing of the turbine. The AP1000 Internal Missile safety case does not credit this energy mitigation feature. In conjunction with structural calculations of wall 11.2, the turbine casing is determined to be a defence-in-depth feature.

The deterministic defence-in-depth provisions included within the design of the AP1000 to ensure essential safe-shutdown safety functions are maintained in the event of internal missile generation as a result of turbine rotor failure. These are:

- Adherence to applicable design codes, standards and criteria

  Turbine rotor integrity is ensured by appropriate material selection, design (including fracture toughness, over-speed protection and safety margin specification), manufacture, through-life testing and inspection, including quality assurance application at all stages. Via the combination of these measures, the probability of rotor burst is reduced to a level that is outside the design basis of the plant (i.e., to a frequency of occurrence that does not exceed 1E-5 per year).

  In accordance with the hierarchy of control for nuclear hazards, adherence to design codes, standards and criteria provides the first line of defence (prevention) against internal missile generation.

- Turbine orientation

  In accordance with relevant good practice as recommended in Reference 11.119, the turbine is oriented so that the axis of its shaft rotation is perpendicular to the NI. This orientation ensures that high-energy low-trajectory missiles generated on rotor disintegration are ejected within a limited range of angles essentially perpendicular to the axis of the turbine. As a result, turbine missile 'strike zones' are formed to either side of the turbine (by lines inclined at 25°, 45^0 and 90^0 to the turbine wheel planes and passing through the end wheels of the low-pressure stages), thereby defining areas from within which Class 1 essential safe-shutdown SSCs are excluded. The probability that a missile is directed away from the perpendicular decreases as the angle to the turbine axis decreases. In addition, for the AP1000 design, a significant safety margin (clearance angle) exists between the 25° turbine missile strike zone boundary and the bounding trajectory angles of the NI, as shown in Figure 11.6-1.

- Missile impact withstand capability of NI civil structures

  The Class 1 essential safe-shutdown SSCs incorporated within the AP1000 design are only located within the Containment /Shield Building and Auxiliary Building which, together, form the NI. These buildings are designed to protect the SSCs within them from seismic events and other external hazards, including tornado-induced missiles.

  In accordance with the hierarchy of control for nuclear hazards, the missile impact withstand capability of NI civil structures provide a third line of passive engineered safety protection against internal missile generation.

11.6.6 Sensitivity and Cliff Edge Effects

To combine insights from probabilistic safety analyses combined with deterministic methods, margins of safety were developed to avoid cliff edge effects. The results of sensitivity studies were analysed to assess appropriate safety margins throughout the planning phase of the both the concrete missile penetration calculation (Reference 11.114) and the turbine missile assessment (Reference 11.115).

As an example, in the concrete missile penetration calculation, missile diameters and weight were varied and used as inputs to the modified NDRC equation to determine the most conservative penetration depths. In the valve missile case, it was determined that the most realistic worst case valve missile to be examined was one with a weight of the full valve and a diameter of 1.5 times the connecting pipe size. In reality, a smaller diameter missile would penetrate concrete deeper, but it is not realistic to examine a smaller missile diameter with a weight of a full valve. The weight of the missile were maximised and the inputs into the modified NDRC formula provided results that were conservative and in line with what would be expected for worst case missiles. Similar sensitivity studies were performed for pressure vessel and rotating equipment missiles.

Margins of safety vary depending on the room analysed. For example, the passive barrier (walls) margin of safety to wall penetration for room 12306 is approximately 60 for valve missiles, approximately 50 for pressure vessel missiles, and approximately 4 for rotating equipment missiles. Refer to Reference 11.110 for more information.

In addition, for the turbine missile assessment, turbine missile weights were maximised to provide worst case results. A turbine missile mass of ~ 2800 kg consisting of a partial disc fragment was used rather than the largest turbine blade mass which has a weight of ~ 100 kg. The chosen weight creates a higher energy and thus, leads to a much deeper concrete penetration depth. Although the range of high-energy, low-trajectory turbine missile is limited due to the perpendicular orientation of the turbine axis to the Nuclear Island (Reference 11.114), various trajectory angles were studied for concrete penetration depth. Turbine missiles were considered to eject at 0, 45 and 90 degrees from the plane of rotation. Additional sensitivity analysis was conducted on the turbine with consideration of the missile generating both with and without the outer casing as to study the effects of the casing providing a passive barrier to slow down the missile.

For more information on the deterministic results using the highly conservative speed cases studied, refer to Reference 11.115.

11.6.7 Combined Hazards Discussion

The internal missile hazard analyses, summarized in Reference 11.110, deterministically evaluate a missile generated in each of the rooms having a potential internal missile source. The analysis also considers the potential penetration depth of a missile through structural barriers.

Consideration of credible combinations of internal missile with other postulated initiating events likely to occur independently of a missile is discussed in Section 11.12.

Combinations of independent internal and external hazards (e.g., internal explosion and extreme low temperatures) are considered to be outside of the design basis and have not been explicitly considered in this report. However, compliance with relevant equipment and structural design codes ensure that combinations of internal hazards with the relevant abnormal operating occurrences (including environmental hazards) are addressed.

Discussion of combined and consequential hazards is presented within the Combination of Hazards section (see Section 11.12).ALARP Assessment and Discussion

Deterministic analysis of postulated, design basis, internal missile events shows that all Class 1 SSCs will continue to provide their Category A safety functions following the worst case postulated internal missile scenario, even in the presence of an unrelated single failure elsewhere in the plant design. In the unlikely event that the Class 1 SSCs fail for some unrelated reason, the Category A and supporting post 72-hour Category B safety functions would be maintained by other, additional and redundant, Class 2 SSCs. The internal missile safety design for AP1000 has been achieved by:

- Removing potential missile sources by design where practicable with:
  - Relevant good practice using codes and standards
  - Pressurised part protection
  - Structural Integrity
- Ensuring that redundant SSCs are protected from a missile by utilising appropriate combinations of physical separation and passive barriers;
- Protect delivery of safety functions by favourable orientation of components, such as the main turbine, to direct any missile away from Safety Class 1 SSCs;
- Providing sufficient redundancy in the design such that if one train of protection fails as a result of an internal missile, coincidental with an unrelated single fault elsewhere, the safety functions continue to be provided by the equipment that remains unaffected;

This layered approach to safety is seen to reduce the threat from internal missiles to ALARP. The AP1000 design employs a mixture of the approaches stated above to form levels of defence in reducing the likelihood of an internal missile and also reduces the consequences of an internally generated missile to ALARP.

In support of the safety case presented for internal missiles, the room-by-room assessment within the Nuclear Island identifies the potential origination source and the impact on the AP1000 safety design. A summary of engineering design provisions are substantiated in Reference 11.110, including design modifications that improve the safety of the design as addressing changes to the Normal Residual Heat Removal System (RNS), Spent Fuel Pool Cooling System (SFS), and Component Cooling Water System (CCS) and Service Water System (SWS).

Since the Category A and supporting post 72-hour Category B safety functions is assured, even when considering the detrimental impact of internal missiles, the safety of the plant is ensured. It is judged that only minimal safety benefit may result from the introduction of further design measures to reduce the risks further.

11.7 Release of Toxic, Corrosive, or Flammable Material

11.7.1 Introduction

This section addresses the hazards originating from toxic, corrosive, or flammable materials that may be required to be stored onsite.

Hazardous non-nuclear materials could potentially threaten nuclear safety in the following ways should the hazard be accidentally released:

- By causing a fire (see Section 11.4 on internal fire)
- By causing an explosion (see Section 11.5 on internal explosions)
- By asphyxiating or poisoning personnel when those personnel are required to respond to a challenge to nuclear safety
- By chemical or corrosive attack on SSCs
- By causing brittle fracture of structural SSCs
- By causing a criticality excursion, should the material be a moderator and it spills onto nuclear material

Table 11.7-1 lists the principal hazardous materials present on an AP1000 plant site and where they are stored. The selection of chemicals and volumes may change based on site-specific requirements and operating experience; therefore, storage and use of chemicals not identified in this chapter or present in significantly greater concentrations or volumes will need to be justified on a site-by-site basis. Other intrinsically hazardous material is present onsite but in such small quantities that it poses a minimal threat.

11.7.2 Toxic, Corrosive, or Flammable Material Claims, Arguments and Evidence

11.7.2.1 Claims Overview

Those SSCs which deliver a Category A safety function are the principal means of ensuring nuclear safety in response to Design Basis Accident (DBA) plant faults (see Chapter 8).

Whether the internal hazard initiates a plant state fault or not, by ensuring that the ability to deliver Category A safety functions is maintained following an internal hazard, the internal hazards safety case aligns with the fault studies in demonstrating that the plant risk is broadly acceptable.

This section presents the claims, arguments and underlying evidence made in relation to toxic, corrosive or flammable material[16] hazards with the potential to impact safe shutdown.

11.7.2.2 High Level Claim

The following high level claim is made in relation to the internal hazard(s) presented by toxic, corrosive, or flammable material:

Claim IH-6.0: **Postulated internal hazards within the design basis presented by toxic, corrosive, or flammable material will not prevent the delivery of the Category A safety functions and supporting post 72 hour Category B safety functions necessary to respond to a postulated initiating event.**

16. The effects of flammable materials are bounded by the assessment of internal fires. For further details regarding the assessment of internal fires, refer to Section 11.2.

The SSCs claimed to provide post-72 hour support functions include only offsite procured SSCs and their associated Class 1 connections.

11.7.2.3 Prevention Claims

Hazardous materials are present in SSCs which, under normal conditions, provide adequate containment such that an unintended release is precluded. This is to say that the container itself will not degrade due to the presence of the hazardous material alone.

However, the deterministic assessment of hazardous materials cannot preclude their release. Given the variability in the design and integrity of hazardous material containers, no specific claim is made on the prevention of the hazard.

11.7.2.4 Protection Claims

It is recognised that, if released, hazardous materials may impair the ability of operators to correctly undertake safety related activities, such as respond to an alarm. All operations required to shut down the reactor plant can be performed from the MCR. Provided the release of hazardous materials does not infiltrate the MCR, operators will be able to undertake safety related activities. The following protection claim is made in regard to the MCR.

Claim IH-6.1: The MCR will remain habitable in the event of a release of hazardous materials

All Class 1 SSCs, delivering Category A safety functions, are located within the NI. A release of hazardous material outside of the NI will therefore not affect Class 1 SSC provided that the hazardous material does not infiltrate the NI. The following protection claim is made:

Claim IH-6.2: Class 1 SSC located within the NI will not be affected by releases of hazardous materials in locations outside of the NI

11.7.2.5 Mitigation Claims

Within the NI, the release of a corrosive chemical could result in damage or loss of a Class 1 SSC. However, provided that a single division remains unaffected, the Category A safety function can continue to be delivered.

Claim IH-6.3: A release of hazardous materials will not cause the loss of all divisions of Class 1 SSC delivering a Category A safety function

11.7.2.6 Arguments and Evidence

Claim IH-6.1: The MCR will remain habitable in the event of a release of hazardous materials

Habitability studies for the MCR (see Chapter 23) have demonstrated that for hydrogen, nitrogen, and carbon dioxide, the maximum concentrations predicted to exist at the control room inlet within 2 minutes of a plume reaching the control room inlet are significantly less than the toxicity levels for those gases. The calculations carried out assumed quantities of the above gases in excess of the maximum credible inventory held at the PGS, storage at a distance of approximately 250 m (820 ft) from the MCR, and worst-case weather conditions. The levels of toxicity reached are approximately 33 percent for liquid hydrogen release, 40 percent for liquid nitrogen release, and less than 20 percent for carbon dioxide release. Even if toxicity limits could be reached, the response time of 2 minutes provides adequate

time for control room personnel to use protective breathing equipment; therefore, this does not represent a significant toxic or asphyxiation hazard to the control room personnel in the event of an accidental catastrophic failure of a storage tank.

For these calculations, the weather conditions assumed the highest ground and ambient air temperatures (corresponding to 42.2°C), with wind direction directly in line with the control room inlet and unchanging, and maximum cloud cover to maximise evaporation rate.

However, conditions such as weather patterns and local topography may vary from the assumptions made in the MCR habitability assessment (see Chapter 23), depending on where in the UK the station is built and where the PGS is located in relation to the MCR air inlet and to other buildings. Therefore, a site-specific safety case justification for the quantities and storage location for hydrogen, nitrogen, and carbon dioxide should be made at each site where a reactor will be constructed.

Claim IH-6.2: Class 1 SSC located within the NI will not be affected by releases of hazardous materials in locations outside of the NI

The site is graded such that the natural flow of liquid releases is away from the NI. Furthermore, the exterior walls of the NI represent significant reinforced concrete or metal structures. While degradation, due to chemical attack, of the NI exterior walls cannot be precluded, the extent would be minor based on the quantity of chemicals involved and the robustness of the walls.

Catastrophic failure of the gas storage tanks resulting in the loss of cryogenic liquids cannot threaten the NI. The PGS is approximately 250 m away from the NI; evaporation would therefore take place before significant quantities could reach the building. Note that this is dependent on the topography and the prevalent local weather conditions at the site, and therefore will need to be justified on a site-by-site basis if plant layout differs significantly.

Claim IH-6.3: A release of hazardous materials will not cause the loss of all divisions of Class 1 SSC delivering a Category A safety function

The layout of the plant and its Class 1 SSCs have been designed so that the complete loss of the equipment within any single room will not result in loss of the Category A safety functions.

The behaviour, in terms of movement, of hazardous liquids would be similar to that of any other liquid. The assessment of Internal Flooding (see Section 11.3) is therefore bounding in terms of the spread of hazardous liquids and their effects.

11.7.3 Toxic, Corrosive, or Flammable Material Safety Case Summary

11.7.3.1 Introduction and Overview

The safety design approach adopted for hazardous materials is based on:

- Minimising the quantities of hazardous materials stored on site;
- Storing hazardous materials at distances remote from the NI and therefore Class 1 SSCs delivering Category A safety functions;
- Maintaining a ‘habitable’ environment for operators in the MCR following the release of toxic gases on-site;

- Separation and segregation of redundant divisions of Class 1 SSCs.

The approaches stated above form levels of defence-in-depth which, together, reduce the risk associated with releases of hazardous materials to a level which is ALARP.

11.7.3.2 Applicable Codes and Standards

The tanks, vessels and pipework associated with the hazardous materials have been designed in accordance with the relevant sections of the ASME Boiler and Pressure Vessel Code (Reference 11.90). The codes and standards have been compared to equivalent UK codes and standards (Reference 11.25) to determine their suitability based on the safety significance of the SSC (Reference 11.26).

With regards to the assessment of the hazard presented by toxic, corrosive and flammable materials, no claim is made on the integrity of tanks, vessels or pipework to prevent their release under fault conditions.

The hazard presented by significant quantities of hazardous materials will be controlled in accordance with the COMAH regulations (Reference 11.117), while the onsite use of chemicals and the potential harm to operators will be managed through appropriate COSHH assessment.

11.7.3.3 Redundancy, Separation, and Segregation

The design of the AP1000 plant incorporates redundant divisions of Class 1 SSC, each of which is capable of delivering the Category A safety function. Where there is the potential for Class 1 SSCs to be compromised by a hazardous material, the redundant Class 1 SSC delivering the Category A safety function is unaffected. The provision of redundancy takes into account the following:

- IAEA-NS-G-1.11 “Protection against Internal Hazards other than Fires and Explosions in the Design of Nuclear Power Plants” (Reference 11.82).
- IAEA NS-R-1, “Safety of Nuclear Power Plants: Design” (Reference 11.21).
- APP-GW-J1R-008, “Safety Criteria for the AP1000 Instrumentation and Control Systems” (Reference 11.51).
- APP-GW-J1R-004, “AP1000 Instrumentation and Control Defence in Depth and Diversity Report” (Reference 11.52).
- ONR Nuclear Safety Technical Assessment Guide NS-TAST-GD-011, “The Single Failure Criterion” (Reference 11.83).

Within the Containment/Shield Building, redundant divisions of Class 1 SSC have been separated, so far as is reasonably practicable, by distance. While the Containment/Shield Building is a largely open space to maintain the free movement of gases, some compartments have been segregated by walls and floors providing some physical segregation.

Outside the Containment/Shield Building, the Auxiliary Building comprises both a RCA and non-RCA, which are physically segregated from one another by walls, floors and ceilings. Adjoining buildings are also physically segregated from the Auxiliary Building by walls, floors and ceilings. Access to either the RCA or non-RCA portions of the Auxiliary Building

is from the adjoining buildings, which are themselves sub-divided into RCA and non-RCA sections by walls, floors and ceilings.

The Containment structure provides a barrier to the intrusion of hazardous materials into the area where the main components of the Class 1 SSCs are sited. Outside the Containment structure, the plant and its Class 1 SSCs have been designed so that the complete loss of the equipment within any single room will not result in loss of the Category A safety functions. The fire barriers protecting redundant trains of the Class 1 SSCs from fire should also provide an adequate barrier to the spread of corrosive liquids, and therefore limit any damage to the equipment in one room.

Taking account of the potential loss of those SSCs affected by the toxic, corrosive, or flammable material concurrent with a credible, unrelated, single failure within the other SSCs, it is concluded that sufficient redundancy, diversity, and segregation is provided in the design and location of the SSCs to ensure that the Category A safety functions are maintained in the worst-case, normally permitted, plant lineup.

11.7.3.4 Toxic, Corrosive, or Flammable Material Assessment Approach

With the exception of releases of toxic materials, for which a habitability study of the MCR has been performed (see Chapter 23), the assessment of releases of hazardous materials has been qualitative. The potential for Class 1 SSCs to be exposed to hazardous materials along with the associated effects have been considered in determining whether or not all divisions of Class 1 SSC delivering a Category A safety function could be lost following a release.

11.7.3.5 Interface with Other Internal Hazards

The release of hazardous materials may be initiated by or the initiator for other internal hazards. For example, corrosive materials may induce pipework failure leading to an Internal Flood. Similarly, a missile may cause a rupture of a vessel containing hazardous materials. These combined hazardous effects are considered in Section 11.12.

Pressure Part Failure (see Section 11.4) and a release of hazardous material may arise simultaneously; the combined effects are also considered in Section 11.12.

Internal Fire (see Section 11.2) may ensue following the release of a flammable material. The analysis of Internal Fires bounds that of flammable materials on the basis that Internal Fires considers all sources of flammable material whether that material is normally contained or not.

11.7.3.6 Conclusions

With the exception of the habitability study of the MCR (see Chapter 23), the hazards presented by toxic, corrosive, or flammable materials have been qualitatively assessed. This assessment has shown that the risk to Class 1 SSCs delivering Category A safety functions, or to personnel required to undertake nuclear safety related actions is low. The reasons for this are:

- Hazardous materials are stored, and used, at concentrations which would have little bearing on the structural or mechanical properties of the SSC they may come in contact with.

- The bulk storage of hazardous materials is outside of the NI, at a distance at which any release would have limited capacity to directly affect either the exterior walls of the NI, or the Class 1 SSC located within.

- Under worst case weather conditions, a release of toxic material would not expose operators present in the MCR to concentrations above which toxic effects would prevail.

- The release of a hazardous material within the NI would either have no direct effect on Class 1 SSC (i.e., the SSC is insensitive to the make-up of the surrounding atmosphere) or would not affect all divisions of Class 1 SSCs delivering a Category A safety function.

11.7.4 Toxic, Corrosive, or Flammable Material Safety Analysis

11.7.4.1 Identification of Hazard Sources

Table 11.7-1 lists the principal hazardous materials present on an AP1000 plant site and where they are stored. The precise selection of chemicals and volumes may change based on site-specific requirements and operating experience; therefore, storage and use of chemicals not identified in this chapter or present in significantly greater concentrations or volumes will need to be justified on a site-by-site basis. Other intrinsically hazardous material is present onsite but in such small quantities that it poses a minimal threat.

11.7.4.2 Assessment of Toxic, Corrosive, or Flammable Materials

Bulk Gas Storage and the Plant Gas System – Hydrogen

The most significant threat from hydrogen is principally that of fire or explosion, should it leak and mix with air or oxygen; additionally, the pipework might explode by virtue of the high gas pressure. These issues are addressed in Section 11.2 on internal fires, Section 11.5 on internal explosions and Section 11.6 on internal missiles. However, hydrogen could potentially also asphyxiate personnel if its presence should exclude the normal air in a room or compartment containing personnel; however, this is unlikely given that the leakage amount and leak rate is limited, and any leaking hydrogen would very likely disperse by floating up and away before any significant mixing took place. Leakage of hydrogen, absent a resultant explosive or fire scenario, has limited potential to disable equipment involved in providing a nuclear safety function, or to prevent an action required for nuclear safety.

The possibility of leaking bulk hydrogen gas being drawn from outside into an HVAC intake for the MRC has been analysed (see Chapter 23), and the analysis shows that, providing the assumptions and criteria are met, the maximum concentration under worst case conditions after two minutes is 22600 ppm (cf. toxic limit of 70000 ppm) and therefore it does not represent a toxic hazard to control room personnel. Also the maximum concentration would not exceed the LFL for hydrogen posing no fire/explosion potential in the MCR. Therefore it is concluded that hydrogen presented as this scenario does not represent a significant toxic hazard or fire/explosion hazard.

Bulk Gas Storage and the Plant Gas System – Carbon Dioxide

The major threat from carbon dioxide is that of asphyxiation of personnel, should its concentration in the air rise above a few percent. There is also the hypothetical possibility of a cloud of carbon dioxide choking operation of various onsite diesel engines; however these SSCs are not Class 1 and their loss is not of immediate nuclear safety significance

Should the storage tank rupture catastrophically, the depressurising carbon dioxide would instantly solidify, thereby reducing the rate of evaporation and lessening the threat. As a result, there is minimal threat to any SSCs should the tank and/or its associated evaporator leak.

Once the carbon dioxide enters the turbine hall, any leak would be minimal in comparison with the volume of the building, given that the supply is through a small-bore pipe. The Turbine Building is also provided with carbon dioxide detection and alarms.

The possibility of leaking carbon dioxide gas being drawn into an HVAC intake (e.g., MCR) is summarised in Chapter 23 and the analysis shows that, subject to the assumptions made, the maximum concentration under worst-case conditions after 2 minutes is 6960 ppm (compared to the toxic limit of 40,000 ppm); therefore, it does not represent a toxic hazard to control room personnel. Therefore, it is concluded that carbon dioxide does not represent a significant toxic hazard.

Bulk Gas Storage and the Plant Gas System – Nitrogen

The threats from nitrogen are over-pressurisation events within the high-pressure subsystem pipework or a high-pressure portable cylinder and asphyxiation of personnel if any part of the system leaks, or should they inadvertently enter a compartment or tank in which the atmosphere is nitrogen rather than air (personnel breathing nitrogen are unaware that there might be little or no oxygen present, as nitrogen is odourless). There is also the hypothetical possibility of a cloud of nitrogen choking the operation of the various DGs onsite; however, these are not Class 1 SSCs, and delivery of Category A safety functions will not be prevented.

Portable nitrogen cylinders are used during plant outages for refilling the valve actuators of the MSIVs and the main feedwater isolation valves, and for the pressure testing of the Containment penetrations. Leakage of nitrogen from this source in contained environments would be an asphyxiation threat to nearby personnel and would be controlled on a site specific basis. There are no actions required to maintain the significant functions in the compartments containing the MSIVs, the main feedwater isolation valves, or the Containment penetrations because of a nitrogen leak.

Nitrogen is present within the RCDT and the WGS at all times other than when personnel access is required for maintenance during outages. Personnel would not need to enter these systems or be in their vicinity to perform any safety-significant required actions, so asphyxiation from leaking nitrogen would not be an issue for nuclear safety.

Nitrogen is present within the secondary side of the SGs and within the main steam lines during shutdown operations. Personnel would not need to be in the vicinity of the SGs or the main steam lines to perform any actions required to maintain Category A safety functions at these times, so asphyxiation from leaking nitrogen would not be an issue.

The scenario of leaking nitrogen gas being drawn into an HVAC intake is summarised in Chapter 23 and the analysis shows that, providing the assumptions and criteria are met, the maximum concentration under worst case conditions after two minutes is 27,700 ppm (compared to the toxic limit of 70,000 ppm). Therefore, this does not represent a toxic hazard to control room personnel. Consequently, it is concluded that nitrogen does not represent a significant toxic hazard.

Bulk Chemical Storage – Boric Acid

The only threat to nuclear safety from leaking boric acid is its potential to corrode the materials, principally the carbon steel of the RCS pressure boundary, especially if it were to be concentrated by evaporation. Leaking boric acid corrodes carbon steel at a high rate. It is postulated that an undetected, very minor leak of boronated coolant could result in corrosion at the leak site, which might then develop suddenly into a much larger leak, resulting in a LOCA (see Chapter 9); alternatively, corrosion-induced damage to valves in the makeup pipework could potentially result in difficulties injecting boron when required.

The RCS pressure boundary is built to the highest integrity because of the obvious challenge to nuclear safety from any loss of coolant. Reactor coolant pressure boundary components are designed, fabricated, inspected, and tested in conformance with the ASME Code, Section III. The part of the CVS that forms a portion of the RCS pressure boundary, the purification loop, is designed in accordance with ANSI/ANS-51.1-1983 (Reference 11.118). All surfaces of the RCS that come in contact with borated water are clad with austenitic stainless steel, or constructed of high nickel content or other non-corroding alloys.

All parts of the CVS in contact with reactor coolant or boronated makeup are constructed of austenitic stainless steel. The piping joints and connections are welded, except where flanged connections are required for equipment removal for maintenance and hydrostatic testing. The design of the CVS is based on the requirements specified in Nuclear Regulatory Commission technical report NUREG-0800 (Reference 11.119, Section 9.3.4).

Only extended duration leaks of boric acid are relevant to nuclear safety, as this is the only mechanism for the concentration and accumulation of the acid to build up to levels at which it might corrode the carbon steel surfaces of Class 1 or Class 2 SSCs. Even boron deposits from a small leak in the RCS or the CVS purification loop would be detected by the operators through regular periodic inspections of components. Surveillance of the CVS CIVs, the reactor coolant pressure boundary isolation valves, and the boron dilution mitigation valves, would detect any consequential accumulation of boric acid in the CVS room within the Containment. Leaks from equipment that contains borated water outside Containment (e.g., RNS, SFS, and CVS) would be quickly detected by regular visual inspection.

In general, boric acid is not especially hazardous to people, having both a low dermal and oral toxicity (Reference 11.51, Table 5.1), and it is considered highly unlikely that leaking boric acid solution could affect personnel engaged in supporting Category A safety functions.

Therefore, it is concluded that boric acid crystals or solution stored onsite do not represent a significant threat to nuclear safety or a toxic hazard.

Bulk Chemical Storage – Lithium Hydroxide

The only identified threat from leaking Lithium hydroxide is its potential to cause damage, by virtue of its caustic nature, to the RCS pressure boundary and to the makeup system pipework and valves, especially if it were to be concentrated by evaporation.

The potential for chemical attack from leaking reactor coolant is bounded by the boric acid, which is also present in the reactor coolant but at a much higher concentration; the maximum inventory of Lithium hydroxide stored in the CVS makeup pump room within the radiological Auxiliary Building is 5 kg (11 lbs) (Reference 11.120, Table 5.3).

There is a slight possibility of the Lithium hydroxide supplied to the site being contaminated with much higher levels of lithium-6 than specified. This would result in a challenge to the

Category A safety function to avoid the dispersion of radioactive material to the environment because of the consequent production and subsequent discharge of tritium. The site-specific operational quality assurance programme will minimise this possibility.

Therefore, it is concluded that Lithium hydroxide poses no significant threat to nuclear safety and does not represent a significant toxic hazard.

Bulk Chemical Storage – Hydrazine

Hydrazine solution is toxic to people if in contact with skin, inhaled, or ingested, and harmful to the environment if it is released.

Hydrazine is neither corrosive nor flammable (as a 35 percent w/v solution); however, it is toxic and would be a threat to the personnel and to the biological environment should it escape. It is not, however, a threat to nuclear safety because of its infrequent use and because personnel involved in actions required to maintain Category A safety functions have no need to go anywhere near where hydrazine could leak or escape (for example, the CVS makeup pump room within the radiological Auxiliary Building). Hydrazine will require a risk and a COSHH assessment for both storage and use.

Therefore, it is concluded that hydrazine does not represent a significant toxic hazard.

Bulk Chemical Storage – Sodium Hydroxide

This material is severely corrosive and toxic, but not flammable. It is not a threat to nuclear safety because of its storage and usage locations; there are no Class 1 or Class 2 SSCs and no actions required to maintain Category A safety functions are located anywhere close by. No nuclear safety claims need to be made. Caustic soda will require a risk and COSHH assessment for both storage and use.

Therefore, it is concluded that sodium hydroxide does not represent a significant threat to nuclear safety.

Bulk Chemical Storage – Diesel Oil

The most significant hazard from spilled diesel oil is fire; however, the combustion by-products from burning diesel may have an effect on the MCR. From the MCR habitability studies (Chapter 23), the maximum concentration under worst-case conditions after 2 minutes are as follows for these by-products: for CO_2, 2610 ppm (compared to the toxic limit of 40,000 ppm); for CO, 1.16 ppm (compared to the toxic limit of 1200 ppm); and for SO_2, 3.14 ppm (compared to the toxic limit of 100 ppm).

Therefore, toxic fumes from burning diesel do not represent a toxic hazard to control room personnel.

Bulk Chemical Storage – Trisodium Phosphate

Contact with TSP can cause chemical burns to the skin and eyes; therefore appropriate protective clothing and eye protection are used when loading or handling the storage baskets.

Bulk Chemical Storage – Hydrogen Peroxide

Contact with hydrogen peroxide can cause chemical burns to the skin and eyes; therefore appropriate protective clothing and eye protection are used when handling.

Bottled Gases

Certain gases (such as argon, acetylene, and oxygen) may be held in small quantities. These gasses are considered to be held in sufficiently small quantities and used for specific purposes (such as welding) that their use and risks will be assessed on an individual basis with appropriate local risk assessments.

Chemical Inhibitors

The specific chemicals used, other than the biocide, are determined by the local site water conditions. Some of these materials are corrosive and toxic, but none of them are flammable. Chemicals used on the site will require COSHH and risk assessments. They will be stored in relatively small quantities within the turbine hall and do not represent a significant threat to any Class 1 or 2 SSCs; no actions required to maintain Category A safety functions take place in that location.

However, it is postulated that biocides could threaten operator actions supporting Category A safety functions by producing noxious gases that are then drawn into HVAC intakes. In particular, the sodium hypochlorite can give off chlorine gas in some circumstances. An analysis (see Chapter 23) shows that these sources do not represent a toxic hazard to control room personnel. In any case, a supply of protective clothing, respirators, and self-contained breathing apparatuses adequate for 11 persons is stored within the MCR pressure boundary for other purposes.

Therefore, an accidental release of the types of chemical inhibitors used on the site does not represent a significant toxic hazard to control room personnel.

Refrigerant Gases

Typical refrigerant gases may be flammable and toxic, but not corrosive. Chemicals used onsite will require COSHH and risk assessments. They will be stored in relatively small quantities within the turbine hall and do not represent a significant threat to any Class 1 or Class 2 SSCs; no actions required to maintain Category A safety functions take place in that location.

It is postulated that the refrigerant could leak and then be drawn into HVAC intakes. An analysis (see Chapter 23) shows that these sources do not represent a toxic hazard to control room personnel. However, a supply of protective clothing, respirators, and self-contained breathing apparatuses adequate for 11 persons is stored within the MCR pressure boundary for other purposes.

Therefore, an accidental release of the types of refrigerant gases used onsite does not represent a toxic hazard to control room personnel.

11.7.4.3 Hazard Schedule

No hazard schedule is presented for toxic, corrosive, or flammable material hazards on the basis that the hazard has been assessed semi-qualitatively.

11.7.4.4 Discussion of Results

The analysis concludes that there are no toxic, corrosive or flammable material hazards which could result in the loss of all divisions of Class 1 SSC delivering a Category A safety

function. Further, the potential hazard to operators required to undertake actions in support of Category A safety functions is low.

The possible exceptions to this include a release of boric acid from the RCS and sodium hydroxide. However, both of these hazards would act slowly and be identified during routine plant maintenance. Should the hazard not be identified, it could be an initiator for a plant level fault, e.g., LOCA, however such a fault would be bounded by the assessment of faults (see Chapter 9).

11.7.5 Sensitivity and Cliff Edge Effects

The analysis of toxic, corrosive, or flammable material hazards has been undertaken semi-qualitatively.

For releases from the bulk gas storage locations, the hazard is realised by operators present in the MCR. The concentration of toxic chemicals in the MCR is dependent upon the source strength and subsequent dispersion. The analysis has assumed that the plant gas store is located at 250 m from the NI. Should it be located nearer, the concentration at the MCR would increase. However, the dispersion model has assumed worst case weather conditions which would not persist for significant periods of time. However, the actual siting of the PGS is subject to site-specific considerations and an analysis will be undertaken at that time to determine an appropriate safe distance from the MCR in the event that one of the bulk gas storage tanks were to leak.

The analyses of the effects of boric acid assume that the solution initially contains 2.5 wt% boric acid. At higher concentrations, the solution would be more acidic and therefore more effective at corroding the RCS pressure boundary. However, the increased boron concentration would have operational implications on reactor performance and as such is a closely monitored reactor chemistry parameter. It is therefore not considered credible that significantly higher concentrations of boric acid could exist in the RCS without being readily identified.

11.7.6 Combined Hazards Discussion

Releases of toxic, corrosive, or flammable materials has not identified a loss of Class 1 SSCs delivering Category A safety functions, or the incapacitation of operators required to undertake actions in support of Category A safety functions. In the event that the release of hazardous materials initiates or is initiated by another internal hazard, the effects would be transcended by the other internal hazard. The combined effects of hazardous materials with other internal hazards has therefore not been considered further, see Section 11.12 for further discussion.

11.7.7 ALARP Assessment and Discussion

The measures outlined above demonstrate that the risk of loss of a nuclear safety-significant system as a result of loss of corrosive, toxic, or flammable materials is low and has been addressed in the design of the plant (or will be addressed on a site-by-site basis), as well as by normal operational procedures and maintenance activities. The risks posed from corrosive, toxic, or flammable materials are at such a low level that no practical measures to reduce the risk further could be identified.

Specific measures taken to reduce risk include maximising the distances between the PGS, standby diesel fuel oil system, and NI so as to minimise the effects from a catastrophic loss of

a bulk container of liquefied gas, and the routing of pipework away from areas where Class 1 or Class 2 SSCs are present or where personnel are involved in safety-related operations.

11.8 Dropped Loads and Load Mishandling

11.8.1 Introduction

The AP1000 design is such that a dropped load event within the design basis will not compromise the ability of the AP1000 plant to safely shutdown. The Category A safety functions required for safe shutdown following a dropped load and the supporting post 72 hour Category B safety functions are shown to be maintained through a combination of claims including the segregation of SSCs.

Loads dropped by cranes and other types of lifting equipment have the potential for preventing delivery of Category A safety functions either directly through the load impacting an SSC, or indirectly because of the collapse of a floor or wall that causes failure of the SSC. The Class 1 SSC delivering Category A safety functions have been identified through fault studies, see Chapter 9. Additionally, potential damage to SSCs required to perform Category A safety functions may be caused by the mishandling of a load. Both load drops and the mishandling of a load are collectively referred to in this section as dropped loads.

The assessment concludes that Category A safety functions can continue to be delivered following a design basis dropped load through a combination of claims including equipment segregation (i.e., no claim has been made on the prevention or limitation of fault occurrence) (Reference 11.123).

11.8.2 Dropped Loads Claims, Arguments and Evidence

11.8.2.1 Claims Overview

This section presents the claims, arguments and underlying evidence made in relation to internal dropped load hazards with the potential to impact safe shutdown.

11.8.2.2 High Level Claim

Dropped loads could cause a transient from normal operation or shutdown conditions of the reactor power plant with the potential to result in a hazard on or off site being realised. In response to such a transient, it may be necessary to shut down the reactor and return it to a safe state. Depending on the exact nature of the transient, there are a number of courses of action to take to shut the reactor down and/or ensure sufficient cooling is provided. Availability of the Class 1 SSCs required to deliver the Category A safety functions will ensure that the reactor can be safely shutdown and cooled and that sufficient cooling can be maintained to irradiated fuel in the SFP. This is the basis of the following high level claim.

Claim IH-7.0: **Postulated dropped loads within the design basis will not prevent the delivery of the Category A safety functions and supporting post 72 hour Category B safety functions necessary to respond to the postulated event.**

This has been achieved by:

- Protecting delivery of Category A safety functions with passive safety features or structural barriers to prevent propagation of damage due to a dropped load;

- Ensuring that redundant SSCs delivering Category A safety functions are sufficiently separated and segregated so that a dropped load cannot prevent delivery of the safety function

- Mitigating the effects of a dropped load through appropriate qualification of SSCs to withstand the effects of vibration due to dropped load

The SSCs claimed to provide post-72 hour support functions include only offsite procured SSCs and their associated Class 1 connections.

11.8.2.3 Prevention Claims

A dropped load is deterministically assumed to occur as a result of a failure of a lifting device. There are therefore no specific claims made on the prevention of dropped load hazards.

Substantiation of the lifting devices is provided in the Sections 17.7 and 17.8, for light and heavy loads handling systems.

11.8.2.4 Protection Claims

Protective measures have been incorporated into the design to protect the delivery of Category A safety functions from the effects of a dropped load. The following specific protective claims are made in support of the overall high level claim:

Claim IH-7.1.1: **A dropped load on the reactor vessel will not prevent adequate cooling of the core**

Claim IH-7.1.2: **The floors of the SFP will not fail in the event of a dropped load onto the SFP**

Claim IH-7.1.3: **A dropped load from the Cask Handling Crane will not impact the SFP**

11.8.2.5 Mitigation Claims

The following mitigation claims are made in support of the overall high level claim:

Claim IH-7.2.1: **A single dropped load event cannot impact all divisions of SSCs delivering a single Category A safety function**

Claim IH-7.2.2: **Class 1 SSC, not directly impacted by a dropped load, will be capable of delivering their Category A safety function**

Claim IH-7.2.3: **There will be no dropped loads within Containment in Modes 1 to 4.**

11.8.2.6 Arguments and Evidence

Prevention Arguments and Evidence

There are no specific claims made on the prevention of dropped loads. Dropped loads are assumed to occur as a result of failures of lifting equipment. However, the cranes and lifting

devices have been designed to appropriate standards and are justified in Sections 17.7 and 17.8.

Protection Arguments and Evidence

Claim IH-7.1.1: A dropped load on the reactor vessel will not prevent adequate cooling of the core

A dropped load onto the RPV will not significantly distort the RPV, its connections or its internals sufficient to preclude cooling.

The reactor vessel and its associated supports and connections provide containment for the water cooling the fuel and support to the core structures that maintain flowpaths within the core.

A dropped load onto the reactor vessel can only happen in Plant Operation Modes 5 and 6, when Containment is open and the lifting equipment within it is used to support refuelling operations. The bounding load that could be dropped onto the reactor vessel is the IHP. Analysis has been conducted (Reference 11.121) that demonstrates that the reactor pressure vessel and associated supports and connections will withstand the impact from the dropped load.

Claim IH-7.1.2: The floors of the SFP will not fail in the event of a dropped load onto the SFP

The SFP liner can withstand the bounding drop, of a fuel assembly including control rod assembly and a handling tool attached, from the fuel handling machine.

The only lifting devices which operate above the SFP are the FHM and the new fuel elevator. Analysis has been conducted (Reference 11.122) that demonstrates that the SFP liner will not be penetrated by a dropped fuel assembly with a control rod assembly and a handling tool attached, which is identified as the bounding dropped load into the SFP. There is therefore no impact on the flood doors in the rooms below the SFP.

Claim IH-7.1.3: A dropped load from the Cask Handling Crane will not impact the SFP

The cask handling crane bridge beam is prevented from travelling sufficiently far in the westerly direction by end stops fitted to the cask handling crane rails.

The Cask Handling Crane rails incorporate passive end stops that prevent the bridge from running off the end of the rails. The end stops also prevent a fuel cask from overhanging the SFP or its supporting walls (Reference 11.123).

Mitigation Arguments and Evidence

Claim IH-7.2.1: A single dropped load event cannot impact all divisions of SSCs delivering a single Category A safety function

Class 1 SSC are spaced sufficiently far apart that a single dropped load cannot directly impact all divisions.

Analysis has been undertaken for a dropped load from each of the lifting devices within the Nuclear Island, which demonstrates that a single dropped load cannot directly impact all

divisions of Class 1 SSC required to deliver a Category A safety function. The hazard schedule (see Table 11.8-3) identifies the Class 1 SSC which may be directly impacted by a dropped load and the location of redundant Class 1 SSC capable of delivering the Category A safety function.

For a drop of the load with the largest footprint[17], anywhere within Containment, an analysis has been undertaken (Reference 11.123) which demonstrates that all divisions of Class 1 SSC delivering a Category A safety function cannot be directly impacted by a single dropped load.

Claim IH-7.2.2: Class 1 SSC, not directly impacted by a dropped load, will be capable of delivering their Category A safety function

Class 1 SSCs are qualified to deliver their Category A safety function following a design basis seismic event, which includes the effects of vibrations. With the duration of a design basis SSE being conservatively larger than impulse felt due to a dropped load, the effects of a design basis seismic event envelope those vibrations due to a dropped load (Reference 11.60).

Environmental qualification tests and methods (see Chapter 5) are based on the guidelines provided in IEEE 323-1974 (Reference 11.124) and IEEE 344-1987 (Reference 11.79), and include:

- Type testing: Testing of equipment in the environment, normal and abnormal, under which it will be required to perform its function;
- Analysis: Review of relevant data for similar components;
- On-going qualification: Maintenance and surveillance of in service equipment.

Equipment qualification program documentation consists principally of:

- Methodology for Qualifying Safety-Related Electrical and Mechanical Equipment (Reference 11.60): Over-arching document detailing the strategy for equipment qualification.
- Equipment Qualification Data Packages: Details the qualification program objectives, methods performance specification and qualification plan for each SSC subject to qualification.
- Equipment Qualification Test Reports: Details of the specific methods used during qualification and the results of the process.

The criterion for equipment qualification depends upon the environment, during normal and abnormal conditions, under which the SSC is required to operate. The Nuclear Island (including Turbine Building – North Bays) has been broken down into 11 environmental zones and a number of associated sub-zones. The normal and abnormal environmental

17. The load with the largest footprint handled within containment is the IHP. Although a load path has been established for the IHP which restricts movement of the IHP to certain areas within containment, the analysis conservatively assumes the IHP could be dropped anywhere within the coverage of the polar crane.

conditions for equipment qualification in each zone/sub-zone have been established (Reference 11.61).

Claim IH-7.2.3: There will be no dropped loads within Containment in Modes 1 to 4.

Lifting devices within Containment cannot be used or activated in Modes 1 to 4. There is no personnel access to Containment in Modes 1 to 4 except for infrequent inspections. Maintenance activities are not anticipated in the Containment during Modes 1-4. Spurious operation of the cranes is not possible during these modes as there is no access to controls.

11.8.3 Dropped Loads Safety Case Summary

11.8.3.1 Introduction and Overview

The safety design approach adopted for dropped load hazards consists of a range of complementary approaches. These are applied as appropriate to reduce the potential disruption to the passive safe shutdown Class 1 SSC. Dropped load events within the design basis do not prevent the delivery of the Category A safety functions necessary to respond to a postulated event. Preservation of required safety functions ensures alignment with fault studies and structural integrity analysis.

Dropped loads are assumed to occur as a result of Postulated Initiating Events (PIEs) leading to failure of lifting equipment to provide adequate support to loads lifted.

In summary, the safety case approaches adopted are as follows:

- Provision of redundant SSC, capable of delivering the Category A safety function, in segregated locations which cannot be affected by a single dropped load hazard;
- Protection of SSC, whose availability is required to deliver Category A safety functions, from the effects of dropped loads. This protection takes the form of a dropped load withstand capability which is demonstrated for certain key structures and the provision of passive safety features;
- Qualification of SSC to withstand the secondary effects of a dropped load (e.g., vibration).

The AP1000 design employs a mixture of the approaches stated above to form levels of defence-in-depth which, together, reduce the risk associated with dropped loads to a level which is As Low As Reasonably Practicable (ALARP).

11.8.3.2 Applicable Codes and Standards

The cranes and lifting equipment have been designed in accordance with relevant US codes and standards and are detailed within the Fuel Handling System Design Specification (Reference 11.125) and Mechanical Handling System Design Specification (Reference 11.126) as appropriate. With regards to the assessment of dropped loads as an internal hazard, no claim is made on the design of the cranes to prevent a dropped load with the exception of the end stop fitted to the Cask Handling Crane rail.

SSC claimed in support of this assessment are designed in accordance with the relevant US codes and standards. To evaluate the codes and standards against the UK expectations,

the codes and standards have been organised by the relative safety significance of the SSCs to which they have been applied (see Chapter 6).

The AP1000 Equivalence/Maturity Study of U.S. Codes and Standards (Reference 11.25), provides a clear and auditable demonstration that all codes and standards to support the design substantiation of UK safety related or safety significant SSCs have been identified and the suitability of the US standard assessed.

11.8.3.3 Redundancy and Segregation

The design of the AP1000 plant incorporates redundant divisions of Class 1 SSC, each of which is capable of delivering the Category A safety function. Where there is the potential for Class 1 SSCs to be compromised by a dropped load, the redundant Class 1 SSC delivering the Category A safety function has been identified. The provision of redundancy takes into account the following:

- IAEA-NS-G-1.11 "Protection against Internal Hazards other than Fires and Explosions in the Design of Nuclear Power Plants" (Reference 11.89).
- IAEA NS-R-1, "Safety of Nuclear Power Plants: Design" (Reference 11.21).
- APP-GW-J1R-008, April 2002, "Safety Criteria for the AP1000 Instrumentation and Control Systems" (Reference 11.51).
- APP-GW-J1R-004, April 2002, "AP1000 Instrumentation and Control Defence in Depth and Diversity Report" (Reference 11.52).
- ONR Nuclear Safety Technical Assessment Guide NS-TAST-GD-011, "The Single Failure Criterion" (Reference 11.127).

Within the Containment/Shield Building, redundant divisions of Class 1 SSC have been separated, so far as is reasonably practicable, by distance. While the Containment/Shield Building is a largely open space to maintain the free movement of gases, some compartments have been segregated by walls and floors providing some physical segregation.

Outside the Containment/Shield Building, the Auxiliary Building comprises both a RCA and non-RCA, which are physically segregated from one another by walls, floors and ceilings. Adjoining buildings are also physically segregated from the Auxiliary Building by walls, floors and ceilings. Access to either the RCA or non-RCA portions of the Auxiliary Building is from the adjoining buildings, which are themselves sub-divided into RCA and non-RCA sections by walls, floors and ceilings.

11.8.4 Dropped Loads Assessment Approach

A list of the cranes and lifting equipment is presented in Tables 11.8-1 and 11.8-2. This is compiled from the Mechanical Handling System Specification (Reference 11.126) and the Fuel Handling System Specification (Reference 11.125).

The cranes and lifting equipment considered are:

- Cranes and lifting platforms within the NI.
- Cranes and lifting platforms not in the NI.
- Monorail hoists.

- Elevators (lifts).
- Other lifting equipment.

Each item of lifting equipment is reviewed to determine the threat that a dropped load could pose and the possible impact on delivery of the Category A safety functions.

Assessment Criteria

The following criteria are used to identify which AP1000 lifting devices do not need to receive an in depth evaluation:

1. The hook coverage of the lifting device does not overlap any Class 1 SSC required to provide the principal means of delivering a Category A Safety Function.

2. The lifting device has passive devices controlling the load path in a safe manner[18].

3. The lifting device is unavailable during plant modes 1-4 and cannot lift a load over Class 1 SSC required to provide the principal means of delivering a Category A Safety Function during refuelling.

Dropped loads from lifting devices that meet all the above criteria cannot damage SSCs required to provide the principal means of safe shutdown and decay heat removal from the reactor and the SFP. These devices are identified and discussed in section 6 of Reference 11.123. Those lifting devices that do not meet all of the above criteria, i.e., have the potential to pose a threat of damaging SSCs required to provide the principal means of safe shutdown and decay heat removal from the reactor and the SFP, are evaluated on a case by case basis in Reference 11.121.

11.8.4.1 Equipment Qualification, Testing, and Maintenance

Systems and components claimed as part of the safety assessment of postulated DBAs, including dropped load/impact[19], are qualified to remain functional after exposure to environmental conditions, see Section 5.8. The plant equipment qualification methodology (Reference 11.60) presents information on the equipment qualification of mechanical and electrical SSCs which demonstrate that they are capable of performing their designated functions, while exposed to applicable normal, abnormal, test, design basis and post-accident environmental conditions. Information presented includes documentation of the qualification process and its applicability.

Active mechanical equipment is qualified for operability via an Operability Program which, combined with qualification of electrical attachments, demonstrates qualification under postulated environmental conditions. Class 1 equipment is qualified to maintain integrity and perform its safety function following a seismic event.

---

18. In practice, this criterion is only used, in conjunction with criteria 1 and 3, to exclude lifting devices, such as elevators, whose operating range is constrained by physical structures (such as lift shafts).
19. With the exception of the SFP liner and RPV, no claim is made within the assessment in Reference 11.123 on any SSC to remain functional following a dropped load/ impact, however SSC which are not directly impacted, but which may experience noise/ vibration are assumed to remain functional.

Procurement specifications include specific equipment qualification for all parts of the SSCs; where appropriate any SSCs that have an active functionality in the internal hazard environment are demonstrated through the appropriate accredited testing program. The qualification results are maintained as part of the equipment qualification file, which is maintained during the equipment selection and procurement process.

Qualification of equipment will be undertaken for those SSCs that are essential to maintaining nuclear safety by applying rigorous environmental qualification criteria.

Section 11.3.6 identifies the applicable environmental conditions conforming to General Design Criterion 4, as follows:

- Normal operating environmental conditions – Those conditions existing during routine plant operations for which the equipment is expected to be available on a continuous basis to perform required functions.

- Abnormal environmental conditions – Those plant conditions for which the equipment is designed to operate for a period of time without accelerating normal periodic tests, inspections, and maintenance schedules for that equipment. The maximum and minimum conditions identified as the abnormal condition are based on the design limits for the affected areas.

- DBA and post-DBA conditions – Those plant conditions resulting from various postulated equipment and piping failures during which the safety related equipment must operate without impairment of the function. The DBA and post-DBA conditions are discussed in the master equipment qualification environmental summary (Reference 11.61).

These environmental conditions are divided into mild and harsh environments, where a mild environment is that which can be expected to prevail during normal service conditions and the extremes of abnormal service. Electrical Equipment required to operate in a harsh environment will be qualified using a combination of type testing and testing and analysis. Mechanical equipment located in harsh environmental zones will be qualified to perform their required safety function. For active equipment, required to achieve a mechanical motion in delivering its safety function, qualification will comprise design, testing and analysis of critical sub-components supported by ongoing maintenance and surveillance programs. For non-active equipment whose safety function is delivered through structural integrity, qualification is achieved through design to appropriate codes and standards.

11.8.4.2 Combined Hazards Discussion

Dropped loads may initiate consequential internal hazards (e.g., pipework failure, missiles), their effect on Class 1 SSC are addressed separately in Section 11.12.

The consideration of credible combinations of dropped loads with other postulated internal hazards likely to occur independently of a dropped load is in Reference 11.75. This reference provides a coherent approach across all internal hazard types (e.g., fire, flooding, explosion, missiles, and pressure part failure).

Combinations of independent internal and external hazards (e.g., dropped load and extreme low ambient air temperatures) are considered to be Beyond Design Basis events and as such have not been explicitly considered in this section. However, compliance with relevant equipment and structural design codes as expressed in Chapter 5 ensure that combinations of

internal hazards discussed in Section 11.12 with the relevant abnormal operating occurrences (including environmental hazards as per References 11.60 and 11.61) are addressed.

11.8.5 Dropped Loads Analysis

11.8.5.1 Cranes and Lifting Equipment

The cranes and lifting equipment for the NI are Table 11.8-1. This table also indicates where in Reference 11.123 the dropped load assessment is summarised.

Cranes and lifting equipment located outside the NI are listed in Table 11.8-2. There are no Class 1 SSCs outside the NI and so dropped loads from these lifting devices are not included within the scope of this assessment as they pose no safety risk to operation of the plant (Reference 11.123).

11.8.5.2 Assessment of Dropped Loads

Within Containment, the bounding hazard is a drop of the IHP from the polar crane. The polar crane can only be used during plant modes 5 & 6. During these modes, the number of plant level faults (see Chapter 8), and therefore Category A safety functions, is greatly reduced. The analysis shows that of the required Category A safety functions, a drop of the IHP does not impact all Divisions of Class 1 SSC. In addition, analysis has shown (Reference 11.121 and 11.127) that, following a drop of the IHP onto the RPV, the RCS and DVI lines remain intact such that cooling of the reactor core can be maintained.

Outside of Containment in the RCA, the bounding hazard is a drop of the spent fuel cask from the cask handling crane. The cask handling crane is prevented from traversing over the SFP by end stops positioned to the west of the crane bridge beam. The analysis has conservatively assumed that a dropped fuel cask could penetrate the flooring of the levels below. Even still, there is sufficient redundancy in the unaffected Divisions of Class 1 SSC that the Category A safety functions can continue to be delivered. A dropped fuel cask could damage piping connections to the SFP resulting in a drain down of the SFP, however the design of the SFP precludes lower of the SFP level sufficient to uncover the spent fuel. The required make-up systems are unaffected by this fault.

A drop from the fuel handling machine operates has the potential to impact the SFP and potentially penetrate the floor leading to an uncontrolled drain down. Analysis has shown (Reference 11.122) that for the bounding drop, the SFP liner and civil structure remain intact. A drop from the fuel handling machine would therefore result in damage to spent fuel only, which is addressed separately as part of the fault analysis (see Chapter 8).

For drops from all other lifting devices installed throughout the plant, no more than one Division of Class 1 SSC could be impacted. As such, the ability to deliver Category A safety functions is unaffected.

11.8.5.3 Hazard Schedule

The dropped loads hazard schedule has been prepared based on the analysis of drops from lifting equipment (Reference 11.123). In accordance with relevant international guidance (Reference 11.82), the dropped loads hazard analysis has considered both primary and secondary effects in determining the bounding case. The dropped loads analysis has been prepared on the basis that:

- Class 1 SSC directly impacted by a dropped load will not be able to deliver the Category A safety function;
- A dropped load is assumed to penetrate all floors directly below the point of impact through to the ground floor;
- A dropped load may occur anywhere within the hook coverage of the lifting device;
- Within Containment, the maximum area of impact is equivalent to the footprint of the IHP;
- Outside of Containment, all Class 1 SSC present in a room are damaged where a dropped load impacts that room. Class 1 SSC in adjacent rooms are unaffected by the dropped load.

The dropped loads hazard schedule presents, for each lifting device, the:

- Divisions of each SSC affected;
- Category A safety function at risk;
- Unmitigated consequences should the plant be unable to effect safe shutdown;
- Redundant SSC available to deliver the Category A safety function, which have not been exposed to the same internal hazard.

The hazard schedule is presented in tabular form in Table 11.8-3, providing a concise and comprehensive summary of the postulated dropped loads, their significance and how the AP1000 plant is designed to cope with the hazard.

11.8.6 Sensitivity and Cliff Edge Effects

Based on the degree of conservatism applied to the drop calculations and the margin between the results and acceptance criteria, the value of sensitivity analyses or determination of cliff edge effects is considered minimal.

11.8.7 Combined Hazards Discussion

Dropped loads may initiate consequential internal hazards (e.g., pipework failure, missiles), their effect on Class 1 SSC are addressed separately in Section 11.12.

The consideration of credible combinations of dropped loads with other postulated internal hazards likely to occur independently of a dropped load is in Reference 11.75. This reference provides a coherent approach across all internal hazard types (e.g., fire, flooding, explosion, missiles, and pressure part failure).

Combinations of independent internal and external hazards (e.g., dropped load and extreme low ambient air temperatures) are considered to be Beyond Design Basis events and as such have not been explicitly considered in this section. However, compliance with relevant equipment and structural design codes as expressed in Chapter 5 ensure that combinations of internal hazards discussed in Section 11.12 with the relevant abnormal operating occurrences (including environmental hazards as per References 11.60 and 11.61) are addressed.

11.8.8 ALARP Assessment and Discussion

Deterministic analysis of postulated, design basis, dropped load events shows that the Category A safety functions will be available to provide a safe shutdown following the worst case dropped load.

The number of lifting operations required during normal operation has been minimised by design. Examples of where this has occurred include:

- Older PWR designs require multiple disassembly and lift operations to remove the reactor head. For the AP1000 design, only one lift is required to remove the integrated head package and place it on its storage stand.

- If a reactor coolant pump lift is required it can be carried out as a single lift as the pump and motor are removed and replaced as a single unit.

Although no account is taken within the assessment presented in this report of the frequency with which dropped loads occur, minimising the number of lifts will correspondingly lower the frequency with which loads are potentially dropped and therefore the overall risk.

Lifting plans have been established with a safe load path, which minimises the potential for a load to impact (either directly or following a dropped load) Class 1 SSC. Furthermore, the lift plans have been developed to minimise the height at which the load is carried and therefore the consequences following a drop.

A number of the cranes have been designed to codes and standards providing a high integrity design for nuclear lifting, or incorporate high integrity design features, such as redundant load paths and braking systems, and protective devices (e.g., limit switches) to reduce the likelihood of a dropped load. For these lifting devices, which lift the most sensitive loads or in the most sensitive areas, the likelihood of a dropped load is minimised.

Significant portions of the NI are seismically qualified for a design basis earthquake. With the exception of a fuel element drop onto the SFP, no credit has been taken for the ability of the civil structure to protect SSC present on lower levels from a direct impact. It is however reasonable to assume that, for a number of the loads, the floor would successfully terminate the fault progression although spalling of the ceiling into the room below could not be discounted.

On the basis of the above discussion, and given that Category A safety functions can be maintained in the event of a dropped load, it is judged that there would be minimal safety benefit from introducing additional measures to protect or mitigate a dropped load; the risk from dropped loads is therefore considered to be broadly acceptable and ALARP.

11.9 Biological Agents

11.9.1 Introduction

This section addresses the potential hazards arising from the ingress of biological agents and the lines of defence designed to prevent adverse influences to the safety of the generic AP1000 facility. It provides sufficient arguments and evidence to show that the delivery of Category A safety functions or supporting post 72 hour Category B safety functions will not be impaired by the influences attributable to biological agents. Claims required to meet this assertion are detailed throughout subsection 11.9.2, whilst a number of additional ALARP

measures are identified within subsection 11.9.7 to support the safety case made around these claims.

Biological agents discussed within this section are separated and addressed into the following categories:

- Microbiological (e.g., algae).
- Marine or freshwater life (e.g., fish, molluscs, and seaweed).
- Vermin (e.g., birds, insects, bats, and rodents).

Detrimental effects on the delivery of nuclear safety have been postulated for each of these biological agents, with the delivery mechanisms described in greater detail within subsection 11.9.4. As biological agent intrusion into AP1000 plant can emanate from outside the site boundary, it should be noted that these hazards are also identified within the external hazard analysis within Section 12.15.

Discussion of interfaces, applicable codes and the redundancy of systems is presented within subsection 11.9.3.

11.9.2 Biological Agents Claims, Arguments and Evidence

11.9.2.1 Claims Overview

To control intrusion by biological agents that may otherwise threaten the functionality of SSCs providing Category A safety functions or supporting post 72 hour Category B safety functions, the AP1000 takes the dual approach of preventing biological agent ingress coupled with early detection and remediation of any ingress. This approach is reflected in the prevention and mitigation claims defined within this section (claims 1 and 2, respectively). Additionally and although not formerly claimed, a number of ALARP measures are also defined to support the safety case made around these claims (see subsection 11.9.7).

11.9.2.2 High Level Claim

Although infrequent and of a low probability, biological agents may potentially cause a deviance from the normal operation of the reactor power plant with the potential to result in a hazard being realised. In response to such a deviance, it may be infrequently required to shut down the reactor and return it to a safe state or simply reduce power levels in maintaining a safe state of operation. Depending on the exact nature of the transient, there are a number of courses of action to take to shut the reactor down. Availability of the Class 1 SSCs required in delivering the Category A safety functions will ensure that the reactor can be safely shutdown, and is the basis of the following high level claim.

Claim IH-8.0: **Postulated biological agent ingress within the design basis will not prevent the delivery of the Category A safety functions and supporting post 72 hour Category B safety functions necessary to respond to the postulated event.**

Within the design of the AP1000, this has been achieved by ingress prevention, detection and remediation of the intrusion. The SSCs claimed to provide post-72 hour support functions include only offsite procured SSCs and their associated Class 1 connections.

11.9.2.3 Prevention Claims

Prevention against the risk from biological agents in support of the overall high level claim is provided by:

Claim IH-8.1: **Intrusion of biological agents is prevented by the incorporation of structural design features that bar entry into areas containing SSCs delivering Category A safety functions or supporting post 72 hour Category B safety functions.**

11.9.2.4 Protection Claims

As safety case claims are made against the prevention of biological agent ingress and by identifying and controlling biological agent ingress, no protective claims are made. Although not formerly claimed, however, a number of protective ALARP measures are identified (see subsection 11.9.7).

11.9.2.5 Mitigation Claims

Mitigation against the risk from biological agents in support of the overall high level claim is provided by:

Claim IH-8.2: **Detection and remediation of biological agents that may have entered the AP1000 plant will be undertaken before their ingress can result in the impaired performance of SSCs and prevent the delivery of a Category A safety functions or supporting post 72 hour Category B safety functions.**

11.9.2.6 Arguments and Evidence

Claim IH-8.1: **Intrusion of biological agents into the AP1000 plant is prevented by the incorporation of design features that bar their entry into areas containing SSCs delivering Category A safety functions or supporting post 72 hour Category B safety functions.**

The SSCs of the NI within the AP1000 design are designed to minimise the intrusion of biological agents into the NI through the incorporation of structural design features specified in appropriate building and design codes.

The primary functions of the buildings in the NI are to provide shielding and to maintain nuclear containment. The massive concrete and steel construction of the AP1000 NI and provision of secured access and egress routes for personnel ensure that buildings are adequately robust against the ingress of vermin.

Areas of potential vulnerability include penetrations into buildings and ventilation inlet and exhaust systems. Building codes and the design and construction of the NI will effectively prevent ingress via these routes, for example, by the incorporation of screens in the Shield Building air inlet and exhaust diffuser. To prevent ingress into the Shield Building via the PCS air inlets or discharge, No. 10 mesh screening (10 mesh per inch (25.4 mm) with 0.025 inch (0.635 mm) diameter wire) is typically placed behind the air inlet opening louvers and in the air discharge path leading to the elevated exhaust structure. To prevent vermin, such as insects, birds, and rats, from gaining access and fouling or damaging systems via other

ventilation systems, such as the DG inlet and exhaust systems, screens, meshes, and filters are installed.

The types of waterborne biological agents that could potentially affect nuclear safety are heavily dependent on the environment in which the station is operated, specifically on the source of the turbine condenser heat sink. This may be from a cooling tower, from a freshwater source, or most typically for the UK, from the marine environment. Therefore, the prevention methods for ingress by waterborne agents (e.g., algae blooms, sea weed, and molluscs) will be determined by the chosen heat sink for a particular site, and this will be addressed in the site-specific safety case. Similar prevention methods to those currently deployed at operating plants across the UK, such as the use of drum screens, will be available to control the potential intrusion of marine life.

The potential hazards microbiological agents create are difficult to exclude purely by design, but may be effectively mitigated by monitoring, detection, and routine treatment with appropriate biocides (see Claim 2 below).

Claim IH-8.2: **Detection and remediation of biological agents that may have entered the AP1000 plant will be undertaken before such ingress can result in prevention of the delivery of a Category A safety functions or supporting post 72 hour Category B safety functions.**

In addition to the protection to the Class 1 SSCs provided by the NI buildings, additional measures will be in place to control an infestation by biological agents from disrupting the provision of the Category A safety functions. See, for example, the biological fouling safety design approach identified in Chapter 12, Section 12.15. These measures follow the best practice approaches from existing NPPs of using chemical control to minimise the risk of microorganisms fouling tanks, HXs, and pipework and, a regime of regular inspection and surveillance of the safety significant SSCs within the NI and across the remaining AP1000 plant structures for the early detection of infiltration of any biological agents (macro or microscopic).

A regime of routine monitoring, sampling, and analyses of all systems containing water will ensure that the presence of microbiological growths are detected in the early stages, well before they could present any challenge to nuclear safety, and can then be treated and controlled with the appropriate biocide or algaecide. As part of the auxiliary systems, there are various water systems with piping, tanks, HXs, and other components. These systems are routinely treated or dosed with biocides and/or algaecides to control the growth of microorganisms that cause fouling and to limit the formation of biological films that may reduce heat transfer in condensers and HXs.

For open cooling water systems like the CWS or the SWS that cool the CCS HXs, the addition of biocide is performed by local feed injection, monitored, and adjusted as necessary. Biocides, such as sodium hypochlorite, are recommended in preference to toxic gases, such as chlorine, which may increase the toxic gas risk.

In the PCS, the PCCWST and PCCAWST are periodically monitored and dosed with hydrogen peroxide to control biological growth.

Other water systems like the DTS do not typically require treatment, since this water is constantly being used and replenished. This water is treated to maintain a very low oxygen content, which minimises the potential for algae or other biological growth.

The ingress of freshwater or marine life into systems like the CWS when direct cooling is employed is already prevented by the use of drum screens and treatment systems suitable for the local conditions. Additionally, biological growth as a consequence of marine or freshwater life would either be detected directly by routine monitoring and maintenance, or noticed as a gradual loss of system performance. Any growth would be rectified during routine testing and maintenance outages.

Similarly, a regime of routine monitoring and maintenance throughout the life of the station will detect the entry of any animals or birds into the NI, whereupon remedial actions can be undertaken to remove the creatures and the repair of entry routes.

11.9.3 Biological Agents Safety Case Summary

11.9.3.1 Introduction and Overview

The biological agent hazard challenging the AP1000 is categorised as microbiological (e.g., algae), marine or freshwater life, such as fish, molluscs, and seaweed, and vermin, such as birds, insects, bats, and rodents. Detrimental effects on the delivery of nuclear safety have been postulated for each of these biological agents (see subsection 11.9.4), with the potential to prevent the delivery of Category A safety functions or supporting post 72 hour Category B safety functions. The safety case for control of biological agents is based principally on the demonstration of the following:

- Ingress prevention
- Detection and remediation of intrusion

Specific claims are detailed in subsection 11.9.2, whilst a number of additional ALARP measures are identified within subsection 11.9.7 supporting the safety case made around those claims. The inherently robust structural design of the plant, normal operating procedures and maintenance activities form the basis of the measures to prevent, detect and control the ingress of biological agents. The redundancy, separation, and segregation of the plant involved in the postulated biological agent ingress is discussed below along with identification of any applicable codes and standards, and any interfaces with the assessment of other internal hazards.

11.9.3.2 Applicable Codes and Standards

The appropriate building and design codes used throughout the AP1000 plant (see Chapter 16) mean it is inherently designed to minimise the intrusion of biological agents, e.g., the incorporation of screens in the Shield Building air inlet and exhaust diffusers.

11.9.3.3 Redundancy, Separation, and Segregation

Sufficient redundancy, separation, and segregation in the design and location of the Class 1 SSCs ensure that the Category A safety functions can be maintained in the worst-case, normally permitted, plant line-up, despite loss of those SSCs affected by biological agent ingress and the presence of a credible, unrelated, single failure within the other SSCs.

The Containment structure provides a robust barrier to the intrusion of biological agents into the area where Class 1 SSCs are sited. Outside the Containment structure, the Class 1 SSCs in the Auxiliary Building have been designed so that the complete loss of the equipment within any single room will not result in loss of Category A safety functions. The concrete fire barriers protecting redundant trains of the Class 1 SSCs from fire should also provide an

adequate barrier to spread of biological agents, and therefore limit any damage to the equipment in only the affected room. Materials used in the construction of the Class 1 SSCs are generally not susceptible to attack by biological agents.

Large quantities or swarms of insects that could cause blockage of the large, multiple PCS air inlets or large PCS outlet are highly unlikely. Additionally, the PCS inlets and outlets are subject to periodic inspection to ensure that no such blockage exists. Furthermore, the heat removal capability of the PCS is still maintained by the application of water onto the outside surface of the Containment shell. A decrease in air flow would impact the ability of the PCS to attain low Containment pressure following a DBA, since water evaporation at low temperature would be decreased, but boiling would still be effective in removing heat.

Large quantities or swarms of insects could conceivably cause the blockage of the intakes for HVAC, DGs, or other systems that rely on an air supply to maintain their function. Typically for DGs, protection is afforded by having separation by distance between DG intakes and exhaust, and by the standard practice of having screens and air filters on intakes. Additionally, the DGs are a defense in depth function, not depended upon to provide power to any Class 1 SSC for the AP1000 plant, so a loss of one or all DGs does not affect safe shutdown of the plant. The batteries providing power to the Class 1 SSCs would clearly not be susceptible to this hazard.

Adequate redundancy is provided within each Class 1 safety system such that even in the loss of a single SSC, for example, as a result of a fire (which is assumed to disable the whole train), the Category A safety function can still be provided by a redundant train located in a different fire compartment (or fire zone within the Containment). This compartmentalisation of safety systems also provides protection from system damage resulting from animal ingress, as any significant damage in one area would be confined, detected, and mitigated before it could spread to other areas.

In addition, penetrations between compartments are minimised mainly to reduce the potential routes for the spread of fire and hot gases, but this would also limit access and egress routes for vermin. Class 1 cables are routed in separate raceways in galvanised steel solid-bottomed and lidded trays, which again would reduce the opportunity for vermin to cause damage.

11.9.3.4 Biological Agents Assessment Approach

Principally, the AP1000 design takes the dual approach of ingress prevention and, detection and remediation of any intrusion to control the risks associated with biological agents. Detailed analysis of the hazard presented by biological agents is not appropriate for a generic assessment as the environmental conditions of each site will vary as will the specific challenges to each site necessitating finely tailored control measures, particularly those in relation to the site-specific heat sink. As such this will be addressed during the detailed design phase and in the site-specific safety case.

11.9.3.5 Interface with Other Internal Hazards

Control of biological agent impact on the AP1000 has an indirect reliance on the inherent compartmentalisation and redundancy within the design (see Chapter 16), e.g., fire barriers protecting redundant trains of the Class 1 SSCs from fire (discussed within Section 11.2) limits the spread of biological agents by also acting as a barrier to their propagation.

Discussion of the use of biocides to control biological ingress, e.g., sodium hypochlorite is presented within the Chemical Inhibitors discussion of subsection 11.7.4.2. There is also a

less significant interface with internal flooding, as nesting material is identified as an initiator of block drains and therefore flooding (see Section 11.3).

Where biological hazards originate outside the AP1000 plant site boundary they are also addressed within the external hazard analysis. Section 12.15 covers the external threat from biological agents.

11.9.3.6 Conclusions

Sufficient evidence has been shown throughout this section that the risk of loss of a nuclear safety-significant system as a result of biological agents is low and controlled. Biological agents have been shown to not prevent the delivery of the Category A safety functions and the post 72-hour Category B safety functions. This is due to the combination of inherent design features, routine and non-routine early detection regimes, and the application of routine and non-routine remediation actions, respectively preventing, detecting and controlling the risk to the AP1000 from biological agents.

11.9.4 Biological Agents Safety Analysis

11.9.4.1 Identification of Hazard Sources

Microbiological growth has the potential to form a biological film that can reduce the effectiveness of heat transfer in condensers and HXs and to contaminate potable water supplies. In the extreme, algae growths (blooms) could restrict the flow of water and block filters.

Similarly, marine (or freshwater) life such as fish could be drawn into water inlets and restrict water flow to condensers or HXs.

Bird, animal and insect infestations are a threat to nuclear safety through the following potential mechanisms:

- Nest material could block drains, resulting in flooding.
- Fouling and waste products could cause corrosion.
- Electrical cables could be gnawed, causing broken circuits and short circuits.
- Mechanical damage to delicate systems could result from creatures getting into them.
- Seals between compartments could be damaged by creatures physically forcing passage through, subsequently allowing smoke and noxious gas to pass.
- Radioactive material could be spread from radiologically controlled areas to clean areas or even the external environment by the movement of creatures.
- The bodies of dead creatures could be drawn into pump suction pipework, clogging them or damaging the pump mechanism.

11.9.4.2 Assessment of Biological Agent Impact and Control

The potential for biological agent ingress is constantly present within the plant environment. As such it is not possible to eliminate the hazard presented by biological agent ingress and

therefore the AP1000 design takes the dual approach of ingress prevention and, detection and remediation of any ingress to control the risks associated with biological agents. The inherently robust design of the plant, normal operating procedures and maintenance activities form the basis of the measures to prevent, detect and control the ingress of biological agents.

Analysis of the hazard presented by biological agents is not appropriate for a generic assessment as the specific environmental conditions of each particular site will mean the specific hazard challenging each site may vary, necessitating finely tailored control measures, particularly those preventing in relation to the site-specific heat sink. As such this will be addressed during the detailed design phase and in the site-specific safety case.

11.9.4.3 Hazard Schedule

Whilst subsection 11.9.4.1 postulates generic detrimental effects of the expected categories of biological agents, no specific hazard schedule is presented for biological agents as the hazard presented by each agent in its constituent environment remains to be finalised during the detailed design phase. These hazards will be captured and recorded within the site-specific safety case.

11.9.4.4 Discussion of Results

Analysis of the threat posed by biological agents is fundamentally site-specific; as such this level of detailed assessment will be undertaken during the detailed design phase and captured within the site-specific safety case. Therefore no results are presented here.

11.9.5 Sensitivity and Cliff Edge Results

Analysis of the threat posed by biological agents is fundamentally site-specific; as such this level of detailed assessment will be undertaken during the detailed design phase and captured within the site-specific safety case. Therefore no discussion of cliff edge transition effects is presented here.

11.9.6 Combination of Hazards and Consequential Hazards

Biological Agents as a hazard initiating consequential internal hazards and, their effect on Class 1 SSC are addressed separately in Section 11.12.

Consideration of credible combinations of Biological Agents with other postulated internal hazards likely to occur as the result of a biological event is considered unlikely the basis that this internal hazard does not result in the loss or damage of Class 1 SSCs and, as such, its contribution to combinations of internal hazards is of no consequence (Reference 11.75).

Combinations of independent internal and external hazards (e.g., dropped load and extreme low ambient air temperatures) are considered to be Beyond Design Basis events and as such have not been explicitly considered. However, compliance with relevant equipment and structural design codes as expressed in Chapter 5 ensure that combinations of internal hazards discussed in Section 11.12 with the relevant abnormal operating occurrences (including environmental hazards as per References 11.60 and 11.61) are addressed.

11.9.7 ALARP Assessment and Discussion

The biological agent safety case is based principally on the preventative and mitigative claims of, precluding ingress where possible, and, detecting and remediating it where not. To further

support this case and although not formerly claimed, a number of controls are also identified as ALARP measures. These include:

- All Class 1 SSCs are separated into zones for the prevention of loss by any single event, such as fire. This has the additional benefit that animal ingress is extremely unlikely to penetrate multiple barriers and cause any significant damage without operators becoming aware and initiating corrective actions. This is also pertinent in relation to the unlikely possibility of animal ingress leading to the spread of contamination across zones.

- Class 1 cables are routed in separate raceways in galvanised steel solid-bottomed and lidded trays to reduce the opportunity for vermin to cause broken circuits and short circuits from gnawing.

- Materials used in the construction of the Class 1 SSCs are generally not susceptible to attack by biological agents.

In concert with the safety case claims, the measures outlined above provide sufficient evidence that the risk of loss of a nuclear safety-significant system as a result of biological agents is low and has been addressed in the design of the plant (or will be addressed on a site-by-site basis) and by normal operational procedures and maintenance activities. Thus, the risks posed from biological agents are at such a low level that further measures to reduce the risk further are not considered to be practical.

11.10 Onsite Transport

11.10.1 Introduction

This section covers the potential threats to nuclear safety from onsite transport accidents, including collisions between transports and with AP1000 plant civil structures, as well purely vehicular accidents and their effects on the loads transported.

The onsite transport hazard sources are described in subsection 11.10.4.1, with the impact of the hazard and its means of control addressed in subsection 11.10.4.2, the claims, argument and evidence of control being provided in subsections 11.10.2.

11.10.2 Onsite Transport Claims, Arguments and Evidence

11.10.2.1 Claims Overview

Whilst most of the claims to control the risk of an onsite transport accidents are by definition dependent on site specifics and local procedures, the primary claim placed at this stage is the physical protection provided by the buildings to the material and systems within them, i.e., the structure of AP1000 plant NI buildings fully protect the SSCs delivering the Category A safety functions within them. This is complemented by the siting of NI buildings and defined areas of onsite travel, as shown within Chapter 6, which establish protection against onsite vehicular impact.

11.10.2.2 High Level Claim

Incidents involving onsite transport have the potential to cause the failure of AP1000 SSCs due to vehicular impacts. This in turn may either initiate a transient from normal operation of the reactor power plant with the potential to result in a hazard on or off-site being realised, or

detrimentally affect the response to a transient. The availability of the Class 1 SSCs required to deliver the Category A safety functions will ensure that the reactor can be safely shutdown, and is the basis of the following high level claim.

Claim IH-9.0: **Postulated onsite transport within the design basis will not prevent the delivery of the Category A safety functions and supporting post 72 hour Category B safety functions necessary to respond to the postulated event.**

This high level claim is delivered by a set of three claims for the protection provided to systems from onsite transport events. These being:

- Protection to Class 1 SSCs provided by the NI structure
- Protection to the NI provided by adjacent structures
- Protection provided by the transport container

The SSCs claimed to provide post-72 hour support functions include only offsite procured SSCs and their associated Class 1 connections.

11.10.2.3 Prevention Claims

No prevention claims against the risk of onsite transport accidents are made as it is not practicable to prevent vehicle access to the AP1000 plant site (primarily the auxiliary and Turbine Buildings) for the various removals or deliveries required to safely operate the station.

11.10.2.4 Protection Claims

It is not possible to eliminate onsite transport as it is required for the normal operation of AP1000 plant; therefore Class 1 SSCs have to be protected from a transport incident and its effects. The following protective claims are made in support of the overall high level claim:

Claim IH-9.1: **The NI will protect the Class 1 SSCs from the effects of an onsite transport event.**

Claim IH-9.2: **The Radwaste Building, Annex Building and turbine hall protect the NI from an onsite transport collision.**

Claim IH-9.3: **Radioactive material transported onsite is protected by its transport package.**

11.10.2.5 Mitigation Claims

No mitigation claims against the risk of onsite transport accidents are made.

11.10.2.6 Arguments and Evidence

The risks associated with onsite transport accidents do not prevent the delivery of the Category A safety functions and the post 72-hour Category B safety functions, due primarily to the inherently robust civil structural design of the building, which is justified to protect against external hazards, see Chapter 12. This in concert with the siting of plant buildings, providing the maximum impact protection to the safety significant systems sited within the

NI buildings. Where radioactive material is transported onsite, the integrity of transport containers provides protection to the loads in accordance with nuclear industry standards.

Thus, the risks from an onsite transport accident leading to the loss of Class 1 and 2 SSCs as a result of an onsite transport incident is low and is suitably controlled by these measures. The following sections expand on these arguments.

Claim IH-9.1: The NI will protect the Class 1 SSCs from the effects of an onsite transport event.

Controlled vehicular access is required to the AP1000 plant site to deliver and pick up equipment, supplies, and nuclear materials required for the operation of the plant. Additionally, maintenance and repair work onsite will also require vehicles to access the site to support these activities. Such access is reasonably expected to fall within the site security plan in limiting and controlling vehicles inside the protected zone.

Appropriate AP1000 plant buildings have receipt and loading bays designed to be accessed by vehicles. The radiological portion of the Auxiliary Building has a loading bay suitable for trucks or a railroad car. This bay is used for the delivery and collection of new nuclear fuel, for the removal of spent nuclear fuel in transfer casks, and for the removal of used filter cartridges and spent resin. The Radwaste Building has a loading bay for the removal of other solid radiological waste material and for use by temporary equipment that may be employed for waste treatment. The Turbine Building has a bay for the delivery of equipment and supplies and removal of spent condensate treatment resin. Additionally, bulk supplies will be delivered to other AP1000 plant facilities, including those outside the plant security zone, to ensure the ongoing operation of the AP1000 reactor. Examples of these supplies include diesel fuel, bulk liquefied gases, compressed gas, and chemicals. Thus, it is not practicable to prevent vehicle access to the AP1000 plant site.

Additional measures are in place to minimise the frequency and consequences of an incident involving a collision of a vehicle with either another vehicle onsite or an SSC of the AP1000 plant. These are discussed in subsection 11.10.6 and cover procedural controls on vehicle movements and best practice in road layout and facility siting.

The AP1000 plant Class 1 SSCs are located in the buildings of the NI (Containment/Shield Building and Auxiliary Building). These are C-I buildings that are designed to protect the SSCs within them from seismic events and external hazards (for example, tornado-induced missiles). See Chapter 12 for a discussion of the design External Hazards and Chapter 16 for seismic analysis and qualification. No Class 1 SSCs are located in the Turbine Building, Annex Building, Radwaste Building, or other AP1000 plant facilities outside the NI. Class 2 SSCs are located both within the Shield and Auxiliary Buildings and in other structures of the AP1000 plant.

The Containment, Shield Building, and the Auxiliary Building provide a high level of protection to the SSCs within them. As C-I structures, they are designed to withstand the effects of earthquake while maintaining their integrity. Their seismic category, analysis methods, and results are discussed within Chapter 16. Additionally, the NI structures provide protection to the SSCs within them from externally-generated impacting objects. In Chapter 12, it is shown that a tornado-created missile (car of mass 1.81 tonnes travelling at 46.9 meters per second (105 mph)) that impacts the buildings of the NI will not cause a breach of a NI structure. The structures of the NI (Containment Vessel/Shield Building and Auxiliary Building) are, therefore, demonstrated to be robust when impacted by a significant mass travelling at speed.

Vehicle movement onsite will cover a wide range of loads from small loads to significant loads such as nuclear fuel casks, which may weigh up to 110 tonnes. While specific calculations for a worst-case vehicle collision with an AP1000 plant building have not been carried out, the analyses for seismic response and tornado missiles provide a high degree of confidence that the buildings will prevent a vehicle impact from disrupting SSCs located within the NI.

Claim IH-9.2: The Radwaste Building, Annex Building and turbine hall protect the NI from an onsite transport collision.

In addition, the Containment, Shield Building, and Auxiliary Building are protected on three sides by other AP1000 plant structures; including the Turbine Building, Radwaste Building, Annex Building. Chapter 6 provides a site layout drawing showing the positions of the main buildings and facilities.

The Turbine Building, Radwaste Building, Annex Building, and DG building do not contain Class 1 SSCs but will contain Class 2 SSCs. The portions of the Turbine Building, Radwaste Building, and Annex Building closest to the NI are designed to survive a C-II event. These C-II portions of the buildings consist of reinforced concrete and steel-framed structures with reinforced concrete walls and floor slabs. Roof slabs will be of reinforced concrete or metal decking.

The remaining portions of these buildings, while not designed to survive a C-II event, are of high-quality commercial construction, consisting of reinforced concrete and steel-framed structures with either reinforced concrete walls or insulated metal sidings. Floor and roof slabs will be of reinforced concrete or metal decking. General statements of intent regarding the construction of the buildings are provided within Chapter 16. These buildings are judged to provide some protection to the SSCs contained within them. A vehicle impact with these buildings could breach the building perimeter, but this impact would not affect the Class 1 or Class 2 SSCs in the C-I buildings, nor the Class 2 SSCs in the C-II portion of these buildings. If Class 2 SSCs are lost, the plant may experience a DB transient or entry into a Technical Specification (Tech Spec) condition. In either case, the Class 1 SSCs are available to ensure the delivery of the Category A safety functions.

Where access is required to receipt and loading bay areas within the AP1000 plant building, there is a possibility of a low-speed vehicle impact with the building structure. An impact with the building structure at the low speeds applicable during entry and exit from loading bays (5 mph or less) is judged not to cause failure of a C-I or C-II structure.

Any consequential hazards arising as a result of vehicle impact, such as fire, explosion, or missile generation, is bounded by the consideration of these hazards within Section 11.2, 11.5, and 11.6, and the consideration of consequential hazards presented in Section 11.12.

Claim IH-9.3: Radioactive material transported onsite is protected by its transport package.

Movement of radioactive materials such as LLW or ILW or spent fuel to onsite stores, or dispatch to offsite disposal facilities, is not fully defined at this stage. However, movements of nuclear materials that are to be dispatched offsite will be carried out in IAEA-approved packages in accordance with the requirements specified in TS-R-1 (Reference 11.129). These will provide a suitable level of protection to their contents from transport accidents. Transport of radioactive material in these approved packages will prevent uncontrolled dispersion of radioactivity or uncontrolled exposure of plant personnel or the public to radiation from a transport package.

Transport of radioactive material in transport packages will be subject to site administrative controls. These will be developed by the site licensee, and are expected to be in accordance with applicable radioactive material transportation regulations.

Radioactive material will also be moved onsite from the facilities where it is generated (the radiological Auxiliary Building and Containment structure) to the storage and packaging facilities within the Radwaste Building. The packaging arrangements for this material, its waste route, and means of transport will be defined by the site licensee prior to the operational phase.

Hence, accidents involving onsite transport of radioactive material will not result in the failure to deliver Category A safety functions.

11.10.3 Onsite Transport Safety Case Summary

11.10.3.1 Introduction and Overview

The onsite transport safety case is built on the demonstration of three claims, these being:

- Protection to Class 1 SSCs from the NI structure
- Protection to the NI provided by adjacent structures
- Protection provided by the transport container

These claims are argued (subsection 11.10.2.6), to be true based on the layout of the AP1000 structures and the protection provided by the NI to the SSCs that are located within it. Additional control and mitigation measures are presented in subsection 11.10.6 that apply to future onsite controls that a Licensee would be expected to apply. The safety case also addresses the transport of radioactive material onsite. Protection is provided by the transport containers for these movements.

11.10.3.2 Applicable Codes and Standards

Adherence to appropriate building and design codes (Chapter 16) mean the buildings of the AP1000 are designed to protect their contents from bounding external events (such as seismic or tornado-induced missiles) and therefore are protected against the effects of onsite transport accidents.

Transport of radioactive material within transport package loads will be in accordance with applicable radioactive material transportation regulations. Where packages are dispatched offsite, they will meet the requirements of TS-R-1 (Reference 11.129).

11.10.3.3 Redundancy, Separation, and Segregation

The distribution of Class 1 and 2 SSCs on an AP1000 plant is such that complete loss of operability of the SSCs within a room or compartment because of disruption resulting from an onsite transport accident would not result in loss of the Category A function.

Adequate redundancy is provided within each Class 1 safety system such that, even if the loss of a single SSC were to occur (for example, as a result of a resultant secondary fire), the Category A safety function can still be provided by a redundant train located in a different compartment or area of the Containment. This compartmentalisation of safety systems provides some protection from system disruption resulting from an impact with an AP1000

plant building, if the impacting object were to penetrate the building perimeter or cause a localised failure of systems within a building.

11.10.3.4 Onsite Transport Assessment Approach

The assessment approach taken to control the risks associated with onsite transport accidents presented throughout this section is principally based on the qualitative arguments of a robust inherent civil structural design and the siting of buildings with respect to protecting the NI. Discussion of the integrity of radioactive material loads carried by onsite transports is also presented below. These measures are supplemented by various site-specific protections and local transport procedures that will be implemented by the Licensee (see subsection 11.10.6).

11.10.3.5 Interface with Other Internal Hazards

The primary claim that the structure of the NI buildings of the AP1000 plant fully protects the SSCs delivering the Category A safety functions within them from structural collapse and shock-induced vibration damage caused by onsite transport accidents relies upon its inherently robust civil structural design (Chapter 16). This is justified elsewhere for bounding external hazards such as tornado or seismic events (see Chapter 12).

Indirectly fire, flooding, internal missile and other explosion effects are identified as possible additional outcomes of an onsite transport accident. Previous sections of this chapter (e.g., Section 11.2 for internal fire, Section 11.3 for flooding, Section 11.6 for internal missiles and Section 11.5 for explosions) have shown that any consequential hazards arising as a result of vehicle impact, are bounded by the consideration the effects of those hazards (also see Section 11.2 for consideration of consequential hazards).

11.10.3.6 Conclusions

Sufficient evidence that the risk of loss of a nuclear safety-significant system as a result of onsite transport accidents is low and well controlled has been shown throughout this section. The integrity of the plant's civil structural design, the siting of plant buildings and the integrity of the radioactive loads transported onsite provide the primary protection against the risk of an accident. It is anticipated that these will be supported by site-specific measures and local procedures as defined by the Licensee specifically for the site.

11.10.4 Onsite Transport Safety Analysis

11.10.4.1 Identification of Hazard Sources

Onsite transports accidents could directly damage the civil structures of the AP1000 plant buildings leading to structural collapse onto Class 1 or 2 SSCs, or cause shock-induced vibration damage to such SSCs inside; indirectly, there is the possibility of fire, flooding, and explosion effects. Additionally, the movement of radioactive material around the site could potentially be affected by a transport accident, releasing the radioactivity.

The principal buildings of concern are the NI and the Radwaste Building. The NI is where the Class 1 SSCs are located and most Class 2 SSCs are located. The Radwaste Building includes storage facilities for holding and processing the various categories of waste generated onsite prior to packaging and shipping offsite in approved containers. No Class 1 SSCs are located in the Radwaste Building.

The following buildings and structures of the AP1000 plant do not contain Class 1 SSCs but will contain Class 2 SSCs, and have been shown in previous sections of this chapter not to pose a secondary hazard (e.g., Section 11.6 for internal missiles, Section 11.5 for explosions, or Section 11.3 for flooding) to the safety-significant SSCs elsewhere onsite:

- Turbine hall
- Annex building
- DG building
- Service water cooling towers
- Onsite storage tanks (water, diesel fuel, boric acid)

Damage to any of these from an onsite transport accident would have one of two effects: it could initiate a DB operational transient, such as loss of grid; alternatively, it could force entry into a Tech Spec action condition, because of loss of availability of required systems, such as reactor coolant makeup through the CVS. Design Basis operational transients are addressed in Chapter 9. Entry into a Tech Spec condition would, in the worst case, lead to a controlled shutdown of the reactor. These two conditions are not considered further in this chapter.

11.10.4.2 Assessment of Onsite Transport Impact and Control

The safety justification for the onsite transport is based on the location of Class 1 SSCs and the protection of these SSCs from transport hazards by the NI structures. Detailed analysis of the onsite transport hazard has not been carried out as the site layout and requirements for vehicular deliveries will only be defined during the licensing phase. Assessments have been carried out of the capability of the NI to withstand a range of external hazards (Chapter 12), which are argued to provide confidence that the NI will provide protection from a vehicular impact. Detailed analysis of the onsite transport of radioactive material has not been carried out as it is argued that transport containers will be specified to comply with transport regulations and so no release of radioactive material will occur in the event of an onsite transport incident.

11.10.4.3 Hazard Schedule

No hazard schedule is presented for onsite transport as the hazard is dependent on site layout which is anticipate to be defined at the Licensing stage.

11.10.4.4 Discussion of Results

The safety justification for the onsite transport is based on the location of Class 1 SSCs and the protection of these SSCs from transport hazards by the NI structures. Additionally protection to the NI is provided by the other AP1000 buildings grouped around the NI. This approach is discussed in subsection 11.10.2.6. Detailed analysis of the onsite transport hazard has not been carried out as the site layout and requirements for vehicular deliveries will only be defined during the licensing phase.

11.10.4.5 Sensitivity and Cliff Edge Results

The argument and evidence in support of the onsite transport claims is not dependent on the assessment of onsite transport, rather it is dependent on AP1000 location of Class 1 SSCs, protection provided to the SSCs from the NI and the protection of the NI by adjacent

buildings. With all Class 1 SSCs located in the Containment and Auxiliary Building, protection from on-site transport hazards is provided by both the robust design of these structures (see External Hazards, Chapter 12, and sections 11.5, Internal Missiles, and 11.6, Internal Explosions) and the plant layout (Chapter 6) which places the Annex Building, Turbine Building, and Radwaste Building between normal transport routes and the Class 1 SSC locations. This cumulative passive protection, as well as anticipated active site security restrictions, does not lend itself to the consideration for cliff edge effects for onsite transport hazards.

11.10.5 Combination of Hazards and Consequential Hazards

Discussion of combined and consequential hazards is presented within the Combination of Hazards section (see Section 11.12).

11.10.6 ALARP Assessment and Discussion

The measures outlined in subsection 11.10.2.6 demonstrate that the likelihood of loss of Class 1 and 2 SSCs as a result of an onsite transport incident is low and has been addressed in the design of the plant or will be addressed on a site-by-site basis. In addition to the physical protection that the buildings provide to material and systems within them, additional external protection measures will be specified as required during the detailed site design phase. These measures are reasonably expected to include the following:

- Control of vehicular access to the site, including speed limitations, and escorting of significant loads
- Layout of access roads to minimise the potential for vehicles to reach high impact speeds.
- Definition of site access routes to minimise the potential for vehicle to vehicle collisions.
- Provision of armoured barriers to protect buildings from vehicle impacts
- Design of landscaping features to provide protection to buildings from vehicle impacts.

The risks posed from onsite transport are at such a low level that measures to reduce the risk further are not considered to be practicable.

11.11 Electromagnetic Interference

11.11.1 Introduction

This section covers the potential threats to nuclear safety from EMI originating onsite. Within this section, EMI includes radio frequency interference (RFI) and electrostatic discharge (ESD). Offsite-originated EMI (including lightning) is addressed within Section 12.16.

The EMI hazards sources are described in subsection 11.11.4.1, with the impact of the hazard and its means of control addressed in subsection 11.11.4.2, the claims, argument and evidence of control being provided in subsections 11.11.2.

11.11.2 Electromagnetic Interference Claims, Arguments and Evidence

11.11.2.1 Claims Overview

Two claims are made for the control of the hazard from EMI; prevention of EMI at source (i.e., emissions) and protection of systems from EMI (i.e., susceptibility).

11.11.2.2 High Level Claim

Internal electromagnetic interference has the potential to disable sensitive electronic equipment in the AP1000 plant, or may cause it to activate spuriously. This in turn may either initiate a transient from normal operation of the reactor power plant with the potential to result in a hazard on or off site being realised, or detrimentally affect the response to a transient. The availability of the Class 1 SSCs required in delivering the Category A safety functions will ensure that the reactor can be safely shutdown, and is the basis of the following high level claim.

Claim IH-10.0: **Postulated internally generated electromagnetic interference within the design basis will not prevent the delivery of the Category A safety functions and supporting post 72 hour Category B safety functions necessary to respond to the postulated event.**

This claim is delivered by a claim on the prevention of EMI and a claim for the protection provided to systems from EMI. The SSCs claimed to provide post-72 hour support functions include only offsite procured SSCs and their associated Class 1 connections.

11.11.2.3 Prevention Claims

The generation of levels of onsite EMI that could potentially disable sensitive electronic equipment in the AP1000 plant, or cause it to activate spuriously are prevented by the design and selection of electrical and electronic systems deployed on the AP1000 site.

The following preventative claim is therefore made in support of the overall high level claim:

Claim IH-10.1: **Electrical and electronic equipment, and communication systems, are designed, tested, and located so as not to generate levels of EMI emissions that will interfere with delivery of Category A safety functions.**

11.11.2.4 Protection Claims

It is not possible to eliminate all sources of EMI and so systems and components that could be adversely affected by EMI have to be protected. The following protective claims are made in support of the overall high level claim:

Claim IH-10.2: **Where appropriate, electrical and electronic equipment, and communication systems, will be protected from the effects of EMI through established system design measures.**

11.11.2.5 Mitigation Claims

No claim is made for the mitigation of EMI.

11.11.2.6 Arguments and Evidence

The risks associated with electromagnetic interference do not prevent the delivery of the Category A safety functions and the post 72-hour Category B safety functions, due principally to the complementary twofold approach of minimising EMI emissions (Claim 1) at source and protecting susceptible systems from EMI (Claim 2).

Claim IH-10.1: **Electrical and electronic equipment, and communication systems, are designed, tested, and located so as not to generate levels of EMI emissions that will interfere with delivery of Category A safety functions.**

All likely generators of EMI within the AP1000 plant have been identified. Electrical equipment can generate EMI by conduction through cables, radiated magnetic fields, radiated electric fields, or ESD. Likely generators of EMI have been specified to minimise the risk of them spuriously generating levels of EMI that could cause a hazard to AP1000 plant equipment, including Class 1 equipment. EMI generated from sources outside the AP1000 plant are addressed within external hazard analysis (Section 12.16).

The philosophy for the management of EMI for the AP1000 design is set out in the EMC management philosophy (Reference 11.130). It defines the standards that the AP1000 design will meet in the UK and how the requirements of SI 3418 (Reference 11.131) will be applied by Westinghouse.

While compliance with SI 3418 does not directly regulate safety-related matters, poor control of EMC can have a significant and detrimental effect on the reliable operation of electrical, electronic, and programmable electronic systems. This is recognised in Reference 11.132, regarding C&I safety, which sets out general requirements for systems. Measures in place to ensure that the electrical and electronic systems of the AP1000 plant are not susceptible to EMI are addressed below. The correct operation of the systems is also dependent on ensuring that the electromagnetic environment within which electrical and electronic systems operate is known and controlled to remain within acceptable limits. SI 3418 (Reference 11.131) requires that equipment shall be designed and manufactured having regard to the state of the art so as to ensure the EMI it generates does not exceed a level above which radio and telecommunication equipment or other equipment cannot operate as intended.

The electrical and electronic equipment of the AP1000 plant will comply with SI 3418 (Reference 11.131) and so will maintain an electromagnetic environment that allows the correct operation of other electrical and electronic equipment. This will be ensured by application of the EMC management philosophy (Reference 11.130) and the Westinghouse procurement system.

A small number of exclusions to SI 3418 (Reference 11.131) is set out in the EMC management philosophy (Reference 11.130). These cover the following:

- Equipment that is considered inherently benign in terms of EMC
- Electrical equipment having no active electronic parts

Electrical equipment that is not intended for a fixed installation and is not otherwise commercially available will follow a different acceptance route. The EMC management philosophy (Reference 11.130) mandates the following process:

- Characterisation of the electromagnetic environment (Reference 11.130, Section 6.0) to understand the potential operating conditions of the various plant areas and the impact on equipment.

- EMC management plan (Reference 11.130, Section 7.1), defining the strategy for the project to achieve EMC between equipment.

- EMC risk log (Reference 11.130, Section 7.2), covering potential hazards and mitigations.

- EMC control plan (Reference 11.130, Section 7.3), detailing how the requirements of the EMC management plan and statutory obligations will be met.

- EMC installation code of practice (Reference 11.130, Section 7.4), detailing installation requirements that comply with best practice in EMI design, installation, and the EN61000-5 series of standards. The EN61000-5 series provides guidance on installation and EMI mitigation. System and component selection, design, installation, and testing of electrical equipment will be in accordance with the EMC emission requirements of the C&I general design criteria. Detailed management will be exercised over selection, testing, and operational use of communication systems that are inherently EMI emitters, including frequency allocations and power levels/antenna gains.

- EMC test specification (Reference 11.130, Section 7.5), detailing EMC tests on individual apparatus, systems, and sites to demonstrate that EMC requirements are met. This will capture the IEC 61000-4 series of standards that address requirements for testing against EMI. AP1000 plant electrical equipment (safety related and non-safety related) will be EMC-qualified for emissions primarily by type-testing, rather than by analysis. This testing will include conducted emissions through cables (30 to 2 MHz), radiated magnetic fields (30 to 100 kHz) and radiated electric fields (2 MHz to 10 GHz).

Claim IH-10.2: **Where appropriate, electrical and electronic equipment, and communication systems, will be protected from the effects of EMI through established system design measures.**

EMI is a potential threat to the correct operation of electronic equipment. It has the potential to cause malfunction, damage, or spurious operation of C&I equipment. In the AP1000 plant, electronic equipment supports the delivery of all categories of safety function through its roles in monitoring the plant and providing a means of plant control. In particular, Category A safety functions that require C&I to deliver them are supported by the systems discussed below.

The categorisation document and Classification of C&I systems is provided in Appendix A of Chapter 15. This classification includes the following systems and functions:

- PMS
- PLS
- DAS
- Operation and control centre system (OCS)

- DDS
- In-core instrumentation system (IIS)
- Special monitoring system (SMS)

Any of these C&I systems could be susceptible to onsite EMI. EMI has the potential to cause the system to behave in an unpredictable manner, by doing the following:

- Causing the system to provide incorrect indications
- Initiating actions when not required
- Preventing the initiation of actions when required

To ensure that the C&I systems operate correctly in the presence of EMI, the AP1000 design adheres to standards and follows best practice in the characterisation of the electromagnetic environment, the design of the systems, the selection of system components, the placing of the systems equipment, and the testing of the systems when installed. This philosophy for the management of EMC for the AP1000 design is set out in Reference 11.130 in defining the standards that the AP1000 design will meet in the UK and how the requirements of Statutory Instrument (SI) 3418 regarding EMC (Reference 11.131), will be applied. The principal means by which the effects of EMI on the C&I systems of the AP1000 plant will be minimised are the following:

- The architectural design of the C&I systems takes into account the presence of EMI and incorporates features to minimise the potential impact of EMI on the correct operation of the C&I. This is in compliance with BS IEC 61513:2001 (Reference 11.132), which sets out general requirements for design response to EMI. Features incorporated into the design are discussed within subsection 11.11.3.3.

- An EMC installation code of practice is an element of the EMC management philosophy (Reference 11.130). This will capture best practice in the EMI design, procurement, and installation of systems to minimise their EMI susceptibility. System/component selection, design, installation, and testing of electrical equipment will be carried out in accordance with the EMC susceptibility requirements of C&I general design criteria.

- An EMC test specification is another significant element of the EMC management philosophy (Reference 11.130). This will capture the IEC 61000-4 series of standards that address requirements for testing against EMI. AP1000 electrical plant equipment will be EMC-qualified for susceptibility primarily by type-testing, rather than by analysis. This testing will include conducted susceptibility through cables (16 to 30 MHz), radiated susceptibility magnetic fields (30 to 100 kHz), and radiated susceptibility electric fields (30 MHz to 10 GHz), assuming the equipment is Conformité Européene (CE) marked. If the equipment is not CE marked, then more stringent tests will be applied.

While much of the activity to control EMI and to deliver systems that are compatible with each other will occur at the build stage, there are design features within the AP1000 plant C&I systems that reduce the susceptibility of C&I to EMI. These provide confidence that the C&I design will not be susceptible to EMI, as follows:

- Category A and 72 hour supporting Category B equipment is placed in areas of low EMI fields.

- Fibre optic communications are used in areas with potentially high EMI fields.
- C&I electronics and sensors are grounded with regard to EMI protection.
- Class 1 cables that carry electrical signals that are assessed as potentially susceptible to EMI are routed in separate raceways in galvanised steel solid-bottomed and lidded trays, which provide some shielding to EMI. These cables will also be routed away from MV/LV electrical cables.
- Cabinets containing C&I equipment provide some shielding to their contents.

The structure of the AP1000 plant buildings provides a degree of protection to the propagation of EMI by ensuring that internal metal structures are earthed in accordance with best practice (Reference 11.133).

Input and output signal conditioning units, are used within systems that are required to withstand the EMI and ESD conditions that exist in specific areas of the plant.

The AP1000 plant Class 1 equipment has electrical surge withstand capability and can withstand EMI, RFI, and ESD conditions that would exist before, during, and after a DBA without loss of safety function for the time required to perform the safety function.

11.11.3 Electromagnetic Interference Safety Case Summary

11.11.3.1 Introduction and Overview

The electromagnetic interference safety case is built on the demonstration of two claims, these being:

- Prevention of level of plant generated EMI that could cause failure of Class 1 SSCs (Emissions)
- Protection of Class 1 SSCs from EMI that could cause its failure or spurious operation (Susceptibility)

These claims are argued (subsection 11.11.2), to be true based on the application of relevant codes and standards for the control of the EMI environment (subsection 11.11.3.2) and the control of system susceptibility to EMI. Additionally design features of the Class 1 control and instrumentation systems have been highlighted (subsection 11.11.3.3) which either reduce or eliminate the potential for an EMI induced failure. Sources of onsite EMI are identified (see subsection 11.11.4.1), to provide additional confidence that the measures set out in the arguments for emissions and susceptibility can be applied to those EMI sources. Although not the core of the case, supplementary operational measures, e.g., limiting static, access control and training also provide additional EMI controls on a site-specific basis. Thus, the risks from electromagnetic interference leading to the loss of Class 1 and 2 SSCs are low and suitably controlled.

11.11.3.2 Applicable Codes and Standards

Management of EMI and the standards that the AP1000 design will meet in the UK is set out in the EMC management philosophy (Reference 11.130). This document outlines how the requirements of how the UK statuary instrument on electromagnetic compatibility (SI 3418 [Reference 11.131]) will be applied.

SI 3418 does not directly regulate safety-related matters, but adherence to it does provide reliable operation of electrical, electronic, and programmable electronic systems that minimises the emission of potentially detrimental EMI. EMI generated should therefore not exceed a level above which radio and telecommunication equipment or other equipment cannot operate as intended. Equipment that is considered inherently benign in terms of EMC and electrical equipment having no active electronic parts are noted exclusions from requirements of SI 3418 (Reference 11.131) (see EMC management philosophy [Reference 11.130]).

To address the safety case claims of minimising EMI at source and protecting against EMI, adherence to two series of International Electrotechnical Commission (IEC) standards is stipulated. The IEC61000-4 series outlines testing and measurement techniques, whilst the IEC61000-5 series outlines installation and mitigation guidelines.

This section also cites the more generic 'Nuclear Power Plants, Instrumentation and Control for Systems Important to Safety, General Requirements for Systems' (BS IEC 61513-2001 [Reference 11.132]) and 'IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations' (IEEE 603-1991 [Reference 11.133]) as supplementing the more directly applicable EMI codes and standards discussed above.

11.11.3.3 Redundancy, Separation, and Segregation

The distribution of safety-significant SSCs in an AP1000 plant is such that complete loss of operability of the safety-significant SSCs within a room or compartment because of EMI would not result in the loss of a safety function.

Adequate redundancy is provided within each Class 1 safety system such that even if the loss of a single SSC were to occur (for example as a result of a fire), the Category A safety function can still be provided by a redundant train located in a different compartment or area of the Containment. This compartmentalisation of safety systems provides protection from system disruption resulting from EMI. It is recognised that the form of the physical barriers and the separation, while adequate for physical hazards such as fire are flood, may not be completely adequate for EMI, which can propagate widely. However, the physical barriers and the redundancy, separation, and segregation of systems do provide some protection to AP1000 plant systems.

Each of the four divisions of the protection and safety monitoring is completely segregated from the others, so any onsite EMI would have to affect more than one division before any nuclear safety consequences could occur. The complete loss of operability of electronic equipment within a cabinet would not result in a challenge to a safety function.

11.11.3.4 Electromagnetic Interference Assessment Approach

The AP1000 design takes two complementary approaches to the control of the hazard from EMI. These are the minimisation of EMI at source (i.e., emissions) and the protection of systems from EMI (i.e., susceptibility). These two approaches are summarised in subsection 11.11.2.6, respectively. Analysis of the EMI hazard for the AP1000 reactor plant is directly dependent on the selection and placement of electrical and electronic equipment with the AP1000 site. This level of detail will be completed during detailed design and supplier selection.

11.11.3.5 Interface with Other Internal Hazards

No interfaces with other internal hazards are identified, though the external hazard analysis assesses offsite-originated EMI (including lightning) within Section 12.16.

11.11.3.6 Conclusions

Sufficient evidence has been shown throughout this section that the risk of loss of a nuclear safety-significant system as a result of EMI is low and well controlled. The combination of minimising emissions and protecting susceptible systems form the principle basis of the case. Additional site-specific measures that will be finalised by the operator during the Licensing phase to support the case.

11.11.4 Electromagnetic Interference Safety Analysis

11.11.4.1 Identification of Hazard Sources

Onsite EMI can arise from either the intentional generation of electromagnetic radiation from communication systems, or the unplanned, unintentional, or unwanted generation of EMI from the normal or abnormal operation of an electrical plant and equipment. Any EMI is potentially capable of disabling sensitive electronic equipment in the AP1000 plant, or may cause it to activate spuriously. Either way, it could initiate fault sequences or prevent the safety measures in place from performing their required functions, thereby resulting in the loss of safety functions.

The principal area of EMI concern is the NI, as this is where the safety-significant elements of the C&I systems are located. The possible sources of EMI are identified below, and the threats to specific safety-significant equipment are reviewed within subsection 11.11.4.1. None of the other buildings and structures of the AP1000 plant contain safety-significant C&I systems. They are, therefore, not considered further as far as EMI is concerned.

There are many potential sources of onsite EMI within the AP1000 plant. These come from the deliberate generation of electromagnetic radiation for communication purposes (e.g., using radio frequencies) and the unplanned, unintentional, or unwanted generation of EMI from the normal or abnormal operation of electrical plant and equipment, as discussed below.

Intentional Sources of EMI within the AP1000 Plant

The AP1000 plant will have both fixed and mobile communication systems onsite and a separate normal business network for communications:

- Communications networks
  - There are multiple redundant and diverse communication networks distributed widely throughout the plant, including voice over internet protocol, digital enhanced cordless telecommunications, pagers, land mobile radio, and a sound powered telephone system. The mobile communication system relies on distributed relay transmitters throughout the NI, resulting in the intentional presence of electromagnetic radiation in all rooms and compartments. None of the communication system components are Class 1SSCs.
- Business network

– The extensive network for normal administration will use a fibre ring with switches to copper/wireless connected peripherals. This is distributed widely throughout the plant, and will include the following peripheral equipment: telephones, workstations, television/video, cameras, laptops, handheld computers. This network is not used for nuclear safety, and does not contain Class 1 SSCs. Failure of the business network will not prevent a safe plant shutdown.

Unintentional Sources of EMI within the AP1000 Plant

EMI will also be created by the normal or abnormal operation of electrical plant and equipment onsite. The principal sources of unintentional EMI that have been identified are:

- Reactor trip switchgear and RCP switchgear; these are within the clean Auxiliary Building and are potential sources of arcing.
- Relays used in the instrument and motor control rooms.
- The MOVs used throughout the NI.
- The battery charger rectifiers within the clean Auxiliary Building; these are potential sources of high-frequency interference.
- Equipment containing thyristors, relays, and circuit breakers.
- Wireless crane controllers.

11.11.4.2 Assessment of Electromagnetic Interference Impact and Control

The potential for EMI from either intention or unintentional generation is constantly present on the site. It is not possible to eliminate EMI and so a layered approach to its control is adopted. This consists of the minimisation of EMI at source through the design and specification of possible EMI generators and then the minimisation of its impact through the protection provided to sensitive components and systems. Thus the careful choice of components and compliance with codes and standards are argued to address the claims made for prevention and protection. This is supported by measurement of the delivered EMI environment and testing of systems and components within that environment. This approach therefore does not depend on the prior analysis of EMI for the AP1000 plant.

11.11.4.3 Hazard Schedule

No hazard schedule is presented for EMI as the EMI hazard does not create distinct and localised failure of SSCs in a predictable manner. The EMI hazard has to be controlled through minimisation of harmful EMI generation and suitable and sufficient protection of susceptible SSCs.

11.11.4.4 Discussion of Results

The safety justification for the EMI internal hazard is based on two complementary approaches to the control of the hazard from EMI. These are the minimisation of EMI at source (i.e., emissions) and the protection of systems from EMI (i.e., susceptibility). These two approaches are summarised in subsection 11.11.2.6, respectively. Analysis of the EMI hazard for the AP1000 reactor plant will be directly dependent on the selection and

placement of electrical and electronic equipment with the AP1000 site. This level of detail will be completed during detailed design and supplier selection.

11.11.4.5 Sensitivity and Cliff Edge Results

The argument and evidence in support of the EMI claims is not dependent on the assessment of EMI, rather it is dependent on system and component selection, design, installation, and testing of electrical equipment in accordance with the EMC emission requirements of the C&I general design criteria. These approaches are applied to ensure that levels of EMI on the AP1000 plant do not reach levels at which a cliff edge transition occurs.

11.11.5 Combination of Hazards and Consequential Hazards

Discussion of combined and consequential hazards is presented within the Combination of Hazards section (see Section 11.12).

11.11.6 ALARP Assessment and Discussion

The arguments presented in subsection 11.11.2.6 demonstrate that the risk of loss of a nuclear safety significant system as a result of EMI is low and has been addressed in the design of the plant (or will be addressed on a site-by-site basis), and by normal operational procedures and maintenance activities. Specific measures taken to reduce risk include the application of relevant good practice as contained in standards and referred to from the EMC regulations (Reference 11.131), application of a management system to the control of EMI (Reference 11.130), and incorporation of features into the design of the Class 1 C&I systems to provide redundancy, separation, and segregation. In addition the following operational measures are reasonably expected to be implemented:

- A “responsible person” will be appointed to ensure EMI is managed through life (design, construction, commissioning, operation, and decommissioning). During the early stages (design up to handover), the responsible person will be a Westinghouse appointment. After handover, the responsible person will be appointed by the Operator. Significant and detailed files will be maintained of EMI design and operating features, which will be subject to formal configuration control throughout the plant life.

- Plant personnel will be trained in the effects of ESD and its potential damage to equipment.

- Plant personnel have knowledge of any plant equipment that is ESD-sensitive, including being clearly highlighted by warning signs.

- Access to electronic cabinets will be under strict administrative control.

- Antistatic floor tiles, mats, and wrist straps will be used when necessary as defined in the equipment operation and maintenance manuals.

- Use of two-way radios and cell-phones will be restricted in the vicinity of sensitive equipment, and an exclusion zone will be established for the use of such communications equipment.

Thus, the risks posed from EMI have been argued to be at such a low level that additional measures to reduce the risk further are not considered to be practicable.

11.12 Combinations of Hazards

A Combined Hazard Analysis has been performed in order to identify and assess the effects to SSCs as resulting from the combined effects of internal hazards as well as consideration of hazards with the potential to initiate plant level faults. The AP1000 plant has been designed such that internal hazards and any combination of hazards within the design basis will not compromise the ability of the plant to safely shutdown and maintain it in a safe condition. The Category A safety functions required for safe shutdown following a combined hazard event, and the supporting post 72 hour Category B safety functions, are shown to be maintained through a combination of claims made on:

- Minimising the inventory of hazardous material;
- Equipment design;
- Segregation of hazards and SSCs delivering Category A safety functions;
- Structural barriers and partitions.

Consequences from combined hazards, which have the potential to directly damage SSCs required to deliver Category A or supporting post-72 hour Category B safety functions have been systematically identified on a conservative deterministic basis. The results of this assessment are provided in more detail within the Combined Hazards Topic Report (Reference 11.75). The barriers that protect these safety functions are also identified and evaluated to confirm that they will provide protection against the identified combination of hazards.

The assessment of combined hazards has been undertaken using the same conservative assumptions as the individual internal hazard assessments (References 11.73, 11.76, 11.77, 11.93, 11.110 and 11.123). Where a causal link is identified between correlated[20] internal hazards, the combined impact on Category A safety functions is assessed. Where the conservative assumptions underpinning the assessment of individual hazards are no longer valid, revised assumptions are presented and the assessment updated to reflect this accordingly.

This assessment concludes that the Category A safety functions of Class 1 SSCs are protected from the effects of all credible combinations of internal hazards and can therefore continue to be delivered. Further, post 72-hour supporting Category B functions necessary to respond to the postulated event, and their Class 1 connections, are preserved.

11.12.1 Scope of Combined Hazards and Process

The AP1000 design has been evaluated for the impact of internal hazards in confirmation that SSCs required to deliver Category A or supporting Post-72 hours Category B safety functions will perform as required following an internal hazard (Sections 11.2 through 11.11).

[20] Internal hazards are considered to be correlated where the effects of the primary internal hazard are experienced by the source of the subsequently initiated internal hazard.

When the results of engineering judgement, deterministic safety assessments and probabilistic safety assessments indicate that combinations of events could lead to anticipated operational occurrences or to accident conditions, then such combinations of event are considered to be design basis events depending on the likelihood of occurrence (Reference 11.134). To this end, combinations of internal hazards within the design basis will be evaluated where:

- An internal hazard induces sequential internal hazard(s); or
- A common initiator results in simultaneous internal hazards;
- Independent internal hazards with a combined event frequency > 1E-05 / reactor year.

The AP1000 NI was systematically assessed for hazard combinations followed by areas outside the NI, but within the plant envelope. More severe[21] hazard combinations were also assessed for effects on Category A and supporting post-72 hour Category B safety functions.

All credible combinations of hazards, either consequential, correlated or independent, are captured in the hazard schedule which clearly identifies all divisions of Class 1 SSC affected, as well as links to the fault schedule where relevant.

This assessment concluded that Category A safety functions will continue to be delivered following various design basis combined hazards through a combination of claims made on structural barriers, equipment qualification, passive flood relief systems and, where necessary, minimal operator actions to isolate inexhaustible sources of flooding following identification by a level sensor (i.e. no claim has been made on the prevention or limitation of fault occurrence). These claims are consistent with the claims made through each individual hazard assessments summarized in Sections 11.2 through 11.6 and Section 11.8.

11.12.2 Claims, Arguments and Evidence

This section presents the key claims, arguments and underlying evidence made in relation to combinations of internal hazards with the potential to impair safe shutdown.

11.12.2.1 High Level Claims

SSCs important for nuclear safety must be protected from dynamic and environmental effects within the plant, including those of internal hazards. An internal hazard could cause a Postulated Initiating Event (PIE) and potentially lead to an accident condition. In response to a PIE, Class 1 SSC may be required to return the reactor to a safe shutdown state. Depending on the nature of the transient, there are a number of actions required to shut the reactor down. Availability of the Class 1 SSCs required delivering the Category A safety functions will ensure that the reactor can be safely shutdown, and is the basis of the following high level claim:

Claim IH-11.0: **Postulated combinations of internal hazards within the design basis will not prevent the delivery of the Category A safety functions and the supporting post-72 hour Category B safety functions necessary to respond to the postulated event.**

[21] A more severe hazard combination is one which results in more severe consequences than those previously assessed, for example where the primary internal hazard initiates multiple flood sources leading to a higher flood elevation than that previously assessed.

The SSCs claimed to provide post-72 hour support functions include only offsite procured SSCs and their associated Class 1 connections.

The assessment of combined internal hazards has, as a basis, used the output from each of the individually assessed internal hazards. The assessment has therefore also taken cognisance of the SSC claimed to prevent, protect or mitigate the individual internal hazard progression, for each individual internal hazard (for example the Class 1 fire barriers which are claimed to protect redundant Divisions of Class 1 SSC from the spread of fire). These individual claims have not been repeated here. This assessment has shown that combinations of internal hazards:

- Do not invalidate the claims made for individual internal hazards;
- Do not result in damage to all Divisions of Class 1 SSC delivering Category A safety functions such that the ability to safely shutdown the reactor is maintained.

There are therefore no claims, arguments or evidence made specifically in regard to combinations of internal hazards.

11.12.3 Safety Case Summary

11.12.3.1 Introduction and Overview

The safety design approach adopted for internal hazards is based on hazards not preventing delivery of the Category A safety functions as necessary to respond to a postulated initiating event. Preservation of the required safety functions has ensured alignment with the fault studies and structural integrity analysis. It is however conceivable that the combined effects of one (or more) internal hazards may be present simultaneously or sequentially. In order to maintain alignment with the fault studies and structural analysis, credible combinations of internal hazards have been assessed to evaluate their cumulative effects on the plant.

Throughout the AP1000 plant, a combination of measures designed to prevent, protect and mitigate the consequences of internal hazards ensures that the Category A safety functions can continue to be delivered and, as such, reduces risk to a level which is ALARP.

11.12.3.2 Applicable Codes and Standards

There are no design codes or standards specific to the assessment of combined hazards. The design codes and standards as applicable to each of the individual internal hazards remain applicable to the assessment of combined hazards.

11.12.3.3 Redundancy, Separation and Segregation

There are no new redundancy, separation or segregation design features specific to the assessment of combined hazards. The design features of redundancy, separation and segregation to each of the individual internal hazards remain applicable to the assessment of combined hazards.

11.12.3.4 Assessment Approach

11.12.3.4.1 Identification of Credible Combinations

The approach adopted for assessing the combined effects of internal hazards is broadly similar whether the combination is consequential, correlated or independent.

The following sub-sections discuss the methodology used to determine whether or not combinations of internal hazards are credible and as such require consideration as part of this assessment.

Consequential Internal Hazards

In order to determine whether an internal hazard could initiate another internal hazard, a review was undertaken using technical experts and key contributors to the assessment of individual internal hazards to establish the root causes and contributing factors leading to initiation of the internal hazards (Reference 11.135). The expert panel review considered the following:

- The unacceptable performance of plant or equipment which could give rise to an internal hazard (e.g. mechanical failure of hoist ropes leading to a dropped load);
- The conditions which must exist for the unacceptable performance to be realised (e.g. stress or fatigue of hoist ropes);
- Whether the existence of an internal hazard could give rise to the conditions necessary to cause unacceptable performance of plant or equipment.

The output from the review identified root causes of internal hazards and, where applicable, those internal hazards which provide the necessary conditions for the root cause.

Although a secondary internal hazard could credibly be initiated as a consequence of a primary internal hazard, not all primary internal hazards will prevail in those rooms or areas where plant/ equipment giving rise to the secondary internal hazard are present. rooms or areas in which either the plant or equipment, whose unacceptable performance could give rise to an internal hazard, or conditions necessary for the primary internal hazard to trigger the unacceptable performance do not exist, are screened as potential locations for consequential internal hazards.

Correlated Internal Hazards

Correlated internal hazards are assumed to arise where the root cause is a common initiator to the unacceptable performance of multiple items of plant and equipment. In contrast to consequential internal hazards, for which the initiator is local, correlated internal hazards may arise where the root cause is experienced globally. In such situations, the result may be that the same internal hazard is initiated in more than one area of the plant.

Independent Internal Hazards

Independent internal hazards are assessed where two (or more) completely independent internal hazards (i.e. where there is no common cause or mode for hazard initiation) occur (or for which the effects persist) at the same time.

Independent internal hazards have been assessed as within the design basis where the best estimate initiating event frequency for the two (or more) hazards is greater than 1.0 E-5/reactor year. Combinations of internal hazards with an initiating event frequency less than 1.0 E-5/reactor year are either considered for cliff edge effects or screened from further consideration where the combined initiating event frequency is less than the BSO benchmark. The effects of the internal hazards are assumed to exist until such time as the post event recovery period is complete[22].

Assessment of Credible Combinations

Where a mechanism has been identified to link two (or more) internal hazards, a room-by-room analysis has been undertaken (Reference 11.75) identify locations where the two internal hazards and associated mechanism exist. Where this is the case, the combination of internal hazards has been subject to detailed assessment.

The consequences of combinations of internal hazards are based on the combined effects of the individual hazards. The effects of the individual internal hazards are taken from the respective hazard schedules. Unless one of the internal hazards causes the loss of SSC provided to prevent, protect or mitigate the internal hazard progression, the effect of each individual internal hazard is taken as the fully mitigated consequences.

11.12.3.4.2 Assessment and Screening for Consequential Internal Hazards

Deterministic links have been identified between internal hazards as follows:

- An internal fire may be initiated by internal flooding, missiles or dropped loads;
- An internal flood may be initiated by internal missiles, dropped loads or pressure part failure[23];
- An internal missile may be initiated by internal fire, flooding or dropped loads;
- A dropped load may be initiated by internal missiles or pressure part failure;
- An internal explosion may be initiated by internal fire, flooding, missiles, dropped loads or pressure part failure;
- A pressure part failure may be initiated by internal missiles or a dropped load.

Mechanisms as possible causes for initiating internal hazards associated with onsite transport, biological fouling, toxic, corrosive or flammable chemicals and electromagnetic interference have not been identified on the basis that these internal hazards do not result in loss or damage of Class 1 SSC and as such their contribution to combinations of internal hazards is of no consequence.

A summary of the credible consequential internal hazards is presented in

Table 11.12-1.

---

[22] The post event recovery period is the duration from hazard initiation until the plant is returned to its normal state either by repairing or replacing the affected SSC.

[23] Pressure part failure is also a source of flooding in its own right.

11.12.3.4.3 Assessment and Screening for Correlated Internal Hazards

External hazards, as described in Chapter 12, have been considered as potential causes of correlated internal hazards. Each of the external hazards has been evaluated for the potential to initiate internal hazards; with the exception of earthquake, the plant or equipment giving rise to the internal hazard is located within the NI and, as such, is protected from the effects of the external hazards by the exterior walls of the NI. Therefore, earthquake is the only common cause of correlated internal hazards as summarised in Table 11.12-2. It is conservatively assumed that all non-seismic components may fail due to the earthquake.

11.12.3.4.4 Assessment for Independent Internal Hazards

Although not explicitly derived, the majority of internal hazards are considered to be infrequent faults with an initiating frequency of 1.0 E-4/reactor year or less. As a result, having two of these events occur as independent events at the same time would be less than 1.0 E-8/reactor year, which is below the cut-off frequency for explicit assessment within the design.

The one hazard that is more frequent is internal fires; the initiating event frequency for internal fires is informed from operating plant experience to be about 2.0 E-1/reactor year (summation of mean values in Table 4-4 from NUREG-2169 [Reference 11.13611.136]). The effect of internal fires has been considered within the PSA (see chapter 10) in terms of core damage frequency. The assessment shows that, under such conditions, the core damage frequency is below the BSL.

On this basis, it has not been considered credible that two independent internal hazards could occur together. The consequences of combinations of independent internal hazards have therefore not been explicitly assessed.

11.12.3.5 Conclusions

The purpose of assessing combinations of internal hazards has been to determine the response of the plant to combinations of internal hazards and in doing so validate the ability to safely shut down, in response to design basis plant level faults. The assessment has been undertaken in a conservative manner, assessing combinations of hazards in a deterministic fashion and as such, explores the sensitivity of the plant to withstand the individual internal hazards.

The individual internal hazard assessments have been performed on a deterministic basis. These assessments conclude that the Category A safety functions will be available to provide a safe shutdown following the worst case postulated internal hazard initiating event. In the unlikely event that the Class 1 SSCs fail for some unrelated reason, the Category A safety function would, for the less severe events, be maintained by other, additional and redundant, Class 2 SSCs.

The individual internal hazard assessments consider the plant response to discrete hazards, whereas this report analyses the possible combination of internal hazards (consequential and concurrent) that could occur. The analysis of combinations of internal hazards has used the same deterministic basis to demonstrate that the conclusions of the discrete analyses (that the Category A safety functions will be available to provide a safe shutdown following the worst case postulated internal hazard initiating event) remain valid and that there is a significant design margin of the AP1000 against design basis internal hazards.

On the basis that the AP1000 design has been shown to be ALARP for each of the individual internal hazards, and given that there are no combinations of internal hazards which the plant cannot tolerate, it is judged that the AP1000 design is also ALARP from a combined hazards perspective.

11.12.4 Combined Hazards Analysis and Assessment

11.12.4.1 Assessment of Consequential Internal Hazards

Consequential Hazards Initiated by Internal Fire

A postulated internal fire scenario could consequentially initiate an internal missile due to shorting of electrical equipment. Such a missile would arise from rotating equipment, such as pumps, and the source is assumed to generate multiple missiles. While the effects of a missile are bounded by those of an internal fire, both of which place a claim on internal walls to protect redundant divisions of Class 1 SSC, a missile could consequentially initiate internal flooding which would progress beyond the physical boundary of a room or area.

The combined consequences of internal fires, missiles and flooding do not result in the loss of all divisions of Class 1 SSCs delivering Category A safety functions such that there remains sufficient Class 1 SSCs to safely shut down the plant in response to a plant fault. The only exception to this is a fire in 1250 AF 01 which could consequentially result in the DWS, FPS and VWS source terms being released in room 12501. During all modes, the flooding is no more onerous than that described by flooding scenario FL16.

Internal fire could also initiate an internal explosion; however, should the internal fire result in the direct release of flammable material it would be expected to burn in the presence of a direct heat source rather than generate an explosive atmosphere. The exception to this is an internal fire which damages or disables the HVAC servicing the battery rooms. In such a scenario, the loss of HVAC would be detected by the low exhaust flow sensors while the presence of hydrogen in the battery rooms would be detected by the hydrogen detectors. Both measures are claimed in the assessment of Internal Explosions (see Section 11.5) as preventative measures and as such the possibility of an internal explosion is precluded.

Consequential Hazards Initiated by Internal Flooding

Internal flooding is a potential initiator for fire, missiles and explosions.

A postulated internal flooding scenario could consequentially initiate an internal fire where the flooding affects high voltage electrical equipment. The only high voltage systems are associated with the RCP and CVS pumps; however the cables and junction boxes are qualified for a submerged environment and would therefore not initiate an arc flash.

Internal missiles could potentially arise where the maximum flood height comes into contact with rotating equipment leading to an over speed of the motor. It is noted that shorting out such rotating equipment due to flooding would more likely simply shutdown such equipment. However, given that redundant divisions of Class 1 SSC are protected from the consequences of missiles by internal walls and floors, the combined effects of internal flooding and missiles would only be more onerous than the flooding itself where the missile is initiated in a room containing Class 1 SSC. Of all the type II rooms containing rotating equipment, only rooms 12162, 12163 and 12306 have a flood height sufficient to submerge rotating equipment, the combined effects of which are as follows:

- Flooding scenario FL21 would completely submerge rooms 12162, 12163. The additional hazard presented by an internal missile is therefore bounded by the flooding event and there are no combined consequences.

- Flooding scenario FL11 could generate a missile in room 12306. A missile in room 12306 would be more onerous than the assessed bounding internal flood; however, it would still be bounded by an Internal Fire (scenario Fire 26; Reference 11.73) which results in total burnout of the room. Therefore, based on evaluation, the combined consequences are tolerable.

An internal explosion could occur where flooding affects the HVAC system serving the battery rooms. However, the formation of a flammable atmosphere is prevented by SSC which would remain unaffected by the flooding (Section 11.3).

Consequential Hazards Initiated by Pressure Part Failure

An internal Pressure Part Failure could consequentially initiate Internal Flooding. However, it is reasoned that Pressure Part Failure and Internal Flooding are mutually-inclusive events rather than consequential. The essential SSCs within the room which are required to function following a Pressure Part Failure are either protected from the dynamic effects, and/ or qualified for the environmental effects, of Pressure Part Failure (see Section 11.4). Similarly, the essential SSCs in the room which may be exposed to Internal Flooding are either above the maximum flood height or qualified for submergence (see Section 11.3). On this basis, detailed analysis of the combined effects of Pressure Part Failure and Internal Flooding is not warranted.

A pressure part failure is also a potential initiator for dropped loads and internal explosions. However, there are no pressure part failures with the potential to impact lifting equipment and therefore a subsequent dropped load is not credible. Similarly, a pressure part failure could result in the release of flammable material; however, the assessment of internal explosions (see Section 11.5) concludes that it is not possible to generate an explosive atmosphere due to the preventative measures identified.

Internal Hazards Initiated by Internal Explosions

Internal explosions are prevented within the NI (see Section 11.5). On this basis it is not possible for an explosion to be the initiator for combined consequential internal hazards.

Internal Hazards Initiated by Internal Missiles

An internal missile could initiate internal flooding and/or a pressure part failure. Missiles originating from high energy systems or rotating equipment may generate multiple missile sources which in turn could initiate a number of flooding sources. Whereas, low or moderate energy systems will only initiate a single missile source which can initiate at most a single other flooding source[24]. Where the missile source originates in a Type III room, the consequential effects will be those associated with flooding, while a missile in a Type II room will have the combined consequential effects of a missile and the associated flooding source(s). The consequential flooding is bounded by that which is assessed in the Internal Flooding Topic Report (Reference 11.76), with the following exceptions:

[24] The missile source could be, for example, a valve stem, which will itself constitute a source of flooding.

- A failure of the SFS pump in room 12272 could impact the FPS, CCS, SFS, WLS, WSS and CVS lines. The total source volume for this fault exceeds that described by flooding scenario FL21. This scenario places a claim on operator action to isolate sources of flooding in response to alarms in the MCR triggered by redundant flood level sensors located in room 12154. The additional source inventory associated with this fault would not significantly reduce the response time and as such the claim made with regards to FL21 is considered to remain valid for this fault.

- A missile generated within room 12501 could result in additional sources of flooding being initiated to that which is described by flooding scenario FL16. However, when the FPS is serviced by the PCCWST, the maximum flood height on level 1 does not exceed 17.8 cm (7 in), which is below the critical flood height on this level.

- A missile generated within rooms 12306, 12405 or 12505 could result in a larger source volume than that described by flooding scenarios FL11, FL14 or FL17, respectively. However, these rooms communicate directly with the Turbine Building 1st bay and flooding would therefore be restricted to the room of inception which is bounded by the effects of the initiating missile (i.e. total loss of all SSC in the room).

In all other rooms, the missile initiated flooding is bounded by the assessment undertaken for internal flooding (see Section 11.3).

In all cases, redundant Class 1 SSC is either located in a room that is not affected by the consequential flooding hazard or (in the case of some in-Containment SSCs) are qualified to continue to perform their safety function when submerged. It is demonstrated, therefore, that the consequential flooding hazards do not compromise the claimed redundancy against missile damage for Category A safety functions.

Furthermore a missile could initiate a dropped load. However the effects of a dropped load, which could damage SSC in multiple rooms, will bound those of a missile hazard, which is assumed to only damage SSC within a single room. The assessment of consequential hazards initiated by a dropped load (see Section 11.8) is therefore bounding.

A missile could also initiate, or be the precursor to, pressure part failure. The effects of both missiles and pressure part failure are restricted to the room identified as the source location based on claims made on the civil structure (see Sections 11.4 and 11.6). The effects of a missile will bound those of pressure part failure on the basis that the missile hazard will result in the damage/ loss of all SSCs present in the room and the combined effects of missiles and pressure part failure are no more onerous than those of missiles alone (see Section 11.6).

Consequential Hazards Initiated by a Dropped Load

A dropped load is assumed to consequentially initiate an internal flood and/or pressure part failure where the dropped load damages pipework. However, the effects of pressure part failure are confined to the room in which the hazard initiates and are therefore bounded by a dropped load which assumes complete loss of all SSC in the affected room(s), regardless of the dropped load footprint.

Within Containment, all Class 1 SSC required for safe shutdown are qualified for the effects of flooding (see Section 11.3). A dropped load within Containment cannot result in the loss of all divisions of Class 1 SSC (see Section 11.8), therefore the combined effects of a dropped load and flooding within Containment are bounded by the effects of a dropped load.

Within the RCA of the Auxiliary Building, a dropped load could initiate a flooding event which is more onerous than that described by flooding scenario FL21. However, the additional sources are not significant and, as such, the claims made for internal flooding (see Section 11.3) remain valid. The combined effects of a dropped load from the cask handling crane and flooding, as described by FL21, do not result in the loss of all divisions of Class 1 SSC delivering a Category A safety function.

In the non-RCA side of the Auxiliary Building, the only lifting equipment are the MSIV monorail hoists. A dropped load in the MSIV compartments may potentially impact the pipework in this area and the rooms below. The MSIV monorail hoists are only operated during an outage (i.e. during plant modes 5 & 6) when the fluid systems located within the MSIV compartments are isolated and the bounding flood event for the MSIV rooms, as described by flooding scenario FL13 (see Section 11.3), would not be realised. However, a drop from the MSIV hoist in room 12404 during mode 5 or 6 operations may potentially impact the FPS piping in room 12300 before impacting Division B of the IDS batteries in 12104. The potential flood source term associated with the FPS during all modes is no more onerous than that already defined in FL09. While a dropped load in room 12404 could therefore result in the loss of Division B of the IDS batteries, there would remain Divisions A, C & D of the IDS batteries to deliver the Category A safety functions.

11.12.4.2 Assessment of Correlated Internal Hazards

The only reasonable means by which correlated internal hazards could be initiated is through a significant seismic event. All non-seismically qualified SSC are assumed to potentially fail and where these SSC are the sources of internal hazards (e.g. flooding from pipework rupture), the internal hazard is assumed to arise. Furthermore, the correlated internal hazards may initiate consequential internal hazards.

In the detailed analysis, each of the internal hazards has been evaluated in turn to derive the consequences of correlated hazard initiation; this detailed analysis concludes:

- Within Containment, non-seismically qualified pipework may fail but the subsequent flooding would be bounded by the analysis undertaken as part of the flooding assessment (see Section 11.3). All other sources of internal hazards or consequential internal hazards are qualified for both seismic and flooding and as such the correlated internal hazard is no more onerous than that already assessed.

- Within the Auxiliary Building RCA, a number of flooding sources are non-seismically qualified and could potentially result in flooding. In addition, there are three non-seismically qualified lifting devices which may result in a dropped load. However, given the infrequent use of these devices, and the low probability of a seismic event, this contribution to a combined dropped load / flooding scenario would logically be characterized as very small. The dropped load could potentially result in consequential flooding due to impact with additional flooding source terms, while flooding has the potential to initiate internal missiles.

- Within the Auxiliary Building non-RCA, the only significant source of flooding is potentially from the non-seismically qualified PWS; however, the MSIV monorail hoists are also non-seismically qualified and could lead to a dropped load. During use of the MSIV hoists (plant modes 5&6 only), the potential flooding source terms which may be impacted are isolated with the exception of the FPS. All four divisions of the IDS batteries could potentially be affected by the subsequent flooding, however the flood-up level sensor (see Section 11.3), which is seismically qualified, would alert operators to the flooding and prompt isolation.

Although a seismic event has the potential to initiate a number of internal hazards at a number of locations, their combined effect does not result in the loss of all divisions of Class 1 SSC delivering a Category A safety function (i.e. there remain redundant divisions which are unaffected by the totality of the hazard).

11.12.4.3 Hazards Schedule

The Combined Hazards Schedule (Table 11.12-3) has been prepared based on the results of the Combined Consequence Analysis. The hazard schedule is presented in tabular form and combines the bounding primary hazard and bounding consequential hazards into each schedule entry. The schedule presents, for each combination of internal hazards, the:

- SSCs affected by the combination of internal hazards;
- Category A safety function at risk;
- Unmitigated consequences should the plant equipment be unable to support safe shutdown;
- Redundant SSC available to deliver the Category A safety function, which has not been exposed to the same internal hazard combination.

The schedule is presented in two main sections:

- The first presents the primary and consequential internal hazards resulting from internal fire, internal flooding, internal dropped loads and internal missiles.
- The second presents the correlated internal hazards (i.e. hazards that can occur concurrently) during or immediately following a seismic event.

To simplify the presentation of correlated internal hazards, dropped load hazards are not tabulated where the dropped load cannot directly impact a Class 1 SSC. Secondary flooding hazards as a consequence of impacts on piping and vessels are, however, included in the schedule.

The combined hazards schedule does not present any consequential internal hazards associated with Pressure Part Failure (PPF). The PPF safety case is made on the basis that the SSC lost/damaged are either not essential or if they are then they are protected from the dynamic effects of PPF and qualified for the subsequent environmental effects in the room.

Depending on the failure mode for the pressure part it may be a source of internal flooding only, or a source of both internal flooding and internal missiles. The assessment of internal missiles (Section 11.6) has assessed the effects of internal missiles resulting from PPF and conservatively assumes that SSCs in the room will be lost or damaged. The internal flooding assessment (Section 11.3) has included PPF as a source of internal flood hazards. Internal flooding within the room in which the PPF occurs will have no additional consequences compared to the assumption that all SSCs in the room are lost.

The consequential flooding will however migrate to other areas of the plant. The combined effects of PPF and flooding in other areas of the NPP are therefore bounded by the internal flooding analysis, which shows acceptability, in terms of Class 1 SSC redundancy, to either lose SSCs located below the maximum flood height or credit SSCs as qualified for the flooded environment.

11.12.5 Conclusions and Discussion

The purpose of the combined hazards assessment has been to assess the response of the AP1000 plant to combinations of internal hazards and, in doing so, validate the ability to safely shut down in response to design basis plant level faults. This assessment has been undertaken in a conservative manner, assessing combinations of hazards in a deterministic fashion and as such, exploring the sensitivity of the plant to withstand combinations of individual internal hazards.

Deterministic analyses of postulated, design basis, internal hazards have been performed (Sections 11.2 to 11.6 and 11.8). These analyses show that the Category A safety functions will be available to provide a safe shutdown following the worst case postulated internal hazard initiating event.

The analysis of combined hazards demonstrates that the conclusions of the discrete analyses of individual internal hazards are substantiated in that the Category A safety functions are available to provide a safe shutdown following the worst case combined internal hazard initiating event. The individual internal hazard analyses have been shown to remain valid and that there exists a significant design margin against design basis internal hazards.

On the basis that the AP1000 design has been shown to be ALARP for each of the individual internal hazards, and given that there are no combinations of internal hazards which the plant cannot tolerate, it is judged that the AP1000 design is also ALARP from a combined hazards perspective.

11.13 Conclusions

The following internal hazards that have the potential to affect the safety of the AP1000 plant have been identified:

- Internal Fire;
- Internal Flooding;
- Internal Missiles;
- Internal Explosion;
- Pressure Part Failure;
- Dropped Loads;

- Toxic, corrosive and flammable materials;
- On-site transport;
- Biological Material;
- Electromagnetic Interference.

Additionally, credible combinations of internal hazards have been identified and their effects analysed.

Each hazard, or credible combination of, has been assessed for its potential to challenge the high level claim and, where necessary, further Sub-Claims, supported by arguments and evidence, have been made to ensure that the high level claim is not compromised.

The assessment has shown that the Class 1 SSCs delivering the Category A safety functions are adequately protected from internal hazards such that if one division is lost, the safety function can still be delivered. Protection from internal hazards of Class 2 SSCs delivering Category A safety functions and providing defence in depth and Class 2 SSCs delivering supporting Category B safety functions have also been assessed, where appropriate.

Where an internal hazard also has the potential to initiate an internal fault, this has been identified with an appropriate link to the fault schedule in each of the relevant hazard schedule(s). Analysis and assessments have established to high degree of reliability that there are no internal hazards which can both initiate a plant level fault (including impacts on the spent fuel storage) and result in the loss of all divisions of Class 1 SSC (or Class 2 SSC as appropriate) delivering Category A safety functions claimed in response to the PIE.

The assessment has considered the potential for there to be a single failure in active components and shown that there remains sufficient division of redundancy to deliver the Category A safety function.

Sensitivity analysis has been undertaken for each of the internal hazards, confirming that there are no cliff edge effects. The assumptions used throughout the assessment are conservative; a small change in these assumptions does not lead to a significant increase in the hazard.

The assessments covering each of the systematically-identified internal hazards in this chapter conclude that the high level, prevention, protection, and mitigation claims and arguments have been validated, and therefore that the AP1000 design is robust, being tolerant to faults arising from internal hazards, and that the designed safety measures are effective.

11.14 References

11.1 Westinghouse Report UKP-GW-GLR-115, Rev. 0, "AP1000 Identification of Internal Hazards," October 2016. This reference was formerly identified as: "Serco PGEN/E.004067/02/01/094, Rev. 0, "AP 1000 Identification of Internal Hazards", Wheeler FA, August 2010".

11.2 Westinghouse Document APP-1200-ARX-001, Rev. 1, "List of AP1000 Auxiliary Building Room Numbers," January 2013.

11.3 Westinghouse Report UKP-GW-GL-060, Rev. 10, "AP1000 Design Reference Point for UK GDA," January 2017.

11.4 BS9999:2008, "Code of Practice for the Fire Safety in the Design, Management and Use of Buildings," October 2008.

11.5 BS EN 13501-1:2002, "Fire Classification of Construction Products and Building Elements; Classification Using Test Data From Reaction To Fire Tests," March 2002.

11.6 BS 476-6, "Fire Tests on Building Materials and Structures. Method of Test for Fire Propagation for Products," March 1989.

11.7 BS 476-7:1997, "Fire Tests on Building Materials and Structures. Method of Test to Determine the Classification of the Surface Spread of Flame of Products," January 1997.

11.8 Westinghouse Report APP-GW-N4C-003, Rev. F, "Fire Protection Analysis Combustible Loading and Fire Severity," May 2014.

11.9 Westinghouse Report UKP-1000-GEC-004, Rev. 1, "AP1000 Barrier Matrix," January 2017.

11.10 Westinghouse Report UKP-GW-AF-101, Rev. 0, "AP1000 Plant Fire Resistance Rating Report for Nuclear Island Reinforced Concrete Structures," March 2016.

11.11 BS EN 1992-1-2:2004, "Eurocode 2: Design of Concrete Structures – Part 1-2: General rules – Structural fire design," July 2008.

11.12 Westinghouse Report UKP-GW-GL-123, Rev. 0, "Heat Transfer Analysis of SC Walls and Floors in a Three-Hour Standard Fire," March 2016.

11.13 Westinghouse Document CPP-AB01-Z0X-002, Rev. 3, "Design Specification – Penetrations Seal Schedule for Containment, Shield and Auxiliary Buildings," December 2015.

11.14 Westinghouse Report UKP-GW-GLR-118, Rev. 0, "UK AP1000: Review of Claims for Internal Fires within Containment," November 2016.

11.15 Westinghouse Document APP-AB01-Z0-001, Rev. 5, "Design Specification: Blockouts and Barriers (Penetrations, Seals and Fire Stops," December 2015.

11.16 BS EN 1366-3, "Fire resistance tests for service installations Part 3: Penetration seals," March 2009.

11.17 Westinghouse Report UKP-GW-AF-001, Rev. 1, "AP1000 Fire Protection Dampers – UK Compliance Report," August 2016.

11.18 ISO 10294-1:1996+A1:2014, "Fire Resistance tests – Fire Dampers for Air Distribution Systems – Part 1: Test method," May 1997.

11.19 BS EN 1366-2, "Fire resistance tests for service installations Part 2: Fire dampers," June 2015.

11.20 BS 476: Part 24, Fire Tests on Building Materials and Structures Part 24: Method for Determination of the Fire Resistance of Ventilation Ducts," May 1987.

11.21 IAEA NS-R-1, "Safety of Nuclear Power Plants," October 2000.

11.22 NUREG-0800, U. S. Nuclear Regulatory Commission Standard Review Plan, Section 9.5.1, "Fire Protection Program," Rev. 3, July 1981, including Branch Technical Position (BTP) CMEB 9.5-1, "Guidelines for Fire Protection for Nuclear Power Plants," Rev. 2, July 1981.

11.23 IAEA NS-G-1.7, "Protection against Internal Fires and Explosions in the Design of Nuclear Power Plants," September 2004.

11.24 IAEA NS-G-2.1, "Fire Safety in the Operation of Nuclear Power Plants," September 2000.

11.25 Westinghouse Report UKP-GW-GL-045, Rev. 2, "AP1000 Equivalence/Maturity Study of U.S. Codes and Standards," September 2011.

11.26 Westinghouse Report UKP-GW-GL-044, Rev. 1, "AP1000 UK Safety Categorisation and Classification Methodology," April 2010.

11.27 Not Used.

11.28 Not Used.

11.29 Not Used.

11.30 Not Used

11.31 Not Used.

11.32 Not Used.

11.33 NFPA 804, "Standard for Fire Protection for Advanced Light Water Reactor Electric Generating Plants," 2010.

11.34 Not Used.

11.35 Not Used.

11.36 Not Used.

11.37 IEEE 1202, "Standard for Flame-Propagation Testing of Wire and Cable," June 2006.

11.38 IEEE 383, "Qualifying Class 1E Electric Cables and Field Splices for Nuclear Power Generating Stations," December 2003.

11.39 NEMA VE-1:2009, "Metal Cable Systems," October 2009.

11.40 NEMA VE-2:2006, "Cable Tray Installation Guidelines," October 2006.

11.41 IEEE 628, "Raceway Standard Criteria for the Design, Installation, and Qualification of Raceway Systems for Class 1E Circuits for Nuclear Power Generating Stations," January 2001.

11.42 IEEE 422, "Guide for the Design and Installation of Cable Systems in Power Generating Stations," 1986.

11.43 BS EN 1991-1-2, "Actions on Structures Exposed to Fire," November 2002.

11.44 BS 476-31.1, "Fire tests on building materials and structures. Methods for measuring smoke penetration through door sets and shutter assemblies. Method of measurement under ambient temperature condition," October 1983.

11.45 ACI-216.1, "Code Requirements for Determining Fire Resistance of Concrete and Masonry Construction Assemblies", January 2014.

11.46 LPS 1056, Issue 3, "Tests and Evaluation Requirements for the LPCB Approved Listing of Fire Door sets, Lift Landing Doors and Shutters," August 1989.

11.47 Not Used.

11.48 ASFP Grey Book, "Fire and Smoke Resisting Dampers," 1st Edition, April 2007.

11.49 ASFP Red Book, "Fire Stopping; Linear Joint Seals, Penetration Seals & Small Cavity Barriers," 3rd Edition, December 2009.

11.50 ASFP Blue Book, "Fire Resisting Ductwork," 2nd Edition, January 2009.

11.51 Westinghouse Report APP-GW-J1R-008, Rev. 0, "Safety Criteria for the AP1000 Instrumentation and Control Systems," August 2007.

11.52 Westinghouse Report APP-GW-J1R-004, Rev. 7, "AP1000 Instrumentation and Control Defence-in-Depth and Diversity Report," November 2015.

11.53 Not Used.

11.54 BS 5839-1:2002+A2:2008, "Fire Detection and Fire Alarm Systems for Buildings. Code of Practice for System Design, Installation, Commissioning and Maintenance." October 2002.

11.55 Loss Prevention Council. LPS 1014, "Requirements for Certificated Fire Detection and Alarm System Firms," May 2002.

11.56 Westinghouse Report APP-FPS-G1R-002, Rev. 1, "AP1000 Fire Induced Multiple Spurious Actuation Report," February 2009.

11.57 NRC Generic Letter 81-12, "Fire Protection Rule," February 1981.

11.58 Westinghouse Report APP-GW-N4R-003, Rev. H, "Fire Protection Analysis Report," July 2014.

11.59 Westinghouse Report UKP-GW-GL-144, Rev. 3, "AP1000 UK Safety Categorisation and Classification of Systems, Structures, and Components," January 2017.

11.60 Westinghouse Report APP-GW-G1-002, Rev. 4, "AP1000 Equipment Qualification Methodology," September 2014.

11.61 Westinghouse Report APP-GW-VP-030, Rev. 5 "AP1000 Environmental Conditions (for Equipment Qualification)," January 2015.

11.62 Not Used.

11.63 Not Used.

11.64 Westinghouse Report APP-GW-M1-002, Rev. 0, "AP1000 Fire Protection Design Criteria and Guidelines," November 2009.

11.65 Not Used.

11.66 Not Used.

11.67 Not Used.

11.68 Not Used.

11.69 Westinghouse Report APP-PRA-GSC-379, Rev. D, "AP1000® Fire Modeling Assessment of Wall Exposure Temperature Profiles for Select Rooms," December 2016.

11.70 NUREG-1805, Fire Dynamics Tools (FDTs) Quantitative Fire Hazard Analysis Methods for the U.S. Nuclear Regulatory Commission Fire Protection Inspection Program, December 2004, U.S. Nuclear Regulatory Commission, Washington, D.C.

11.71 Westinghouse Document APP-FPS-M6-001 through APP-FPS-M6-011, Various Revisions, "Piping and Instrument Diagrams: Fire Protection System," October 2015.

11.72 Westinghouse Report UKP-GW-GLR-004, Rev. 3, "AP1000 UK Structural Integrity Classification," January 2017.

11.73 Westinghouse Report UKP-GW-GLR-111, Rev. 1, "UK AP1000 Internal Hazards Topic Report – Fire Protection," January 2017.

11.74 Westinghouse letter to file, DCP_DCP_007935, Rev. 0, "AP1000 Hazard Barrier Classification for the United Kingdom GDA Assessment," April 2016.

11.75 Westinghouse Report UKP-GW-GLR-036, Rev. 0, "UK AP1000 Internal Hazards–Combined Hazards Topic Report," August 2016.

11.76 Westinghouse Report UKP-GW-GLR-107, Rev. 1, "UK AP1000 Internal Hazards–Flooding Topic Report," January 2017.

11.77 Westinghouse Report UKP-GW-GLR-114, Rev. 1, "Internal Hazards Topic Report – Pressure Part Failure," January 2017.

11.78 Westinghouse Report APP-GW-N1-007, Rev. 5, "AP1000 Design Criteria for Protection from Flooding," December 2015.

11.79 IEEE 344-1987, "IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations," 1987.

11.80 Westinghouse Document APP-AY20-Z0-003, Rev. 1, "Design Specification for MSIV Compartment Lower Relief Panels" November 2016.

11.81 Westinghouse Report APP-GW-N1-001, Rev. 5, "Pipe Rupture Protection Design Criteria for the AP1000 Plant," April 2015.

11.82 IAEA NS-G-1.11, "Protection against Internal Hazards other than Fires and Explosions in the Design of Nuclear Power Plants," September 2004.

11.83 ONR Technical Assessment Guide, NS-TAST-GD-011, Rev. 2, "The Single Failure Criterion," May 2015.

11.84 ANSI/ANS Standard 58.2-1988, "Design Basis for Protection Light Water Nuclear Power Plants Against the Effects of Postulated Pipe Rupture".

11.85 ANSI/ANS Standard 56.11-1988, "Design Criteria for Protection Against the Effects of Compartment Flooding in Light Water Reactor Plants".

11.86 Not Used.

11.87 EPRI Utility Requirements Document, Rev. 8, "Advanced Light Water Reactor," March 1999.

11.88 US Nuclear Regulatory Commission Branch Technical Position SPLB 3-1, NUREG-0800, Rev. 2, "Plant Design for Protection against Postulated Piping Failures in Fluid Systems Outside Containment." (US NRC ADAMS Accession Number ML052340548)

11.89 Safety Guide No. NS-G-1.11, "Protection against Internal Hazards other than Fires and Explosions in the Design of Nuclear Power Plants," International Atomic Energy Agency, 2004.

11.90 ASME Boiler and Pressure Vessel Code, Section III, "Rules for Construction of Nuclear Power Plant Components," 1998 Edition with 2000 Addenda, The American Society of Mechanical Engineers.

11.91 ASME B31.1, "Power Piping," 1989 Edition with 1989 Addenda, The American Society of Mechanical Engineers.

11.92 Westinghouse Report UKP-GW-GL-500, Rev. 0, "AP1000® UK Limits and Condition Process Description," December 2015.

11.93 Westinghouse Report UKP-GW-GLR-109, Rev. 1, "UK AP1000 Internal Hazards Topic Report – Explosions," January 2017.

11.94 Westinghouse Report UKP-1000-N4C-006, Rev. 0, "UKP AP1000 Hydrogen Explosion Evaluation of Battery Rooms with the Annex and Radwaste Buildings," July 2016.

11.95 Westinghouse Report UKP-GW-M3C-002, Rev. 0, "AP1000 Chemical Explosion Evaluation," July 2016.

11.96 Westinghouse Report UKP-1000-N4C-005, Rev. 0, "AP1000 Hydrogen Gas Explosion Evaluation using TNO MEM," June 2016.

11.97 Westinghouse Report UKP-GW-GL-114, Rev. 0, "AP1000 Auxiliary Building Battery Rooms – Hydrogen Assessment," June 2016.

11.98 BS EN 60079 Part 10-1:2015, "Explosive Atmospheres Part 10-1: Classification of Areas – Explosive Gas Atmospheres".

11.99 Westinghouse Report APP-VBS-GJP-401, Rev. 0, "Alarm Response – Nuclear Island Nonradioactive Ventilation System," July 2014.

11.100 Westinghouse Report UKP-1000-N4C-004, Rev. 0, "UK AP1000 WLS and WGS Hydrogen Assessment," July 2016.

11.101 Westinghouse Report APP-WLS-M3C-041, Rev. 2, "WLS Gas Generation," September 2009.

11.102 US NRC Regulatory Guide 1.91, Rev. 2, "Evaluations of Explosions Postulated to Occur at Nearby Facilities and on Transportation Routes Near Nuclear Power Plants," April 2013.

11.103 Health & Safety Laboratory HSL/2001/04, "Explosion Hazard Assessment: A Study of the Feasibility and Benefits of Extending Current HSE Methodology to Take Account of Blast Sheltering," 2001.

11.104 Westinghouse Document APP-1231-CC-103, Rev. 7, "Auxiliary Building Concrete Outline Area 1 Floor El. 100'-0"," February 2016.

11.105 Westinghouse Report UKP-1000-N4C-002, Rev. 0, "UKP AP1000 Assessment of the Potential for Hydrogen Combustion due to Leakage from Hydrogen Injection Lines in the Auxiliary Building," June 2016.

11.106 Westinghouse Report UKP-1000-N4C-003, Rev. 0, "UKP AP1000 Assessment of the Potential for Hydrogen Combustion due to Leakage from the Hydrogen Injection Line in Containment," June 2016.

11.107 Westinghouse Report APP-GW-C1-001, Rev. 3, "AP1000 Civil/Structural Design Criteria," February 2015.

11.108 Not Used.

11.109 Health and Safety, Statutory Instruments, 2002, No. 2776, "The Dangerous Substances and Explosive Atmospheres Regulations 2002."

11.110 Westinghouse Report UKP-GW-GLR-108, Rev. 1, "UK AP1000 Internal Hazards Topic Report – Internal Missiles," January 2017.

11.111 Westinghouse Report UKP-1000-N4C-001, Rev. 0, "UK AP1000 Nuclear Island Missile Penetration Calculation," April 2016.

11.112 Westinghouse Report UKP-GW-N4C-001, Rev. 0, "UK AP1000 Turbine Missile Assessment," June 2016.

11.113 Westinghouse Report APP-MTS-GSA-021-NP, Rev. 0, "Analysis of the Probability of the Generation of Missiles from Fully Integral Nuclear Low Pressure Turbines," September 2007.

11.114 NUREG Guide 1.115, Rev. 1, "Protection Against Low-Trajectory Turbine Missiles," 1977.

11.115 Hagg, A.C. & Sankey G.O., "The Containment of Disk Burst Fragments by Cylindrical Shells," ASME Paper 73-WA-Pwr-2, 11/73, Journal of Engineering for Power, Trans. of ASME, April 1974, pp. 114-123.

11.116 Not Used.

11.117 Health and Safety Executive, "Control of Major Accident Hazards (COMAH) Regulations 2015, L111, Third Edition," HSE, 2015.

11.118 ANSI/ANS-51.1-1983, "Nuclear Safety Criteria for the Design of Stationary Pressurized Water Reactor Plants".

11.119 NUREG-0800, Rev. 2, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition," September 2009.

11.120 Westinghouse Report UKP-GW-GL-037, Rev. 2, "Applicability of COMAH Regulations to AP1000," December 2016.

11.121 Westinghouse Report UKP-MV01-Z0C-081, Rev. 0, "AP1000 Reactor Vessel Head Drop Evaluation," March 2016.

11.122 Westinghouse Report UKP-FHS-S0C-001, Rev. 0, "UK AP1000 Fuel Assembly Drop Accident Report," July 2016.

11.123 Westinghouse Report UKP-GW-GLR-110, Rev. 1, "UK AP1000 Internal Hazards Topic Report- Dropped Loads," January 2017.

11.124 IEEE 323-1974, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations," 1974.

11.125 Westinghouse Document APP-FHS-M3-001, Rev. 2, "Fuel Handling System Design Specification," October 2014.

11.126 Westinghouse Document APP-MHS-M3-101, Rev. 2, "Mechanical Handling System Design Specification," July 2014.

11.127 ONR Guide, Nuclear Safety Technical Assessment Guide NS-TAST-GD-011, Rev. 2, "The Single Failure Criterion," May 2015.

11.128 Not Used.

11.129 IAEA Safety Standards Series No. TS-R-1, "Regulations for the Safe Transport of Radioactive Material" International Atomic Energy Agency, July 2009.

11.130 Westinghouse Report UKP-GW-GL-062, Rev. 1, "UK AP1000 Electromagnetic Compatibility – Management Philosophy Document," WEC, April 2011.

11.131 UK Statutory Instrument No. 3418, "The Electromagnetic Compatibility Regulations" 2006.

11.132 BS IEC 61513:2001, "Nuclear Power Plants. Instrumentation and Control for Systems Important To Safety. General Requirements for Systems" British Standards Institution, August 2001.

11.133 IEEE 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations" Institute of Electrical and Electronics Engineers, June 1991.

11.134 SSR-2/1, Rev. 1, "IAEA Safety Standards-Safety of Nuclear Power Plants: Design", February 2016.

11.135 Westinghouse Report UKP-GW-N4R-001, Rev. 0, "UKP AP1000 Combined Hazards Assessment Approach Preliminary Design Review," September 2016.

11.136 NUREG-2169 (EPRI 3002002936), "Nuclear Power Plant Fire Ignition Frequency and Non-Suppression Probability Estimation Using the Update Fire Events Database – United States Fire Event Experience through 2009", January 2015

11.137 ONR-GDA-AR-11-001, Rev. 0, "Generic Design Assessment – New Civil Reactor Build – Step 4 Internal Hazards Assessment of the Westinghouse AP1000 Reactor", November 2011.

11.138 ISBN 978-0877658214, "SFPE Handbook of Fire Protection Engineering", National Fire Protection Association, 4th Edition, 2008.

11.139 BS EN 13501-3:2005+A1:2009, "Fire classification of construction products and building elements. Classification using data from fire resistance tests on products and elements used in building service installations: fire resisting ducts and fire dampers", British Standards Institution, January 2006.

11.140 Westinghouse Report GW-A1-001, Rev. 3, "AP600 Architectural Design Criteria," November 1997.

11.141 Westinghouse Report APP-GW-G1-001, Rev. 4, "AP1000 Plant Design Criteria," January 2011.

11.142 Westinghouse Report UKP-1000-N4C-007, Rev. 1, "AP1000 Hydrogen Migration Analysis for CVS Hydrogen Line Break in Selected Rooms of the Auxiliary Building and Containment Building," January 2017.

11.143 Westinghouse Report UKP-1000-N4C-008, Rev. 0, "Unimitigated Explosion Hazard Analysis for AP1000 Division B Battery Room 1 (Room 12104)," January 2017.

11.144 Westinghouse Document APP-VCS-M3-001, Rev. 0, "Containment Recirculation Cooling System (VCS) System Specification Document," August 2012.

11.145 Westinghouse Report APP-GW-N1-004, Rev. 1, "Design Criteria for the Protection from Internally Generated Missiles," November 2008.

1. APP-GW-GEE-5405, Rev. 0, "UK AP1000 Internal Hazards Criteria Changes", November 2016.

11.146 Westinghouse Report APP-GW-M3C-013, Rev. 0, "AP1000 Valve Missile Protection," May 2014.

11.147 Westinghouse Report UKP-GW-GL-200, Rev. 1, "AP1000 Squib Valve Safety Case," December 2016.

Table 11.2-1 Rooms Comprising the Nuclear Island grouped by Fire Area or Fire Zone

Fire Area or Zone	Rooms
1100 AF 11105	11105, 11205
1100 AF 11204	11104, 11204
1100 AF 11206	11206
1100 AF 11207	11207
1100 AF 11208	11208
1100 AF 11209	11209
1100 AF 11300A	11300, 11400
1100 AF 11300B	11300, 11400
1100 AF 11301	11201, 11301, 11401, 11501, 11601, 11701
1100 AF 11302	11202, 11302, 11402, 11502, 11602, 11702
1100 AF 11303	11303, 11304 ,11503
1100 AF 11303A	11603
1100 AF 11303B	11703
1100 AF 11500	11500, 11504, 11306
1200 AF 12341	12341
1200 AF 12541	12541
1250 AF 12555	12555, 12556
1270 AF 12701	12701, S06
1200 AF 01	12241, 12242, 12461, 12362, 12365, 12151, 12153, 12155, 12156, 12158, 12258, 12171, 12152, 12154, 12254, 12354, 12161, 12162, 12166, 12167, 12168, 12169, 12268, 12264, 12265, 12251, 12172, 12255, 12259, 12256, 12269, 12253, 12272, 12273, 12274, 12275, 12252, 12261, 12271, 12262, 12351, 12352, 12363, 12451, 12452, 12454, 12361, 12561, 12553, 12554, 12651
1200 AF 02	12462, 12463 ,12472, 12562, 12563, 12564, 12371, 12374, 12372, 12373, 12471
1220 AF 02	12244
1200 AF 03	12311, 12411
1201 AF 01	S02
1201 AF 02	12104, 12204, 12207, 12304, 12344
1201 AF 03	12105, 12205, 12305, 12345
1201 AF 04	12405, 12505
1201 AF 05	12406, 12506, 12306
1201 AF 06	12404, 12504
1202 AF 01	S01

Table 11.2-1 Rooms Comprising the Nuclear Island grouped by Fire Area or Fire Zone (cont.)

Fire Area or Zone	Rooms
1202 AF 03	12102, 12202, 12203, 12302, 12312, 12313, 12343
1202 AF 04	12101, 12201, 12301
1202 AF 05	S05
1204 AF 01	12163
1204 AF 02	S03
1205 AF 01	S04
1210 AF 01	12111, 12103, 12112, 12113
1220 AF 01	12212, 12213, 12211
1220 AF 02	12244
1230 AF 01	12300
1230 AF 02	12321
1232 AF 01	12303
1240 AF 01	12421
1242 AF 01	12401
1242 AF 02	12412
1243 AF 01	12423
1243 AF 02	12422
1250 AF 01	12501

Table 11.2-2 Internal Fire Hazard Schedule – Nuclear Island

Table 11.2-2 Internal Fire Hazard Schedule – Nuclear Island

Table 11.2-2 Internal Fire Hazard Schedule – Nuclear Island

Table 11.2-2 Internal Fire Hazard Schedule – Nuclear Island

Table 11.2-2 Internal Fire Hazard Schedule – Nuclear Island

Table 11.2-2 Internal Fire Hazard Schedule – Nuclear Island

Table 11.2-2 Internal Fire Hazard Schedule – Nuclear Island

Table 11.2-2 Internal Fire Hazard Schedule – Nuclear Island

Table 11.2-2 Internal Fire Hazard Schedule – Nuclear Island

Table 11.2-2 Internal Fire Hazard Schedule – Nuclear Island

Table 11.2-2 Internal Fire Hazard Schedule – Nuclear Island

Table 11.2-2 Internal Fire Hazard Schedule – Nuclear Island

Table 11.2-2 Internal Fire Hazard Schedule – Nuclear Island

Table 11.2-2 Internal Fire Hazard Schedule – Nuclear Island

Table 11.2-2 Internal Fire Hazard Schedule – Nuclear Island

Table 11.2-2 Internal Fire Hazard Schedule – Nuclear Island

Table 11.2-2 Internal Fire Hazard Schedule – Nuclear Island

Table 11.2-2 Internal Fire Hazard Schedule – Nuclear Island

Table 11.2-3 Internal Fire Hazard Schedule – Non-Nuclear Island

Table 11.2-3 Internal Fire Hazard Schedule – Non-Nuclear Island

Table 11.2-3 Internal Fire Hazard Schedule – Non-Nuclear Island

Table 11.2-3 Internal Fire Hazard Schedule – Non-Nuclear Island

Table 11.2-3 Internal Fire Hazard Schedule – Non-Nuclear Island

Table 11.2-3 Internal Fire Hazard Schedule – Non-Nuclear Island

Table 11.2-3 Internal Fire Hazard Schedule – Non-Nuclear Island

Table 11.2-3 Internal Fire Hazard Schedule – Non-Nuclear Island

Table 11.3-1 Sources of Flooding in the Auxiliary Building – RCA & Non-RCA

Table 11.3-2 Sources of Flooding in the Containment Building

Table 11.3-3 Internal Flooding Hazard Schedule

Table 11.3-3 Internal Flooding Hazard Schedule

Table 11.3-3 Internal Flooding Hazard Schedule

Table 11.3-3 Internal Flooding Hazard Schedule

Table 11.3-3 Internal Flooding Hazard Schedule

Table 11.3-3 Internal Flooding Hazard Schedule

Table 11.3-3 Internal Flooding Hazard Schedule

Table 11.3-3 Internal Flooding Hazard Schedule

Table 11.3-3 Internal Flooding Hazard Schedule

Table 11.3-3 Internal Flooding Hazard Schedule

Table 11.3-3 Internal Flooding Hazard Schedule

Table 11.3-3 Internal Flooding Hazard Schedule

Table 11.3-3 Internal Flooding Hazard Schedule

Table 11.3-3 Internal Flooding Hazard Schedule

Table 11.3-3 Internal Flooding Hazard Schedule

Table 11.3-3 Internal Flooding Hazard Schedule

Table 11.3-3 Internal Flooding Hazard Schedule

Table 11.3-3 Internal Flooding Hazard Schedule

Table 11.3-3 Internal Flooding Hazard Schedule

Table 11.3-3 Internal Flooding Hazard Schedule

Table 11.3-3 Internal Flooding Hazard Schedule

Table 11.4-1 Pressure Part Failure Containment Hazard Schedule

Table 11.4-1 Pressure Part Failure Containment Hazard Schedule (cont.)

Table 11.4-1 Pressure Part Failure Containment Hazard Schedule (cont.)

Table 11.4-1 Pressure Part Failure Containment Hazard Schedule (cont.)

Table 11.4-1 Pressure Part Failure Containment Hazard Schedule (cont.)

Table 11.4-1 Pressure Part Failure Containment Hazard Schedule (cont.)

Table 11.4-1 Pressure Part Failure Containment Hazard Schedule (cont.)

Table 11.4-1 Pressure Part Failure Containment Hazard Schedule (cont.)

Table 11.4-1 Pressure Part Failure Containment Hazard Schedule (cont.)

Table 11.4-1 Pressure Part Failure Containment Hazard Schedule (cont.)

Table 11.4-1 Pressure Part Failure Containment Hazard Schedule (cont.)

Table 11.4-1 Pressure Part Failure Containment Hazard Schedule (cont.)

Table 11.4-1 Pressure Part Failure Containment Hazard Schedule (cont.)

Table 11.4-1 Pressure Part Failure Containment Hazard Schedule (cont.)

Table 11.4-1 Pressure Part Failure Containment Hazard Schedule (cont.)

Table 11.4-1 Pressure Part Failure Containment Hazard Schedule (cont.)

Table 11.4-1 Pressure Part Failure Containment Hazard Schedule (cont.)

Table 11.4-1 Pressure Part Failure Containment Hazard Schedule (cont.)

Table 11.4-1 Pressure Part Failure Containment Hazard Schedule (cont.)

Table 11.4-1 Pressure Part Failure Containment Hazard Schedule (cont.)

Table 11.4-1 Pressure Part Failure Containment Hazard Schedule (cont.)

Table 11.4-1 Pressure Part Failure Containment Hazard Schedule (cont.)

Table 11.4-2 Pressure Part Failure Auxiliary and Shield Building Hazard Schedule

Table 11.4-2 Pressure Part Failure Auxiliary and Shield Building Hazard Schedule (cont.)

Table 11.4-2 Pressure Part Failure Auxiliary and Shield Building Hazard Schedule (cont.)

Table 11.4-2 Pressure Part Failure Auxiliary and Shield Building Hazard Schedule (cont.)

Table 11.4-2 Pressure Part Failure Auxiliary and Shield Building Hazard Schedule (cont.)

Table 11.4-2 Pressure Part Failure Auxiliary and Shield Building Hazard Schedule (cont.)

Table 11.4-2 Pressure Part Failure Auxiliary and Shield Building Hazard Schedule (cont.)

Table 11.4-2 Pressure Part Failure Auxiliary and Shield Building Hazard Schedule (cont.)

Table 11.4-2 Pressure Part Failure Auxiliary and Shield Building Hazard Schedule (cont.)

Table 11.4-2 Pressure Part Failure Auxiliary and Shield Building Hazard Schedule (cont.)

Table 11.4-2 Pressure Part Failure Auxiliary and Shield Building Hazard Schedule (cont.)

Table 11.4-2 Pressure Part Failure Auxiliary and Shield Building Hazard Schedule (cont.)

Table 11.4-2 Pressure Part Failure Auxiliary and Shield Building Hazard Schedule (cont.)

Table 11.4-2 Pressure Part Failure Auxiliary and Shield Building Hazard Schedule (cont.)

Table 11.4-2 Pressure Part Failure Auxiliary and Shield Building Hazard Schedule (cont.)

Table 11.4-2 Pressure Part Failure Auxiliary and Shield Building Hazard Schedule (cont.)

Table 11.4-2 Pressure Part Failure Auxiliary and Shield Building Hazard Schedule (cont.)

Table 11.4-2 Pressure Part Failure Auxiliary and Shield Building Hazard Schedule (cont.)

Table 11.4-2 Pressure Part Failure Auxiliary and Shield Building Hazard Schedule (cont.)

Table 11.4-2 Pressure Part Failure Auxiliary and Shield Building Hazard Schedule (cont.)

Table 11.4-2 Pressure Part Failure Auxiliary and Shield Building Hazard Schedule (cont.)

Table 11.4-2 Pressure Part Failure Auxiliary and Shield Building Hazard Schedule (cont.)

Table 11.4-2 Pressure Part Failure Auxiliary and Shield Building Hazard Schedule (cont.)

Table 11.4-2 Pressure Part Failure Auxiliary and Shield Building Hazard Schedule (cont.)

Table 11.4-2 Pressure Part Failure Auxiliary and Shield Building Hazard Schedule (cont.)

Table 11.4-2 Pressure Part Failure Auxiliary and Shield Building Hazard Schedule (cont.)

Table 11.5-1 Flammable Substances

Tank Tag	Flammable Substance	Volume (m^3)(4)
CFS-MT-01	Hydrazine	3
CFS-MT-02	Hydrazine	3
CFS-MT-03(1)	3-Methoxypropylamine	3
CFS-MT-04(1)	3-Methoxypropylamine	2
CFS-MT-13(2)	3-Methoxypropylamine	3
DOS-MT-01A	Number 2 Diesel Oil	356
DOS-MT-01B	Number 2 Diesel Oil	356
DOS-MT-02A	Number 2 Diesel Oil	8
DOS-MT-02B	Number 2 Diesel Oil	8
DOS-MT-03	Number 2 Diesel Oil	3
FPS-MT-02	Number 2 Diesel Oil	2
LOS-MT-01(3)	Turbine Lubricating Oil	79
LOS-MT-2A(3)	Turbine Lubricating Oil	50
LOS-MT-2B(3)	Turbine Lubricating Oil	50
WWS-MV-01	Waste Oil	1
ASS-EP-006	Number 2 Diesel Oil	4
PGS-MT-05	Liquified Hydrogen	4470
PGS-MT-07A	Gaseous Hydrogen	15
PGS-MT-07B	Gaseous Hydrogen	15
PGS-MT-08A	Gaseous Hydrogen	15
PGS-MT-08B	Gaseous Hydrogen	15

Notes:

1. Ammonium Hydroxide, Ethanolamine, and Morphaline in CFS-MT-03 and CFS-MT-04 are excluded as flammable liquids because they are bounded by other chemicals in the same tanks, in this case 3-Methoxypropylamine.
2. Ethanolamine, and Morphaline in CFS-MT-13 are excluded as flammable liquids because they are bounded by other chemicals in the same tank, in this case 3-Methoxypropylamine.
3. The volume of gases are reported as at STP.
4. The volume of flammable substances are reported as whole numbers; the exact quantity may vary slightly.

Table 11.5-2 Internal Explosions Hazard Schedule

Table 11.5-2 Internal Explosions Hazard Schedule

Table 11.5-2 Internal Explosions Hazard Schedule

Table 11.5-2 Internal Explosions Hazard Schedule

Table 11.5-2 Internal Explosions Hazard Schedule

Table 11.5-2 Internal Explosions Hazard Schedule

Table 11.5-2 Internal Explosions Hazard Schedule

Table 11.6-1 Internal Missile Hazard Schedule

Table 11.6-1 Internal Missile Hazard Schedule

Table 11.6-1 Internal Missile Hazard Schedule

Table 11.6-1 Internal Missile Hazard Schedule

Table 11.6-1 Internal Missile Hazard Schedule

Table 11.6-1 Internal Missile Hazard Schedule

Table 11.6-1 Internal Missile Hazard Schedule

Table 11.6-1 Internal Missile Hazard Schedule

Table 11.6-1 Internal Missile Hazard Schedule

Table 11.6-1 Internal Missile Hazard Schedule

Table 11.6-1 Internal Missile Hazard Schedule

Table 11.6-1 Internal Missile Hazard Schedule

Table 11.6-1 Internal Missile Hazard Schedule

Table 11.6-1 Internal Missile Hazard Schedule

Table 11.6-1 Internal Missile Hazard Schedule

Table 11.6-1 Internal Missile Hazard Schedule

Table 11.6-1 Internal Missile Hazard Schedule

Table 11.7-1 Form, Maximum Quantity, and Location of Bulk Gases and Chemicals Stored on Site

Table 11.8-1 Nuclear Island Cranes and Lifting Equipment

Table 11.8-2 Non-Nuclear Island Cranes and Lifting Equipment

Table 11.8-3 Dropped Loads Hazard Schedule

Table 11.8-3 Dropped Loads Hazard Schedule

Table 11.8-3 Dropped Loads Hazard Schedule

Table 11.8-3 Dropped Loads Hazard Schedule

Table 11.8-3 Dropped Loads Hazard Schedule

Table 11.8-3 Dropped Loads Hazard Schedule

Table 11.8-3 Dropped Loads Hazard Schedule

Table 11.8-3 Dropped Loads Hazard Schedule

Table 11.8-3 Dropped Loads Hazard Schedule

Table 11.8-3 Dropped Loads Hazard Schedule

Table 11.8-3 Dropped Loads Hazard Schedule

Table 11.8-3 Dropped Loads Hazard Schedule

Table 11.8-3 Dropped Loads Hazard Schedule

Table 11.8-3 Dropped Loads Hazard Schedule

Table 11.8-3 Dropped Loads Hazard Schedule

Table 11.8-3 Dropped Loads Hazard Schedule

Table 11.8-3 Dropped Loads Hazard Schedule

Table 11.8-3 Dropped Loads Hazard Schedule

Table 11.8-3 Dropped Loads Hazard Schedule

Table 11.8-3 Dropped Loads Hazard Schedule

Table 11.8-3 Dropped Loads Hazard Schedule

Table 11.8-3 Dropped Loads Hazard Schedule

Table 11.8-3 Dropped Loads Hazard Schedule

Table 11.8-3 Dropped Loads Hazard Schedule

Table 11.8-3 Dropped Loads Hazard Schedule

Table 11.8-3 Dropped Loads Hazard Schedule

Table 11.8-3 Dropped Loads Hazard Schedule

Table 11.8-3 Dropped Loads Hazard Schedule

Table 11.8-3 Dropped Loads Hazard Schedule

Table 11.8-3 Dropped Loads Hazard Schedule

Table 11.8-3 Dropped Loads Hazard Schedule

Table 11.8-3 Dropped Loads Hazard Schedule

Table 11.8-3 Dropped Loads Hazard Schedule

Table 11.8-3 Dropped Loads Hazard Schedule

Table 11.8-3 Dropped Loads Hazard Schedule

Table 11.8-3 Dropped Loads Hazard Schedule

Table 11.8-3 Dropped Loads Hazard Schedule

Table 11.12-1: Combined Consequential Hazards Credibility Matrix

		Consequential Hazard					
		Fire	**Flood**	**Missile**	**Drop Loads**	**Explosion**	**PPF**
Initiating Hazard	**Fire**		N	Y – when fire causes over speed of rotating equipment or over heating of valves	N	Y – Only if fire damages motors leading to loss of HVAC	N
	Flood	Y - Only where flooding contact high voltage power cables/Equipment		Y - when flooding causes a failure of over speed control	N	Y - Only if flood water damages motors leading to loss of HVAC	N
	Missile	Y - where there exists the potential to damage high voltage	Y – Where the missile is low energy a single flood else for high energy all sources.		Y – consequences of missile are bounded by dropped loads	Y	Y
	Drop Loads	Y - Only where dropped load contacts high voltage power cables/Equipment	Y - Where flooding sources are impacted by dropped	Y – consequences of missile are bounded by dropped load		Y – Only if piping containing H_2 can be damaged by drop	Y - Where piping is impacted by dropped load
	Explosion	N	N	N	N		N
	PPF	N	Y - high energy / pipe whip create cascading flooding events	N	Y	Y – only when pipe whip can cause leak of H_2	

"Y" indicates a positive response; "N" indicates a negative response

Table 11.12-2: Combined Correlated Hazards Credibility Matrix

		Correlated Hazards					
		Fire	Flood	Missile	Drop	Explosion	PPF
Initiating Hazard	Earthquakes	Y – Only if high voltage cable is routed using non-seismic raceway or conduit.	Y – Where non-seismic qualified piping exists with a significant volume.	N – Non-seismic qualified equipment is comprised of moderate or low pressure systems – not capable of producing missiles.	Y- Where non-seismic lifting equipment could drop a load.	Y – Only where hydrogen sources are generated or routed around non-seismic qualified equipment.	N – Non-seismic qualified equipment is not located near high energy piping or SSCs.
	External Flooding	N	N	N	N	N	N
	Accidental Aircraft Crash	N	N	N	N	N	N
	External Explosion	N	N	N	N	N	N
	Extreme Ambient Temperatures	N	N	N	N	N	N
	Meteorology	N	N	N	N	N	N
	Extreme Wind	N	N	N	N	N	N
	Offsite Fire and Smoke	N	N	N	N	N	N
	Offsite Missiles	N	N	N	N	N	N
	Biological Phenomena	N	N	N	N	N	N
	Electromagnetic Interference	N	N	N	N	N	N

"Y" indicates a positive response; "N" indicates a negative response

Table 11.12-3: Combined Consequences Hazard Schedule

Table 11.12-3: Combined Consequences Hazard Schedule (cont.)

Table 11.12-3: Combined Consequences Hazard Schedule (cont.)

Table 11.12-3: Combined Consequences Hazard Schedule (cont.)

Table 11.12-3: Combined Consequences Hazard Schedule (cont.)

Table 11.12-3: Combined Consequences Hazard Schedule (cont.)

Table 11.12-3: Combined Consequences Hazard Schedule (cont.)

Table 11.12-3: Combined Consequences Hazard Schedule (cont.)

Table 11.12-3: Combined Consequences Hazard Schedule (cont.)

Table 11.12-3: Combined Consequences Hazard Schedule (cont.)

Table 11.12-3: Combined Consequences Hazard Schedule (cont.)

Table 11.12-3: Combined Consequences Hazard Schedule (cont.)

Table 11.12-3: Combined Consequences Hazard Schedule (cont.)

Table 11.12-3: Combined Consequences Hazard Schedule (cont.)

Table 11.12-3: Combined Consequences Hazard Schedule (cont.)

Table 11.12-3: Combined Consequences Hazard Schedule (cont.)

Table 11.12-3: Combined Consequences Hazard Schedule (cont.)

Table 11.12-3: Combined Consequences Hazard Schedule (cont.)

Table 11.12-3: Combined Consequences Hazard Schedule (cont.)

Table 11.12-3: Combined Consequences Hazard Schedule (cont.)

Table 11.12-3: Combined Consequences Hazard Schedule (cont.)

Table 11.12-3: Combined Consequences Hazard Schedule (cont.)

Table 11.12-3: Combined Consequences Hazard Schedule (cont.)

Table 11.12-3: Combined Consequences Hazard Schedule (cont.)

Table 11.12-3: Combined Consequences Hazard Schedule (cont.)

Table 11.12-3: Combined Consequences Hazard Schedule (cont.)

Table 11.12-3: Combined Consequences Hazard Schedule (cont.)

Table 11.12-3: Combined Consequences Hazard Schedule (cont.)

Table 11.12-3: Combined Consequences Hazard Schedule (cont.)

Table 11.12-3: Combined Consequences Hazard Schedule (cont.)

Table 11.12-3: Combined Consequences Hazard Schedule (cont.)

Table 11.12-3: Combined Consequences Hazard Schedule (cont.)

Table 11.12-3: Combined Consequences Hazard Schedule (cont.)

Table 11.12-3: Combined Consequences Hazard Schedule (cont.)

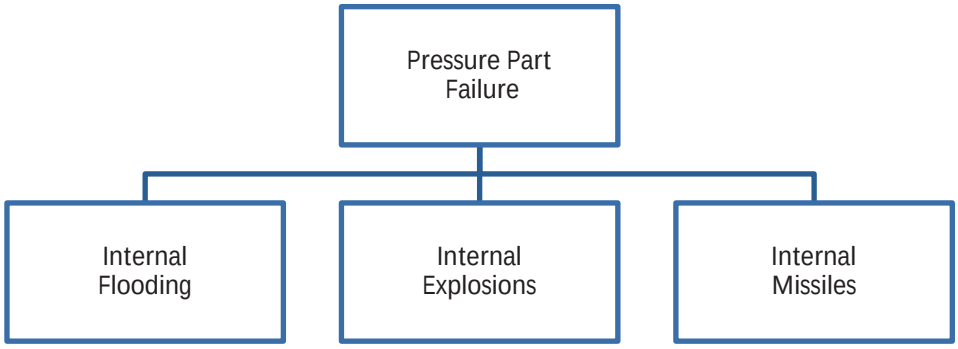


Figure 11.4-1 Internal Hazard Interfaces

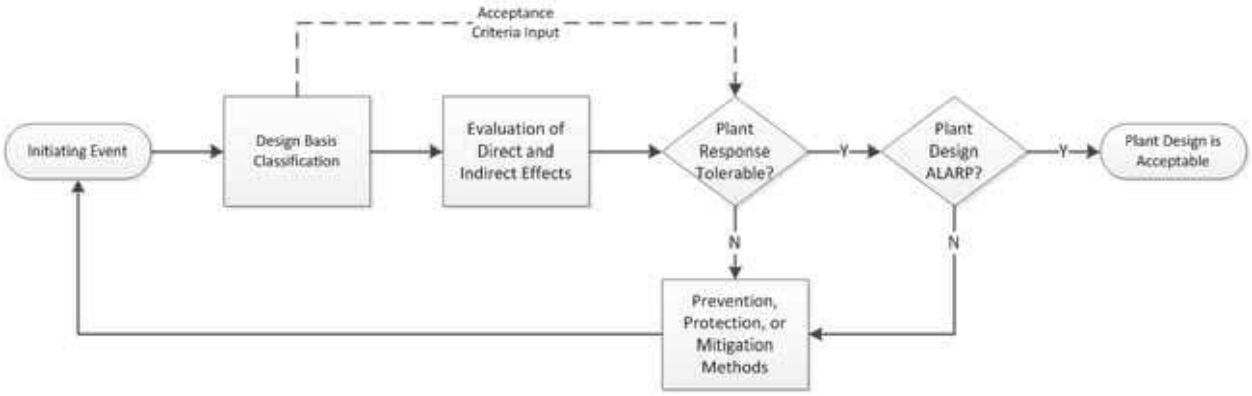


Figure 11.4-2 Evaluation of Pressure Part Failure Initiating Events

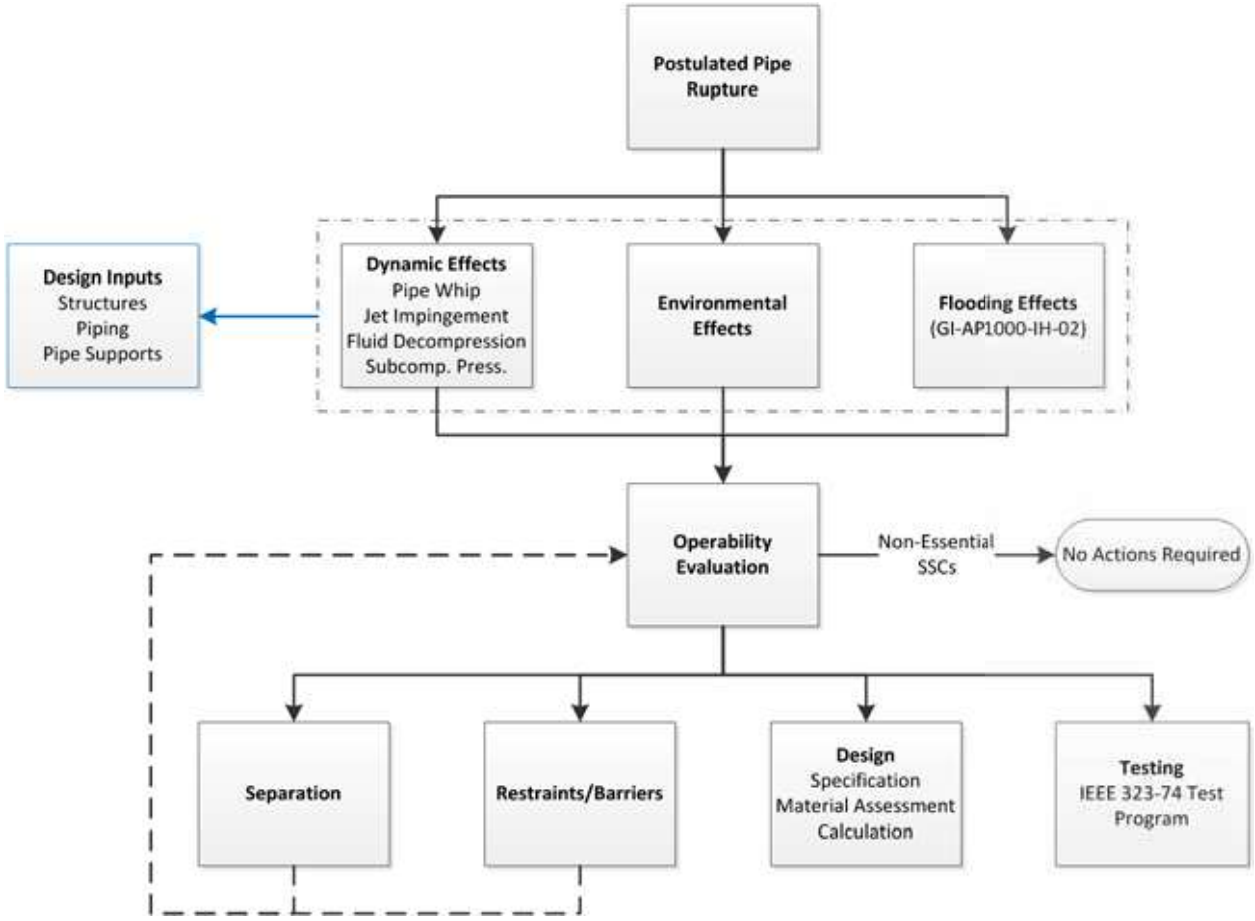


Figure 11.4-3 Overview of Pipe Rupture Hazards Analysis

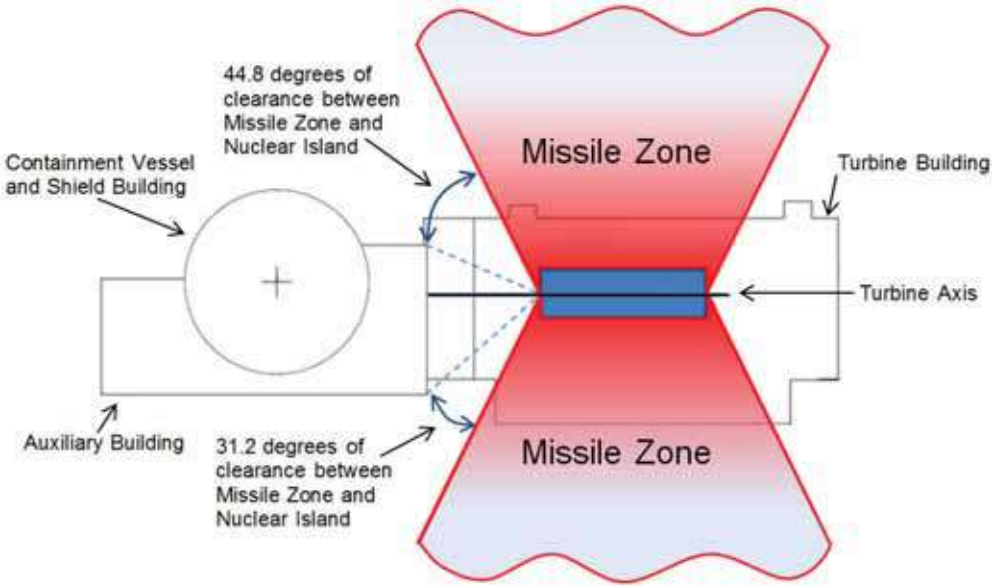


Figure 11.6-1 Low-Trajectory Turbine Missile Strike Zone for an AP1000

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS AND ACRONYMS

AC	alternating current
ASCE	American Society of Civil Engineers
BDB	beyond design basis
BS	British Standard
C-I	Category I
C-II	Category II
CA	Competent Authority
COMAH	Control of Major Accident Hazards
CSA	control support area
CSDRS	certified seismic design response spectra
DBA	design basis accident
DBE	design basis event
DC	direct current
DEFRA	Department for Environment, Food and Rural Affairs
EA	Environment Agency
EHA	external and internal hazards
EMI	electromagnetic interference
EN	European Standards
ETA	effective target area
EU	European Union
FRS	floor response spectra
HCLPF	high confidence of low probability of failure
HSE	Health and Safety Executive
HVAC	heating, ventilation, and air conditioning
IAEA	International Atomic Energy Agency
IBC	International Building Code
IRWST	in-containment refuelling water storage tank
LNG	liquefied natural gas
LOOP	loss of offsite power
MCA	military combat aircraft
MCR	main control room
MSL	mean sea level
NFPA	National Fire Protection Association
NI	nuclear island
NNS	non-nuclear seismic
NPP	nuclear power plant
ONR	Office for Nuclear Regulation
PCCWST	passive containment cooling water storage tank
PCS	passive containment cooling system
PCSR	Pre-Construction Safety Report
PGA	peak ground acceleration
PML	Principia Mechanica Ltd
PMS	protection and safety monitoring system
PSA	probabilistic safety assessment
PXS	passive core cooling system
RLE	review level earthquake
RS	response spectra
SAP	safety assessment principle
SBO	station black out
SFP	spent fuel pool
SMA	seismic margin assessment

LIST OF ABBREVIATIONS AND ACRONYMS (cont.)

SME	seismic margin earthquake
SSC	system, structure, or component
SSE	safe shutdown earthquake
SWS	service water system
TAG	Technical Assessment Guide
Tech Spec	technical specification
TNT	trinitrotoluene
UBC	Uniform Building Code
UHS	ultimate heat sink
UK	United Kingdom
UKAEA	United Kingdom Atomic Energy Authority
UKCP09	United Kingdom Climate Projections 2009
US	United States
VAS	radiologically controlled area ventilation system
VBS	nuclear island nonradioactive ventilation system
VFS	containment air filtration system

12 EXTERNAL HAZARDS

12.1 INTRODUCTION

This chapter contains specific supporting information on the nuclear safety withstand of the AP1000 design in response to design basis external hazards. The definition of an external hazard as applied in this chapter is a natural or man-made hazard that is initiated from outside the AP1000 plant site boundary. Figure 6-8 shows the standard AP1000 plant site layout. The site boundary will lie beyond this but will only be defined as part of the licensing process for a specific United Kingdom (UK) site.

The Office for Nuclear Regulation (ONR) Safety Assessment Principles (SAPs) (Reference 12.2) specifies that the effect of external hazards on nuclear facilities be identified and considered in the safety assessments. The safety assessment should demonstrate that risks from the external hazards are removed, minimised, or are tolerable. This can be done by showing that necessary plant and equipment are designed to meet appropriate performance criteria against the postulated hazard.

The ONR SAPs external and internal hazards (EHA) EHA.1 to EHA.17 relate to external hazards that could have a detrimental effect on nuclear safety. These SAPs include the following three engineering principles applicable to both external and internal hazards:

- **EHA.4** – For natural external hazards, characterised by frequency of exceedance hazard curves and internal hazards, the design basis event for an internal or external hazard should be derived to have a predicted frequency of exceedance that accords with Fault Analysis Principle FA.5.

  The thresholds set in Principle FA.5 for design basis events are 1 in 10,000 years for external hazards and 1 in 100,000 years for man-made external hazards.

- **EHA.7** – A small change in design basis fault or event assumptions should not lead to a disproportionate increase in radiological consequences.

- **EHA.11** – Facilities should be shown to withstand weather conditions that meet design basis event criteria. Weather conditions beyond the design basis that have the potential to lead to a severe accident should also be analysed.

More detailed background information regarding the implementation of the SAPs is provided in the ONR Technical Assessment Guide (TAG) NS-TAST-GD-013 (Reference 12.3).

For natural hazards, SAP EHA.4 (see also SAP FA.5) defines the frequency of exceedance for a UK design basis event that should conservatively have a predicted frequency of not greater than 1.0E-04/yr; i.e., equivalent to a 1 in 10,000 year event (Reference 12.3, Section 5.5). The 1.0E-05/yr design basis criterion should be applicable to man-made external hazards (Reference 12.3, Section 5.6).

A UK design basis assessment requires a deterministic analysis of an internally initiated event that is expected to occur more frequently than 1.0E-05 per year (Reference 12.3 and 12.60). Any event that occurs less frequently than this is regarded either as beyond design basis (BDB) or, if its frequency is less than 1.0E-07 per year, as incredible. Specifically, SAP EHA.1 Paragraph 235 states that any non-discrete hazards with a frequency on their hazard curve which is below once in ten million years; i.e., less than 1.0E-07 per year may be excluded (Reference 12.2).

The hazard grouping and screening process is described in Section 12.5; Table 12-1 and Table 12-2 provide the detailed analysis. Some UK external hazards such as volcanic action, meteorite and asteroid activity have been screened out because of their low frequency. Hazards such as fog and mist have been excluded because their effect will have no direct impact on the safety of the facility.

12.1.1 Design Basis Event Values

So that a comparison can be made with the AP1000 design values, the loading associated with a 1 in 10,000 year event are derived for:

- Rain
- Ambient temperature
- Wind speed
- Snow loading

Additionally, the Principia Mechanica seismic response spectra (RS) for the UK (Reference 12.5) cited in this report is defined for a 1 in 10,000 year event. Other natural hazards that have been considered generically in this report, such as coastal flooding, are considered to be site-specific and will be addressed further in the site-specific Pre-Construction Safety Report (PCSR).

12.1.2 Climate Change

Where appropriate, climate change in the form of increased ambient temperatures has been considered based on United Kingdom Climate Projections 2009 (UKCP09) (Reference 12.6). The climate change projections considered here are the maximum published projections to the year 2080 and therefore encompass the 60-year design operating life of the AP1000 Plant (Refer to Section 1.4.1). The effect of climate change post-operation, when the plant is being decommissioned, should be considered when appropriate climate change data becomes available.

12.2 CATEGORISATION AND CLASSIFICATION OF SYSTEMS, STRUCTURES AND COMPONENTS

The AP1000 design categorisation and classifications scheme for the UK is described in detail in Chapter 5.

12.3 NUCLEAR SAFETY CLAIMS

The systems, structures, and components (SSCs) and their ability to provide their defined Category A safety functions are the principal means of maintaining nuclear safety in response to each of the identified external events.

Since the Class 1 SSCs are capable of mitigating design basis accidents (DBAs), the external hazards safety is substantiated by demonstrating protection of Class 1 SSCs from design basis external hazards. Specific external hazard protection is also provided within the design basis to protect the Class 2 SSCs that are provided to support Class 1 SSC operations after 72 hours following a design basis accident. Note that these Class 2 SSCs are backed up by use of offsite SSCs connected to class 1 connections in the plant and as a result are only intended to reduce the probability that the offsite SSCs will need to be used. The protection provided is based on risk informed insights (PCSR Section 5.9.1.1).

The high level claim is made that postulated external hazards within the design basis do not prevent the delivery of the Category A safety functions. This will be demonstrated with supporting sub-claims, arguments, and evidence in the following sections for each external hazard in turn in Sections 12.6 to 12.16.

12.4 AP1000 NUCLEAR SITE

In the AP1000 plant coordinate system, the plant grade elevation is defined at an elevation of 100 m (100 ft), with grade being defined as the ground level within a half-mile radius of the nuclear island (NI).

The principal building structures of the AP1000 plant site are the following:

- NI
- Turbine building
- Annex building
- Radwaste building
- Diesel generator building

The NI of the AP1000 plant consists of the following:

- Shield building
- Containment vessel
- Auxiliary building

The foundation for the NI is an integral basemat that supports these buildings. Only these structures of the NI are classified as UK Class 1 structures. The external hazards in this chapter are assessed against the Class 1 SSCs and those SSCs with the potential to adversely interact with the Class 1 SSCs of the NI.

12.5 SCOPE OF EXTERNAL HAZARDS

12.5.1 External Hazards Grouping

Tables 12-1 and 12-2 identify the external hazards grouping for man-made and naturally occurring hazards respectively. For each hazard category, the potential source(s) of the hazards are identified. For identified hazard source(s), postulated initiating events that could result from the source(s) are cited. The initiating events in Tables 12-1 and 12-2 have been compiled primarily from the ONR guidance (Reference 12.3) and International Atomic Energy Agency (IAEA) sources (References 12.8, 12.9, and 12.10). Table 12-2 provides definitions of some of the cited hazards.

Table 12-1 and Table 12-2 identify the potential consequences of initiating events and the safety features in place to mitigate the consequences. For each initiating event, one of the following six outcomes is stated:

1. The initiating event is addressed in this chapter.

2. The initiating event can be screened out because of a low probability of occurrence or negligible consequences.

3. It can be bounded by another initiating event.

4. The initiating event can be considered under another hazard grouping.

5. The initiating event is specific to a site and consequently requires site-specific information and will be considered in a site-specific PCSR.

6. The initiating event (e.g., fire) is addressed as part of Internal Hazards as described in Chapter 11.

The identified groups of hazards in Tables 12-1 and 12-2, after the screening process cited in these tables, were reduced to 11 generic external hazards categories that are discussed in Sections 12.6 to 12.16.

12.5.2 Hazards Selected for Detailed Review

The eleven generic external hazards categories in this chapter are assessed against the Class 1 SSCs of the AP1000 plant NI to ensure that they do not prevent the delivery of Category A safety functions.

The following hazards are identified in Tables 12-1 and 12-2 as requiring detailed consideration in this chapter:

- Earthquakes
- External flooding
- Accidental aircraft crash
- External explosion
- Extreme ambient temperatures
- Meteorology
- Extreme wind
- Offsite fire and smoke
- Offsite missiles
- Biological fouling
- Electromagnetic interference (EMI) and lightning

Licence applicants referencing the standard AP1000 design will provide site-specific information related to site location and description, exclusion area authority and control, and population distribution as follows:

- **Site information** – Site-specific information on the site and its location will include political subdivisions, natural and man-made features, population, highways, railways, waterways, and other significant features of the area.

- **Exclusion area** – Site-specific information on the exclusion area will include the size of the area and the exclusion area authority and control. Activity that may be permitted within the exclusion area will be included in the discussion.

- **Population distribution** – Site-specific information will be included on population distribution.

The plant has the inherent capability to withstand certain types of external accidents as a result of the specified design conditions associated with earthquakes, wind loading, and radiation shielding. Acceptability for external accidents associated with a given site will be covered in the licence application.

Each licence applicant referencing the AP1000 design will provide analyses of accidents external to the nuclear plant relative to a specific site. The determination of the probability of occurrence of potential accidents that could have severe consequences will be based on analyses of available statistical data on the occurrence of the accident together with analyses of the effects of the accident on the plant's required supporting structures and components.

12.6 EARTHQUAKES

12.6.1 Safety Design Approach

The safe shutdown earthquake (SSE) is used as a design basis for AP1000 plant Class 1 SSCs. The operating basis earthquake has been eliminated as a design requirement following the recommendations of SECY-93-087 (Reference 12.59). In specifying design criteria for the SSE, consideration is given to lower magnitude earthquakes having a greater probability of occurrence, as well as to larger magnitude earthquakes having a lower probability (see section 12.6.3.4).

The AP1000 plant has been designed so that any seismic event within the design basis will not prevent the delivery of Category A safety functions.

12.6.2 Seismic Categorisation of Safety-Related Systems

A method for categorisation of safety functions and classification of SSCs has been developed specific to the UK, which is presented in detail in Chapter 5. Structures are assigned a seismic category depending on their required performance during and following a seismic event. Civil engineering structures are categorised according to their safety function and are classified according to their significance in delivering this function according to UK practice. A seismic category is assigned accordingly.

The seismic category definitions are presented below.

- **Seismic Category I (C-I)** – Applies to safety-significant SSCs. C-I SSCs are designed to maintain both functionality and integrity under seismic loading within the design basis.

- **Seismic Category II (C-II)** – Seismic C-II SSCs are designed so that an SSE does not cause unacceptable structural failure of, or interaction with, C-I items that could degrade the functioning of a safety significant SSC to an unacceptable level, or could result in incapacitating injury to occupants of the main control room (MCR).

- **Non-nuclear seismic category** – Non-nuclear seismic (NNS) SSCs are those that are not classified as C-I or C-II. Even though a structure has been assigned as NNS, some form of seismic justification is undertaken. Normal industrial practice is to provide some form of seismic protection to all new nuclear structures.

Tables 15A-1 through 15A-4 present the seismic categories that have been assigned to the AP1000 plant safety significant equipment and buildings.

Non-seismic structures are evaluated to determine that their seismic response does not preclude the safety functions of C-I SSCs. This is satisfied by compliance with one of three options:

- The collapse of the non-seismic structure will not cause the non-seismic structure to strike a C-I SSC.
- The collapse of the non-seismic structure will not impair the integrity of C-I SSCs.
- The structure is reclassified as C-II and is analysed and designed to prevent its collapse under the SSE.

12.6.3 Ground Motions

12.6.3.1 UK Ground Response for Nuclear Facilities

UK seismic RS have typically been based on the Principia Mechanica Ltd (PML) derived spectra and have generally been accepted in the UK as a reasonable surrogate to the ground motion of the hazard (Reference 12.3, Annex 3). These are appropriate for typical forms of building construction. The PML spectra address three generic types of site ground conditions: hard (frequency of soil column > 5Hz), intermediate (frequency of soil column in the range 2 to 5 Hz) and soft (frequency of soil column < 2 Hz). A number of UK nuclear-licensed sites have undertaken a site-specific seismic hazard to determine appropriate free field horizontal peak ground acceleration (PGA) at their location. The maximum value this can achieve in the UK is 0.25g for a 1 in 10,000 year earthquake (Reference 12.13). The vertical spectrum is usually taken as two-thirds of the horizontal value (Reference 12.3). Where the building mass is significant in comparison to the mass of the soil volume (such as for heavy shielding associated with reactor buildings), the PML spectra may not be appropriate and soil-structure interaction on a site-specific, case-by-case basis is normally undertaken to evaluate the response of the system.

12.6.3.2 AP1000 Design Spectra

Chapter 16 and Reference 12.61 describe the derivation of RS for the AP1000 design for C-I and C-II SSCs. A bounding series of ground motion and floor response spectra (FRS) for a range of critical damping ratios has been generated using an extensive range of synthetic time-history ground accelerations for six different soil profiles, together with FRS at key levels within the NI structures based on soil-structure models and industry-accepted software including ANSYS and SASSI. The spectra comply with industry guidance with respect to power density requirements and minimum amplitude content across the frequency range. The design basis event (DBE) ground motion is stated as 0.3g both horizontally and vertically.

The AP1000 plant is designed for an earthquake defined by a PGA of 0.3g horizontally and vertically and can be compared to the UK PGA values provided in Section 12.6.3.1. The AP1000 Design earthquake is referred to as the certified seismic design response spectra (CSDRS). Figures within Reference 12.52 depict the horizontal and vertical design RS for the AP1000 plant, scaled to the SSE at 0.3g.

Chapter 16 and Reference 12.52 discuss the FRS at a number of levels within the NI structures for the six soil profiles considered (i.e., hard rock, firm rock, soft rock, upper-bound soft-to-medium soil, soft-to-medium soil, and soft soil) derived from the SASSI soil-structure interaction analyses for the NI buildings. The frequencies for rock and medium and soft soil columns have been determined from the shear wave velocities cited in Reference 12.52:

- The frequencies for the AP1000 design rock profiles range from 5.4 to 16.7 Hz and thus bound the PML rock values.

- The AP1000 plant upper-bound soft-medium and soft to medium frequencies range from 2.8 to 3.98 Hz and would reasonably represent the PML intermediate soil spectra.

- The AP1000 plant soft soil profile has a frequency of approximately 2.2 Hz and would fall within the PML intermediate soil profile, rather than the PML soft-site spectra.

The UK design basis RS horizontal acceleration with a PGA of 0.25g marginally exceeds the AP1000 design SSE RS in the range of 8 to 12Hz. However, the probabilistic seismic margin analysis utilising a 0.5g review level earthquake provides confidence in the deterministic 0.3g PGA assessment undertaken for the AP1000 design and that the loading demand of the UK design basis RS will be met. Accordingly, it should be confirmed on a site-specific basis there will be no loss of Category A safety functions resulting from a UK design basis earthquake. The design RS are applied at foundation level in the free field at hard rock sites and at finished grade (100 m/100'-0") in the free field at firm rock. A comparison of spectra associated with sites other than hard rock requires the use of soil structure interaction analysis (such as SASSI analysis). Therefore, comparison to PML spectra and the AP1000 spectra is made. This comparison between the UK PML spectra and AP1000 spectra is discussed in Section 12.6.3.3.

The geological conditions that apply to the AP1000 design are summarised in Chapter 4. The specific ground conditions at sites in the UK would need to be confirmed by site-specific ground investigation to confirm the adequacy of the soil for compliance with the AP1000 design parameters. Where these fall outside the given specifications, justification on a site-specific basis would be undertaken by the licence applicant.

The AP1000 plant will be demonstrated to satisfy all seismic design acceptance criteria using the site specific input. This demonstration may include a combination of comparisons on ground motion and soil conditions, and site specific analyses. The nuclear island has been designed to the CSDRS for a wide variety of soil conditions. It is therefore expected tha the site specific demand will be lower than the standard plant design basis. It is not expected that there will be significant changes for the AP1000 plant in the UK. The basic design will retain the existing design and hence retain the margins inherent in the enveloping parameters of the standard plant seismic design. Where design changes are required for other reasons, the revised design will be demonstrated to satisfy site specific requirements.

Non-seismic AP1000 plant buildings are designed to Uniform Building Code (UBC) requirements for various ground motions, depending on the safety requirement. Note however that the Turbine building and Annex 4 office building are built to the International Building Code (IBC).

12.6.3.3 Comparison of UK PML and AP1000 Design Spectra

Figure 12C-1 in Appendix 12C shows a comparison of the PML RS accelerations for the hard, intermediate, and soft sites for 5 percent damping with a peak horizontal ground

acceleration of 0.25g against the AP1000 design spectra for 5 percent damping and a peak ground acceleration of 0.3g. The graph shows that for each PML site type, there is a limited frequency range over which the AP1000 design RS is less onerous than PML. The maximum differential response is approximately 15 percent for the soft site at 8 Hz, 15 percent for the intermediate site at 10 Hz, and 11 percent for the hard site at 12 Hz. This implies that over a tight frequency band the design requirement of the AP1000 design may be less conservative than PML. However, the severity of this apparent deficiency can be moderated to a considerable extent, as the design demand (i.e., seismic forces generated) is also dependent on the participating mass within that frequency range and the method used to combine the modal responses.

The FRS presented (Reference 12.61) suggests that for a number of the FRS levels, the peak response over the 8 to 12 Hz range is governed by the hard site input motion.

12.6.3.4 Seismic Margin Analysis

A Seismic Margin Assessment (SMA) is a study employed to identify those SSCs important to seismic risk to assess the capacity of components required to bring the plant to a safe, stable condition and to identify potential vulnerabilities.

The purpose of the SMA is to identify the magnitude of seismic event that an SSC is able to withstand, or perform its required duties.

With regard to SMA, a seismic margin earthquake (SME) is specified such that, for safety-significant systems required for safe shutdown, the seismic adequacy is verified to the level of the SME. When an SMA has been performed for the safety-relevant components of that plant, the consequences of an increased seismic hazard above the SME for the SSE can be understood, thereby demonstrating the absence of any cliff-edge effects. To this extent, the SME can be considered as the beyond-design-basis earthquake.

An SMA based on a probabilistic safety assessment (PSA) considers sequence-level high-confidence, low-probability failures (HCLPF) and fragilities for all sequences leading to core damage or containment failures, up to approximately one-and-two-thirds of the ground motion acceleration of the design basis SSE. It is conservatively assumed for the risk-based SMA that no credit is taken for the mitigation functions of the non-safety-significant components and systems.

The SMA for the AP1000 design has been performed based on established criteria, design specifications, existing qualification test reports, established basic design characteristics and configurations and public domain generic data in AP1000 plant PSA.

For the AP1000 design, the SMA has established a review level earthquake (RLE) equal to 0.5g. It is demonstrated in Section 10.18 that for the Class 1 SSCs, the magnitudes of high-confidence, low-probability failure events are equal to or greater than 0.5g which provides confidence in the deterministic 0.3g PGA assessment undertaken for the AP1000 design and that the loading demand of the UK design basis PML RS will be met. A 0.5g RLE withstand capability is beyond that required by UK seismic conditions, which generally would require a design basis earthquake of 0.25g (Reference 12.15) with seismic margins being considered at 0.35g.

For the AP1000 design, SMA provides assurance that the design satisfies EHA.7 (i.e. small change in design basis fault or event assumptions should not lead to a disproportionate increase in radiological consequences) as well as assuring margin for BDB earthquakes.

SMA provides reasonable assurance that the AP1000 design can withstand earthquakes with a return period of 1.0E-7 /yr (EHA.1 implies consideration of events with this return period).

Design to SSE with near-elastic response is conservative and provides margin for BDB Basis earthquakes.

12.6.3.5 Ground Rupture, Liquefaction, and Bearing Capacity

The ONR advises that it is generally impractical to design nuclear plants to resist ground rupture (Reference 12.3). The potential for liquefaction occurs for certain types of soil (typically saturated loose sands or hydraulically deposited sands with uniform grading), but techniques exist for assessing the potential for liquefaction and improving ground conditions to negate its effects. The AP1000 plant has not been specifically designed to account for either ground rupture or liquefaction effects. The licence applicants will be required to address the following regional and site-specific geological, seismological and geophysical information, as well as conditions caused by human activities:

- Structural geology of the site
- Seismicity of the site
- Correlation of earthquake activity with seismic sources
- Seismic wave transmission characteristics of the site
- Geological history
- Evidence of paleoseismicity
- Site stratigraphy and lithology
- Engineering significance of geological features
- Site groundwater conditions
- Dynamic behaviour during prior earthquakes
- Zones of alteration, irregular weathering, or structural weakness
- Unrelieved residual stresses in bedrock
- Materials that could be unstable because of mineralogy or unstable physical properties
- Effect of human activities in the area

Seiches and tsunami are addressed generically in Section 12.7.5.

The licence applicant will also address the following site-specific information related to the stability and uniformity of subsurface materials and foundations:

- Excavation
- Bearing capacity
- Settlement
- Liquefaction

The licence applicant may identify site-specific features and parameters that are not clearly within the site envelope. These features and parameters may be demonstrated to be acceptable by performing site-specific seismic analyses. A site-specific evaluation can be performed if the site-specific spectra are outside the range evaluated for the standard AP1000 design.

12.6.4 Long Period Ground Motion

The ONR external hazards TAG (Reference 12.3, Table 1) cites long period ground motion as a seismic hazard that should be considered. Water contained in tanks is susceptible to long period motion i.e., low frequency response.

The hydrodynamic mass effect of the water within the passive containment cooling water storage tank (PCCWST) on the shield building roof, the in-containment refuelling water storage tank (IRWST) within the containment internal structures, and the spent fuel pool (SFP) in the auxiliary building is evaluated. Since the water in the PCCWST responds at a very low frequency (sloshing) and does not affect building response, the horizontal mass is reduced to exclude the low frequency water sloshing mass. The total mass of the water in the IRWST and the SFP in the auxiliary building is included in the NI seismic model (Reference 12.61):

- **PCCWST** –The seismic analysis indicates that significant sloshing may take place in the PCCWST. The tank is lidded and will not lose water during a seismic event.

- **IRWST** – The seismic analysis indicates that sloshing is unlikely to take place in the IRWST and therefore it is not expected to lose water during a seismic event.

- **SFP** – For the fuel handling area, Appendix C of Reference 12.16, considers the effect of an SSE during normal operation with water in the SFP and associated pools with the seismic hydrodynamic load acting on the pool walls. The SSE may result in sloshing of the free water surface with loss of water from the pools.

12.6.5 Systems, Structures, and Components Outside the Nuclear Island

As there are no Class 1 SSCs outside the NI, seismic-induced damage to SSCs outside the NI will not prevent the delivery of Category A safety functions.

The radwaste building is designated as non-seismic and analysed to the UBC. A separation gap is provided between adjacent structural components of the two buildings above grade, the greater of either two times the absolute sum of the maximum displacement of each building under the most unfavourable load combination or 10.16 cm (4 in), whichever is more. In addition, an impact analysis based on the kinetic energy associated with the maximum velocities of the two buildings has been undertaken to show that the collapse of the radwaste building does not undermine the safety function of the NI structures. The radwaste building form comprises a steel frame which is comparatively light in relation to the robust, heavy concrete components used for the NI structures. Accordingly, it would be expected that the radwaste building impact effects would not compromise the integrity or function of the NI structures.

The portion of the annex building adjacent to the NI is designated as C-II and analysed according to the SSE.

The turbine building is divided into two sections: The first bay adjacent to the NI is designated as C-II and designed to address the SSE ground motion. The remaining bays are classified as non-seismic and analysed according to the UBC or IBC (see Section 12.6.3.2).

The interfacing of the adjoining annex building and the turbine building with the NI is discussed in Chapter 16.

12.7 EXTERNAL FLOODING

12.7.1 Safety Design Approach

External flooding of the nuclear power plant from natural causes can be attributed to probable maximum flood, site and adjacent area probable maximum precipitation run-off, seiches or tsunamis, and ground water.

Contributors to generic site flooding considered here are:

- Extreme rainfall or precipitation
- Groundwater flow
- Extreme river and sea levels
- Seiches and tsunamis

However, site-specific issues such as surface runoff and upstream dam failure, which are not considered here, may provide local flooding.

The AP1000 plant has been designed so that an extreme flooding event within the design basis will not prevent the delivery of Category A safety functions.

12.7.2 Extreme Rainfall

12.7.2.1 Diversion of Rainwater from the Nuclear Island

The NI structures are designed to resist the incursion of a design basis rainfall.

The roofs of the shield and auxiliary buildings do not have internal roof drains thus minimising water ingress. The roofs are sloped such that rainfall is directed towards gutters located along the edges of the roofs or over the roof edge; therefore, ponding on the roofs is precluded. Water from roof drains and scuppers, as well as run-off from the plant site, is conveyed to catch basins, underground pipes, or directly to open ditches.

Dynamic forces associated with the probable maximum precipitation are not factors in the analysis or design of the AP1000 plant, since the finished grade is adequately sloped to prevent water accumulating on the NI.

12.7.2.2 Change in UK Rainfall Resulting from Climate Change

The Department for Environment, Food and Rural Affairs (DEFRA) UKCP09 (Reference 12.17) discusses precipitation changes. In winter, UKCP09 shows projected increases by 54 percent for the 2080 medium emissions scenario at the 90 percent probability level in areas of southern England. In the summer, there are corresponding increases of 7 percent over parts of southern England.

12.7.2.3 Extreme Recorded UK Rainfall

The Meteorological Office recorded data on extreme rainfall in England and Wales (Reference 12.18) provides the following time-related rainfall maxima figures: 92 mm/hr (3.6 in/hr) and 32 mm/5 min (1.26 in/5 min). These extreme UK rainfall intensity values are bounded by the AP1000 design envelope of 525.8 mm/hr (20.7 in/hr) and 160.0 mm/5 min (6.3 in/5 min) respectively (see Table 12-4), resulting in AP1000 design rainfall intensity values that are a factor of five greater than predicted UK maxima. Such a factor bounds the predicted precipitation increase of 54 percent for the UK previously discussed.

12.7.2.4 Predicted UK Rainfall for Design Basis Event

The ONR TAG for External Hazards NS-TAST-GD-013 (Reference 12.3) refers to British Standard (BS) European Standards (EN) 12056-3: 2000 for drainage systems to buildings. This standard defines rainfall intensity in litres per second, but the rainfall values are equivalent to that given in BS 6367:1983 (Reference 12.19) which provides rainfall intensity values in millimetres per minute for the UK for various storm durations and a range of return periods up to 1 in 35,000 years.

From Appendix A of BS 6367: 1983 (Reference 12.19), the return period associated with the AP1000 design storm rain intensity value of 160 mm/5 min (6.3 in/5 min) duration exceeds the 1 in 35,000 year event for the heaviest intensity of rainfall within mainland UK (i.e., excluding Northern Ireland). The intensity for a 1 in 10,000 year return period for the 5-minute storm duration storm is 42 mm (1.7 in). Hence, there is a factor of 3.8 in the design capacity of the NI to remove rain water compared to the 1 in 10,000 year return period design basis rain intensity value.

Consequently, the AP1000 design is conservative compared to the UK design basis rainfall, even allowing for climate change over the life of the facility that could result in a predicted increase of 54 percent precipitation increase for the UK, discussed in Section 12.7.2.2.

12.7.3 Groundwater

The NI structures are designed to resist the infiltration of normal ground water up to a plant elevation of 99.39 m (98 ft). A waterproof system for the Class 1 structures below grade (below ground level) will be installed to limit the infiltration of subsurface water as described in Section 16.9.1.

The actual site soil properties of the various layers under possible groundwater conditions during the life of the plant, as part of a site-specific assessment, will be compared to the range of values assumed in the standard design.

12.7.4 Extreme River and Sea Levels

The NI structures have been designed to withstand and prevent ingress of water from land or sea-based external flooding events.

The highest possible sea-water level would be caused by a combination of a high spring tide, a coincidental surge and coincidental maximum wave height conditions.

Adequate coastal defences as well as site elevation prevent flooding from seawater, which can include extreme high tides, tsunamis, seiches and storm surges. Flood defences and their levels will vary from site to site; however, most UK sites are likely to be coastal or estuarine and subject to the risk of flooding from the sea directly or through interactions between excess river flow and tidal conditions. Accordingly, the maximum seawater level, including the level of storm surge, is site-specific and should be assessed on a case-by-case basis.

Sea level change predictions from DEFRA UKCP09 (Reference 12.20) in the period from 1990 to 2080 for the average sea-level rise for the medium emissions scenario at the 50-percent probability level is projected to be between 244 and 363 mm (9.6 and 14.29 in). This range does not allow for contribution from land movements so this should be covered in the site-specific assessment. However, it should be noted that the maximum vertical land movement is predicted to occur in South Western England by a lowering of the region of 2.5 mm/yr (0.09 in/yr) (Reference 12.21).

12.7.4.1 High Tides and Storm Surges

High spring tide levels are gravitationally induced and depend locally on topographical influences.

Storm surges are short-lived local increases in water level above that of the tide and are driven by wind and atmospheric pressure gradients. The effects of climate change also need to be taken into consideration. Combined changes in storm surges and relative sea level rise can be estimated by adding together the two components (Reference 12.22). When they occur at the same time as a high tide, storm surges can cause overtopping of sea defences and flooding. The projected long-term trends in storm surge around the UK are relatively small and even the 1 in 50 year return surge is not projected to increase by more than 90 mm (3.5 in) anywhere around the UK coast (Reference 12.22) by 2080. A site-specific assessment will be required to identify current storm surge levels, and therefore, the risk from an increase in storm-surge heights.

12.7.5 Tsunamis & Seiches

Seiches are bounded by tsunamis in magnitude (Reference 12.23, Section 3.2(11)), and therefore, have been screened out of this assessment.

The most likely scenario (Reference 12.24) for a significantly damaging tsunami in the UK is an anomalously large, relatively close earthquake producing a tsunami that would only be severe locally. Such earthquakes are themselves rare, and are unlikely to produce a tsunami. For most scenarios, the heights of tsunami waves arriving close to the shore will be comparable to those of typical storm surges (Reference 12.24). All major UK centres of population have flood defence infrastructure designed to cope with the expected range of storm surges.

However, certain characteristics of tsunami events (e.g., the number of waves and the range of wavelengths) are likely to create sea conditions different from those during a storm surge. Also, tsunami events may occur at any time; they are not associated with adverse meteorological conditions. Therefore, it cannot be assumed that the impact of a tsunami would be comparable to that of a storm surge simply on the basis of a similar wave height.

The largest tsunami to impact the shores of the British Isles was that caused by the great Lisbon earthquake of 1st November 1755 (Reference 12.25). For such a Lisbon-type tsunami, travel times are approximately 4-1/2 hours to the Cornish coast, which provides in most scenarios adequate time to mitigate the impact of the tsunami; e.g., by shutting the reactor down.

Coastal sea defences and site elevation are the primary defence against a tsunami in the UK. The actual defences and site elevation will vary significantly around the coastline of the UK and the risk from a tsunami and seiches should, in conjunction with the local coastal defences, be evaluated on a site-specific basis.

12.7.6 Flood Design of the Nuclear Island

12.7.6.1 Siting of the Nuclear Island Platform Level

The AP1000 reactor is designed for a normal groundwater elevation up to plant elevation 99.39 m (98 ft) and for a flood level up to a plant elevation of 100.0 m (100 ft). For structural analysis purposes, grade elevation is established as a plant elevation of 100.0 m (100 ft) with grade being defined as the ground level within a 0.8-km (0.5 mi) radius of the NI (PCSR Table 4-9). Actual grade will be a few centimetres lower to prevent surface water from entering doorways. Site-specific considerations will be required to determine if the maximum probable flood height is bounded by the maximum designed probable flood height. At the time of site licensing, the applicant will need to demonstrate that the probable maximum 1 in 10,000 year flood is below this elevation.

At the time of site licensing, the applicant will need to demonstrate that the probable maximum flood from sources such as streams and rivers, potential dam failures, probable maximum surge, and tsunami flooding is below the actual sites grade elevation.

Flooding of water intake structures, cooling canals, reservoirs or channel diversions would not prevent safe operation of the plant.

There is minimal dynamic water force associated with the probable maximum flood or high groundwater level because these water levels are below the finished grade.

12.7.6.2 Nuclear Island Flood Withstand – Penetrations

Because the probable maximum flood for the generic AP1000 design is less than grade elevation the exterior doors are not required to be watertight for protection from external flooding. Also, there are no access openings or tunnels penetrating the exterior walls of the NI below grade.

The shield building penetrations are designed to maintain containment integrity under DBA conditions. Process piping penetrations through the exterior walls of the NI below grade are embedded in the wall or are welded to a steel sleeve embedded in the wall.

The effect of high tides will be dependent on the location of the plant relative to the sea which will require a site-specific assessment. Climate change will need to be taken into consideration for high tides. Sea-level rises will vary from region to region.

12.7.6.3 Nuclear Island Flood Withstand – Basemat

The NI basemat is designed to withstand the upwards hydrostatic pressure of groundwater up to an elevation of 610 mm (24 in.) below grade, and therefore will resist overturning and sliding effects following a design basis flood.

12.7.7 Systems, Structures, and Components Outside the Nuclear Island

As there are no Class 1 SSCs outside the NI, flood-induced damage outside the NI will not prevent the delivery of Category A safety functions.

Flood-induced damage to SSCs outside the NI is not a safety concern and will not compromise Class 1 SSCs in the NI. The annex, radwaste, and diesel generator buildings have parapets with large weir openings to drain water to scuppers and drains to preclude the accumulation of water on the roofs.

12.7.8 Combined Hazards

The most credible combination of hazards involving external flooding is judged to be extreme wind and flooding (sea water or precipitation). However, the biggest risk to the site would be from an extreme rainfall event and an extremely high sea level with a storm surge. High winds could potentially lead to greater wave heights, leading to overtopping of the sea or river defences. Accordingly in conjunction with local coastal defences, such a scenario should be assessed on a site-specific basis.

Buoyancy effects on the NI basemat are considered in turn with wind, earthquake, and tornado loading.

Flooding of the AP1000 plant site resulting in physical isolation of the site by the inaccessibility of access roads would not be an issue for at least 7 days following a design basis flood.

12.8 ACCIDENTAL AIRCRAFT CRASH

This section considers the threat to the AP1000 plant from accidental aircraft impact. The deterministic study of aircraft impact, including the effects of shock-induced vibration and fire effects, on the plant is addressed under external hazards malicious acts – which are not presented in the PCSR due to their sensitive nature. Separate documentation is provided to address malicious aircraft impact. Design features which provide protection against malevolent aircraft impact are as follows:

- Shield Building design such that aircraft impact would not inhibit core cooling capability or not impact containment integrity.
- Auxiliary Building and spent fuel pool design such that SFP integrity is not compromised.
- Diverse key systems and separation of key systems.

UK air navigation regulations (Reference 12.26) restrict flying in the vicinity of UK nuclear sites. All of the designated UK nuclear new build sites with either an existing or a decommissioned nuclear power plant (NPP) have over-flying restricted to a height above 610 m (2000 ft) and a radius greater than 3.7 km (2 nautical mi).

The first stage in calculating the frequency of an aircraft striking an installation is to establish a background crash rate. The background crash rates cited in Reference 12.27 are applicable to all UK sites and only need to be modified when a site lies close to an airfield or a flight path. These crash rates have been derived by Atkinson and Thompson as an update to the report by Byrne (Reference 12.28).

Assuming the facility is not located within 8 km (5 mi) of an airfield (Reference 12.27, Paragraph 151) or close to a flight path (which is not allowed by legislation as previously described), the combined crash rate for light, small and large transport, helicopters and Military Combat Aircraft (MCA) is 4.8E-07 and 51.3E-07 crashes per year for the NI and the AP1000 generic site, respectively (see Table 12A-1 in Appendix 12A). Thus, considering the NI only, compared to the generic AP1000 site, this reduces by an order of magnitude the effective target area (ETA) and the corresponding crash frequency per annum.

Aircraft impact has been screened-out because it requires a site-specific location to fully substantiate. It should be confirmed on a site-specific basis that the generic background crash rate and the UK legislation that restricts flying in the vicinity of UK nuclear sites are applicable to the designated AP1000 plant site.

12.9 EXTERNAL EXPLOSIONS

According to the combustion mode, an explosion can take the form of a deflagration, which generates moderate pressures, heat, or fire, or a detonation which generates very high near-field pressures and usually thermal effects. These types of explosions can occur only in the case of special fuel-air mixtures; whether the ignition of a particular chemical vapour or gas behaves as a deflagration or as a detonation depends primarily on the concentration of the chemical vapour or gas present (Reference 12.10, Section 6.5).

12.9.1 Safety Design Approach

The AP1000 plant has been designed so that external explosions will not prevent the delivery of Category A safety functions.

12.9.2 Nuclear Island Explosion Withstand

The NI structures can resist an off-site explosion. IAEA Safety Guide NS-G-1.5 (Reference 12.10, Paragraph 6.27) notes that structures will often have been designed to accommodate extreme loadings such as those resulting from aircraft impacts, tornado-generated pressure and missile loads, or earthquakes. The reinforced concrete walls are a minimum of about 0.6 m (2 ft) thick compared with the shield building, which has a nominal wall thickness of 0.914 m (3 ft). It is often unnecessary, therefore, to apply additional design measures to mitigate the effects of design basis external explosions, unless their effects are found to be more severe than those corresponding to the other extreme loadings already considered.

The screening distance value for an initiating explosive event based on conservative approaches (Reference 12.29) can be determined by calculating the scaled distance corresponding to safe values of overpressures based on a trinitrotoluene (TNT) equivalent initiating explosion.

In determining the load from solid detonation explosions (e.g., by a TNT equivalent) in the context of NPP, design and operating experience has shown that explosive hazards have

effects close to and often enveloped by other hazard sources such as impacts and wind (Reference 12.10, Paragraph 6.20).

An explosion involving the detonation of high explosives, munitions, chemicals or liquid and gaseous fuel from facilities and activities in the vicinity of the plant will be considered on a site-specific basis as the AP1000 plant design has an inherent capability to withstand external explosions.

12.9.3 Operator Intervention

Various detectors and alarms (e.g., seismic alarms) are available that have the potential to alert the operators that an external explosion event has occurred and if necessary to shut the reactor down. For situations where the possibility of external explosion has been identified, a site-specific emergency-plan must be adopted.

12.9.4 Regulations

The risk of an external explosion at UK sites has been reduced by the introduction of Control of Major Accident Hazards (COMAH) regulations.

COMAH regulations identify hazards from surrounding sites, which will help to reduce the risk posed by the surrounding sites. The implementation of COMAH regulations (Reference 12.30) provides significant controls on hazardous activities that may lead to an explosion. The COMAH is enforced by the Competent Authority (CA) which comprises the ONR, Environment Agency (EA), Health and Safety Executive (HSE), Scottish Environmental Protection Agency, and Natural Resources Wales working in partnership. The CA is overseen and coordinated by the Competent Authority Strategic Management Group. Planning legislation may be used to restrict the development of installations and facilities that could adversely affect the safety of an NPP.

12.9.5 Systems, Structures, and Components Outside the Nuclear Island

As there are no Class 1 SSCs outside the NI, explosion-induced damage outside the NI will not prevent the delivery of Category A safety functions.

Extreme explosion damage to SSCs outside the NI is judged to be bounded by the consideration of earthquake loading which has been shown will not compromise Class 1 SSCs on the NI.

12.9.6 Combined or Sequential Hazards

There will be no loss of Class 1 SSCs as a result of combined hazards arising from a design basis explosion event.

During periods of extremely high temperatures, there is a possible risk of bush fires and fuel tank explosions. The combined effects of these hazards, however, are judged to be no more severe than the individual consequences. The risk to nuclear safety would be during periods of drought and high ambient temperature when a demand is put on the fire water supplies. This issue is covered in Section 12.10.5.

12.10 EXTREME AMBIENT TEMPERATURES

12.10.1 Safety Design Approach

The plant has been designed so that an extreme ambient temperature within the design basis will not prevent the delivery of Category A safety functions.

12.10.2 Minimum Ambient Temperature

12.10.2.1 AP1000 Design is Bounding of UK Minimum Air Temperature

The minimum daily air temperature recorded in England, Wales and Scotland was -27.2°C (-16.9°F) (Reference 12.31 and Table 12-4). However, the UK minimum ambient air temperature for a 1 in 10,000 year event is lower than the minimum recorded temperature as discussed below.

BS EN 1991-1-5:2003 (Reference 12.32) and its UK national annex document (Reference 12.34) defines minimum shade air temperature actions for the 1 in 50 year and methodology to calculate 1 in 10,000 year events. For the 1 in 50 year return period, Figure NA.1 of Reference 12.32 gives the minimum ambient shade air temperature based on hourly recorded values (Reference 12.32, Section 1.5.3) as -21°C (-5.8 °F) (at Inverness). Converting this temperature using the 1.0E-04/yr correction factor of 1.830 (Annex A.2 of Reference 12.32) gives the minimum UK ambient by 1 in 10,000 year air temperature as -38.4°C (-37.1°F).

These figures need to be adjusted for altitude relative to mean sea level (MSL) and for climate change. BS EN 1991-1-5:2003 (Reference 12.32) suggests reducing the minimum shade air temperature by 0.5°C (0.9 °F) for every 100 m (328 ft) increase in altitude. Hence, for a site at 140 m (459.3 ft) above MSL, the minimum temperature would be -39.1°C (-38.4 °F).

Annex 5 of NS-TAST-GD-013 (Reference 12.3) notes that ambient temperature is likely to be affected by climate change. Climate change predictions from DEFRA UKCP09 (Reference 12.33) show that the average UK winter temperature rise is predicted to be +4.2°C (7.6 °F) for the 2080 medium emissions scenario at the 90 percent probability level. Hence, the minimum ambient air temperature in the UK would increase from -38.4°C (-37.1°F) to -34.2°C (-29.6 °F) at MSL in 2080 which is bounded by the plant design temperature of -40.0°C (-40°F) (see Table 12-4).

Consequently, not allowing for climate change that is predicted to raise the minimum ambient air temperature, the minimum recorded UK mainland temperature (-27.2°C (-16.96°F)) and the 1 in 10,000 year return period minimum ambient temperature based on minimum hourly recorded values (-38.4°C (37.1°F)) are bounded by the plant minimum design temperature of -40.0°C (-40°F) (see Table 12-4).

Additionally, BS EN 1991-1-5:2003 (Reference 12.32) suggests that local features such as sheltered low-lying areas may need to be considered on a site-specific basis using local meteorological data.

12.10.2.2 Minimum Sea-Water Temperature

The minimum achievable sea temperature is -2°C (28.4°F) as this is the temperature at which sea water with an average salinity freezes.

The service water system (SWS) supplies cooling water to remove heat from the heat exchangers cooling water in the turbine building. The AP1000 UK design specifies that the SWS will be served via cooling towers to act as a heat sink and is therefore not based on sea or estuary water cooling. Consequently, the SWS is dependent on ambient air temperature rather than sea temperature.

12.10.2.3 Shield Building

The shield building houses the PCCWST. This tank contains water that is used to augment cooling of the external containment surface in the event of an accident. There is an engineered heating system to keep the water temperature in the PCCWST above the technical specification (Tech Spec) limit of 4.4°C (40°F).

During plant outages in cold weather, the hot water heating system supplies hot water to the plant chilled-water piping that serves the containment building recirculation fan coil units to maintain acceptable ambient air temperatures inside the containment. During a loss of normal alternating current (ac) power, provisions are made to power the hot water heating system from the onsite standby diesel generators.

The containment shell is a path for the removal of decay heat from the containment atmosphere to the environment. However, this process is effective at the minimum ambient temperature.

12.10.3 Maximum Ambient Temperature

12.10.3.1 AP1000 Design is Bounding of UK Maximum Air Temperature

The maximum daily air temperature recorded in England, Wales, and Scotland was 38.5°C (101.3°F) on 10 August 2003 in Faversham, Kent (Reference 12.31). However, for a 1 in 10,000 year event, this peak recorded temperature is exceeded as discussed below.

Annex A.1 of BS EN 1991-1-5 (Reference 12.32) (and its UK national application document (Reference 12.34)) define maximum shade air temperature for the 1 in 50 year and methodology to calculate 1 in 10,000 year events based on maximum hourly recorded values (Reference 12.32, Section 1.5.3). For the 1 in 50 year return period, Figure NA.2 of Reference 12.34, the UK National Annex of Reference 12.32, gives the maximum UK ambient coastal shade air temperature as +31°C (87.8°F) (on the east and south coasts of England). Converting this figure using the 1.0E-04/year correction factor of 1.30 (Annex A.2 of the standard Reference 12.32) gives the maximum UK temperature as +40.3°C (104.5°F).

These figures should be adjusted for altitude relative to MSL and for climate change. BS EN 1991-1-5:2003 (Reference 12.32) suggests applying +1.0°C (1.8°F) to the maximum shade air temperature for every 100 m (328 ft) above MSL. Hence, for a site at 140 m (459.3 ft) above MSL, the maximum temperature would increase to +41.3°C (106.3°F).

ONR TAG NS-TAST-GD-013 (Reference 12.3) notes that temperature is likely to be affected by climate change. Climate change predictions from DEFRA UKCP09 (Reference 12.33) show that the average UK summer temperature rise is projected to be +5.7°C (10.26°F) for the 2080 medium emissions scenario at the 90 percent probability level. Hence, the maximum coastal shade air temperature in the UK may equal +45°C (113°F) at MSL which is less than the AP1000 plant maximum design temperature of +46.11°C (115°F) (see Table 12-4).

The approximate maximum shade air temperatures for coastal locations around the mainland UK for a 1.0E-04/year return period at MSL and incorporating climate change values of +5.7°C (10.26°F) at 2080 are:

- East and South coasts of England: +45°C (113°F).
- Welsh coast: +46°C (114.8°F).
- Scottish coast: +42°C to +45°C (107.6°F to 113°F)

Consequently, the maximum recorded UK mainland temperature (38.5°C (101.3°F)) and the predicted 1 in 10,000 year return period (including climate change at 2080) UK mainland maximum coastal ambient temperature based on hourly recorded air temperatures (+46°C) (114.8°F) are bounded by the AP1000 plant maximum design temperature of +46.11°C (115°F) on the external walls and roof of the NI (see Table 12-4). The site-specific survey in conjunction with DEFRA UKCP09 will determine what is the appropriate climate change temperature increase to apply to the site.

Annex 5.4 of NS-TAST-GD-013 (Reference 12.3) refers to BS 5400 to assess solar gain in safety-related structures, but does not identify a standard or code of practice to evaluate air temperatures. However, solar gain is to some extent site-specific even within the UK and should be considered on a site-specific basis. Additionally, BS EN 1991-1-5:2003 (Reference 12.32) suggests that local features such as sheltered low-lying areas may need to be considered on a site-specific basis using local meteorological data.

12.10.3.2 Maximum Sea-Water Temperature

The UK climate projections predict the UK shelf sea temperatures to rise by between 1.5°C and 4°C (2.7°F to 7.2°F) by the end of the 21st century. This will give rise to maximum sea temperatures in UK waters of approximately 24°C (75.2°F) by the end of the 21st century (Reference 12.35).

As discussed in Section 12.10.2.2, the SWS is dependent on ambient air temperature rather than sea temperature.

The licence applicant will address water supply sources to provide makeup water to the SWS cooling towers.

12.10.3.3 Containment and Shield Buildings

The containment and shield building structures are not affected by the maximum expected ambient temperatures cited above.

The qualification of equipment for expected accident conditions inside the containment bounds any effects of maximum ambient temperature. Engineered cooling functions are capable of maintaining containment temperatures below the Tech Spec limit of 49°C (120°F) if required.

The steel containment vessel provides the path for the removal of decay heat from the containment atmosphere to the environment following an accident and its performance is affected by the ambient temperature. The passive containment cooling system (PCS) meets the AP1000 design ambient temperature of 46.11°C (115°F).

The shield building houses the PCCWST. This tank contains water that is used to augment cooling of the external containment surface in the event of an accident. The PCCWST

maximum water temperature has a Tech Spec limit of 49°C (120°F). It is unlikely that the contents of the PCCWST will ever reach a maximum water temperature of 49°C (120°F) considering that the AP1000 plant maximum air design temperature is 46.11°C (115°F).

12.10.3.4 Spent Fuel Pond

The spent fuel storage facility is located within the auxiliary building fuel handling area and contains post-irradiated fuel which requires active cooling. The spent fuel pond can have the cooling water supply interrupted for a period of up to 7 days without fuel uncovering. The cooling pond has a sufficient heat sink and local make-up water volume to maintain cooling for this period. Although extreme ambient temperature will be a factor in the rate of evaporation, there are appropriate alarms and indications in place to detect when the water level drops below a specific point.

12.10.4 Systems, Structures, and Components Outside the Nuclear Island

As there are no Class 1 SSCs outside the NI; extreme ambient temperature-induced damage outside the NI will not prevent the delivery of Category A safety functions.

12.10.5 Combined Hazards

There will be no loss of Class 1 SSCs as a result of combined hazards arising from a design basis extreme temperature event.

No credible combination of hazards has been identified that could result in greater impact on nuclear safety than would be achieved by each hazard occurring independently.

It is feasible, during periods of extremely high temperature that there will be an increased risk of bush and forest fire. However, the combined effects of these hazards are judged to be no more severe than the individual consequences. The greatest risk to nuclear safety would be during periods of drought and high ambient temperature when a demand is put on the fire water supplies.

Extreme ambient temperatures themselves are not considered to lead to any consequential hazard. There is, however, the potential for pipe work failures in systems containing liquids that are not subject to trace heating or other protection during periods of extreme cold. The consequences of the flooding would be no worse than the internal flooding considered in Chapter 11.

Extreme ambient temperatures of –40.0°C (–40.0°F) and 46.11°C (115°F) are considered for the Class 1 structures in combination with the SSE.

12.11 METEOROLOGY

12.11.1 Safety Design Approach

The AP1000 plant has been designed so that an extreme meteorological event within the design basis will not prevent the delivery of Category A safety functions.

12.11.2 Snow Loading

The load on roofs caused by extreme snowfall, uniform and drifted, is discussed in Section 16.4.1.3.

The AP1000 Plant Civil Structural Design Criteria (Reference 12.16) specifies the imposed ground snow loading as 3.6 kN/m^2 (75 lbs/ft^2) as a uniform blanket determined in accordance with American Society of Civil Engineers (ASCE) 7-98 (Reference 12.55). The potential of snow sliding from a higher sloping roof and being deposited onto a lower roof, is bounded by missiles discussed in Section 12.11.2.2. The ASCE 7-98 snow load corresponds to the 1 in 50 year return period for the AP1000 design. Such a snow loading is applicable to the NI as all the structures of the NI have a concrete roof (see Section 12.4) methodology for the application of snow loading on structures is delineated in Section 16.4.1.3 and Reference 12.16.

The ONR TAG for External Hazards (NS-TAST-GD-013, Annex 5.2, Reference 12.3), states that snow loading should be at least as onerous as given in BS 6399-3 1988 (Reference 12.56), taking account of drifting effects where this can occur.

Uniform Snow Loading

Figure 1 of BS 6399-3: 1988 (Reference 12.56) gives a maximum 1 in 50 year return period snow-on-ground loading value of 1.0kN/m^2 (0.145 lbs/ft^2) (associated with a region of the Scottish Highlands). More typical regional values are 0.8kN/m^2 (0.116 lbs/ft^2) (North-east coastline) and 0.5kN/m^2 (0.073 lbs/ft^2) (elsewhere). Applying an altitude factor of 1.076, equivalent to 140 m (459.3 ft) above MSL, provides 1.076kN/m^2 (0.156 lbs/ft^2), 0.86 kN/m^2 (0.124 lbs/ft^2) and 0.54kN/m^2 (0.078 lbs/ft^2) respectively for the snow on ground loading. The roofs of the shield building and auxiliary building (i.e., the Class 1 structures) attract a maximum snow-on-roof coefficient of 0.8 (Reference 12.56, Figure 2) for a uniform blanket loading, thus giving 0.86 kN/m^2 (0.124 lbs/ft^2), 0.69 kN/m^2 (0.1 lbs/ft^2) and 0.43 kN/m^2 (0.062 lbs/ft^2) for the three regions considered.

For a 1 in 10,000 year snow loading, a return period probability factor of 2.28 is applied to the 1 in 50 year return period event magnitude. This return period probability factor is the same factor adopted for United Kingdom Atomic Energy Authority (UKAEA) sites (Reference 12.57), as provided in the first issue of BS6399-3: 1988. Consequently, the AP1000 design ground snow loading of 3.6 kN/m^2 (0.052 lbs/ft^2) roofs still bounds the maximum UK uniform snow loading for a 1 in 10,000 year event of 2.28 kN/m^2 (0.33 lbs/ft^2).

The methodology for the application of snow loading on structures is delineated in Section 16.4.1.3 and Reference 12.16.

Drift Snow

Drifted snow is considered to be an exceptional event in BS 6399-3: 1988 (Reference 12.56, Section 7.4.1) Drifted snow is characterised by a triangular snow (rather than a uniform) distribution in locations where it can possibly occur (e.g., where the Class 1 auxiliary building roof abuts the upper shield building wall). The methodology for the application of snow loading on structures is delineated in Section 16.4.1.3 and Reference 12.16.

UK practice also highlights the possibility for snow dropping off sloping high level roofs onto low level roofs below. As the adjacent shield building is warm and uses the ventilation as a cooling system to the reactor, it is conceivable that snow could avalanche down the inclined roof of the shield building onto a drift onto the auxiliary building roof creating a ‘double loading’ effect in conjunction with possible dynamic amplification from the cascaded snow.

However, the dynamic amplification of avalanching snow from the shield building onto the low level roofs of the surrounding structures will be bounded by the external missiles considered in Section 12.14.

It is concluded that the AP1000 design parameters exceed the UK requirements for ground snow loading for a 1 in 10,000 year event. Additionally, the UK design basis snow event for both uniform and drifting snow is unlikely to exceed the AP1000 design snow loading on the concrete roof members in the auxiliary building. Additionally, allowing for snow avalanched off the adjacent shield building onto the low level roofs of the surrounding structures will be bounded by the design basis external missiles. This should be confirmed on a site-specific basis.

12.11.2.1 AP1000 Design is Bounding of UK Maximum Snow Loading

The shield and auxiliary buildings roofs of the NI are designed for a ground snow load of 3.6 kN/m^2 (0.052 lbs/ft^2), which bounds the UK 1 in 10,000 year ground snow loading of 2.28 kN/m^2 (0.33 lbs/ft^2).

No allowance for change in snow loading resulting from climate change has been considered as the DEFRA United Kingdom Climate Projections 2009 (UKCP09) projections (Reference 12.6) for snowfall do not yield consistent or robust estimates.

12.11.2.2 Avalanche

Snow dropping off sloping high-level roofs onto low-level roofs below is discussed within the snow drift section of Section 12.11.2.

12.11.2.3 Air Ducts

Other than those on the shield building, no Class 1 air ducts have been identified in the safe shutdown components table.

The air inlets on the shield building are equipped with screens. The screens are designed to help prevent foreign objects or debris from entering the air flow path. In the event of a snow or ice storm, some fraction of these air inlets could temporarily become blocked with snow or ice. The air inlets are designed such that a portion of the inlet area can be blocked without a significant effect on the peak containment pressure for DBE.

The PCS radiant heaters ensure the PCS air flow path is free from blockage of snow and ice prior to an accident. Radiant heaters are provided at the shield building inlet to prevent inlet blockage due to a build-up of snow or ice. The system provides for heating the inlet structures to ensure they are clear of ice and snow to provide for assumed air flow through the system. The system also provides for heating the chimney base plate (shield plate) to keep that region clear of ice and snow and prevent any air-flow blockage.

12.11.2.4 Combined Hazards

There will be no loss of Class 1 SSCs as a result of combined hazards in conjunction with snow loading.

Seismic loads are combined with the specified live loads as delineated in Reference 12.16.

12.11.3 Drought

12.11.3.1 Lead Time

Substantial lead time will ensure that preventative measures can be put into place so that drought will not affect the safety functions. Because of the nature of this hazard, there will be a substantial lead-time before drought impacts upon the plant. Ultimately, the supply of water for plant systems and fire protection will be governed by monitoring procedures such that any shortfalls will stimulate protective actions by operators.

12.11.3.2 Safe Shutdown

Water storage systems that are required for safe shutdown include the passive core cooling system (PXS) and the PCS. Both systems use water storage tanks, which are filled during normal operating conditions and will, therefore, be full before an extreme drought scenario. After 7 days, additional water will be required for PCS and SFP makeup. This water can be transported from the nearby river / sea.

12.11.3.3 Ground Water

There is a potential effect of drought on the building foundations resulting from changes in the groundwater level. This will need to be considered on a site-by-site basis because of differences in geology and groundwater tables. On a site-specific basis, the soil properties of the various layers under possible groundwater conditions during the life of the plant will be compared to the range of values assumed in the standard design.

12.11.3.4 Combined or Consequential Hazards

There will be no loss of Class 1 SSCs resulting from combined hazards arising from drought.

No credible combination of hazards has been identified that could result in greater impact on nuclear safety than would be achieved by each occurring independently. The potential for combined hazards associated with drought is discussed in the section on extreme ambient temperatures (Section 12.10).

12.11.4 System, Structures, and Components Outside the Nuclear Island

As there are no Class 1 SSCs outside the NI, snow and drought-induced damage outside the NI will not prevent the delivery of Category A safety functions.

Snow-loading damage to SSCs outside the NI is judged to be bounded by consideration of missile loading which has been shown not to prevent the delivery of Category A safety functions of the NI. Ice effects do not have to be considered outside the NI.

It is judged that drought-induced damage to SSCs outside the NI will not prevent the delivery of Category A safety functions of the NI.

12.12 EXTREME WIND

This section considers the threat to the nuclear safety-significant features from extreme winds. Wind comes in many forms and is influenced by many factors, including location, altitude, direction, and topography.

Sources of extreme wind include:

- Hurricanes
- Cyclones
- Tornadoes or water spouts
- Tropical typhoons
- Sustained wind
- Gusting wind
- Sand storm

Wind-induced missiles are discussed in the section on missile hazards (see Section 12.14).

12.12.1 Safety Design Approach

Extreme winds can affect plant structures in the following ways:

- If wind forces exceed the load capacity of a building or other external facility, the building fabric or framing might collapse.

- Damage caused by wind may result in loss of off-site power (LOOP). This is a DBE covered in the design basis fault analysis presented in the AP1000 Fault Schedule located in Appendix 8A. In the event of LOOP, the Class 1 safety systems will maintain the plant in a safe state for an indefinite time with support from post 72 hour SSCs including either onsite or offsite ancillary equipment.

The AP1000 design wind is specified as a basic wind speed of 64.82 m/s (145 mph) with an annual probability of occurrence of 0.02. Wind loads are calculated for exposure Category C, which is applicable to shorelines in hurricane-prone areas with an Importance Factor of 1.15. The site parameters for the design wind may be demonstrated to be acceptable for other exposures or topographic factors by comparison of the wind loads on the structures. For example, for a site at a location with exposure Category D, the wind speed should be equal to or less than 58 m/s (129.7 mph).

The plant has been designed so that an extreme wind loading within the design basis will not prevent the delivery of Category A safety functions.

12.12.2 Tornadoes

A tornado is a violent rotating column of air and is the most intense of all atmospheric phenomena occurring typically in the form of a visible condensation funnel, whose narrow end touches the earth and is often encircled by a cloud of debris and dust. Most tornadoes have wind speeds between 32 m/s to 50 m/s (71.6 mph to 111.8 mph), are approximately 20 to 100 m (65 ft to 328 ft) across and travel a few kilometres before dissipating (Reference 12.37). If the tornado reaches a water body (such as the sea, a lake or a reservoir) it is termed a waterspout. A tornado may become a waterspout as the rotation moves from land to sea (and vice-versa).

12.12.2.1 Nuclear Island Tornado Withstand

The procedures described in Section 16.7.6 are used to determine the tornado wind loading in conjunction with the differential atmospheric pressure cited in Table 12-4 as effective loads on NI structures at a wind velocity of 134 m/s (300 mph). Additionally, the NI is checked for

resistance against sliding and overturning resulting from the safe shutdown winds and tornadoes as described in Section 16.13.6.2.

The containment air baffle is located within the upper annulus of the shield building, providing an air flow path for the PCS. The air baffle separates the downward air flow entering at the air inlets from the upward air flow that cools the containment vessel and flows out of the discharge stack. The air baffle is a Class 1 structure designed to withstand the wind and tornado loads defined in Table 12-4.

The NI nonradioactive ventilation system includes tornado-protection dampers designed to close automatically and protect against the effect of 134 m/s (300mph) wind.

12.12.2.2 AP1000 Design is Bounding of UK Historical Tornado Data

The UK has the highest frequency of reported tornadoes per unit area in the world. About 30 to 50 tornadoes are reported each year in the UK. Many tornado reports are from the western Midlands, eastern Midlands, central-southern England, south-eastern England, and East Anglia (Reference 12.42).

Two tornadoes in Britain are known to have reached T8 on the International Tornado Intensity Scale (Reference 12.39) based on their wind speed. However, because these two tornadoes occurred many years ago (in 1091 and 1810), their actual intensities are not known; and it is possible that they may have been even stronger.

A tornado with an intensity of T8 has a maximum wind speed of 107 m/s (239.4 mph) (Reference 12.40). This compares to the design parameters for a Class 1 structure for a design basis tornado (see Table 12-4) velocity of 134 m/s (300 mph) which is the sum of the maximum rotational speed (107.3 m/s (240 mph)) and the maximum translational speed (26.8 m/s (60 mph)) of the tornado. A velocity of 134 m/s (300 mph) is equivalent to T10 on the International Tornado Intensity Scale (Reference 12.39). As Class 1 structures are designed to resist tornado wind loads corresponding to wind speeds of 134 m/s (300 mph) without exceeding the allowable structural design stresses, the design basis tornado velocity for a Class 1 structure bounds the maximum recorded tornado velocity. Climate change may affect worldwide weather patterns but the UK DEFRA climate change projections do not make any predictions of the frequency and intensity of future UK tornadoes. It is considered to be extremely unlikely that a UK tornado will exceed the design basis tornado velocity of the plant design over the plant lifetime.

The following are the design parameters applicable to the AP1000 design basis tornado:

- Maximum wind speed – 134 m/s (300 mph)
- Maximum rotational speed – 107 m/s (240 mph)
- Maximum translational speed – 26.8 m/s (60 mph)
- Radius of maximum rotational wind from centre of tornado – 45.7m (150 ft)
- Atmospheric pressure drop – 13.8 kPa (2.0 psi)
- Rate of pressure change – 8 kPa/s (1.2 psi/s)

It is also noted that tornado wind speeds greater than the plant design basis have a return frequency of between 1.0E-06 and 1.0E-07 per year for a plant sited anywhere in the contiguous United States (US).

12.12.2.3 AP1000 Design is Bounding of UK Design Basis Tornado Loading

ONR NS-TAST-GD-013 (Reference 12.3) refers to the Meaden Report (Reference 12.41) for UK tornado risk assessment which states that the Sussex coast has the highest recorded annual tornado-density in Britain with a 1 in 10,000 year horizontal tornado wind speed of 65.3 m/s (146 mph) (Reference 12.41, pg. 107). This tornado wind speed is bounded by the design of Class 1 structures which are designed to withstand tornado wind speeds of 134 m/s.

For the UK, Table 5.19 of Reference 12.41 gives the pressure drop and rate of pressure change for a range of tornado wind speeds (55 m/s, 60 m/s, 65 m/s and 70 m/s (123 mph, 134 mph, 145 mph, 157 mph)) for four different combinations of translational and rotational components. The maximum pressure drop for a 65 m/s (145 mph) tornado (translation velocity 5 m/s and rotational velocity 60 m/s (134 mph)) is 3.7 kPa (0.53 psi) and a reported maximum of 7 kPa (1.0 psi). The maximum rate of pressure drop for the 65 m/s (145 mph) tornado is given as 1.140 kPa/s (0.165 psi/s). These values are significantly lower than the AP1000 plant tornado design values which allow for a maximum atmospheric pressure drop of 13.8 kPa (2.0 psi) and rate of pressure change of 8 kPa/s (1.2 psi/s) (Table 12-4).

12.12.3 Hurricanes or Tropical Cyclones

Hurricanes are tropical features and generally require sea temperatures much higher than those around the UK, even in the summer. Hence, hurricanes are extremely unlikely to form at UK latitudes. However, the UK does sometimes experience the remnants of old hurricanes coming out of the tropics; as they get entrained into the Atlantic westerly flow at higher latitudes, they can reach the UK and Western Europe (Reference 12.42), where they become conventional storms in the UK and are reflected in UK extreme wind conditions.

The class 2 SSCs that provide the installed post 72-hour plant support of the Class 1 SSCs that are outside the NI are designed for hurricane wind loading. The hurricane wind speed is defined as a 3 second gust at 89.4 m/s (200 mph) (Reference 12.16, Section 5.2).

12.12.4 Wind Loading

The shield and auxiliary buildings are designed to resist an exterior wall wind load corresponding to a 1 in 50 years return period wind speed for a 3 second gust of 64.8 m/s (145 mph) (see Table 12-4). The wind loads are developed using an Importance Factor of 1.15, thus increasing the effective return period to 1 in 100 years.

12.12.4.1 AP1000 Design is Bounding of UK Design Basis Wind Loading

Using conservative assumptions for wind direction and site location, Table 12-5 compares UK 1 in 50 year and 1 in 10,000 year wind pressures, derived from the corresponding wind speeds, to the AP1000 1 in 50 year design wind pressures over the height of the AP1000 plant buildings cited in Table 4 of the Wind Evaluation and Code Requirements (Reference 12.43).

No allowance for change in wind speed resulting from climate change has been considered as the DEFRA UKCP09 climate change projections for wind do not yield consistent or robust estimates of wind speed (Reference 12.44).

From Table 12-5, the AP1000 plant 1 in 50 year design wind pressures significantly exceed the conservatively derived British Standard 1 in 10,000 year wind pressure loading values. It is, therefore, concluded that the AP1000 design wind loading bound the UK wind loading for a 1 in 10,000 year event.

1 in 50 year wind

The ONR Technical Assessment Guide for External Hazards (NS-TAST-GD-013, Annex 5.1, Reference 12.3), states the hazard should be at least as onerous as given in BS 6399-2:1997 (Reference 12.54) for the derivation of extreme wind loading.

The 1 in 50 year 3 second gust design wind speed for the AP1000 plant is 64.82 m/s (145 mph). Figure 6 in BS6399-2: 1997 (Reference 12.54), provides a maximum average hourly wind speed of 27 m/s (60.4 mph) for the 1 in 50 year return period event that occurs at the north Scottish coast. Allowing for an enhancement for altitude and topography (140 m (459.3 ft) above MSL), provides a mean hourly wind speed of 30.78 m/s (68.9 mph). This 1 in 50 year hourly wind speed is converted to a 3 second gust speed the (the effective wind speed used in structural design) using the terrain and building factor S_b factor of (Reference 12.54) (see Table 12-5), which is dependent on the site location relative to the sea, height above ground, and building component dimension.

From Table 12-5, the AP1000 design pressures for the 1 in 50 year wind significantly exceed the British Standard 1 in 10,000 year wind pressure loading values. Further conservatism is present in the AP1000 design of the nuclear island by use of an Importance factor of 1.15 in calculation of the wind pressures. Application of this Importance Factor is equivalent to designing the nuclear island for a 1 in 100 year wind.

1 in 10,000 year wind

The 1 in 50 year effective wind speed is converted to a 1 in 10,000 year effective wind speed by multiplying by a probability factor, S_p derived from Annex D.1 of Reference 12.54. Using conservative assumptions for wind direction and site location, Table 12-5 compares BS 6399-2:1997 (Reference 12.54) design wind pressures, derived from the corresponding wind speeds in (Reference 12.54, Section 2.1.2.1) to the 1 in 50 year AP1000 design wind pressures over the height of the buildings cited in Reference 12.43, Table 4.

The AP1000 plant is not designed for a 1 in 10,000 year wind because this condition is enveloped by the tornado with a maximum wind speed of 134.2 m/sec (300 mph). This wind speed exceeds the 1in 10,000 year wind. From Table 12-5, the AP1000 design pressures for the 1 in 50 year wind exceed the conservatively derived British Standard 1 in 10,000 year wind pressure loading values. Further conservatism is included because the US design includes the Importance Factor of 1.15 discussed above and also applies a load factor for concrete structures, which constitutes the exterior fabric of the entire NI, of 1.7) to the values cited in Table 12-5, whilst the UK would normally apply a load factor of 1.0 to the 1 in 10,000 year design pressures. This margin would be expected to account for any discrepancies in local pressure differences, arising from e.g., vortices, determined using ASCE 7-98 (Reference 12.55) and BS 6399-2 (Reference 12.54).

It is, therefore, concluded that the AP1000 design parameters significantly exceed the UK requirements for a 1 in 10,000 year wind loading.

12.12.5 Sand Storms

This hazard is most relevant to sites in desert areas, and therefore, does not strictly apply in the UK, except conceivably in very dry and windy conditions from soil and dust, and at coastal sites from beach sand. The hazard would be readily apparent and operational measures would be available to control the effects. Also, important building ventilation systems where dust ingress might be undesirable generally have installed plenum inlet filtration to exclude airborne solids.

12.12.6 Sea Spray

Sea spray caused by high winds coming in from the sea could cause possible corrosion of the open power lines to the site with the potential to cause a LOOP. This DBE is covered in the design basis fault analysis presented in the AP1000 Fault Schedule. In the event of LOOP, the Class 1 safety systems will maintain the plant in a safe state for an indefinite time with support from post 72 hour SSCs including either onsite or offsite ancillary equipment. Consequently, sea spray is not considered to be a threat to nuclear safety. Details of appropriate inspections will be described on a site-specific basis and will be carried out by the site licence applicants.

12.12.7 Systems, Structures, and Components Outside the Nuclear Island

As there are no Class 1 SSCs outside the NI, extreme wind induced damage outside the NI will not prevent the delivery of Category A safety functions.

The failure of structures not designed for tornado loadings, and hence, by inference wind gusting, will not affect the capability of Class 1 SSCs. The structures adjacent to the NI are the annex building, the radwaste building, and the turbine building.

- The portion of the annex building adjacent to the NI is classified as seismic Category II and is designed to Seismic Category I structure tornado loading.

- The radwaste building is a small steel-frame building. If it were to collapse in the tornado, it would not impair the integrity of the NI.

- The turbine building First Bay, which is adjacent to the NI, is classified as Seismic Category II and is designed to the same tornado loading as seismic Category I structures. The other portions of the turbine building are classified as NNS and designed per the IBC. The main structure is designed for tornado loading. The impact of tornado-driven sheet metal siding from the turbine building on the NI is evaluated.

More detail on the tornado withstand of the buildings outside of the NI are given in Sections 16.4.2.1 and 16.4.3.

The passive containment cooling ancillary water storage tank is a cylindrical steel tank located at ground level near the auxiliary building. It is analysed, designed, and constructed using the method and criteria for seismic Category II building structures and is also designed and analysed for hurricanes including the effects of sustained winds, maximum gusts and associated wind-borne missiles. Also as noted in Section 12.12.3, Class 2 SSCs intended to support Class 1 SSCs after 72-hours following a design basis fault are designed so they are designed to survive hurricane wind loading.

12.13 OFFSITE FIRE AND SMOKE

Sources of fires considered in this section are:

- Marine-based
- Land-based (including bush and forest fires)

Marine fires, such as fires aboard a ship, and land-based fires (for example, bush or forest fires) pose a threat to nuclear safety through the possibility of smoke and toxic or hot fumes entering the building and affecting personnel and equipment, restricting access to the site or

affecting off-site power. Man-made external fire hazards may arise from fixed hazardous facilities or from transport of combustible material. These hazards should be assessed on a site-specific basis.

The effects of fires external to the site boundary are considered to be bounded by internal fires onsite originating outside plant buildings, and are addressed in Chapter 11. Accordingly, smoke infiltrating the site boundary, rather than fire, is the consideration of this section.

12.13.1 Safety Design Approach

The plant has been designed so that external fire and smoke will not prevent the delivery of Category A safety functions.

12.13.2 Nuclear Island Ventilation System

The NI heating and ventilation air intakes will detect smoke, and their intakes will be isolated, thus, preventing ingress of smoke.

The heating, ventilation, and air conditioning (HVAC) system of the AP1000 design NI comprises three separate ventilation systems:

- NI non-radioactive ventilation system (VBS)
- Radiologically controlled area ventilation system (VAS)
- Containment air filtration system (VFS)

In addition, the radwaste, annex, turbine and diesel generator buildings are designed with independent ventilation systems and are not discussed as part of this chapter.

12.13.2.1 Nonradioactive Ventilation System

The VBS intakes are designed such that upon detection of external smoke, fire dampers are closed so that smoke does not reach safety-significant systems.

The outside air of the MCR and the control support area (CSA) is continuously monitored by smoke detectors located at the outside air intake plenum and the return air is monitored for smoke upstream of the supply air handling units.

The VBS isolates the MCR and or the CSA area from the normal outdoor air intake and provides 100 percent recirculation air to the MCR and CSA areas when a high concentration of smoke is detected in the outside air intake.

The portion of the VBS servicing the auxiliary building is designed so that smoke, hot gases and fire suppressant will not migrate from one fire area to another. Fire or combination smoke and fire dampers are provided to isolate each fire area from adjacent fire areas. These combination smoke and fire dampers close in response to smoke detector signals or in response to the heat from a fire.

12.13.2.2 Radiologically Controlled Area Ventilation Subsystem

The VAS serves radiologically controlled equipment. The ventilation air of the VAS system is continuously monitored by smoke detectors located in the common ductwork downstream of the supply-air handling units and upstream of the exhaust fans.

12.13.2.3 Containment Air Filtration System

VFS is located on the NI and the seismic C-II part of the annex building.

Fire dampers are provided where the ductwork penetrates a fire barrier to maintain the fire resistance rating of the fire barriers. The supply of outside air is continuously monitored by a smoke detector located in the ductwork downstream of the supply-air handling units.

12.13.3 Smoke Barriers

The design of the AP1000 plant is such that routes of entry of external smoke (other than air intake systems) are blocked by fire doors, and smoke entry is unlikely because of long transition spaces.

External fires could affect SSCs or operations if smoke were to enter the MCR or the remote shutdown room. There are no likely smoke paths into the MCR from surrounding areas, with the exception of the HVAC ductwork which is previously addressed. For smoke to leak into the MCR through corridors and doors, smoke would have to pass from within the annex building through a set of fire doors and through the two MCR vestibule doors (one vestibule door will always be closed). The MCR and CSA are positively pressurised, thus, eliminating the potential for smoke to migrate from a low-pressure area to a high-pressure area through the doors and corridors.

12.13.4 Systems, Structures, and Components Outside the Nuclear Island

As there are no Class 1 SSCs outside the NI, smoke-induced damage outside the NI will not prevent the delivery of Category A safety functions.

12.13.5 Combined or Consequential Hazards

No credible combination of hazards has been identified that could result in more impact on nuclear safety than would be achieved by each occurring independently.

There will be no loss of Class 1 SSCs from consequential hazards arising from an external fire, as no credible consequential hazards have been identified as a result of an external fire.

12.14 OFF-SITE MISSILES

The term “missile” is used to describe a moving object that is capable of striking any component of the plant. Malicious missiles, whether explosive or not (for example, improvised explosive devices and rockets), are specifically excluded from consideration. Missiles covered in this chapter include:

- Wind-induced missiles
- From adjacent sites

12.14.1 Safety Design Approach

The plant has been designed so that an external missile within the design basis will not prevent the delivery of Category A safety functions.

12.14.2 Wind Borne Missiles

12.14.2.1 Nuclear Island Tornado Missile Withstand

Class 1 SSCs are enclosed in structures that are designed to withstand the design basis missiles. Impacting missiles into the NI protective barriers are defined in the Reference 12.16 Section 5.2.3.3. Three such design basis missiles are considered to be tornado borne:

- A (deformable) 1814.4-kg (4000 lb) automobile with an impact velocity of 47 m/s (105 mph) horizontally or 33 m/s (74 mph) vertically considered to be able to impact at all plant elevations up to 9.1m (30 ft) above grade. The assessment for this missile and impact velocities were subsequently extended up to 59 m (193 ft) above grade in Reference 12.7 to address higher wall elevations and roof impacts.

- A rigid missile with a mass of 125 kg (275 lb) and 203 mm (8 in) in diameter impacting with a horizontal velocity of 47 m/s (105 mph) or 33 m/s (74 mph) vertically.

- A rigid, solid sphere with a mass of 0.065 kg (0.14 lb)and sufficiently small size (25 mm (1 in) diameter) to pass through any openings in the protective barriers with an impact velocity of 47 m/s (105 mph).

The methodology for justifying missile and protective structures for postulated missiles is discussed in Section 16.5.1.3. One formula for estimating the penetration of steel plate is from the Ballistic Research Laboratory cited in the R3 Impact Procedure (Reference 12.45) which is the recognised impact procedure manual within the UK nuclear industry. The Ballistic Research Laboratory formula employs a rigid missile, which is a conservative assumption as all the energy is assumed to be dissipated into the target rather than being partially absorbed by the missile itself.

Class 1 structures are permitted to sustain local missile damage such as partial penetration and local cracking or permanent deformation or both, provided that structural integrity is maintained and Class 1 SSCs required to function during or after passage of a tornado are not subject to damage by secondary missiles, such as from concrete spalling.

12.14.2.2 AP1000 Design is Bounding of UK Design Basis Missile Loading

Reference 12.3 refers to the Meaden Report (Reference 12.41, Section 5.14) for UK tornado risk assessment which cites several missile configurations:

- 63-kg (138.9 lbs) timber plank (0.1 m x 0.3 m x 3.65 m (3.9 in x 11.8 in x 143.7 in)) at a speed of 32.2 m/s (72 mph) horizontally or 21.5 m/s (48 mph) vertically at a height up to 60 m (196 ft).

- 34.5-kg (76 lbs) steel pipe (75 mm (2.95 in) diameter x 3 m (118.1 in) long) at a horizontal speed of 22.3 m/s (49.88 mph) or 14.8 m/s (33.1 mph) vertically, at a height of up to 30 m (98.4 ft).

In consideration of the AP1000 design basis for missiles, as previously discussed, it can be concluded that the AP1000 design parameters exceed the likely UK extremes for tornado effects.

12.14.3 Missiles from Adjacent Sites

Deflagrations and detonations on adjacent facilities have the potential to result in missiles that could impact the site structures. Such events will be assessed on a site-specific basis, although it is unlikely that such missiles would be outside the design basis missiles defined in Section 12.14.2.

12.14.4 Systems, Structures, and Components Outside the Nuclear Island

As there are no Class 1 SSCs outside the NI, design basis missile-induced damage outside the NI will not prevent the delivery of Category A safety functions.

Class 2 SSCs intended to support Class 1 SSCs after 72-hours that are located outside the NI are designed for impact from hurricane borne missiles defined in Reference 12.16 (Section 5.2.3.2). Offsite SSCs provide a backup to the installed SSCs.

12.15 BIOLOGICAL FOULING

12.15.1 Safety Design Approach

The ONR technical assessment guide on external hazards (Reference 12.3, Annex 7) states that such hazards should be considered as part of SAP EHA.1 addressing the general need to cover all credible hazards.

The plant has been designed such that biological fouling will not prevent the delivery of Category A safety functions. This is achieved in the design and operation by:

- Plant cleanliness
- Screens on air and water inlets
- Inspection of screens

There have been instances on UK nuclear power stations where micro-organisms, birds, animals, and fish have entered into safety-significant areas and have compromised nuclear safety. The principal mechanisms that have been observed are blocking of cooling water systems, gnawing through electrical cables, and blocking of drains with nest material; there are potentially other mechanisms that should also be considered. The hazards are managed by the licensee or operator control programmes and good housekeeping. However, damage to electrical and control cabling (caused by rodents) may affect Class 1 and Class 2 systems; this is addressed in Chapter 11.

A related issue, outside the scope of assessment of external hazards and plant safety, is the possibility of radioactive contamination being spread beyond controlled areas by animal life. This is generally managed on site by measures aimed at limiting the population of animals and birds, and even low-level activity will not be readily accessible to them as the radioactivity is contained within structures and not open to the environment.

Examples of land or air-based biological hazards are:

- Rodents and birds
- Insects (airborne swarms, infestation)
- Tree roots (site-specific)

Examples of water-based biological hazards are:

- Seaweed (marine growth)
- Fish or jellyfish
- Microbes (organic materials)

12.15.2 Land and Air Inlet Systems

Potential hazards from animal entry include blockage to the safety-significant air inlets to the NI buildings.

The use of the appropriate building design and construction codes, which ensure reasonable precautions are taken, supplemented with routine inspections and surveillance by the licensee or operator throughout the life of the plant, will preclude the entry of animals to the AP1000 plant buildings. Grounds maintenance, to include the maintenance of trees on and near the site, will be site-specific.

Large quantities or swarms of insects could conceivably cause the blockage of intakes such as the HVAC or other systems that rely on an air supply to maintain their function. Although there are no AP1000 design features to explicitly protect against ingress of an infestation, measures to preclude bird and animal entry are applicable such as:

- Intake filters for instrument air, service air and high-pressure air compressors.
- Shield building air inlets are fitted with screens.
- The MCR and CSA have features to isolate these areas from the normal outdoor air intake and also provide filtered outdoor air.

12.15.3 Water Inlet Systems

The NI structures are designed to resist biological fouling through the protective features used in the design of the water inlet systems. The AP1000 design does not require external water sources to achieve Category A and post 72-hour Category B safety functions and these systems are classified accordingly.

12.15.4 Systems, Structures, and Components Outside the Nuclear Island

As there are no Class 1 SSCs outside the NI, biologically induced damage outside the NI will not prevent the delivery of Category A safety functions.

Design features to protect against biological entry of Class 2 and 3 water systems include:

- The SWS supplies cooling water to remove heat from cooling water system heat exchangers in the turbine building. Chemical treatment processes are designed to limit biological film formation in the SWS.
- The potable water system is designed to furnish water for domestic use and human consumption. Tests for microbiological and bacteria presence in potable water are conducted periodically.

There are no safety-significant water systems outside the NI that could adversely affect safe shutdown by the entry of biological agents. The effects of damage to SSCs within non-NI buildings and the structures of these buildings or on safety significant plant located on the NI are bounded by the consideration of seismic hazards.

12.15.5 Combined or Consequential Hazards

There will be no loss of Class 1 SSCs from combined hazards arising from a biological fouling event as no credible combination of hazards has been identified that could result in greater degradation of nuclear safety than would be achieved by each occurring independently.

There will be no loss of Class 1 SSCs from consequential hazards arising from a biological fouling event as no credible consequential hazards have been identified as a result of such an event.

It is possible that flooding or high sea levels could increase the amount of biological fouling. This will be a site-specific issue dependent upon the location of the service water supply connection; adequate inspections will be needed to maintain connection pathways.

12.16 ELECTROMAGNETIC INTERFERENCE AND LIGHTNING

12.16.1 Safety Design Approach

The plant has been designed so that EMI and lightning will not prevent the delivery of Category A safety functions.

12.16.2 Electromagnetic Interference

The following have been considered as external sources emitting EMI:

- **Natural EMI sources** – Sources that are associated with natural phenomena. They include atmospheric charge or discharge phenomena such as lightning and precipitation static; extraterrestrial sources including radiation from the sun; and galactic sources such as radio stars, galaxies, and other cosmic sources.

- **Man-made EMI sources** – Sources associated with man-made devices such as power lines.

- **Conducted EMI** – Noise signals transmitted via electrical conduction paths (such as wires and ground planes).

- **Radiated EMI** – Electric and magnetic fields transmitted through space from source to receptor.

- **Intentional radiating emitters** – Emitters whose primary function depends on radiated emitters. Examples include electronic licensed communication systems such as communication, navigation, and radar systems.

- **Unintentional (incidental) radiating devices** – Devices that radiate radio frequencies, but that is not considered their primary function.

- **Restricted radiating devices** – Devices that intentionally use electromagnetic radiation for purposes other than communication or data transfer (such as operating systems and wireless microphones).

Although the man-made EMI sources previously listed are defined as external EMI sources to the plant site, they can be considered in conjunction with internal EMI sources within the site boundary and consequently are addressed in Chapter 11. Natural EMI sources are considered to be bounded by lightning and are addressed in Section 12.16.3.

All Class 1 electrical power is provided from the Class 1 direct current (dc) power system: No AC power system is required to operate the Class 1 safety systems. The Class 1 system provides 250 V DC power for Class 1 SSCs and vital control instrumentation loads including monitoring and control room emergency lighting. It is required for safe shutdown of the plant during a loss of AC power and during a DBA with or without concurrent LOOP.

The protection and safety monitoring system (PMS) has electrical surge withstand capability and can withstand EMI, radio frequency interference and electrostatic discharge conditions that would exist before, during and after a DBA without loss of safety function.

12.16.3 Lightning Protection

The AP1000 design lightning protection system, consisting of air terminals and ground conductors provides protection of exposed structures and buildings housing safety-related and fire protection equipment in accordance with National Fire Protection Association (NFPA) 780 (Reference 12.50). Also, lightning arresters are provided for the transmission lines and at the high-voltage terminals of the outdoor transformers. The isophase bus circuit, which carries a large current, connecting the main generator and the main transformer and the medium-voltage switchgear is provided with lightning arresters. In addition, surge suppressors are provided to protect the plant instrumentation and monitoring system from lightning-induced surges in the signal and power cables that are connected to external devices.

Direct-strike lightning protection for facilities is accomplished by providing a low-impedance path by which the lightning strike discharge can enter the earth directly. The direct-strike lightning protection system, consisting of air terminals, interconnecting cables, and down conductors to ground, are provided external to the facility in accordance with NFPA 780 (Reference 12.50). The system is connected directly to the ground to facilitate dissipation of the large current of a direct lightning strike. The lightning arresters and the surge suppressors connected directly to the ground provide a low-impedance path to the ground for the surges caused or induced by lightning. Thus, fire or damage to facilities and equipment resulting from a lightning strike is avoided.

The design of direct-strike lightning protection and the associated grounding depends on the lightning activity at the plant site and the soil resistivity of the ground. These are site-specific issues and need to be considered on a site-by-site basis.

Lightning is not considered to have a significant impact on the operation of the plant (Reference 12.8, Table I.2).

12.16.4 Systems, Structures, and Components Outside the Nuclear Island

As there are no Class 1 SSCs outside the NI, EMI and lightning-induced damage outside the NI will not prevent the delivery of Category A safety functions.

12.16.5 Combined or Consequential Hazards

Provision of lightning protection to the relevant standard will eliminate the potential for fire in protected buildings and structures. Lightning strikes to surrounding areas, buildings or structures may initiate a fire within the site boundary. The consequences of on-site fire are covered in Section 11.2 and demonstrated to not prevent the delivery of Category A and post-72-hour Category B safety functions.

No other credible combined hazards have been identified involving EMI or lightning.

12.17 CONCLUSIONS

This chapter provides specific supporting information on the nuclear safety withstand of the AP1000 plant against design basis external hazards.

Tables 12-1 and 12-2 identify the external hazards grouping for man-made and naturally occurring hazards respectively. For each hazard category, potential source(s) of the hazards are identified. Postulated initiating events that could result from the identified sources are cited.

The identified groups of hazards in Tables 12-1 and 12-2, after the screening process have been reduced to 11 generic external hazards categories. These have been assessed in this chapter against the Class 1 SSCs of the AP1000 design to ensure that the ability to deliver Category A safety functions is not compromised.

Where relevant, the effect of combined and consequential hazards has been reviewed. The majority of the external hazards assessed in this document fall within the bounds of the generic site parameters (see Table 12-4) and may thus be regarded as within the design basis of the plant. This is mainly due to the inherent robustness of the AP1000 design.

The following paragraphs summarise the safety design approach for each of the hazards considered in detail in Sections 12.6 to 12.16.

12.17.1 Seismic Hazards

The AP1000 plant has been designed so that an earthquake with a 0.3g PGA, defined as the SSE, will not prevent the delivery of Category A safety functions.

The UK design basis RS horizontal acceleration with a PGA of 0.25g marginally exceeds the AP1000 design SSE RS in the range of 8 to 12Hz. However, the probabilistic seismic margin analysis utilising a 0.5g review level earthquake provides confidence in the deterministic 0.3g PGA assessment undertaken for the AP1000 design and that the loading demand of the UK design basis RS will be met. Accordingly, it should be confirmed on a site-specific basis there will be no loss of Category A safety functions resulting from a UK design basis earthquake. SMA provides reasonable assurance that the AP1000 design can with withstand BDB earthquakes

12.17.2 External Flooding

The plant is designed for a floodwater level up to site grade elevation at 100 m (reference elevation 100.0 ft). At the time of site licensing, the applicant will need to demonstrate that the maximum flood from sources such as streams and rivers, potential dam failures, probable maximum surge, and tsunami flooding is below the actual site grade elevation.

The design can conservatively manage UK design basis rainfall, even allowing for climate change over the life of the facility.

12.17.3 Accidental Aircraft Impact

Aircraft impact has been screened-out because it requires a site-specific location to fully substantiate. It should be confirmed on a site-specific basis that accidental aircraft crash frequencies and UK legislation that restricts flying in the vicinity of UK nuclear sites are applicable to the specific site under consideration.

12.17.4 Explosion

In the context of design for an NPP, design and operating experience has shown that explosive hazard has effects close to and often surpassed by other hazards sources such as impacts, earthquakes and tornado loading.

The risk of an external explosion at UK sites has been reduced by the introduction of COMAH regulations.

Various detector and alarms (for example, seismic detectors) are available to alert the operators that an external explosion event has occurred and if necessary take appropriate action; e.g., to shut the reactor down.

An explosion involving detonation of high explosives, munitions, chemicals or liquid and gaseous fuel from facilities and activities in the vicinity of the plant will be considered on a site-specific basis as the design of the AP1000 plant design has an inherent capability to withstand external explosions.

12.17.5 Extreme Ambient Temperature

The minimum recorded UK temperature and the 1 in 10,000 year return period minimum ambient temperature are bounded by AP1000 design minimum ambient design temperature. Taking into account climate change, which is predicted to increase the minimum ambient air temperature, will not impact this assessment.

The maximum recorded UK ambient temperature and the UK maximum temperature for a 1 in 10,000 year return period, including climate change, are bounded by the AP1000 plant maximum design temperature.

The AP1000 UK design specifies that the service water will be cooled via cooling towers (which act as the heat sink) and therefore sea water cooling is not required.

12.17.6 Extreme Wind

The AP1000 design basis tornado wind velocity for a Class 1 structure bounds the maximum recorded and 1 in 10,000 year event tornado velocity. Climate change may affect the

frequency and intensity of future UK tornadoes; but over the lifetime of the plant it is unlikely to exceed the design basis tornado velocity of the AP1000 design.

The AP1000 design wind loading bounds the UK 3 second gust wind loading for a 1 in 10,000 year event.

12.17.7 Other Extreme Meteorological Effects

The shield and auxiliary buildings roofs of the NI are designed for a uniform snow load that bounds the maximum UK snow for uniform loading for a 1 in 10,000 year event.

It is considered that the design basis external missiles discussed in Section 12.14 bound snow avalanching from the roof of the shield building onto the low level roofs below, and therefore, will not threaten any Class 1 SSCs and will bound the potential for avalanche from any other NI buildings.

Substantial lead time will ensure that preventative measures can be put into place so that drought will not affect the safety functions. Due to the nature of this hazard, there will be a substantial lead-time before drought impacts upon the plant. Ultimately, the supply of water for plant systems and fire protection will be governed by monitoring procedures such that any shortfalls will stimulate protective actions by operators.

12.17.8 Offsite Smoke and Fire

Any fires that penetrate the site boundary are considered to be internal fires and are addressed in Chapter 11. Accordingly, smoke infiltrating the site boundary, rather than fire is the consideration of this chapter.

The NI heating and ventilation system air intakes will detect smoke, and the intakes will be isolated, thus preventing ingress of smoke.

12.17.9 Offsite Missiles

AP1000 design Class 1 SSCs are enclosed in structures that are designed to withstand the three design basis missiles. These design basis missiles bound the identified UK design basis external missile loading.

12.17.10 Biological Fouling

Potential hazards from animal entry include blockage to the safety-significant air and water inlet systems of the NI.

The use of the appropriate building design and construction codes, which ensure reasonable precautions are taken, supplemented with routine inspections and surveillance throughout life will preclude the entry of animals to the AP1000 site buildings. Ground maintenance, to include the maintenance of trees on and near the site, will be site-specific.

Ingress of birds and insects is prevented by screens, filters and isolation from normal outdoor air on air intakes.

A common hazard for NPPs is biological fouling entering through open water systems. The AP1000 design has taken this into account by including features to prevent and protect against such occurrences.

12.17.11 Electromagnetic Interference and Lightning

The PMS has electrical surge withstand capability and can withstand EMI, radio frequency interference, and electrostatic discharge conditions that would exist before, during, and after a DBA without loss of safety function for the time required to perform its function.

The lightning arresters and the surge suppressors connected directly to ground provide a low-impedance path to ground for the surges caused or induced by lightning. Thus, fire or damage to facilities and equipment resulting from a lightning strike is avoided.

12.17.12 Summary of Key Conclusions

This chapter has considered the threat to nuclear safety from identified UK external hazards on the AP1000 plant at a generic site. The PCSR and supporting references demonstrate that the AP1000 plant has an adequate design to ensure that the identified external hazards will not prevent the delivery of Category A safety functions.

A number of site-specific assessment requirements have been identified in this report for specific external hazards. In addition to these hazard-specific assessments, there are a number of overall site requirements including accident or incident management and emergency preparedness that will need further consideration at the appropriate stage.

12.18 REFERENCES

12.1 Not Used.

12.2 ONR, “Safety Assessment Principles for Nuclear Facilities,” Rev. 0, Office for Nuclear Regulations, 2014.

12.3 ONR Nuclear Safety Technical Assessment Guide, NS-TAST-GD-013, Rev. 5, “External Hazards,” Office for Nuclear Regulation, September 2014.

12.4 Not Used.

12.5 BNFL Report SRZ/1.130, “Seismic Ground Motion Specification,” British Nuclear Fuels Limited, April 1989.

12.6 DEFRA UKCP09, “United Kingdom Climate Projections,” UK Department for Environment, Food and Rural Affairs.

12.7 Westinghouse Report APP-GW-GLR-133, Rev. 1, “Summary of Automobile Tornado Missile 30’ Above Grade,” May 2010.

12.8 IAEA-TECDOC-1341, “Extreme External Events in the Design and Assessment of Nuclear Power Plants,” International Atomic Energy Agency, 2003.

12.9 IAEA Safety Guide, NS-G-3.1, “External Human Induced Events in Site Evaluation for Nuclear Power Plants,” International Atomic Energy Agency, 2002.

12.10 IAEA Safety Guide, NS-G-1.5, “External Events Excluding Earthquakes in the Design of Nuclear Power Plants,” International Atomic Energy Agency, 2003.

12.11 Not Used.

12.12 Not Used.

12.13 J. Irving, "Seismic Hazard in the UK," in *Seismic Qualification of Safety Related Nuclear Plant and Equipment, Institution of Mechanical Engineers*, 1984.

12.14 Not Used.

12.15 "Consultation on the Strategic Siting Assessment Process and Siting Criteria for New Nuclear Power Stations in the UK," Department for Business Enterprise & Regulatory Reform, July 2008.

12.16 Westinghouse Report APP-GW-C1-001, Rev. 3, "AP1000 Civil/Structural Design Criteria," February 2015.

12.17 DEFRA UKCP09, "Projected Changes in Precipitation," UK Department for Environment, Food and Rural Affairs.

12.18 "Fact Sheet No. 9 – Weather Extremes," National Meteorological Library and Archive, UK Meteorological Office, September 2007.

12.19 BS 6367:1983, "Code of practice for drainage of roofs and paved areas," British Standards Institution, September 1983 (Superseded).

12.20 DEFRA UKCP09, "United Kingdom Projected Sea Level Rise," UK Department for Environment, Food and Rural Affairs, June 2010.

12.21 DEFRA UKCP09, "United Kingdom Observed Vertical Land Movements," UK Department for Environment, Food and Rural Affairs, June 2010.

12.22 DEFRA UKCP09, "United Kingdom Projected Changes in Storm Surges," UK Department for Environment, Food and Rural Affairs, June 2010.

12.23 David J. Dowrick, "Earthquake Resistant Design and Risk Reduction," Wiley, John & Sons, 1987.

12.24 "The Threat Posed by Tsunami to the UK," Study commissioned by Department for Environment, Food and Rural Affairs, Flood Management Division, June 2005.

12.25 "Tsunamis – Assessing the Hazard for the UK and Irish Coasts," Study commissioned by Department for Environment, Food and Rural Affairs, Flood Management Division; Health and Safety Executive; and Geological Survey of Ireland, June 2006.

12.26 UK Statutory Instrument No. 1929, "The Air Navigation (Restriction of Flying) (Nuclear Installations) Regulations 2007."

12.27 "Failure Rate and Event Data for Use within Land Use Planning Risk Assessments," Health and Safety Executive, May 2010.

12.28 J. Byrne, "The Calculation of Aircraft Crash Risk in the UK," AEA Technology plc for the Health and Safety Executive, 1997.

12.29 ARMY TM 5-1300, "Structures to Resist the Effects of Accidental Explosions," US Department of the Army, Navy and Air Force, November 1990. Superseded by UFC 3-340-02, "Unified Facilities Criteria," December 2008.

12.30 UK Statutory Instrument No. 483, "The Control of Major Accident Hazards Regulations," 2015.

12.31 "Weather Extremes," UK Meteorological Office, April 2015.

12.32 BS EN 1991-1-5:2003, "Eurocode 1. Actions on structures, Part 1–5. General actions. Thermal actions," British Standards Institution, March 2004.

12.33 DEFRA UKCP09, "United Kingdom Temperature Rises," UK Department for Environment, Food and Rural Affairs.

12.34 NA to BS EN 1991-1-5:2003, "UK National Annex to Eurocode 1. Actions on structures, Part 1–5. General actions. Thermal actions," British Standards Institution, April 2007.

12.35 DEFRA UKCP09, "Projected Changes in Sub-surface Ocean Variables," UK Department for Environment, Food and Rural Affairs.

12.36 Not Used.

12.37 "Tornado Facts," Tornado and Storm Research Organisation, April 2010.

12.38 Not Used.

12.39 "British & European Tornado Extremes," Tornado and Storm Research Organisation, April 2010.

12.40 "International Tornado Intensity Scale," Tornado and Storm Research Organisation, April 2010.

12.41 "A Study of Tornadoes in Britain with Assessments of the General Tornado Risk Potential and Specific Risk Potential at Particular Regional Sites," Health and Safety Executive, Nuclear Directorate, December 1985.

12.42 UK Meteorological Office.

12.43 Westinghouse Report APP-GW-C1C-001, Rev. 0, "Wind Evaluation Procedures and Code Requirements," April 2004.

12.44 DEFRA UKCP09, "United Kingdom Wind Speed," UK Department for Environment, Food and Rural Affairs.

12.45 BNFL Report, "R3 Impact Assessment Procedure, Missile, Blast, Jets, Pipewhip and Impact: Appendix G – Steel Plate & Pipe Perforation," British Nuclear Fuels Limited, October 2005.

12.46 Not Used.

12.47 Stephen A. Nelson, "Natural Disasters: Meteorites, Impacts, and Mass Extinction," Tulane University.

12.48 Not Used.

12.49 Not Used.

12.50 NFPA 780, "Standard for the Installation of Lightning Protection Systems," US National Fire Protection Association, 2000.

12.51 Not Used.

12.52 Westinghouse Report APP-GW-G1-003, Rev. 6, "AP1000 Seismic Design Criteria," August 2011.

12.53 Westinghouse Reports APP-1000-P2-901 and APP-1000-P2-902, Rev. 4, "NI General Arrangement Section A-A" and "Section B-B," March 2012.

12.54 BS 6399-2:1997, "Loading for buildings. Code of practice for wind loads," British Standards Institution, July 1997 (Superseded).

12.55 ASCE 7-98, "Guide to the Use of the Wind Load Provisions," American Society of Civil Engineers, January 1998 (Superseded).

12.56 BS 6399-3:1988, "Loading for buildings. Code of practice for imposed roof loads." British Standards Institution, March 1988 (Superseded).

12.57 UKAEA/SAH/M20, Safety Assessment Handbook, Issue 2, "External Hazards – Snow Loading," United Kingdom Atomic Energy Authority, February 2006.

12.58 Not Used.

12.59 SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light Water Reactor (ALWR) Designs."

12.60 ONR Nuclear Safety Technical Assessment Guide, NS-TAST-GD-034, Rev. 2, "Transient Analysis for DBAs in Nuclear Reactors," Office for Nuclear Regulation, June 2013.

12.61 Westinghouse Report APP-GW-S2R-010, Rev. 5, "Extension of Nuclear Island Seismic Analysis to Soil Sites," March 2011.

Tables 12-1 and 12-2

The following list of external hazard initiating events is compiled from a variety of sources (References 12.3, 12.8, 12.9, 12.10). The list is divided into two tables: man-made events and natural events.

For the postulated initiating events, the potential consequences are identified and the safety features that are in place to mitigate the consequences are identified. For each initiating event, one of the following six outcomes is stated:

1. The initiating event is addressed in this chapter.

2. The initiating event can be screened out because of a low probability of occurrence or negligible consequences.

3. It can be bounded by another initiating event.

4. The initiating event can be considered under another hazard grouping.

5. The initiating event is specific to a site and consequently requires site-specific information and will be considered in a site-specific PCSR.

6. The initiating event (e.g., fire) is addressed in Chapter 11.

Table 12-1: External Hazards Man-Made Initiating Events

Hazard Grouping		Hazard Source	Initiating Event	Consequence	Mitigating or Safety Feature	Comment
1.	Explosions	Oil refinery Chemical plant Nuclear plant Pipelines Mining Quarrying Marine	Site-specific but given generic consideration in Section 12.9. AP1000 plant requires design review if frequency > 1.0E-05/yr.			
			Deflagrations Detonations	Over-pressure: Collapse of parts of the plant or disruption of systems and components (Reference 12.9)	-	Pending site-specific information regarding explosion risks, the concrete construction of the AP1000 NI should be capable of withstanding substantial overpressures (see Section 12.9.1).
				Fire	-	Considered in Section 12.13 to be addressed as an internal hazard fire (Reference PCSR Chapter 11).
				Ground vibrations	AP1000 plant designed for a design basis earthquake.	Screened-out; pending site-specific information, considered to be bounded by the SSE seismic ground motion.
				Missiles	If the plant had been designed to accommodate the effects of externally generated missiles resulting from other events such as a hurricane, typhoon, tornado, or aircraft crash, the effects of missiles generated by an explosion may already have been taken into account (Reference 12.10, Paragraph 6.10).	Pending site-specific information, addressed by design basis external missiles in Section 12.14.
				Temperature	-	Considered in Item 2 below.
				Release of toxic gases	-	Screened-out as site specific. AP1000 plant requires design review if frequency >1.0E-05/yr (Section 12.1).
				Release of radioactive substances	-	Addressed Chapter 11.

Table 12-1: External Hazards Man-Made Initiating Events (cont.)

Hazard Grouping		Hazard Source	Initiating Event	Consequence	Mitigating or Safety Feature	Comment
2.	Fire	Oil refinery Chemical plant Nuclear plant Pipelines Mining Quarrying Marine Bush/forest Seismic	Conflagration	Fire	-	Fire is addressed in Chapter 11 as to the affect on the NPP an external fire has to transverse the site boundary – where by definition it becomes an internal hazard.
				Temperature: Impaired habitability of main control room, disruption of systems and components, ignition of combustibles	The NI comprises wholly of concrete clad structures that house the Class 1 SSCs and therefore affords protection from external heat sources.	Screened-out: externally initiated fire is an initiator to fire within the NI. Survivability of Class 1 SSCs in a design basis fire is demonstrated in Section 11.2.
				Sparks	The NI structures and equipment will protect against smoke and debris entering the buildings.	Screened-out: ingress into the NI is addressed the same as smoke.
				Smoke, dust: Blockage of intake filters, impaired habitability of control and other important rooms		Considered in Section 12.13.
3.	Missiles	Turbine disintegration Wind borne Deflagrations Detonation	Impact	Penetration, perforation or spalling of systems and components that would impair Class 1 safety functions.	Designed to withstand design basis wind borne missiles.	Turbine disintegration from AP1000 turbine building is considered in Section 11.6. Adjacent plant will be considered in site-specific assessment. Missile impact considered in Section 12.14.
			Loss of grid	-	Off-site power is assumed to be unavailable if missile trips a turbine-generator or reactor protection system.	Screened-out: the passive reactor protection systems can maintain safe shutdown conditions after DBE, following a LOOP for an indefinite time with support from post 72 hour SSCs including either onsite or offsite ancillary equipment.

Table 12-1: External Hazards Man-Made Initiating Events (cont.)

Hazard Grouping		Hazard Source	Initiating Event	Consequence	Mitigating or Safety Feature	Comment
4.	Air traffic Corridor	Light aircraft		Impact onto the NI	UK legislation restricts flying in the vicinity of UK sites (considered in Section 12.8).	Screened-out Requires a site-specific location to fully substantiate (e.g., in terms of target area).
		Helicopters			UK legislation restricts flying in the vicinity of UK sites (considered in Section 12.8).	
		Large or small Transport Aircraft			Has a probability of occurrence of < 1.0E-07 per year (see Appendix 12A).	
5.	Aircraft crash: military			Impact onto the NI	Has a generic probability of occurrence of < 1.0E-07 per year (see Appendix 12A).	Screened-outRequires a site-specific location to fully substantiate.
6.	Windfarms		Missile generation	Impact onto the NI	-	Considered in Item 3 above.
			Electromagnetic Interference	-	-	Considered in Item 22 below.
7.	General infrastructure	Electrical sub stations, Phone masts	Electromagnetic Interference	-	-	Considered in Item 22 below.
		Dam failure	Flooding	-	-	Site-specific considered generically in Item 13 below.

Table 12-1: External Hazards Man-Made Initiating Events (cont.)

Hazard Grouping		Hazard Source	Initiating Event	Consequence	Mitigating or Safety Feature	Comment
8.	External Transport	Liquified natural gas (LNG) vessel	Fire	Loss of Category A safety functions	-	Considered in Item 2 above.
			Missile generation	Impact onto the NI	-	Considered as a DBE in Item 3 above.
			LNG explosion	Over-pressure: Collapse of parts of the plant or disruption of systems and components (Reference 12.9)	-	Considered in Item 1 above.
		Ship collision	Impact	-	-	Screened-out as site specific.
			Oil contamination	Blockage or damage of plant water intakes	-	Addressed in Item 9 below: Non-biological fouling.
		Railway	-	Damage to the infrastructure of the AP1000 site	-	Screened-out as site specific.
		Road vehicles	-	Impact into the NI	AP1000 design basis missile considers an automobile impacting at 47 m/s.	Considered in Section 12.14.2.1 as a tornado borne missile.
		Barges	-	Damage to the infrastructure of the AP1000 site.	-	Screened-out as site specific.
9.	Non-biological fouling	-	Oil contamination	Blockage or damage of plant water intakes	AP1000 has protective features to prevent ingress through its open water systems.	Addressed by Item 20 below as the same precautions apply for the water inlet systems.
		-	Rubbish or domestic waste		-	Addressed by Item 20 below: biological phenomena.

Table 12-1: External Hazards Man-Made Initiating Events (cont.)

Hazard Grouping		Hazard Source	Initiating Event	Consequence	Mitigating or Safety Feature	Comment
10.	Eddy currents into ground (Reference 12.9)	-	Electric potential into ground	-	-	Bounded by lightning and earthing considerations.
11.	Toxic chemical	Containment leak from adjacent plant	-	Release to the environment	-	Screened-out as site specific. Requires design review if frequency >1.0E-5/yr. (Section 12.1)

Table 12-2: External Hazards Naturally Induced Initiating Events

Hazard Grouping		Initiating Events	Consequence	Mitigating or Safety Feature	Comment
12.	Seismicity	Earthquake ground motion	Internal and external structural and infrastructure damage.	AP1000 has been designed to a 0.3g PGA earthquake loading.	Considered in Section 12.6 as a 1 in 10,000 UK DBE.
		Tsunamis	"	"	Addressed in Item 13 below: flooding.
		Seiches	"	"	Addressed in Item 13 below: flooding.
		Long period ground motion (Reference 12.3, Table 1)	"	"	Considered in Section 12.6.
		Liquefaction	"	"	Addressed in Item 26 below: surrounding influences.
		Subsidence	"	"	
		Settlement	"	"	
		Fire	"	"	Seismically initiated events are considered as generic internal fires addressed in Chapter 11.

Table 12-2: External Hazards Naturally Induced Initiating Events (cont.)

Hazard Grouping		Initiating Events	Consequence	Mitigating or Safety Feature	Comment
13.	Flooding	Tides		The AP1000 design; e.g., orifices in the NI, are sited above the level of the maximum probable flood so as not to allow water ingress. Basemat and exterior wall of the NI are designed to resist upward and lateral pressures caused by the probable maximum flood	Pending site-specific information addressed by design basis external floods in Section 12.7.
		Sea- and river-based flood	Overturning or sliding of the NI as described in Section 12.7.6.		
		Rain	Flooding of NI internal structures	Ponding of water on the sloping roofs of the NI cannot occur. The design capacity of the NI to remove rain water bounds the 1 in 10,000 year return period design basis rain intensity value.	Considered in Section 12.7.2 as a 1 in 10,000 UK DBE.
		Barometric effects	Increased water levels	-	Included as a contribution to storm surges in Section 12.7.4.
		Tsunamis	Overtopping of sea defences	The heights of tsunami waves arriving close to the shore are comparable to those in typical storm surges. All major UK centres of population have flood defence infrastructure designed to cope with the expected range of surges (Reference 12.24).	Pending site-specific information, considered generically in Section 12.7.5.
		Seiches	"	-	Bounded by tsunamis in magnitude (Reference 12.23, Section 3.2(11)).
		Storm surges	Overtopping of sea defences	-	Site specific: Predicted trends in storm surges due to climate change considered in Section 12.7.4.1.
		Ground water levels	Flotation, uplift of the NI.	The AP1000 plant is designed for a normal groundwater elevation up to plant elevation 99.39 m (98 ft) above.	Site specific. Licence applicant will address site–specific information on ground water Pending site-specific information, considered generically in Section 12.7.3.

Table 12-2: External Hazards Naturally Induced Initiating Events (cont.)

Hazard Grouping		Initiating Events	Consequence	Mitigating or Safety Feature	Comment
13. (cont.)	Flooding (cont.)	Snow/Ice melt	Flooding of NI internal structures	"	Screened-out considered as contributing to external flooding.
		Wind induced waves	Overtopping of sea defences	"	Screened-out pending site-specific information considered generically as a contribution to storm surges in Section 12.7.4.
		Natural obstruction (Dam forming) in water courses	Flooding of site/ disruption to plant infrastructure	"	Pending site-specific information is considered to be addressed under external flooding.
		Channel changes	Flooding of site/ disruption to plant infrastructure	"	Screened-out as site-specific issue.
		Surface run-off	Flooding of site/ disruption to plant infrastructure	"	Screened-out as site-specific issue.
		Landslides or avalanche into bodies of water	Disruption to plant/ plant infrastructure	"	Screened-out as a site-specific issue. Site-specific analysis should be carried out to ensure that there is no risk from surrounding land formations.
		Failure of water retaining structures (Dam Failure)	Flooding of site/ disruption to plant infrastructure	"	Site specific issue.
		Climate Change	Increased flood water depth	"	Considered in Sections 12.7.2 and 12.7.4.

Table 12-2: External Hazards Naturally Induced Initiating Events (cont.)

Hazard Grouping		Initiating Events	Consequence	Mitigating or Safety Feature	Comment
14.	Extreme Ambient Temperature	Low ambient air temperature	Embrittlement/ equipment malfunction	UK minimum ambient temperature for a 1 in 10,000 year event bounded by AP1000 design basis.	Considered in Section 12.10.2.1 as a 1 in 10,000 UK DBE.
		High ambient air temperature	Equipment malfunction.	UK maximum ambient temperature for a 1 in 10,000 year predicted bounded by AP1000 design basis.	Considered in Section 12.10.3.1 as a 1 in 10,000 UK DBE.
		Extremes of ambient ground temperature	-	-	Screened-out as a site-specific issue dependent on site characteristics.
		Extremes of ambient sea/river temperature	Blockage of plant water outflows or coolant water.	-	The AP1000 design is not dependent on sea and river temperatures as the service water removing heat from the heat exchangers cooling water of the UK AP1000 design envisages the service water will be served via cooling towers to act as a heat sink and therefore does require sea water cooling (see Sections 12.10.2.2 and 12.10.3.2).
		Solar effects	Enhances ambient temperature on external surfaces	-	Pending site-specific information, considered generically in Section 12.10.3.1.

Table 12-2: External Hazards Naturally Induced Initiating Events (cont.)

Hazard Grouping		Initiating Events	Consequence	Mitigating or Safety Feature	Comment
15.	Meteorological	Snow	Roof damage	UK maximum snow loading for a 1 in 10,000 year event is bounded by AP1000 design basis.	Considered in Section 12.11.2 as a 1 in 10,000 UK DBE.
		Snow/Ice air inlet Blockage	Blockage to PCS	-	Considered in Section 12.11.2.
		Hail		-	Considered as a missile – other missiles bound (Reference 12.8, Table I.2). Bounded by design basis missiles considered in Item 3 above.
		Roof Avalanche	Roof Damage	-	For the AP1000 design, sliding snow avalanching from the shield building which is the biggest/highest building on the NI would not be expected to threaten adjacent structures on the NI as this scenario would be bounded by the design basis missiles considered in Item 3 above (see Section 12.11.2.2).
		Frost	Water freezing	-	Screened-out: Bounded by snow and ice considerations (Reference 12.8, Table I.2.).
		Humidity	Condensation of water vapour on cool surfaces	-	Screened-out: Conventional engineering design provisions such as electrical systems situated outdoors will provide adequate protection and humidity does not represent a significant hazards and will not be considered further.
		Frazil (see Table 12-3 for definition)	-	-	Bounded by sea ice.

Table 12-2: External Hazards Naturally Induced Initiating Events (cont.)

Hazard Grouping		Initiating Events	Consequence	Mitigating or Safety Feature	Comment
15. (cont.)	Meteorological (cont.)	Sea Ice	Blockage of plant water outflows or coolant water.	-	Screened-out as a site-specific issue: Water supply sources will be addressed by the licence applicant.
		Rime Ice (see Table 12-3 for definition)	Roof damage. Downing of grid. cables	-	Screened-out: Considered bounded by snow loading. The passive reactor systems can maintain safe shutdown conditions following a LOOP for an indefinite time post 72 hours with support from post 72 hour ancillary equipment and onsite and offsite water sources..
		Ice Storm	Damage to fabric of building	-	Screened-out: Considered bounded by snow and design basis external missile loading.
		Drought	Effect on building Foundations	Substantial lead time will ensure that preventive measures can be put in place to ensure that drought will not affect safety functions.	Considered in Section 12.11.3.
16.	Extreme Wind	Hurricane (see Table 12-3 for definition)	Structural damage	AP1000 design tornado wind velocity bounds the hurricane wind velocity (see Table 12-4).	Screened out: by the location of the UK. Remnant of North Atlantic hurricanes are reflected in UK meteorological data (see Section 12.12.3).
		Cyclones			
		Tropical Typhoons (see Table 12-3 for definition)			
		Tornadoes/Water Spouts (see Table 12-3 for definition)	Structural damage	AP1000 tornado design for Class 1 structures is bounding of UK historical tornado data.	Tornado governs water spouts (Reference 12.8, Table I.2). Considered in Section 12.12.2.
		Wind: Sustained Wind: Gusts	Structural damage	Extreme UK Wind Loading for a 1 in 10,000 year event, is bounded by the AP1000 design basis of the plant.	Considered in Section 12.12.4 as a 1 in 10,000 UK design basis.

Table 12-2: External Hazards Naturally Induced Initiating Events (cont.)

Hazard Grouping		Initiating Events	Consequence	Mitigating or Safety Feature	Comment
17.	Airborne Activity	Abrasive dust	Blocking of penetrations/vents and disruption to the grid supply	-	Judged equivalent. Sand storms considered in Section 12.12.5.
		Sand storms		-	
		Sea spray	-	-	Considered in Section 12.12.6.
		Fog/Mist	Could increase the probability of human made hazard involving surface vehicles or air.	-	Screened-out: A phenomenon which by itself has no significant impact on the operation of a nuclear power plant and its design basis (Reference 12.8, Table I.2).
18.	Volcanic Activity	Volcanic Activity	Structural collapse	-	Screened-out: For a UK site there is no indigenous volcanic activity. Therefore assumed to have a probability of occurrence of less than 1.0E-07/yr (Reference 12.8, Table I.2). There are currently no design criteria to counter volcanic activity.
		Volcanic Ash	Blocking of penetrations/vents.	-	Screened out: The distance from the UK to any active volcanoes is such that ash particulate will be small and well dispersed.
19.	Geotechnic Faults/Fissures	-	-	-	Screened-out: There are no known surface faults in the UK.

Table 12-2: External Hazards Naturally Induced Initiating Events (cont.)

Hazard Grouping		Initiating Events	Consequence	Mitigating or Safety Feature	Comment
20.	Biological Phenomena	Rodents Birds Fish Jellyfish Insects Marine growth Tree roots Microbes Leaves	Blockage of inlets, vents and penetrations. Damage by rodents and corrosion resulting from bird residue.	-	Considered in Section 12.15.
21.	Natural Collisions	Tree Logs	Blockage of water inlets	-	Screened-out: Bounded by ice blockage in Item 15 above.
22.	Electromagnetic Interference	Solar flares Static electricity Electromagnetic pulse External EMI Variation in the grid Frequency	Fire Electric & electronic malfunction. Electrocution.	-	Considered in Section 12.16.
23.	Lightning	-	Fire Electric & electronic malfunction. Electrocution	-	Considered in Section 12.16.
24.	Glaciations	-	-	-	Screened-out as a site-specific issue.

Table 12-2: External Hazards Naturally Induced Initiating Events (cont.)

Hazard Grouping		Initiating Events	Consequence	Mitigating or Safety Feature	Comment
25.	Meteorite/ Asteroid	Meteorite	Impacting of Plant	-	Screened-out: Probability of occurrence. Less than 1.0E-07/yr depending on latitude (Reference 12.8, Table I.2). Therefore can be screen-out owing to their low frequency of occurrence).
		Asteroid		-	Screened-out: Probability of occurrence less than 1.0E-07/yr (Reference 12.47) for an asteroid > 1 km (0.62 mi) in diameter. Therefore is BDB and can be screened out owing to their low frequency of occurrence
26.	Surrounding Influences	Settlement/Subsidence Ground heave Mining Caverns Leaching Contaminated land Radon Geysers Coastal erosion Slope instability Soil stability	-	-	Screened-out as site-specific issues (Reference 12.8, Table I.2).
		Liquefaction	-	-	Screened-out: Site specific. The Licence applicant will demonstrate for soil sites that the potential for liquefaction is negligible for both the soil underneath the NI foundation and the soil adjacent to the NI.

Table 12-3: Hazard Definitions

Deflagration	Is a technical term describing subsonic combustion that usually propagates through thermal conductivity. Deflagrations (Reference 12.10, Paragraph 6.15) are usually associated with relatively dilute gas or vapour for which most of the chemical energy is dissipated in the form of heat.
Detonation	Is a supersonic combustion and propagates through shock compression.
Boiling Liquid Expanding Vapour Explosion	This is a type of explosion that can occur when a vessel containing a pressurised liquid is ruptured.
Precipitation	Is any product of the condensation of atmospheric water vapour that is pulled down by gravity and deposited on the earth's surface.
Frazil Ice	Is a collection of loose, randomly oriented needle-shaped ice crystals in water and resembles slush. It sporadically forms in rivers, lakes and oceans, on clear nights when the weather is colder, and air temperature reaches minus 6°C (42.8°F) or lower. Frazil ice is the first stage in the formation of sea ice.
Rime Ice	A coating of ice; e.g., on grass and trees, formed when extremely cold water droplets freeze almost instantly on a cold surface.
Hurricane	Hurricanes form in the north Atlantic Ocean and the northeast Pacific Ocean, east of the dateline. A hurricane only forms in the tropics where the sea-surface temperature is at least 27°C (80.6°F) in the north Atlantic Ocean and the northeast Pacific Ocean. It is characterised by a large low-pressure centre and numerous thunderstorms that produce strong winds and heavy rain. Collectively, hurricanes, typhoons and cyclones are known as tropical cyclones.
Tornadoes	A major whirlwind is termed a *tornado*, if it reaches a water body (such as a sea, lake or reservoir) it is termed a *waterspout*. A tornado may become a waterspout as the rotation moves from land to sea (and *vice-versa*). A tornado is a violent rotating column of air and is the most intense of all atmospheric phenomena occurring typically in the form of a visible condensation funnel, whose narrow end touches the earth and is often encircled by a cloud of debris and dust. Most tornadoes have wind speeds between 32 m/s and 50 m/s (71.6 mph to 111.8 mph), are approximately 20 to 100 m (65 ft to 328 ft) across, and travel a few kilometres before dissipating. However, the most extreme can attain wind speeds of more than 134 m/s (300 mph), are more than 1.6 km (1 mi) across and can travel for more than 100 km (62 mi).
Typhoons	In the western Pacific hurricanes are called typhoons, and in the Indian Ocean they are called cyclones. Collectively, hurricanes, typhoons, and cyclones are known as tropical cyclones.

Table 12-4: Comparison of Extreme UK Hazards Values and AP1000 Design Values

Event Description		AP1000 Design Values	Comment	Extreme Weather Events Recorded in the UK	Comment	UK Design Basis	Comment
Natural Events							
Ambient Air Temperature	Maximum	46.11°C (115°F) dry bulb 30.06°C (86.1°F) wet bulb (Table 4-9).	All exterior walls of the NI are designed for 46.11°C (115°F) and -40°C (-40°F). (Reference 12.16)	38.5°C (101.3°F)	Recorded on the 10th August 2003 in Faversham, Kent (Reference 12.31). (see Section 12.10.3.1).	For a 1 in 10,000 year event at 2080: shade air temperature of 46°C (114.8°F) (including climate change considerations at a UK coastal site) (see Section 12.10.3.1)	-
	Minimum	-40°C (-40°F) (Table 4-9).		-27.2°C (-16.96°F)	Recorded on the 11th February 1895 in the Highlands of Scotland and Braemar (Aberdeenshire) on the 10 January 1982. Also at Altnaharra on 30 December 1995 (Reference 12.31). (See Section 12.10.2.1)	For a 1 in 10,000 year event: shade air temperature of -34.2°C (-29.6°C) (including climate change considerations) (see Section12.10.2.1)	-

Table 12-4: Comparison of Extreme UK Hazards Values and AP1000 Design Values (cont.)

Event Description		AP1000 Design Values	Comment	Extreme Weather Events Recorded in the UK	Comment	UK Design Basis	Comment
Natural Events (cont.)							
Sea Temperature	Maximum	Not specified	The AP1000 design is not dependent on sea and river temperatures as the service water removing heat from the heat exchangers cooling water of the UK AP1000 design envisages the service water will be served via cooling towers to act as a heat sink, and therefore, does require sea water cooling (see Sections 12.10.2.2 and 12.10.3.2)	24°C (75.2°F)	Includes climate change projections to 2098 (Reference 12.35) (see Section 12.10.3.2).	-	-
	Minimum	Not specified		-2°C (28.4°F)	See Section 12.10.2.2.	-	-

Table 12-4: Comparison of Extreme UK Hazards Values and AP1000 Design Values (cont.)

Event Description		AP1000 Design Values	Comment	Extreme Weather Events Recorded in the UK	Comment	UK Design Basis	Comment
Natural Events (cont.)							
Rain	Rate of rainfall	24 hr rainfall not recorded.	-	279 mm (11 in) in 24 hr (Reference 12.18)	Recorded near Dorchester, Dorset on the 18/07/1955 (Reference 12.18).	-	-
		525.8 mm/hr (20.7 in/hr) (Table 4-9).	-	92 mm (3.6 in) in 1 hr (Reference 12.18)	Recorded at Maidenhead, Berkshire on 12/07/1901 (Reference 12.18)	-	-
		160.0 mm/5 min (6.3 in/5 min) (Table 4-9).	-	32 mm (1.3 in) in 5 min (Reference 12.18)	Recorded at Preston, Lancashire on 10/08/1893. (Reference 12.18)	For a 1 in 10,000 year event: 42 mm/ 5 min (1.7 in/ 5 min) (see Section 12.7.2.4)	-
Snow/Ice	Ground load	3.6 kPa (75 psi) (Table 4-9, Reference 12.16).	NI roof loads (including drifting) will be calculated in accordance with Reference 12.16	1.0 kPa (0.145 psi) (see Section 12B.2.1)	-	For a 1 in 10,000 year event: ground snow loading of 2.28 kPa (0.33 psi) (see Section 12B.1)	-
Wind Speed Limit	Operating Basis 3 sec gusting	64.82 m/s (145 mph) (Table 4-9).	-	-	-	-	-

Table 12-4: Comparison of Extreme UK Hazards Values and AP1000 Design Values (cont.)

Event Description		AP1000 Design Values	Comment	Extreme Weather Events Recorded in the UK	Comment	UK Design Basis	Comment
Natural Events (cont.)							
Tornado	Maximum Wind Speed	134 m/s (300 mph) (Table 4-9 Reference 12.16)	Is the sum of the maximum rotational speed of 107.3 m/s (240 mph)and translational speed 26.8 m/s (60 mph) (Reference 12.16)	107 m/s (239.4 mph) (Reference 12.40)	Two tornadoes in Britain (in the years 1091 and 1810) are suspected to have reached a tornado wind speed of 107 m/s (239.4 mph) (Reference 12.40)	For a 1 in 10,000 year tornado: 65.3 m/s (146 mph) (Reference 12.41, Page 107)	Applicable to the Sussex coast.
	Radius of maximum rotational wind from tornado centre	45.7 m (150 ft) (Reference 12.16)	-	Not recorded.	-	-	-
	Atmospheric pressure drop	13.8 kPa (2.0 psi) (Reference 12.16)	-	-	-	7 kPa (1 psi) (Reference 12.41)	-
	Rate of Pressure Change	8 kPa/s (1.2 psi/s), (Reference 12.16)	-	-	-	1.140 kPa/s (0.165 psi/s) (Reference 12.41 Page 109)	-
Hurricane	3 second gust	89.4 m/s (200 mph) (Reference 12.16)	-	-	-		Hurricanes are extremely unlikely events at UK latitudes.
Seismic (SSE)	PGA	0.3g (Table 4-9), (Reference 12.52).	-	-	-	For a 1 in 10,000 year earthquake: 0.25g	AP1000 RS does not wholly bound UK RS anchored at these two PGA (see Section 12.6)

Table 12-4: Comparison of Extreme UK Hazards Values and AP1000 Design Values (cont.)

Event Description		AP1000 Design Values	Comment	Extreme Weather Events Recorded in the UK	Comment	UK Design Basis	Comment
Man-made Events							
Tornado borne Missiles	Deformable	A (deformable) 1814.4 kg (4000 lb) automobile with an impact velocity of 46.94 m/s (105 mph) horizontally or 33.1 m/s (74 mph) vertically considered to be able to impact at all plant elevations up to 59 m (193.57 ft) above grade (Reference 12.7) (Table 4-9)	-	-	-	63 kg (139 lb) timber plank impacting at 32 m/s (71.6 mph) (Reference 12.41).	-
	Rigid	124.7 kg (275 lb), 203.2 mm (8 in) shell at 46.94 m/sec (105 mph) horizontal, 33.1 m/sec (74 mph) vertical (Table 4-9)	-	-	-	34.5 kg (76.1 lb) steel pipe impacting horizontally at 22.3 m/s (50 mph) (Reference 12.41)	-
	Rigid	25.4 mm (1 in) diameter steel ball at 46.94 m/sec (105 mph) horizontal and vertical (Table 4-9).	-	-	-	-	-

Table 12-5: Comparison of AP1000 Design and UK 1 in 10,000 Year Wind Pressures

BS 6399-2 values (Reference 12.54)						AP1000
Height m (ft)	S_b	Effective Wind Speed 1 in 50 Year Event m/s (mph)	Corresponding Wind Pressure for a 1 in 50 Year Event kN/m^2 (lb/ft^2)	Effective Wind Speed 1 in 10,000 Year Event m/s (mph)	Wind Pressure 1 in 10,000 Year Event kN/m^2 (lb/ft^2)	Wind pressure 1 in 50 Year Event kN/m^2 (lb/ft^2) (1)
5 (16.4)	1.65	50.8 (113.6)	1.58 (0.23)	64.0 (143.2)	2.51 (0.36)	2.56 (0.37)
10 (32.8)	1.78	54.8 (122.6)	1.84 (0.27)	69.0 (154.3)	2.93 (0.42)	2.95 (0.43)
15 (49.2)	1.85	56.9 (127.3)	1.99 (0.29)	71.7 (160.4)	3.16 (0.46)	3.22 (0.47)
20 (65.6)	1.90	58.5 (130.9)	2.10 (0.30)	73.7 (164.9)	3.33 (0.48)	3.41 (0.49)
30 (98.4)	1.96	60.3 (134.9)	2.23 (0.32)	76.0 (170.0)	3.54 (0.51)	3.72 (0.54)
50 (164)	2.04	62.8 (140.5)	2.42 (0.35)	79.1 (176.9)	3.84 (0.56)	4.14 (0.60)

Note:

1. The AP1000 wind pressures have been calculated from Reference 12.43 (Table 4), disallowing for gust factor (G) and external pressure coefficient (Cp) which are similar to BS 6399-2 factors.

APPENDIX 12A
AIRCRAFT CRASH FREQUENCY

12A.1 Derivation of Target Area

The ETA of the AP1000 Facility and the NI is estimated from the following relationships:

For light aircraft, small and large transport aircraft and MCA accidents initiated over 2000 feet:

$$ETAA = l.w + 0.8.h(w + l)$$ (Reference 12A.1, Equation 13)

For helicopters:

$$ETAH = l.w + 0.62.h(w + l)$$ (Reference 12A.1, Equation 15)

where,

l is the 'envelope' length equal to the length of the facility;
w is the 'envelope' width;
h is the 'envelope' height.

The values assigned for l, w and h for both the entire AP1000 site and the NI are specified in Table 12A-1.

12A.2 Summary of Aircraft Crash Frequencies for AP1000

Table 12A-2 provides an overall crash rate of 4.8E-07 and 5.13E-06 crashes per year for the NI only and the AP1000 site, respectively. Thus, considering the NI only reduces by an order-of-magnitude the ETA for the entire AP1000 generic site and the corresponding crash frequency per annum.

For the NI, the combined crash rate includes all aircraft types. However, the aircraft that form the greatest risk to the NI by virtue of their mass and velocity are small and large transport aircraft and MCA. However, these classes of aircraft can be screened out as they have crash rates of less than 1.0E-07/yr and are, thus, BDB (Reference 12A.2, Annex 2.2).

The background crash rates quoted for MCA assumes that the site in question is not within an area of high crash concentration, which tends to correspond to areas where low-level flying occurs. There are two such areas in the UK; one in Northern England and the other around Lincolnshire. If the site falls within these zones then a value of 5.81E-05 km-yr^{-1} is applied. If the site falls within a transition zone (i.e., within 50 km of the boundary of a high MCA crash concentration zone), then a reduced crash rate per year is applied as outlined in Reference 12A.3, Paragraph 149. Such a transition zone would apply to areas such as Sellafield and Hartlepool.

12A.3 References

12A.1 J. Byrne, "The Calculation of Aircraft Crash Risk in the UK," AEA Technology plc for the Health and Safety Executive, 1997.

12A.2 ONR Nuclear Safety Technical Assessment Guide, NS-TAST-GD-013, Rev. 5, "External Hazards," Office for Nuclear Regulation, September 2014.

12A.3 "Failure Rate and Event Data for Use within Land Use Planning Risk Assessments," Health and Safety Executive, May 2010.

12A.4 Westinghouse Reports APP-1000-P2-901 and APP-1000-P2-902, Rev. 4, "NI General Arrangement Section A-A" and "Section B-B," March 2012.

Table 12A- 1: Dimensions Applied to the ETA

	l m (ft)	w m (ft)	H m (ft)	References	ETAA km^2 (mi^2)	ETAH km^2 (mi^2)
AP1000 Generic Site	426.7 (1400)	236.2 (775)	69.7 (229)	(Reference 12A.4) .	0.1377 (0.053)	0.1294 (0.050)
NI	97.5 (320)	48.3 (158)	69.7 (229)	(Reference 12A.4) .	0.0128 (0.005)	0.0110 (0.004)

Table 12A- 2: Aircraft Crash Frequencies for a Generic UK Crash Site

		AP1000 Generic Site		NI	
Aircraft Category	Background Crash rate (Reference 12A.3, Para 148) (km^{-2} yr^{-1} x 1.0E-05)	Effective Target Area ETAkm^2 (mi^2)	Crash Frequency (yr^{-1} x1.0E-07)	Effective Target Area ETA km^2 (mi^2)	Crash Frequency (yr^{-1} x1.0E-7)
Light aircraft	2.04	0.1337 (0.053)	27.3	0.0128 (0.005)	2.6112
Helicopters	1.05	0.1294 (0.050)	13.6	0.0110 (0.004)	1.1550
Small transport aircraft	0.26	0.1377 (0.053)	3.5	0.0128 (0.005)	0.3328
Large transport aircraft	0.11	0.1377 (0.053)	1.5	0.0128 (0.005)	0.1408
MCA	0.41	0.1377 (0.053)	5.5	0.0128 (0.005)	0.5248
		Combined	51.3	Combined	4.8

APPENDIX 12B
POST-FUKUSHIMA ASSESSMENT

12B.1 Introduction

On March 11, 2011, a magnitude 9 earthquake (on the Richter scale) struck the east coast of Japan. The earthquake, together with the resulting series of large tsunami waves affected several nuclear power facilities, either directly by damaging onsite equipment, or indirectly by impairing the supporting infrastructure, such as the electrical power grid.

Tokyo Electric Power Company Fukushima Dai-ichi Nuclear Power Station faced a particularly challenging situation including a loss of all ac electrical power for four of their six units and a loss of ultimate heat sink (UHS) makeup. Consequently, severe damage to the fuel and a series of hydrogen explosions occurred.

Considering the accident at the Fukushima Dai-ichi nuclear power station in Japan, several initiatives were launched worldwide to assess the lessons learned. These include but are not limited to the European stress tests, the ONR Interim and Final Report (References 12B.1 and 12B.2), and the IAEA Expert Mission Report (Reference 12B.3).

The AP1000 plant design and its passive safety concepts have been developed considering catastrophic events, which may lead to a complete and extended loss of power and infrastructure damage limiting site accessibility. As a result, the AP1000 plant design is very robust against these types of events. However, reviewing lessons learned is a hallmark of the nuclear industry and inherent to the Westinghouse safety culture. Therefore, Westinghouse established an internal expert team to perform a comprehensive review of the AP1000 plant design in light of the events at the Fukushima Dai-ichi nuclear power plant.

The intent of the initial Westinghouse review was to challenge the plant's design and further evaluate the performance of the AP1000 plant design when subjected to extreme hazards, such as those experienced at the Fukushima Dai-ichi site. The initial review was conducted with the best preliminary information available to Westinghouse at the time. The review team challenged the plant's design for combinations of scenarios involving extreme external hazards and loss of station power sources. Information from the initial reviews was utilised to generate summary assessments of AP1000 plant design's ability to cope with station black out (SBO) events, arrangements for spent fuel pool cooling, and protection against external hazards. The review team also identified tasks, as described below, which required further assessment.

As more formalised information and recommendations have become available, the results of the initial internal evaluations have been reviewed, refined, and formalised to be able to respond to government and regulatory requests such as the recommendations presented in HM Chief Inspector final report and the requests from the European Commission.

Following the events at Fukushima, the European Commission declared that "the safety of EU nuclear power plants should be reviewed on the basis of a comprehensive and transparent risk assessment" in the form of a "stress test." Driven by this recommendation, the European Nuclear Safety Regulators Group developed the European Union "Stress Test" specifications (Reference 12B.1). While the stress test is mainly designed for applications to an operating plant, it does provide a framework under which a new plant design such as the AP1000 plant can be 'stressed' to evaluate the robustness of the design. The stress test is defined as a targeted reassessment of the safety margins of nuclear power plants in light of the events which occurred at Fukushima: extreme natural events that challenge the plant safety functions and could lead to a severe accident.

The European Stress test provides an appropriate tool by which to present the results of the AP1000 evaluation and inform the response to Chief Inspector Weightman's recommendations.

This assessment consisted of the following:

- An evaluation of the response of the AP1000 nuclear power plant when facing a set of extreme situations, as defined below in the description of work section.
- Verification of the preventative and mitigating measures chosen following a defence in depth logic – initiating events, consequential loss of safety functions, and severe accident management.

For the assessment of these extreme situations, sequential loss of the lines of defence was assumed using a deterministic approach, irrespective of the probability of this loss. This approach allows for the evaluation of the levels of defence available following different external hazards, both within and BDB. The assessment reports on the response of the plant and on the effectiveness of the preventative measures. The assessment identifies if there are any potential vulnerabilities for the considered extreme events in order to verify the robustness of the plant's defence in depth design, and identify if there are any reasonably practical enhancements that could provide potential margin improvements.

The assessment focused on the impact of such extreme events relative to maintaining the key plant safety functions of core cooling, containment integrity, and spent fuel pool cooling. The focus of the technical scope of the AP1000 plant stress test assessment will be placed on the following issues:

- Initiating events
    - Earthquake
    - Flooding (not limited to a tsunami)
    - Combination of both
    - Other potential limiting external hazards
- Consequences of loss of safety functions from initiating events considered in the standard plant design
    - Loss of electrical power, including SBO
    - Loss of UHS
    - Combination of both
- Severe accident management issues
    - Means to protect from and to manage loss of core cooling functions
    - Means to protect from and to manage loss of cooling functions in the spent fuel pool
    - Means to protect containment integrity

Unlike an operating nuclear facility, site and operator-specific design aspects cannot be completely addressed in the stress test evaluation for the AP1000 design, but generic considerations are provided. These aspects include such items as site location, geography and topology; return period considered in the design basis for extreme events; site-specific emergency responses facilities; and site-specific flooding protection measures.

The UK AP1000 Plant Post-Fukushima Assessment is summarised in Section 12B.3

12B.2 Assessment of Fukushima Lessons Learned

Reviewing lessons learned is a hallmark of the nuclear industry and inherent to the Westinghouse safety culture. As part of Generic Design Assessment, Westinghouse evaluated the lessons learned coming from the various international reviews. The assessment of lessons learned is documented in Reference 12B.4.

12B.3 UK AP1000 Plant Post-Fukushima Assessment

The UK AP1000 Plant Post-Fukushima Assessment is documented in Reference 12B.5. The assessment has 9 sections which are summarised below.

Section 2 provides a description of the AP1000 plant standard site characteristics and a description of the AP1000 standard plant, including AP1000 plant main parameters; the scope and main results of the PSA.

Section 3 discusses the AP1000 seismic design and the margin against BDB seismic events. The AP1000 plant is designed for an earthquake defined by a PGA of 0.30g and the CSDRS specified in the assessment. The magnitude of the AP1000 SSE envelopes the PGA defined in the EUR. The EUR defines the horizontal PGA as 0.25g. Therefore, the AP1000 SSE, in terms of PGA, provides 20 percent margin relative to general European seismic requirements as specified in the EUR. Section 3.2 describes the seismic margin assessment (PCSR Section 12.6.3.4) which as discussed was performed to demonstrate margin over the SSE of 0.3g. The goal of the SMA was to demonstrate that the plant HCLPF is at least 0.5g PGA. The results of the SMA actually show even a greater margin for most of the safety functions.

Section 4 discusses the plant protection and robustness against flooding events. The AP1000 plant is designed for a normal groundwater elevation up to plant elevation 99.4 m (98 ft) and for a probable maximum flood level up to plant elevation 100 m (reference elevation 100.0 ft), which is also the plant reference grade level. The robustness evaluation performed in Section 4.2 has shown that:

- The AP1000 design provides margin beyond the flooding design basis to maintain a safe shutdown condition with no fuel damage or radiological releases to the general public for extreme BDB flood levels.
- The combination of a BDB seismic event with a BDB flood event will not result in more severe consequences than those described for the individual events.

Sections 3 and 4 therefore show that the AP1000 design provides a unique capability to respond to design basis and BDB events due to three fundamental safety advancements:

- The AP1000 Design Self Actuates. For SBOs, critical SSCs will automatically achieve a fail-safe configuration without the need for operator action or ac/dc power.

- The AP1000 Design is Self-Sustained. The AP1000 design's passive approach to safety de-emphasises the importance of ac power and cooling supply.

- The AP1000 Design is Self Contained. SSCs critical to placing the reactor in a safe shutdown condition are protected within the steel containment vessel and further surrounded by a substantial "steel concrete" composite shield building.

Section 5 provides the results of the assessment of the AP1000 design in case of LOOP, SBO, and loss of UHS as a consequence of a BDB seismic event coincident with a BDB flood event to confirm the robustness of the AP1000 design in mitigating extreme natural hazards. The various lines of defence of the plant against LOOP/SBO types of event are described and their robustness against severe BDB external events was assessed.

One of the major differences of the AP1000 design when compared to the currently operating pressurised water reactors, is the extreme robustness of the design to loss of water makeup capability. On the reactor side, heat is removed first from the reactor core by the PXS, which has sufficient water inventory protected inside containment to operate for very long period of times, then heat is removed from the containment by the PCS. The spent fuel decay heat is removed by heating up and boiling off SFP water with steam released to the atmosphere through a vented path. Safety systems (in-containment water inventory, SFP water inventory, PCS water inventory) have sufficient capacity to support the safety functions for at least 72 hours. As discussed in Sections 3.2 and 4.2, those passive safety systems are very robust against extreme BDB events. Even credible BDB events will not result in a challenge to the passive systems to fulfil their functions during the first 72 hours. After 72 hours, makeup will need to be provided to the PCCWST and the SFP, as described above. Note that a MAAP analysis has shown that:

- In the highly unlikely case of an operator not being able to supply water to the top of the containment after 3 days of cooling, air cooling alone will be sufficient to provide an HCLPF after 3 days. The equilibrium containment pressure, while above the ASME Service Level C pressure limit, still corresponds to a low probability of failure.

- In the highly unlikely case of an operator not being able to supply water to the top of the containment after 7 days of cooling, pressure within the containment vessel would slowly increase but would not be expected to reach the normal design pressure for over 2 days. Even in the case of this very unlikely event, considering that the steel containment vessel has a very large margin above the normal design pressure, the peak containment pressure will not exceed the ASME Service Level C pressure limit.

Section 6 describes the severe accident mitigation features of the AP1000 passive plant that are designed to minimise any radiological impact from hypothetical accidents resulting in extensive damage to the nuclear fuel in the reactor core. Severe accident management capabilities have been integrated into the AP1000 plant design from the beginning of the design process. PSA and the associated analyses and testing were used to identify scenarios, boundary conditions and postulated severe accident phenomena that must be mitigated to ensure containment integrity in the event of core damage.

Section 7 provides a brief overview of the human factors considerations important to BDB situations and a discussion of the assumptions made of the site-specific emergency plan. It also includes the human factors assessments conducted on a sample of two limiting operator

actions that would be required after a postulated BDB extreme external event to ensure successful long-term (post-72 hour) cooling of the plant. This BDB extreme external event is postulated to be a BDB seismic event with subsequent BDB tsunami that occurs either at power or during a refuelling outage with full core offload. Both actions are assessed to be feasible and likely to succeed, given the assumptions of the site-specific emergency plan.

Section 8 provides the ALARP arguments to determine if there any enhancements that could be incorporated into the design of the AP1000 plant for the UK to further enhance the plant's design margin against BDB extreme events. As mentioned previously, the AP1000 is robust; no additional changes are required to maintain the key safety functions. However, the proposed design changes enhance the coping capabilities of the AP1000 during BDB extreme external events and improve the margin against external hazards. The proposed design changes have been included in the Design Reference Point (Reference 12B.6) and have been incorporated as appropriate into this PCSR. The design changes are summarised below:

- BDB flood protection for Class 1 batteries – This design enhancement protects the Class 1 electrical supply system batteries from BDB flooding by adding water proof doors, sealing penetrations, adding HVAC snorkels and adding a latched and gasket seal over ancillary diesel generator exhaust.
- Enhanced power supply for communication system – This design enhancement extends the power supply for the communication systems during a SBO.
- Improved post-72 hour cable connections – This design enhancement improves the connection of the offsite diesel generators by significantly reducing the length of temporary cable as well as the cable diameter required to connect the offsite diesel generators to its loads .
- Addition of PCCAWST connection – This enhancement improves the accessibility to the PCCAWST during BDB extreme external events to use the PCCAWST as a source of makeup water for the SFP and Containment cooling. The proposed design enhancement is comprised of adding a new connection line to the PCCAWST, a new isolation valve and a flanged connection.

Section 9 provides a summary of results of the Fukushima assessment performed for the UK AP1000 design and the conclusions. This is summarised in Section 12B.4.

12B.4 Conclusions

It can be concluded that for a Fukushima-like event, the AP1000 design demonstrates robustness with respect to BDB external hazards. The passive safety systems ensure that the core remains cool, the containment remains intact, and SFP cooling is maintained for the first 72 hours. After 72 hours, the AP1000 design has permanently installed ancillary equipment as well as connection points for portable equipment to extend the operation of the passive safety systems indefinitely.

The AP1000 nuclear power plant passive design represents a significant improvement over conventional pressurised water reactors, and is developed around the fundamental design principles of safety, simplification and standardization. The development of the AP1000 plant safety concept based on passive systems allows full realization of the benefits of these fundamental design principles. The adoption of passive systems as the primary means to deliver safety functions, combined with reliable defence in depth active systems, allows achievement of both an unparalleled level of safety and optimised support for investment

protection. These benefits are especially evident when evaluating the AP1000 design's ability to meet the lessons learned and recommendations coming from the international nuclear industry. Westinghouse as a nuclear industry leader, has incorporated lessons learned and will continue to evaluate the plant for design enhancements that may enhance the performance of the AP1000 design in response to BDB extreme events.

For the UK AP1000 generic design, Westinghouse has identified design enhancements that provide additional margin against BDB extreme external events. These enhancements are not required to meet safety goals; however, they provide enhanced coping capabilities and support plant operations following such extreme events.

12B.5 References

12B.1 ENSREG, "EU 'Stress Tests' Specifications, Annex 1," European Nuclear Safety Regulators Group, May 2011.

12B.2 ONR Report, "Japanese Earthquake and Tsunami: Implications for the UK Nuclear Industry, Final Report," Office for Nuclear Regulation, September 2011.

12B.3 IAEA, "International Fast Finding Expert Mission of the Fukushima Dai-ichi NPP Accident Following the Great East Japan Earthquake and Tsunami," International Atomic Energy Agency, June 2011.

12B.4 Westinghouse Report UKP-GW-GL-109, Rev. 0, "Assessment of Fukushima Lessons Learned Reports," June 2016.

12B.5 Westinghouse Report UKP-GW-GGR-201, Rev. 1, "UK AP1000 Plant Post-Fukushima Assessment," July 2016.

12B.6 Westinghouse Report UKP-GW-GL-060, Rev. 10, "AP1000 Design Reference Point for UK GDA," January 2017.

APPENDIX 12C
COMPARISON OF UK PML AND AP1000 EARTHQUAKE SPECTRA

12C.1 Comparison of UK PML and AP1000 Earthquake Spectra

Figure 12C-1 compares the UK PML hard, intermediate and soft site spectra for 5 percent critical damping for PGA of 0.25g with the AP1000 hard site spectra at 5 percent critical damping for a PGA of 0.3g given in Reference 12C.1.

Class 3, non-seismic structures will be designed in accordance with the Eurocode or IBC as defined within Chapter 16.

The vertical spectrum is usually taken as two-thirds of the horizontal value per NS-TAST-GD-013 (Reference 12C.2).

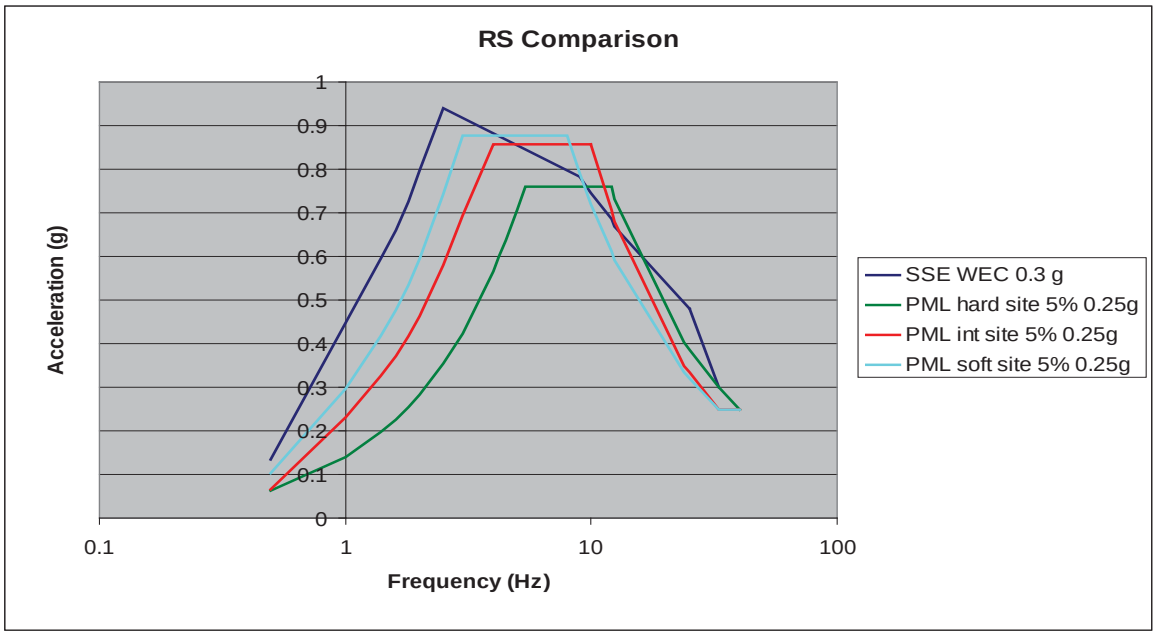


Figure 12C-1: Comparison of PML and AP1000 Earthquake Spectra

Notes: PML values are taken from the digitised tables, interpolating linearly between frequency values when necessary. AP1000 values are taken from Table 2 and Figure 1 of APP-GW-G1-003 (Reference 12C.3).

12C.2 References

12C.1 Westinghouse Report APP-GW-S2R-010, Rev. 5, "Extension of Nuclear Island Seismic Analysis to Soil Sites," March 2011.

12C.2 ONR Nuclear Safety Technical Assessment Guide, NS-TAST-GD-013, Rev. 5, "External Hazards," Office for Nuclear Regulation, September 2014.

12C.2 Westinghouse Report APP-GW-G1-003, Rev. 6, "AP1000 Seismic Design Criteria," August 2011.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS AND ACRONYMS

ac	alternating current
ADS	automatic depressurisation system
ALARP	as low as reasonably practicable
ALWR	advanced light water reactor
AO	auxiliary operator
AOP	abnormal operating procedure
APS	alarm presentation system
ARP	alarm response procedure
BDB	beyond design basis
CDF	core damage frequency
C&I	control and instrumentation
CIM	component interface module
CMT	core makeup tank
COMIT	constructability, operability, maintainability, inspectability, and testability
CPS	computerised procedures system
CSF	critical safety function
CSFT	critical safety function status tree
CVS	chemical and volume control system
DAP	duly authorised person
DAS	diverse actuation system
DBA	design basis analysis
DCIS	distributed control and information system
DCP	design change package
DDS	data display and processing system
DiD	defence in depth
DRP	design reference point
DV	design verification
EOP	emergency operating procedure
EPRI	Electric Power Research Institute
ERM	error reducing mechanism
ESF	engineered safety feature
EUR	European utility requirement
FBTA	function-based task analysis
GDA	generic design assessment
GOP	general operating procedure
HAD	human action database
HBSC	human-based safety claim
HEA	human error analysis
HEART	human error assessment and reduction technique
HED	human engineering discrepancy
HEI	human error identification
HEP	human error probability
HF	human factors
HFE	human failure event
HFI	human factors integration
HRA	human reliability analysis
HSE	Health and Safety Executive
HSI	human system interface
HuP	human performance
HX	heat exchanger

LIST OF ABBREVIATIONS AND ACRONYMS (cont.)

IAEA	International Atomic Energy Agency
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
INPO	Institute of Nuclear Power Operations
IRWST	in-containment refuelling water storage tank
ISO	International Standards Organisation
ISV	integrated systems validation
JTA	job and task analysis
LCS	local control station
LOCA	loss-of-coolant accident
LP&SD	low power and shutdown
LRF	large release frequency
LWR	light water reactor
MCA	main control area
MCR	main control room
MIIE	maintenance-induced initiating events
MLE	maintenance latent error
MTIS	maintenance, testing, inspection, and surveillance
NASA	National Aeronautics and Space Administration
NOP	normal operating procedure
NPP	nuclear power plant
NRC	Nuclear Regulatory Commission
OATC	operator at the controls
OCS	operation and control centre system
OER	operational experience review
OIIE	operator-induced initiating events
ONR	Office for Nuclear Regulation
OSA	operational sequence analysis
OSC	operations support centre
PAM	post-accident monitoring
PCS	passive containment cooling system
PCSR	pre-construction safety report
PDSP	primary dedicated safety panel
PFOE	post-fault operator error
PLS	plant control system
PMS	protection and safety monitoring system
POSS	plant operator selection system
PPE	personal protective equipment
PSA	probabilistic risk assessment
PRHR	passive residual heat removal
PSA	probabilistic safety assessment
PSF	performance shaping factor
PWR	pressurised water reactor
QDPS	qualified data processing system
RAW	risk achievement worth
RCS	reactor coolant system
RFM	refuelling machine
RGP	relevant good practice
RIHA	risk-important human action
RNO	response not obtained

LIST OF ABBREVIATIONS AND ACRONYMS (cont.)

RNS	normal residual heat removal system
RO	reactor operator
RRW	risk reduction worth
RSR	remote shutdown room
RSW	remote shutdown workstation
RTS	reactor trip system
SAA	severe accident analysis
SACRG	severe accident control room guideline
SAG	severe accident guideline
SAMG	severe accident management guideline
SAP	safety assessment principle
SART	situation awareness rating technique
SAT	systematic approach to training
SBO	station blackout
SCG	severe challenge guideline
SDSP	secondary dedicated safety panel
SFAIRP	so far as is reasonably practicable
SFP	spent fuel pool
SFS	spent fuel pool cooling system
SG	steam generator
SGTR	steam generator tube rupture
SM	shift manager
SOP	system operating procedure
SQEP	suitably qualified and experienced person
SRO	senior reactor operator
SS	shift supervisor
SSC	system, structure, or component
SSD	system specification document
STA	shift technical advisor
STP	surveillance test procedure
TAD	target audience description
TAG	technical assessment guide (ONR)
Tech Spec	Technical Specification
TLX	task load index
TPRT	team performance rating technique
TSC	technical support centre
TSV	task support verification
UK	United Kingdom
URD	utility requirements document
US	United States
V&V	verification and validation
VBS	nuclear island non-radioactive ventilation system
VDU	visual display unit
VES	emergency habitability system
WANO	World Association of Nuclear Operators
WPIS	wall panel information system

13 HUMAN FACTORS

13.1 Introduction

This chapter describes how an integrated and managed Human Factors (HF) Engineering programme has been rigorously and systematically applied throughout the concept analysis and design phases of the Standard AP1000 Plant design. The measured and proportional application of HF processes and methodologies has ensured that the design considers at all times the role of the human operator in the safe and efficient operation of AP1000. It further demonstrates, for a sample of scenarios where operators are required to take action in order to maintain or restore nuclear safety, a methodology for conducting Human Error Analysis (HEA) of nuclear-safety related tasks. The HEA methodology results provide input to the substantiation of an argument that risk of failure in those actions has been reduced, as low as reasonably practicable (ALARP), for the Standard AP1000 Plant design.

13.2 Regulatory Expectations, Safety Principles and Standards

This Pre-Construction Safety Report (PCSR) chapter has been constructed within a United Kingdom (UK) regulatory framework as informed by:

- Office for Nuclear Regulation (ONR) Safety Assessment Principles (SAPs) (Reference 13.1);
- Legal requirement for a duty holder to reduce risks, '*as low as reasonably practicable*' (ALARP) (Reference 13.2), which is the concept that drives ONR's 'goal-setting' regulatory regime for nuclear safety (Reference 13.3);
- International and national modern safety standards and industry guidance recognised by ONR as providing the relevant good practice (RGP) underpinning the SAPs and Technical Assessment Guides (TAGs).

13.2.1 Safety Assessment Principles (SAPs)

The SAPs provide the ONR with a framework for consistent regulatory judgements on nuclear safety, radiation protection and radioactive waste management activities of new (proposed) and existing nuclear facilities. The SAPs may also provide guidance to designers and duty-holders on the appropriate content of safety cases in clarifying ONR's expectations in this regard.

The key SAPs in providing guidance on the appropriate content of the HF safety case for AP1000 during the UK generic design assessment (GDA) are the specific HF principles EHF.1 to EHF.11. These cover the HF topics, processes and methodologies that will ensure:

- There has been a systematic, through-life, approach to human factors integration (HFI) within the design, assessment and management of systems and processes
- The allocation of safety actions between humans and engineered structures, systems or components (SSCs) has been substantiated.
- A systematic approach has been taken to identify human actions that can impact safety for all permitted operating modes and all fault and accident conditions identified, in the safety case, including severe accidents.

- Administrative controls needed to keep the facility within its operating rules for normal operation or return the facility back to normal operations have been systematically identified.

- Proportionate analyses have been carried out for all tasks important to safety and used to justify the effective delivery of the safety functions, to which they contribute.

- Workspaces in which operations (including maintenance activities) are conducted have been designed to support reliable task performance. The design should take account of the physical and psychological characteristics of the intended users and the impact of environmental factors.

- Suitable and sufficient user interfaces have been provided at appropriate locations to provide effective monitoring and control of the facility in all normal operating modes, fault and accident conditions.

- A systematic approach to the identification and delivery of personnel competence has been applied.

- Procedures have been produced that support reliable human performance during activities that could impact on safety.

- The number of competent personnel needed to operate the facility safely, in all its operational states, has been assessed and is understood.

- Proportionate analyses of human actions and administrative controls that are necessary for safety as part of the design basis analysis (DBA), probabilistic safety analysis (PSA) and severe accident analysis (SAA) aspects of the safety case.

Because modern nuclear power plants (NPPs) are relatively complex, socio-technical systems with an inter-related reliance on both engineered and human components to maintain nuclear safety, HF becomes a transverse topic spanning numerous other technical areas and safety disciplines. For this reason, a number of the ONR's other SAPs contain guidance that is pertinent to the content of the HF safety case. Key amongst these are:

- Leadership and management for safety - The organisation focuses on achieving and sustaining high standards of safety and establishing and sustaining a positive safety culture (MS.1). Learns from internal and external sources to continually improve safety decision making and safety performance (MS.4).

- Engineering principles - The design concept, of defence in depth (DiD), providing multiple independent barriers to fault progression, should be applied (EKP.3). Safety functions are identified based on an analysis of normal operation and of fault sequences determined through fault analysis (EKP.4) and appropriate safety measures provided to deliver the safety functions (EKP.5). SSCs should be classified on the basis of the safety functions they deliver and their significance to safety (ECS.1). Where safety functions are delivered or supported by human action, those human actions should be identified and classified on the basis of those functions and their significance to safety (ECS.2). Where reliable and rapid protective action is required, automatically initiated, engineered safety measures should be provided (ERL.3). For requirements that are less demanding, or on a longer timescale, administrative safety measures, i.e., those involving operator actions based on procedures, may be acceptable (ERL.3). The design and layout should facilitate access for necessary activities and minimise adverse

interactions while not compromising security aspects (ELO.1).

- Safety systems - For all fast acting faults (typically less than 30 minutes), safety systems should be initiated automatically and no human intervention should then be necessary to deliver the safety function(s) (ESS.8). The design should be such that the operators or other facility personnel cannot negate a correct safety system action, but can initiate safety system functions and perform the necessary actions to deal with circumstances that might prejudice safety (ESS.8). Where human intervention is needed to support a safety system following the start of a requirement for protective action, then the timescales, over which the safety system will need to operate unaided, before intervention, should be demonstrated to be sufficient (ESS.9). In keeping with internationally accepted relevant good practice for power reactors, no human intervention should be necessary for approximately 30 minutes from the start of the safety system initiation (ESS.9). There should be direct means of confirming to operating personnel: (a) that a demand for safety system action has arisen; (b) that the safety systems have operated (actuated) fully and correctly; and (c) whether any limiting condition (operating rule) has been exceeded that takes the safety system beyond its substantiated capability (ESS.13). Suitable and sufficient safety-related system control and instrumentation should be available to the facility operator in a central control room, and as necessary at appropriate secondary control or monitoring locations (ESR.1).

- Fault analysis - Fault analysis should be carried out comprising suitable and sufficient DBA, PSA and SAA to demonstrate that risks are ALARP. Where the fault analysis is in support of a design under development, the analysis should be against a well-defined reference point in the design process. Where facility-specific or site-specific details have yet to be finalised, all the assumptions made in lieu of these should be stated explicitly and then used to support the later design and construction activities. The DBA provides an input into safety classification and the engineering requirements for systems, structures and components performing a safety function; the limits and conditions for safe operation; and the identification of requirements for operator actions (FA.9). The PSA model provides an adequate representation of the facility (FA.13) accounting for contributions to the risk including, but not necessarily restricted to: (d) unavailability due to testing and maintenance; (e) pre-fault human errors (e.g., misalignments and miscalibrations); (f) human errors that lead to initiating faults; (g) human errors during the course of fault sequences, including those required for repair or recovery actions; and (h) potential dependencies between separate human activities (either by the same or by different operators) (FA.13). The PSA is used to inform the design process and help ensure the safe operation of the site and its facilities (FA.14), supporting modifications to design or operation (FA.14) and supporting the demonstration that risks are tolerable and ALARP (FA.14).

13.2.2 As Low As Reasonably Practicable (ALARP)

The term ‘as low as reasonably practicable’ (ALARP) is used to express the Requesting Party’s legal duty to reduce risks so far as is reasonably practicable (SFAIRP), and is a concept that must be applied at all levels of risk, extending below the level that may be deemed broadly acceptable. In simple terms, it is a requirement to take all measures to reduce risk where doing so is reasonable.

To inform and guide its employees engaged in developing ALARP justifications and to enable a standard approach to be taken across the different topic areas of GDA, Westinghouse has provided the basis for determination of appropriate ALARP assessments

(Reference 13.6) and guidance on developing justifications for risks that are ALARP in supporting the safety case.

This guidance, as consistent with Reference 13.4, explains that the substantiation of risk being reduced ALARP requires a balanced argument containing elements of:

- Compliance with RGP, including adequate standards and codes, industry best practice and lessons learned;
- Demonstration of 'optioneering' as outlining the different options and assessing the pros and cons of each before making a decision, on which presents risks ALARP;
- Inclusion of quantitative and qualitative risk assessment, including (where appropriate) numerical assessments of the associated risk levels as derived from the PSA.
- Use of cost benefit analysis as an augmentation to the overall ALARP justification to determine whether the expected costs of implementing the option are grossly disproportionate to the benefits and thus aid in determining which option is ALARP.

13.2.2.1 Relevant Good Practice (RGP)

One of the basic tenets of ALARP is the recognition and use of RGP. Although not the sole criterion, RGP may be referred to as the use of modern standards and practices. In order to demonstrate RGP, it may be necessary to construct an appropriate qualitative argument, consisting of technical quantitative bases as well as recognition of expert-level knowledge.

Demonstration of RGP generally considers one or more of the following:

- Use of Industry Accepted Codes, Standards and Practices
- Use of Proven Technology
- Use of Applicable Testing

Use of Industry Accepted Codes, Standards and Practices

Reference to UK-specific codes and standards is preferable, but not absolutely necessary to define RGP. Demonstration of RGP does not require conformance to UK codes and standards if an equivalency to existing codes or standards has been established.

The HF standards used as RGP in the design and assessment of the AP1000 design (Table 13-1 have undergone an equivalence and maturity study (Reference 13.7 – Section 5.4) to determine whether they have been utilised as RGP in the UK or are recognised in UK and Europe as RGP (i.e., equivalence) and (b) were current good practice or equivalent at the time that design decisions were taken and are not significantly different now (i.e., maturity). The results of this RGP equivalence and maturity study found them to be broadly compatible with UK and International practices.

Use of Proven Technology

The recognition by nuclear industry workers, maintainers and operators of familiar, proven designs of SSCs used in nuclear new build applications contributes substantially to an operations and HF RGP argument. However, ALARP optioneering (Section 13.2.2.2) has

also revealed newer/innovative technologies, such as visual display unit (VDU) based, point and click, soft control human system interface (HSI) in the main control room (MCR) that are able to offer additional advantages over existing technology, but for which there is not extensive operational experience.

Use of Applicable Testing

RGP may be confirmed through the utilisation of applicable test results, in demonstrating suitability of the design, or operational practice. For example, use of the integrated systems validation (ISV) test results (Section 13.7.3 and Reference 13.54) provides evidence in demonstrating RGP, as related to MCR HF design implementation. Such test results verify assumptions on human action times, through direct simulation and analysis of operator practices. This validation then establishes RGP for the assumptions.

13.2.2.2 Optioneering

Inherent within the ALARP decision-making process is appropriate consideration of different options. A formal option assessment process was used in the rationale for the evolution of the AP1000 design (Section 13.6.1) and expert panel optioneering in the selection and development of existing design features through, for example, HF, operations, and HSI design participation in the design change proposal (DCP) process (Reference 13.15).

13.2.2.3 Risk Assessment

Risk is defined as a combination of probability and consequences and may be of a quantitative or qualitative nature. All of these factors are considered in an ALARP evaluation. The results from risk assessments, e.g., DBA, PSA, and SAA are used to support ALARP justifications. HF has taken the output from these, risk-based fault analysis methods, to identify operator actions important to nuclear safety (Section 13.8.1) and screened them for further qualitative HEA (Section 13.8.3) proportionate to the consequence of their failure exceeding certain threshold criteria (Section 13.8.2). The task analysis output from this qualitative HEA will then be used in human reliability analysis (HRA) to substantiate or derive estimations of human error probability (HEP) for human-based safety claims (HBSCs) modelled in the PSA event trees (Reference 13.8).

13.3 Limitations to the HF Safety Substantiation during GDA

The level of safety demonstration that can be reliably performed is dependent upon the design development progress at the time of the assessment. Assessment of a generic design for the UK, pre-construction and prior to there being fully trained and licenced operators, will mean that the development of the HF safety case has been conducted at a generic, non-site specific level, rather than that of a detailed, operating design.

13.3.1 Standard AP1000 Plant Design Development Phase

As illustrated by Figure 13.1, there has been an extensive and comprehensive HF Engineering programme applied to the AP600/AP1000 design over a period of some 20 years preceding GDA. This has resulted in a Standard AP1000 plant design where all necessary systems, displays and controls are provided to maintain or return plant to safe operation in normal, emergency and accident conditions.

13.3.2 Plant Design Configuration

The Standard AP1000 plant design configuration, against which this HF safety case for GDA has been conducted, is defined by the latest revision of the Design Reference Point (DRP) (Reference 13.9) and the high level design documentation pertinent to the issue of a Design Acceptance Certificate and a Statement of Design Acceptance referenced therein. The DRP also includes design changes approved by the designer for implementation in the AP1000 design configuration for GDA.

Whilst HF Engineering, or HFI activities, in earlier AP1000 design development have been focused predominantly on plant operation from the main control centres, the HF guidance that has been provided in the design of local control panels and manually activated local equipment will be significantly enhanced by feedback from AP1000 construction projects currently underway.

13.3.3 Operating Condition Scope

The HF Engineering programme, preparatory analyses, design input, and verification and validation has addressed credible plant operations, comprising all modes of normal operation as well as emergency and accident conditions, and selected abnormal/infrequent operations, test, inspection, surveillance, and maintenance activities.

HF task support verification, HF design verification and an HF ISV tests have been completed for the standard AP1000 plant design. These HF verification and validation (V&V) activities are further described in section 13.7. Completion of the HF V&V activities have resulted in a significant number of 'issues' and operator performance concerns that have been captured, recorded and grouped into human engineering discrepancies (HEDs). The resolution plans for each of the HEDs and HED issues fall into one or more of the following categories: Corrected through design change; Procedure change; Training program change; or justified as-is.

The resolution plan of each HED issue has been assessed and agreed with the requisite Westinghouse engineering disciplines. Re-verification and re-validation of the implemented resolution plans are intended to be conducted during the UK site licencing phase, where the results become substantiation in support of a claim for risk from human error being reduced ALARP.

13.3.4 Operating Location Scope

The AP1000 HF engineering programme adopts a tailored approach to HF analysis. A framework was adopted to establish the level of HF involvement in the different areas or systems in which HF are influential. The level of involvement is dependent on the potential safety or operational consequences of an operator error, degree of human involvement in the task, nature of the task, task complexity, required speed of operator response, or a combination.

The HSI design element of the HF Engineering Programme Plan (Reference 13.10) addresses the HSI resources that are located in the Operation and Control Centre System (OCS). However, the risk-proportionate, tailored approach to the application of HF Engineering resources means that rigorous attention has been paid to the design of the MCR and HSI to monitor and control plant functions important to the maintenance of nuclear safety. Other core areas, in which there is a significant reliance on successful operator performance in order to prevent a risk to safety, or where operator performance is essential to maintain operational integrity, have been given equal importance.

This concentration of HFI effort on the OCS during early AP1000 design activity, in combination with the passive nature of many SSCs to provide their safety function, has meant that direct HF involvement with the design of SSCs for maintenance and maintainability has been limited to the provision of good practice HF guidance principles for designers (Reference 13.57), as informed by the Electric Power Research Institute (EPRI) Utility Requirements Document (Vol. III, Chapter 1, Section 8 of Reference 13.20). More thoroughly assessed from an HF perspective has been the maintenance, test, inspection and surveillance (MTIS) activity associated with the use of Squib valves in the AP1000 design. This has included a demonstration in the use of three dimensional modelling to enhance the HF assessment of squib valve MTIS activity conducted for the analysis of GDA sample actions OPR-011 and OPR-106 (Reference 13.54 and 13.96). In addition, feedback available from AP1000 build projects in China and the United States (US) is designed to inform the ongoing HF assessment of MTIS on SSCs that will be conducted during the UK site licencing phase.

Site licensing is anticipated to include HF maintenance and maintainability assessments of appropriate risk significant maintenance activities as per the HF error screening and analysis process.

13.3.5 Safety Categorisation and Classification Scope

The identification of operator and maintenance actions and the subsequent risk-proportionate, tailored approach to HF assessment has been guided by the classification of a system's importance to safety and the categorisation of the safety function that the system delivers (Reference 13.11).

The operator and maintenance actions that are associated with safety systems and the safety-related DiD systems have been used in the identification of operator actions that are important to safety. These actions have been screened for detailed HEA dependent upon the consequence of the unavailability of these systems on demand.

13.3.6 HF Interfaces with other parts of the PCSR

This chapter provides the main discussion on the HF element of the UK AP1000 safety case. It includes the overall basis for safety, the process for integrating HF into the design, and the safety arguments and evidence that relate to both the holistic HF safety case and to specific HBSCs. Because of this holistic approach to the formulation of an HF basis for safety and of the transverse, cross-cutting nature of the HF topic, there are numerous interfaces with these other technical areas and safety disciplines. Examples of these HF interfaces with other chapters include:

Chapter 7	Lifecycle Engineering and Safety (Design Change Control; MTIS)
Chapter 8	Fault and Accident Analysis (HF; Fault Schedule and Fault Groups)
Chapter 10	Probabilistic Safety Analysis
Chapter 11	Internal Hazards (Fire; Flood)
Chapter 14	Fault Analysis Results and Conclusions (SSCs Identified in the Safety Case; Emergency Instructions Identified in the Safety Case; Assessment that Risks are ALARP)
Chapter 19	Control and Instrumentation (C&I) (Plant Protection)
Chapter 25	Accident Management (Onsite Emergency Response Facilities)

HF has also been integrated across other technical areas of the UK AP1000 programme through support to the resolution of their GDA Issues. When it has been identified that HF has a part to play in the resolution of a GDA Issue or that the safety case for the technical area makes claims on the actions of a human operator, then HF team support is provided as required. The technical disciplines where HF currently provides support and has an interface are more fully reported in Reference 13.95 and by the examples listed below:

- Cross Cutting Issues as relating to lessons learned from the Fukushima event
- Civil Engineering with regards to the Fuel Handling Area
- C&I issues related to the use and safety substantiation of various operator interface panels.
- Electrical Engineering regarding HF input to maintenance philosophy.
- Fuel Design and the use of BEACON™ Core Monitoring System
- Fuel System and the HF contribution to the Safety Case and design input to implementation of diverse flux protection
- Mechanical Engineering procedures for MTIS activity and isolation of systems including squib valves. The operation and maintenance of hybrid metric and imperial systems.
- PSA and the use of detailed HF task analysis and cognitive-level HEA to inform HEPs for inclusion in the Level 1 and 2 PSA models, including Fire PSA.
- Radiation Control and Protection, including HF review of relevant safety case for e.g., primary sampling and spent fuel pool (SFP) criticality, etc.

13.3.7 Considerations for Site Licensing

In the design of AP1000 systems and operational tasks, Westinghouse designers have been guided by HF requirements and constraints influenced by national regulatory and legislative expectations, a US-based population target audience description (TAD), or anticipation that systems will be used in the context of US operating practices and culture. When these situations are identified during HFI assessment and task analysis for HEA, and have been used in the HF safety substantiation for GDA, then they are recorded as ‘assumptions’. A list of assumptions is being maintained in a separate, living document that is intended to be shared with a UK Site Licensee to inform the scope of a site-specific safety substantiation of their Conduct of Operations, operating procedures, organisational culture, training programme, staffing, emergency plans, and maintenance programme, among others.

Assumptions made in the HF analysis and safety substantiation of operator actions for the GDA sample have been recorded under the following generic headings in the Qualitative Error Analysis report (Reference 13.54):

- Conduct of Operations
- Procedure Use and Adherence
- Staffing

- Training
- Human Performance
- Safety Culture
- Human System Interface
- Other/Miscellaneous, e.g., MTIS process

Each of these topic areas are ultimately the responsibility of a future operating utility organisation. The final design of systems and processes adopted by a future UK licensee will be influenced by national legislation, local working practices and industry expectations. This will require that safety substantiation of operator actions are reassessed in light of the implemented site-specific design. Significant deviation from the 'solutions' and assumptions envisaged by Westinghouse designers in the US will require that the licensee substantiate the design given the absence of or alternates to Westinghouse solutions or assumptions.

In addition to assumptions, there remain open 'issues' that are the result of HF Engineering process related to the site-specific HF V&V activity. These HED issues are captured in a formal tracking system (Section 13.5.4 and 13.7.4), for resolution and any required re-verification or re-validation during site licencing, governed by the AP1000 Human Factors Engineering Discrepancy Process (Reference 13.60).

The HED issues currently residing in the formal tracking system tend to be Operations and Control Centre centric, emanating from scenarios enacted using the MCR and RSR simulator. Other areas where the HF Engineering process and risk-proportionate HF analysis require site-specific inputs are in the areas of local control stations and maintenance and maintainability of systems providing safety and safety-related functions.

Many of the local control stations will be supplied as part of separate vendor contracts for systems procured during the site-specific design and construction. The procurement contracts will include appropriate specifications and requirements to ensure that the HSI of a vendor supplied control station is compliant with modern standards and the adopted set of HSI guidelines (Reference 13.46). When locally let contracts are for the procurement of systems providing a safety function, it is expected that a requirement for the vendor organisation to engage the assistance of an 'in-house' HF capability to integrate HF into the design and to interpret HSI requirements will be required.

HFI in the design for maintenance of systems providing safety and safety-related functions has been predominantly informed by HF guidance documents (Reference 13.46 and 13.47). However, a methodology for the HF analysis of MTIS activity on installed systems has been demonstrated for the ADS, IRWST, and containment recirculation squib valves as part of the GDA operator action sample analysis (Reference 13.54 – OPR-011 and OPR-106). This methodology has made use of three dimensional CAD models, in conjunction with relevant maintenance procedures and experienced engineers, to conduct detailed task analysis of selected MTIS operations. This work has resulted in a number of design enhancement HF recommendations. Site licensing activities are expected to include HF maintenance and maintainability assessments of appropriate risk-important maintenance activities per the HF error screening and analysis process.

Issues arising from the HF analysis of MTIS activity on local systems and components that are conducted during the site licensing phase, along with feedback that will emanate from existing AP1000 build projects, would also reside in a formal tracking system, where issue

resolution may result in raising appropriate design change proposals (DCPs).

13.4 Overall Basis for Safety

This Section presents a claims, arguments and evidence 'road map' for the remainder of this chapter and 'signposts' other documents comprising the HF safety case for the standard AP1000 plant design in GDA.

An over-arching HF safety claim is made about the reduction of opportunity for, and risk from, human error, along with under-pinning sub-claims about the part that HFI in design, operating conduct, and human reliability play in the reduction of that risk. Each claim is followed by a bulleted list of arguments to elaborate the claim. Below each argument is an indented list of references to the sections of this HF chapter, and to other PCSR chapters and to documents that comprise the HF safety case for GDA, where evidence may be found to substantiate the claims.

Claims made below about the risk from human error being reduced ALARP are not fully substantiated. There is work yet to be finished with respect to ALARP substantiation. Detailed human error analysis, including ALARP substantiation, was completed for a sample of safety significant human actions (Reference 13.54). This demonstrated methodology needs to be completed for other safety significant human actions as identified and screened from the human action database

13.4.1 Overall HF Safety Claim

The overall HF safety claim is:

> **The role of the operator in ensuring nuclear safety is understood, and the risk to nuclear safety arising from human failure has been identified and reduced ALARP for the Standard AP1000 plant design.**

The role of the operator is to operate equipment controlled from the main control area (MCA) during all modes of normal operation, plant transients and emergencies. This includes manipulating actual controls; monitoring equipment and system parameters; documenting evolutions and significant events; performing operator actions required by Alarm Response Procedures (ARPs), addressing prioritised alarms and interpreting alarm significance and diagnosing and recognising trends (Reference 13.37).

The term "operator," as used in this overall HF claim, also includes the human operator as 'equipment operator' and 'maintenance engineer.' The equipment operator performs operations duties and responsibilities outside the MCR, as directed by the MCR, including locally performed unit evolutions and system operations under the direction and command of the MCA Supervisor; supporting identification, diagnosis, and resolution of abnormal conditions (Reference 13.37). The maintenance engineer maintains equipment and systems important to nuclear safety, conducting scheduled MTIS activities.

The arguments and evidence presented below to support the sub-claims will, in their entirety, substantiate this overall HF safety claim and demonstrate that risk from human failure has been reduced ALARP for GDA.

13.4.2 Human Factors Integration (HFI) into the Standard AP1000 plant design

Claim 1 - The implementation of a comprehensive, integrated and managed HF Engineering Program promotes high levels of confidence in the ability of the Standard

AP1000 plant design to support successful completion of the operational tasks and maintenance activities important to safety and assigned to the human operator.

- The HF Engineering program activities have been delivered and executed by suitably qualified and experienced persons (SQEPs) HF practitioners to support and inform the developing design. A tailored, risk-proportionate approach to the HF Engineering methodologies and analyses has been effectively managed throughout the design development lifecycle phases.

  Section 13.5.1 HF Engineering Program Management

  Section 13.5.2 HF Engineering Management Function

  Section 13.5.3 HF Engineering Qualifications and Expertise

  Section 13.5.4 HF Engineering Technical Process Management

  Reference 13.10 Westinghouse Report APP-OCS-GBH-001, Rev. 1, "Human Factors Engineering Program Plan," April 2009.

- The high-level plant and operational goals and operating philosophy for AP1000 have been identified and formed from successive evolutions of advanced light-water reactor (ALWR) designs, from lessons learned internally from predecessor Westinghouse designs, from operating experience review and externally from similar, high-hazard industry facilities and utility customer's own requirements.

  Section 13.6.1 AP1000 Design Philosophy

  Section 13.6.2 Operating Experience Review

  Section 13.6.4 Concept of Operations

  Reference 13.19 Westinghouse Report APP-GW-GER-005, Rev 1, "Safe and Simple: The Genesis and Process of the AP1000 Design," August 2008.

  Reference 13.20 "Advanced Light Water Reactor Utilities Requirements Document," Volumes I (Rev 2), II (Rev 8) and III (Rev 8), 1999.

- The standard design of AP1000 has been guided by and subject to review against industry relevant good practice and modern HF principles and standards.

  Section 13.2.2.1 Relevant Good Practice

  Section 13.5.4 HF Engineering Technical Process Management

  Section 13.6.6.1 HSI Design Guidelines

  Section 13.7.2 HF Design Verification

- Whenever a change to the configured design is proposed, a member of the integrated HF Engineering team is required to assess the impact of that change as part of a regulatory compliant configuration management process.

  Section 13.3.2 Plant Design Configuration

  Reference 13.15 Westinghouse Procedure APP-GW-GAP-341, Rev 0, "AP1000 Plant Program Design Change Control," January 2016.

  Reference 13.28 Westinghouse Report UKP-GW-GL-116, Rev 0, "AP1000 Supplemental Information for the Human Factors Safety Case – Review of

Selected Design Change Proposals included in the 2015 Design Reference Point for GDA," October 2015.

Claim 2 - The design of the MCR and of the HSI supports safe and reliable operations during normal modes of operation, abnormal and emergency conditions, and recovery operation during severe accident (i.e., core-damage).

Claim 2.1 - The design of the Remote Shutdown Room (RSR) and of the HSI supports the means to safely achieve and maintain Safe Shutdown following evacuation of the MCR.

- HF preparatory analyses have been completed and the results used to inform the HSI design, procedure development, and training program development. The output of these completed analyses included a list of controls, indications, and alarms that must be present in the HSI to safely monitor and control the plant under normal, abnormal and emergency conditions. Early HF analyses also included the assignment of processes to automation or manual (i.e., the human) or to a combination; determination of MCR and plant staffing levels; along with identification of any critical, risk-important or safety-significant human actions.

  Section 13.6.2 Operating Experience Review

  Section 13.6.3 Functional Requirements Analysis and Allocation of Function

  Section 13.6.5 Task Analysis

  Section 13.6.5.2 Operational Sequence Analysis 1

  Section 13.6.5.2.1 Criteria for Critical and Risk-Important Human Actions

  Section 13.6.15 Staffing

  Reference 13.65 Not Used.

- A Concept of Operations was first developed early during the conceptual design phases of the HSI. It presents the HSI resources to be used by operators with a vision of their functionality to support their decision making. The vision of the HSI functionality was based upon past modernisation projects, operating experience reviews, and conceptual integration into a compact, primarily "soft" control environment. The concept of operations describes the operational philosophy of each MCR position and the operational use of the HSI resources at those positions. It is extended to the RSR, local distributed control and information system (DCIS) workstations, and local panels. As such, the concept of operation provides high-level operational concepts and design bases to be used by the HSI resource designers to inform the development of their respective functional requirements and design specifications. As the HSI and control centre design evolved and matured, the concept of operations was revised accordingly to reflect the actual design.

  Section 13.6.4 Concept of Operations

  Section 13.6.6 HIS Design

  Section 13.6.7 Operation and Control Centres

  Section 13.6.8 Main Control Room

  Section 13.6.9 Remote Shutdown Room

  Reference 13.55 Westinghouse Report UKP-OCS-GLR-002, Rev 1, "United

Kingdom AP1000 RSR Control Strategy for Class 1 Displays and Controls – ALARP Justification," December 2016.

Section 13.6.10 Local Control Stations

- The use of modern standards, good practice guidance in the design of HSIs in nuclear power plant control rooms has informed and shaped the design and assessment of the control rooms, other operation and control centres, and their HSI resources.

  Section 13.2.2.1 Relevant Good Practice

  Section 13.6.6.1 HSI Design Guidelines

  Reference 13.46 Westinghouse Report APP-OCS-J1-002, Rev 6, "AP1000 Human System Interface Design Guidelines," July 2016.

  Reference 13.47 Westinghouse Report APP-GW-GRP-001, Rev 2, "AP1000 Local Panels and Maintainability Human Factors Design Guidelines," February 2014.

- HF verification and validation activities are used to verify and validate that the MCR and HSI designs support safe and reliable operation during normal operation, abnormal and emergency conditions. These activities are also used to verify and validate that the RSR and its HSI can be used to safely achieve and maintain safe shutdown.

- The HF task support verification (TSV) verifies that the HSI and control centres include the information and controls required to enable execution of operator tasks.

  Section 13.7.1 HF Task-Support Verification

- The HF design verification (DV) verifies that the HSI and the operation and control centre designs (i.e., MCR, RSR, local control stations, etc.) have been completed per industry accepted guidelines.

  Section 13.7.2 HF Design Verification

- The HF ISV utilises an AP1000 simulator to validate the MCR and RSR designs, the HSI designs, and the plant operating procedures, including the HSIs and procedures for evacuation to the RSR in the event of the MCR becoming uninhabitable due to smoke or fire.

  Section 13.7.3 HF Integrated System Validation

- Any deficiencies resulting from the completion of these V&V activities are documented as HEDs. Resolutions for the HEDs are agreed upon, implemented and then re-verified/re-validated.

  Section 13.7.4 Human Engineering Discrepancy Resolution Verification

- The impact of approved and implemented design changes that occur following the completion of the TSV, DV, and ISV is determined and appropriate regression with respect to the completed HF verification and validation is completed as part of the plant start-up HF engineering verification activity.

  Section 13.7.5 Plant Start-up HF Engineering Design Verification

13.4.3 Design Philosophy Claims

Claim 3 - The design and operating philosophy for the Standard AP1000 plant design reduces reliance on operator action to ensure nuclear safety and reduces the sensitivity of the plant to human error.

- The design of AP1000 is inherently safe, provides DiD, backup systems, is simple in design in having fewer systems, equipment and components to maintain, having less complicated plant evolutions and reliance on the human operator for safety.

  Section 13.6.1 AP1000 Design Philosophy

  Section 13.6.2 Operating Experience Review

  Section 13.6.2.2 Utility Customer Requirements

- Functions have been appropriately allocated between humans and engineered systems and the reliance upon the human operator to maintain safety reduced.

  Section 13.6.2.4 Target Audience Description

  Section 13.6.3 Functional Requirements Analysis and Allocation of Function

- Per the AP1000 HF program, probabilistic and deterministic criteria have been defined to identify both critical human actions and risk important human actions associated with the AP1000 plant. The criteria have been applied and the results documented. No critical human actions are identified from the application of the respective criteria. However, risk important human actions are identified and serve as input to other elements of the HF program (i.e., task analysis, HSI design, and HF verification and validation).

  Section 13.6.5.2.1 Criteria for Critical and Risk-Important Human Actions

  Section 13.6.5.3 Operational Sequence Analysis 2

  Section 13.7.1 HF Task-Support Verification

  Section 13.7.3 HF Integrated System Validation

Claim 4 - The plant procedures, including the Conduct of Operations, applied to the Standard AP1000 plant design support safe and reliable operation during normal operation, abnormal operation, and emergency conditions.

- A full and comprehensive set of plant procedures have been developed to address normal operations, plant system operations, abnormal operations, alarm response, emergency operations, and maintenance, test, inspection, and surveillance operations. Procedure development includes consideration of operating experience, utility input and review, and industry good practice.

  Section 13.6.13 Development of Procedures

  Section 13.6.13.1 Procedures

- Operators are required and trained to use procedures at all times.

  Section 13.6.13.3 Importance of Operating Procedures

  Section 13.6.14 Development of Training Programs

Section 13.6.16 Conduct of Operations

Section 13.7.3 HF Integrated System Validation

- A comprehensive and challenging set of scenarios has been exercised for ISV tests on the AP1000 simulator to assess the effectiveness of plant procedures (general operating, alarm response, abnormal operating and emergency operating procedures), and the effectiveness of the HSI design.

  Section 13.7.3 HF Integrated System Validation

- The workload and work share between operators during normal operation and in emergency and fault conditions has been assessed in operational sequence analysis (OSA) and ISV tests.

  Section 13.6.5.3 Operational Sequence Analysis 2

  Section 13.7.3 HF Integrated System Validation

- The staffing levels assigned to the MCR of the Standard AP1000 plant supports safe and reliable operation of the plant.

  Section 13.6.15 Staffing

Claim 4.1 – The Control Room Severe Accident Management Guidelines (SAMGs), entered from Emergency Operating Procedures (EOPs), guide the Control Room operators in the management of severe accidents (i.e., core damage) in the first 24 hours after core damage.

- The AP1000 SAMGs were developed to focus on managing the accident in the first day (24 hours) after core damage. The guidelines consist of the following three major parts:

  Section 13.6.13.2 Severe Accident Management Guidelines

  1. Control Room Severe Accident Management Guidelines
  2. TSC Severe Accident Management Guidelines
  3. TSC Severe Challenge Response Guidelines

  Reference 13.84 Westinghouse Report UKP-GW-GGR-201, Rev. 1, "UK AP1000 Plant Post-Fukushima Assessment," July 2016.

- The Control Room SAMGs consist of two separate guidelines; the appropriate guideline is determined by the status of the Technical Support Centre (TSC) at the time the SAMGs are implemented. Severe Accident Control Room Guideline Initial Response (SACRG-1) is used by Control Room staff until the TSC is functional. SACRG-1 guides Control Room staff actions in a well-defined and prioritised manner to respond to inadequate core cooling and protection of the fission product barriers. SACRG-2 is used by the Control Room staff after the TSC is established and it is ready to use the TSC SAMG. This guideline is intended to foster communications between the Control Room staff and the TSC technical staff with the goal of enhancing the Control Room acceptance of the recommendations made by the TSC.

- The Control Room personnel are ultimately responsible for all actions taken during

normal operation and the accident until a senior management person assumes this responsibility as will be described in the site specific Emergency Plan (to be developed during Site Licensing). A declaration is made that passes the ultimate decision making responsibility for the senior plant operator in the MCR to the senior plant management official designated in the plant Emergency Plan (typically the TSC Director). In severe accident management, the TSC is expected to make decisions and pass recommendations to the Control Room for implementation.

Reference 13.98 Westinghouse Report APP-GW-GJP-500, Rev 0, "Executive Volume for AP1000 Severe Accident Management Guidelines," March 2015.

13.4.4 Substantiation of Human-Based Safety Claims (HBSCs)

Claim 5 - The HBSCs, identified as part of the DBA, PSA and SAA, have been substantiated ALARP.

- The process of identification and risk-proportionate substantiation of operator actions important to safety has been broad and comprehensive, accounting for areas of the fault analysis (DBA, PSA, and SAA) and the normal plant operating modes, abnormal operations, and emergency operations and beyond design basis condition through application of recognised HF analysis methods.

  Section 13.8.1 Identification of Operator Actions Important to Safety

  Section 13.8.2 Risk Proportionate Screening

  PCSR Chapter 25 Accident Management

- Type A, pre-fault, maintenance latent errors have been identified through a systematic consideration of the MTIS activities conducted on the passive safety and DiD safety-related systems claimed in the PSA event trees, and of other Class 1 and 2 SSCs.

  Section 13.8.1.1.1 Probabilistic Safety Analysis (PSA)

  Section 13.8.1.1.2 Design Basis Analysis (DBA)

- Type B, operator and maintainer induced initiating events have been identified through a systematic consideration of the internally initiated faults, faults initiated by internal and external hazards, faults presented in the Fault Schedule and composite fault list.

  Section 13.8.1.1.2 Design Basis Analysis (DBA)

- Type C, post-fault operator errors have been identified through a systematic consideration of the PSA systems and accident sequence analyses.

  Section 13.8.1.1.1 Probabilistic Safety Analysis (PSA)

- The HFEs and operator action errors identified in the Human Action Database (HAD) have undergone risk-based screening based on criteria relating to core damage frequency (CDF) and large release frequency (LRF) increase thresholds and on the safety classification and safety function category level of error affected SSCs.

  Section 13.8.2 Risk Proportionate Screening

- A methodology for the analysis of human errors has been conducted at a cognitive level

on a sample of Type A, B and C errors in GDA. Completion of this analysis in site licencing of the remaining operator actions important to safety will serve as input to the PSA activity and substantiate the risk to nuclear safety from human error reduced ALARP.

Section 13.9 Substantiation of Human-Based Safety Claims

Reference 13.54 Westinghouse Report UKP-GW-GL-126, Rev 0, "United Kingdom AP1000 Human Factors Qualitative Error Analysis," June 2016.

Claim 6 – A sample of Type A, B and C errors have undergone cognitive-level HEA to identify credible error modes and mechanisms (root cause) and performance shaping factors so that error reduction mechanisms can target the risk of failure ALARP for the Standard AP1000 plant design.

- A credible approach, based on empirical studies of current psychological research, has been devised to conduct HEA on the operator action sample during GDA that has identified context specific cognitive failure modes for the key action steps in the task analysis.

  Section 13.8.3.2 Cognitive-Level

  Reference 13.94 US NRC, NUREG-2114, Rev 1, "Cognitive Basis for Human Reliability Analysis," January 2016.

  Reference 13.54 Westinghouse Report UKP-GW-GL-126, Rev 0, "United Kingdom AP1000 Human Factors Qualitative Error Analysis," June 2016.

- The underlying internal error mechanism and performance shaping factors have targeted proposed error reduction mechanisms and ALARP design recommendations.

  Reference 13.54 Westinghouse Report UKP-GW-GL-126, Rev 0, "United Kingdom AP1000 Human Factors Qualitative Error Analysis," June 2016.

  Reference 13.93 Westinghouse Report UKP-GW-GL-072, Rev 0, "Supplemental Information for the Human Factors Safety Case – Potential Improvements as Proposed in the ALARP Analysis," November 2010.

Claim 7 – The symptom-based approach of the emergency operating procedures (EOPs) and of the incontrovertibly different entry conditions to each EOP has reduced the potential for diagnostic error such that it is considered to be reduced ALARP for the Standard AP1000 plant design.

- A credible approach to the identification of diagnostic error potential has been devised and HEA of the sampled operator errors did not identify increased potential for misdiagnosis and entry to incorrect procedure.

  Section 13.8.3.3 Misdiagnosis

  Reference 13.54 Westinghouse Report UKP-GW-GL-126, Rev 0, "United Kingdom AP1000 Human Factors Qualitative Error Analysis," June 2016.

- The symptom-based nature of the abnormal operating procedures (AOPs) and EOPs means that operators are not required to operate in "knowledge space" and so are not required to try and immediately diagnose the fault or the cause of the fault.

Section 13.6.13.1.2 Abnormal, Emergency Operating and Alarm Response Procedures

Reference 13.54 Westinghouse Report UKP-GW-GL-126, Rev 0, "United Kingdom AP1000 Human Factors Qualitative Error Analysis," June 2016.

- The entry conditions to each of the EOPs are clear and easily discernible and checked from readily available HSI displays.

  Section 13.6.13.1.2 Abnormal, Emergency Operating and Alarm Response Procedures

  Section 13.6.7.1 Distributed Control and Information System

  Section 13.6.7.6 Computerised Procedures System

- The EOP network is always entered through the reactor trip procedure (E-0). The procedure instructs the operator to manually trip the reactor as an "immediate action" (IA), even if automatic reactor trip has occurred, and prompts the operator to verify that reactor trip has occurred and that all the safety systems have operated as required. Following verification of proper safety system operation, the procedure then steps the operator through several diagnostic steps and based upon plant symptoms or state the operator is directed to the appropriate optimal recovery procedure within the EOP network. Therefore, the entry conditions for each EOP are incontrovertibly different and so the potential for entry to and execution of the wrong EOP is considered to be highly unlikely.

  Section 13.6.13.1.2 Abnormal, Emergency Operating and Alarm Response Procedures

- As a result of monitoring the key safety parameters and set-points associated with the critical safety functions, as directed by the EOPs and presented by the computerised procedures system, the operators are directed to the correct function response procedure in a timely manner.

  Section 13.6.13.1.2 Abnormal, Emergency Operating and Alarm Response Procedures

  Section 13.6.7.1 Distributed Control and Information System

  Section 13.6.7.6 Computerised Procedures System

- An HF ISV test was executed to validate, among other objectives, the HSI design and the plant operating procedures (including EOPs). The completion of this test, the identification of any HEDs, and the resolution and re-verification/revalidation of the HEDs ensures the risk of misdiagnosis is ALARP.

  Section 13.7.3 HF Integrated System Validation

  Section 13.7.4 Human Engineering Discrepancy Resolution Verification

  Section 13.7.5 Plant Start-up HF Engineering Design Verification

- The AP1000 Conduct of Operations provides the standards and guidance, governing the behaviour of operations personnel, to achieve a high-level of performance that contributes to safe, reliable plant operations.

Section 13.6.16 Conduct of Operations

Reference 13.66 Administrative Procedure APP-GW-GJP-115, Rev 1, "Conduct of Operations," June 2014.

Claim 8 – The equipment design, task or operating context conditions that may cause behaviour in violation of procedures have been identified through HEA or observed during the HF ISV test. Respective ISV HEDs have been identified. Resolution of these HEDs shall be agreed upon, implemented, and re-verified/re-validated such that the risk for violation is ALARP.

- A credible approach to the identification of violation potential has been devised and the HEA of the Type C post-fault operator errors in the sample did not identify potential high-workload, stress and task goal conflict situations where violation potential may become more likely.

  Section 13.8.3.4 Design Induced Violation

  Reference 13.54 Westinghouse Report UKP-GW-GL-126, Rev 0, "United Kingdom AP1000 Human Factors Qualitative Error Analysis," June 2016.

- The allocation of functions has resulted in a plant design and consequential operator tasks and job design that reduce the likelihood of situations that present conflicting task goals to the operator, high-workload or time-induced stress that might increase the potential for operator behaviours in violation of procedures.

  Section 13.6.3 Functional Requirements Analysis and Allocation of Function

- The HF ISV test, utilising the high-fidelity AP1000 simulator facility, has been completed. HEDs and any contributing HED issues related to violation have been identified and documented. The process for resolution of HEDs, the implementation of the resolutions, and the re-verification and re-validation of the resolutions is defined. Efforts to reach agreement between HF and the respective engineering disciplines on the HED resolutions are in progress. Implementation of the agreed upon resolutions occurs throughout 2017 and the re-verification/re-validation is scheduled for early 2018.

  Section 13.7.3 HF Integrated System Validation

  Section 13.7.4 Human Engineering Discrepancy Resolution Verification

  Section 13.7.5 Plant Start-up HF Engineering Design Verification

13.5 HF Engineering Programme

International Safety Standards and RGP require that the design of a new NPP take a systematic consideration of HF at an early stage in the design process and that it shall continue throughout the entire process (Reference 13.13).

HF Engineering, or the UK analogous HFI, is a good practice approach to the application of HF to system's development. HF Engineering is a methodology that provides both an organising framework to help ensure that all relevant HF technical issues are identified, tracked and addressed, and a management strategy that provides for a timely and appropriate integration of HF activities throughout the design development project.

The HF Engineering programme elements that have been used throughout the design development of AP1000 have been based on the NUREG-0711 HF Engineering Program

Review Model (Reference 13.14). The HF Engineering Program starts in the early planning and concept phase with the high-level safety and operational goals for the plant being identified through examination of:

- Design evolution from predecessor systems (Section 13.6.1
- Operating experience review (Section 13.6.2)
- Utility/Customer design requirements (13.6.2.2)
- A Concept of Operation (Section 13.6.4)

In the 'analysis' phase the functions necessary to achieve the plant's high-level operational and safety goals were defined and refined in to increasing levels of system detail. System and sub-system level functions were then allocated to human and system resources. Decomposition of the human-assigned functions into tasks and of the engineered-assigned functions into delivery SSCs then informs the specification for the necessary alarms, information, controls, and task support that is needed to complete the functional assignments using:

- Function requirements analysis and allocation of function (Section 13.6.3)
- Task analysis (Section 13.6.5)
- Identification and treatment of human actions important to safety (Section 13.6.5.2 and 13.6.5.3)

In the 'design' phase, personnel tasks are analysed to identify the alarms, displays, procedures and controls that will be required for task performance. The detailed design of the HSI, procedures, and training requirements are best designed to support operator assigned tasks:

- Human System Interface Design (Section 13.6.6)
- Procedure Design and Development (Section 13.6.13)
- Job and Role Design, Staffing and Qualifications (Section 13.6.15)
- Conduct of Operation (Section 13.6.16)

During the HF V&V phases, which are currently being conducted for AP1000 build programs in other countries, V&V activities comprehensively determine that the control centre and HSI design conforms to HF Engineering design principles:

- Design Verification (Section 13.7.2)
- Task-Support Verification (Section 13.7.1)
- Integrated Systems Validation (Section 13.7.3)

The HF elements of the HF Engineering programme have been systematically applied in the conceptual and planning phases of the AP600 since the 1980s and early 1990s and remain and continue to be a significant focus for the design development of the AP1000 in 2016 and for GDA (Figure 13.1).

This period of time also encapsulates the ongoing HF Engineering program for AP1000 projects currently in advanced stages of construction, system installation and commissioning. Where appropriate, the HF analysis and output data from the HF

verification and validation activities conducted for the standard AP1000 plant design has been used as supporting evidence in the substantiation of HBSCs for a UK AP1000 in GDA.

The rest of this Section 13.5 provides an abbreviated account of the HF Engineering programme management, methodologies and assessments that has been used to construct a human factors safety case that provides the substantive evidence to support the overall HF claim and reduce the risk from human error ALARP for GDA.

Key to the effectiveness of applying successive HF Engineering technical programme elements throughout the design lifecycle has been the management strategy to ensure that they are integrated in an effective and timely manner with other project design and safety disciplines and executed by suitably qualified and experienced HF practitioners.

The information on how the HF technical and management programme has been conducted for AP1000 is captured in the Westinghouse HF Engineering Program Plan (Reference 13.10), analogous to the HFI Plan in the UK. The stated aims of the HF Engineering Program Plan are, as well as delivering the technical program, to:

- Describe the scope of the HF Engineering program, outline the technical approaches, identify the HF Engineering team, describe the organisational structure, and define roles and responsibilities.

- Assist in avoiding costly re-design via the incorporation of human factors into the design process in a timely manner.

- Detail the documentation required to illustrate that the design was developed in accordance with applicable human factors design, operation, and maintenance principles.

13.5.1 HF Engineering Program Management

The AP1000 project is sizeable and complex, encompassing a large number of technical, safety and management disciplines, such as mechanical, electrical, process, civil, structural, control systems, instrumentation, radiological systems, nuclear safety, and conventional safety. Each discipline or group has clearly defined responsibilities and authorities.

In the early design stages, the primary focus of the HF Engineering Program Plan has been the MCR and the supporting control and monitoring facilities and systems. Therefore, the HF Engineering function has traditionally been placed within the AP1000 C&I project organisation in order to integrate HF Engineering into the C&I design activities.

The AP1000 Project organisation is based on a matrix-type structure, with a relatively flat management hierarchy. The individual engineering, technical, and support groups typically comprise a relatively small number of people. Personnel can be a part of more than one group. This aids flexibility in the use of resources, facilitates communication, and maximises the use and application of the available engineering expertise and experience.

13.5.2 HF Engineering Management Function

The Westinghouse HF Engineering team function resides within the C&I group organisational structure, along with other human performance influencing functions, such as procedures, training and operations. However, there is an appreciation within the group's management structure that HF team coverage extends beyond control centre HSI

and operations and is given sufficient autonomy to reach out and interact with other project technical and safety disciplines as required. An example of this is the ongoing support that the Westinghouse HF team is providing to other project technical areas in order to identify claims that they may be making on operators in compiling the safety case for their systems and in resolving their GDA Issues (Reference 13.95).

By reporting to a single C&I Project Manager, the HF Engineering function is effectively integrated within the larger C&I team, ensuring that all team members are clearly aware of each other's roles and responsibilities. A schematic of the HF Engineering Group is provided in Figure 13.2.

13.5.3 HF Engineering Qualifications and Expertise

The HF Engineering specialists have a background in human factors, psychology, systems engineering, or a combination of these areas. They are qualified and experienced in applying knowledge about human characteristics, skills and limitations to the design, operation, and maintenance of systems or facilities. The HF Engineering specialists are well-versed in the application of human factors knowledge, techniques, and standards to systems or facilities that are potentially hazardous and/or complex, such as nuclear reactors, non-reactor nuclear facilities, and other process industries.

13.5.4 HF Engineering Technical Process Management

The HF Engineering program is managed through an iterative process of detailed task analyses, multi-discipline design review and V&V assessments of the OCS and local C&I HSIs. The design is placed under formal configuration control and proposed design changes are fully assessed by HF and other design disciplines to identify operations or maintenance impacts before formal design change approval (Reference 13.15).

A formal HF Engineering tracking system (Reference 13.10 Section 4.2.5) is used by the HF Engineering Lead to manage the resolution of HF issues or items that result from task analysis, design review, and HF V&V activities and ensure that these items are recorded, dealt with, and resolved in a timely, efficient manner.

The items entered in the HF tracking system constitute one or more of the following:

- An undocumented assessment or analysis required to support a design decision
- An undocumented assessment that is required at a later stage in the design lifecycle when the required level of design or operations detail becomes available
- An issue identified from task analysis results, including the human error analyses of section 13.8.3
- An issue identified from a non AP1000 project that is known or anticipated to be an unresolved issue for AP1000
- A HF action item identified during the course of a design review meeting that cannot be closed as part of the design review process
- An issue identified during human factors V&V activity

Formal design reviews are undertaken at key points in the HF design development process. The objective of these reviews is to provide a systematic evaluation of the AP1000 by a multi-disciplinary team, which includes utility representatives.

Formal engineering tests have been conducted to provide timely feedback during the HSI design process (References 13.16, 13.17, 13.18). A relatively limited scope simulation was utilised to execute these tests to address and evaluate specific design issues (e.g., the use of large screen display units for overview displays, soft controls, alarm presentation, supervisory repeater functionality, etc.). The results of the engineering tests were used to refine the design, as required. The simulator-based tests used a sample of actual reactor control room operators and supervisors in order to obtain realistic results and to benefit from the subjects' operations experience.

These HF engineering tests are considered to be of high importance due to the application of modern standards C&I HSI technology and new passive safety systems used in the design of AP1000. The AP1000 MCR includes operator interfaces comprising of VDU and soft control-based systems. Operator performance data are collected using video and audio recordings of the scenario, verbal communication and feedback from operators and observers during scenarios and by post-scenario questionnaires and debriefing.

The effective management of these integrated, cross-discipline, elements of the human factors programme, as summarised in subsections 13.5.1 through 13.5.4, give confidence and some level of assurance that the operator interfaces of the OCS and local panels are designed to be intuitive to use and will promote effective and safe operational practices. Ultimately, this will be assessed through the HF ISV test carried out on the high fidelity AP1000 simulator (Section 13.7.3).

13.6 Integration of HF in the AP1000 Design

13.6.1 AP1000 Design Philosophy

The current design of AP1000 has evolved from natural circulation cooled reactors that were designed for military applications in the US in the 1970s and 1980s, and based on similar technology and proven components, and which could perform their safety functions without the need for ac power.

The evolution of the AP1000 design from earlier generations of pressurized water reactors (PWRs) is described in Reference 13.19. This reference details some 44 evolutionary changes from previous designs, key of which from a human factors perspective have been:

- Use of digital C&I, giving the opportunities to implement advanced control and monitoring concepts such as soft control, integrated alarm systems, and advanced human interface resources.

- Use of an advanced Control Room, with the main operator-systems interface via computer based monitors, mice and keyboards. The VDU based workstation allows a number of systems to be integrated in to one flexible interface technology, including large screen displays that enable plant overview and alarm status information to be visible from all operator locations, thus facilitating crew situational awareness and decision-making.

The evolutionary improvement to safety is consistent with the ONR's expectations for the demonstration of ALARP with respect to new commercial reactor designs (Reference 13.4). That is:

- New reactor designs should demonstrate a level of safety that is no less than a comparable facility already working or being constructed in the UK or somewhere else in the world.

- Evolutionary designs, which have been designed taking account of experience of earlier designs, must show how the evolution has maintained or improved the design from a safety perspective.

The AP1000 design philosophy has also been one that is consistent with ensuring an inherently safe design, avoiding hazards rather than controlling them. Throughout there has been DiD against potentially significant faults or failures, providing a series of independent barriers (inherent features, equipment and procedures) that prevent faults from occurring in the first instance, and to help ensure that there is appropriate protection or mitigation of accidents in the event that prevention fails. The AP1000 specifically focuses on securing safety through design characteristics at the top of the safety measures hierarchy, with many passive safety features that do not rely on control systems, active safety systems, alternating current (ac) power, or human intervention (Reference 13.19).

13.6.2 Operating Experience Review

The incorporation of operating experience reviews (OERs) into the design and operation of nuclear facilities is good human factors practice (Reference 13.22) and is one of the criteria used by the UK ONR to assess leadership and management for safety.

Nuclear industry guidance on the incorporation of operator experience into design and operations is largely focused on gathering information internally during operations, as well as gathering external data from international organisations, including the World Association of Nuclear Operators (WANO), Institute of Nuclear Power Operations (INPO), and International Atomic Energy Agency (IAEA). Westinghouse has been proactive in gathering operating experience from a large range of sources, including the utilities operating their plants and more recently from AP1000 new build programmes at advanced stages of build, system installation and commissioning in both China and the US.

13.6.2.1 Operating Experience Collected to Support the AP1000 Design

Operating experience has been explicitly addressed by the HF Engineering process that developed the requirements for the AP1000 design and its predecessors. In particular the ALWR Program was organised to make extensive use of the extraordinary database of information and lessons learned from over 40 years of experience in operating over 100 Light Water Reactor (LWR) plants in the US and many more overseas. This operating experience comprises over 1,700 reactor years in the US and over 5,000 reactor years world-wide.

In order to meet these requirements and incorporate appropriate features in the AP1000 plant's design, operations and maintenance, Westinghouse reviewed existing databases of LWR operating experience to identify both positive experiences as well as causes of significant events and unplanned outages. During the design phase of the AP600 and AP1000, extensive reviews of industry operating experience were performed and assessed with respect to their applicability to the AP1000 design.

The results of these OERs are described in References 13.24, 13.25, 13.26 and 13.27, the latter, of which focuses on operating experience documented in US Nuclear Regulatory Commission (NRC) IE Bulletins, Circulars, and Information Notices as well as NRC Generic Letters and regulatory Information Summaries. In particular, a HF Engineering Operating Experience Review (Reference 13.27), assessed pressurised water reactors (PWRs) at both Westinghouse and non-Westinghouse plants; issues for boiling water reactors and a pressurised heavy water reactor designs which were applicable to the AP1000 design; and HSI experience from other industries, where limited experience exists

in the nuclear industry.

Revision 3 of the OER document for AP1000 (Reference 13.27) incorporates operating experience data gathered from 1996 to 2006 and includes issues associated with more advanced system interface design, such as large display screen networks (a "bank" of large displays showing general plant status information), implementation of soft controls, and group situational awareness. Many of the issues identified during this time relate to operator training, teamwork, and the use of procedures and have been addressed by Westinghouse accordingly. In addition, since 2006, Westinghouse continues to collect relevant operating experience from a range of available sources and databases to ensure that new lessons learned are also incorporated into the AP1000. Items that cannot be immediately incorporated are entered into the human factors engineering tracking system for future resolution (Section 4.2.5 of Reference 13.10).

More recently, there is emanating from AP1000 new build projects important construction, equipment installation and commissioning operational experience. The design, safety and operation of the UK AP1000 will ultimately benefit from the experience gained from these, predecessor, AP1000 builds.

13.6.2.2 Utility Customer Requirements

In the mid-1980s, the US utilities, nuclear plant vendors, nuclear architect/engineers and industry consultants such as the EPRI worked together to generate a detailed specification and set of requirements for the next generation of nuclear reactor designs. This resulted in the ALWR Utilities Requirements Document (URD) (Reference 13.20), which set a minimum acceptable standard for plant design.

For Westinghouse, and the design of the AP600/AP1000, the URD set the same basis for comparison of nuclear reactor designs in the US, so that technology selection would be based upon the delivery of the best value whilst meeting the minimum acceptable standard in the URD. A few years later, the European utilities also formed a steering group for new nuclear in Europe under the banner European Passive Plant and developed a derivative URD called the European Utility Requirement (EUR) (Reference 13.21). Both the URD and the EUR have ensured that utility involvement became a part of the development of AP600 and then AP1000, incorporating best practices from around the world and reinforcing worldwide standardisation.

13.6.2.3 Ongoing Consultation with Utilities

The utilities continue to be involved throughout the design development of the AP1000 plant. This involvement has included:

- Attending formal design reviews to review the completeness and technical content of the functional design and the system specification for the control system and operator interfaces (e.g., References 13.29 and 13.30).

- Providing currently licensed and qualified control room operators from existing plants to participate in the HF tests on the early prototype designs and detailed designs of the operator interfaces (References 13.16, 13.17, and 13.18).

- Attendance at workshops to review the detailed designs of the operator interface and, to address outstanding issues from completed HF tests, and to review disposition of actions taken from previous workshops (e.g., Reference 13.31).

- The provision of licensed operator candidates, having completed AP1000 training, to participate in the human HF ISV simulator tests (Reference 13.59)

- Representation (review member) on the plant configuration change control board, where decisions are made on implementation of design changes (Reference 13.15).

- Providing reviews of operating procedures developed for AP1000 that help integrate industry operating experience into the procedures and help ensure the quality and practicality of the procedures.

13.6.2.4 Target Audience Description (TAD)

A part of any decision to allocate safety functions to human elements of the system (Section 13.6.3) will be determined by an understanding that the operator selected to fulfil that safety function will have sufficient mental and physical aptitude to be trained and to reliably perform the actions necessary for the task (see Section 13.6.14). A TAD is the collection of the physiological and psychological attributes possessed by the population, from which operators may be recruited, and, for which system designers, should accommodate in their design.

The AP1000 plant has been designed to physically accommodate the 5th percentile female to the 95th percentile male dimensions based on data initially selected for the U.S. population.

It is good engineering design practice to design workstations so that they shall accommodate from the 5th to the 95th percentiles of dimensions of the intended user population. This is a General Requirement stipulated in BS EN ISO 11064-4 2013 (see Table 13-1), an internationally adopted standard for the effective design of workplaces/spaces. BS EN ISO 11064 is also recognised by the UK ONR as a source of relevant good practice that has informed the advice provided to their inspectors in the TAG on Workplaces and Work Environment (NS-TAST-GD-062, Revision 2, February 2014).

The impact of a UK anthropometric data set and of potential UK nuclear worker stereotypical behaviours on the design of AP1000 is discussed at Section 13.6.17. Invariably however the design of structures and the installation of systems important to safety, when they must also accommodate and interface with human operators and maintainers, will require there to be made design compromise between conflicting operational and structural engineering requirements, e.g., the size of MTIS-access ports that can be made in normally pressurised vessels and still comply with structural integrity codes. Section 13.6.12 describes the maintenance and maintainability activities that have been completed and the scope of HF maintenance assessments to be completed during site licensing.

There is no specific selection criteria developed for the AP1000 plant operators. However it is usual practice within the US nuclear industry to use the Edison Electric Institute Plant Operator Selection System (POSS) test battery to aid in the selection of candidates for electric utility industry operators in fossil, nuclear, or hydro power plants. POSS consists of a group of 5 short aptitude tests – reading comprehension, mechanical concepts, mathematical usage, spatial ability, tables and graphs – that have been found to be related to success in plant operations work.

13.6.3 Functional Requirements Analysis and Allocation of Function

A key HFI process activity in the early design planning and analysis stages is the analysis

of functional requirements to identify those functions that must be performed to satisfy plant safety objectives (functional requirements analysis), and the analysis of the requirements for plant control and the assignment of control functions to (1) personnel (e.g., manual control), (2) system elements (e.g., automatic control and passive, self-controlling phenomena), and (3) combinations of personnel and system elements (e.g., shared control and automatic systems with manual backup).

The Westinghouse design process for functional requirements analysis and allocation of function for AP600/AP1000 (Reference 13.32) has followed the good practice guidance and methodology within NUREG-0711 (Reference 13.14), and was further informed by IAEA TECDOC 668 (Reference 13.33) and so can be deemed comparable to the process outlined in the ONR's TAG (Reference 13.34) on this subject. Reference 13.32 provides both a description of the methodologies used for functional requirement analysis and function allocation and presents the results of applying these processes.

The functional requirements analysis and function allocation process follows a four stage process whereby (1) the functions that need to be allocated are identified; (2) functions are allocated using a set of guidelines and heuristics; (3) the reasons for allocation are justified and documented; and (4) the function allocation is tested and identified problems resolved through an iterative design and test process.

(1) Functional requirements analysis begins with identification of safety functions required to prevent or mitigate the consequences of postulated accidents that could cause undue risk to the health and safety of the public. For each critical safety function (CSF), the set of plant processes (plant system configurations and SSCs for the critical function success paths) that are responsible for or capable of carrying out the function are clearly defined. Key inputs to the functional requirements identification process at that time were the Emergency Response Guidelines and system specification documents for each of the plant systems.

(2) Each system process or component on a CSF success path was then allocated to automatic actuation or manual control on the following heuristic decision basis:

Automatic

- The operator is NOT able to perform the required task due to human limitations.
- Automation is necessary due to regulatory design requirements.
- Automation is necessary due to utility design requirements.
- Automation provides a safety benefit as identified in the PSA.
- Automation is preferred based on operating experience.
- Automation is preferred due to concerns for operator overload.
- Automation is inherent in the passive design.
- Tasks are not well suited to human performance and are better suited to automation.

Manual

- Human performance is required because automation is not technically feasible.

- Human performance is required by design recommendations or requirements.
- Human performance is preferred because of consideration of safety requirements, task complexity, cost/benefit considerations to implement automation, and the value of human judgment.
- As a backup to the automatic functionality

(3) The following HF considerations were incorporated into the early planning and analysis stages of the AP1000 project and function allocation:

- Tasks were not assigned to operators when it was known that they would be unable to accomplish critical safety actions in a timely manner. [There are no critical human actions identified by either deterministic or PSA criteria as defined by Reference 13.35, Section 2.1].
- Tasks are not assigned to operators when they are complex or not routinely performed and when there is a likelihood of error or a high workload may occur due to the initiation of a transient.
- Tasks are not assigned to operators when operating experience indicates that human capabilities may be inadequate to execute tasks with sufficient reliability.
- Tasks are not assigned to operators when the PSA/HRA indicates that HEPs are too high to maintain plant safety.
- Tasks are not assigned to operators when activities are not well-suited to human strengths (for example, the activities require sustained vigilance).

The allocation of functions has resulted in a plant design and consequential operator tasks that reduce the likelihood of situations that present conflicting task goals to the operator and potential violation of procedures. For example, the requirement in current plants for operators to throttle safety systems to prevent the reactor coolant system (RCS) overfill in some post-accident conditions is not required in the AP1000 plant. Also, in current plants the operators are typically required to make a number of actions to cool the RCS and depressurise it to the shutdown cooling system cut in conditions, to align and start-up the shutdown cooling system and to re-align the water cooling systems servicing the shutdown cooling system. None of these operator actions are required for the AP1000.

(4) The basis of the function allocation focuses primarily on the responsibilities of operators with respect to an individual function, system, or process. However, it is recognised that in an operational setting, the operators will have responsibilities across multiple systems. Further HF Engineering process activities define and evaluate the role of the operator to monitor and control multiple plant and safety functions.

The function allocation process (Reference 13.32) concluded by defining a number of principles that have helped to shape a concept for operation (Section 13.6.4) and inform HSI requirements (Section 13.6.6) for AP1000.

- Automatic actuation and control functions are needed for a variety of design reasons (e.g., when an operator may not respond quickly enough or the

workload may be too high to reliably perform control actuation functions).

- For system and component actuation, the human operator serves as a backup to the automated system.

- For system and component control, the human operator serves as a back-up when automation fails, but for certain operating conditions, the use of manual control is preferred.

- The human operator always determines when execution of an EOP is complete and the plant has reached a safe and stable state following a fault condition.

- The operator has limited control over passively actuated and passively controlled functions.

In the design and evaluation of the AP1000 plant, particular attention has been paid to the operators' role as supervisory controller and system monitor of automated systems. This includes the following human factors considerations:

- Situation awareness of the status and operation of the automated systems (that is, the ability to detect and understand changes in automated system performance)

- Ability to detect degradation in automated system performance and establish manual control

- Ability to make a smooth transition from the use of Class 3 SSCs to Class 1 SSCs

- Monitoring and supervisory control of passive systems (including decisions and actions to mitigate events before necessitating a transition to actuation of Class 1, passive SSCs)

- Optimising operator workload and workload transitions

- Operator vigilance and the need to keep the operator involved and knowledgeable of the plant status

Where functions were allocated to human operators, the following principles are applied:

- Develop displays that aid the operator in understanding about the process from both physical system and functional perspectives.

- Use plant systems to monitor for set point violations and other significant changes to aid the operator in identifying important changes.

- Use plant systems for monitoring parameter values that are needed in completing procedures and then informing the operator about the status of those parameters in the context of the procedure step.

- Aid the operator in locating and accessing important plant and system status information that may become relevant to operations.

Supported by this functional analysis, the role of the operators in the AP1000 plant, at a high level, remains the same as in many current nuclear power plants. Operators function as supervisory controllers of the automated systems. The operators monitor the state of the plant, systems, and equipment; they verify that automatic systems have actuated and are responding as required; and they take manual actions when necessary. Also, as in current plants, the operators respond to emergency events guided by EOPs, where the role of the operator includes monitoring the plant state, verifying plant parameters, and monitoring the automatic operation of Class 1 and 2 systems.

13.6.4 Concept of Operations

The difference between the role of the operator in the AP1000 plant and in current plants is one of degree, and not a fundamental change in character. At a detailed level, there will be differences in the specific activities performed by operators due to differences in safety-related systems, automation, and the availability of improved HSI. The HSI includes displays that integrate information to facilitate assessment of plant state and supervisory monitoring of automated systems, and a computerised procedure system that facilitates execution of the AOPs and EOPs.

Some of the distinctions in equipment type that are important from a design and licensing perspective should be relatively transparent from an operational perspective. In particular, the AP1000 employs passive safety systems that automatically protect the plant in the event of an accident, without the need for immediate operator actions. The AP1000 also employs DiD systems that, if available, can automatically protect the plant for the more probable postulated transients and accidents. If these, DiD, systems are available and operate correctly, they may prevent the need for the operation of the safety-related, passive systems. The AP1000 EOPs integrate the use of the DiD systems and the passive safety systems to maximise the protection of the plant for design basis and beyond design basis accidents. During transients, operators are required to monitor the status of both DiD systems and the passive safety systems, and are procedurally guided in the use of both types of systems.

A design aspect of the AP1000 plant that is different from current plants is in the use of passive safety systems. The passive systems rely on natural forces such as gravity or compressed gases, instead of mechanical forces such as pumps, to perform their functions. As with other automatic systems, operators are responsible for monitoring the availability and operational status of the passive systems. Operators are responsible to verify the operation of, or the need for operation of, the passive systems. When termination criteria are met, operators are responsible for terminating the operation of the systems. Monitoring and control activities associated with passive systems are guided by EOPs.

In the design of the HSI, procedures and training, the passive systems are treated as a type of automated system. The HSI will be designed to support supervisory monitoring and control of the passive systems. While the passive systems are different in how they operate, they do not pose fundamentally different challenges for HSI design or operator supervisory control. In addition, some specific passive systems, such as the accumulators, have been installed in current plants and function identically for the AP1000.

A full description of the AP1000 Concept of Operations (Reference 13.36) includes operation from the MCR, RSR, and local control stations (LCS), addressing normal, abnormal, transient, and emergency operations of the AP1000 plant. Also included are the administrative and business activities such as crew meetings/briefings, accessing plant information via the site-specific local area network, and use of the communication systems. The roles of AP1000 operations staff outside the MCR, RSR, and LCS are also presented

in order to provide a complete view of their roles in the concept of operation for the AP1000 and identify interface and communication channels that the OCS HSI must support.

The roles and responsibilities of the MCR staff are defined in Reference 13.37. This document identifies the roles, responsibilities, and staffing assumptions for the MCR personnel, including both minimal and large staff complement and describes how the expected MCR staff, minimal and large complement, interfaces with the MCR HSI resources.

This description of the concept of operation, along with the conclusion of the allocation of safety functions (Reference 13.32) has been used by OCS and HSI resource designers to develop a coordinated set of functional requirements and design specifications.

13.6.5 Task Analysis

Task analysis provides a systematic method for describing and analysing the way that plant operators interact with SSCs and in operational teams with their co-workers. Task analysis describes the requirements and demands of a task in terms of the actions or cognitive processes necessary for the operator to achieve the task goal.

There have been two main complementary task analysis activities used in the AP1000 HF Engineering programme: Function-based Task Analysis (FBTA) and OSA.

The implementation of these task analysis activities had the following objectives:

- Ensure that human performance requirements equate with human capabilities.
- Provide an input to the development of procedures.
- Provide an input to staffing, training, and communications requirements.
- Provide a basis for design decisions, including the identification of the control, indications, and alarm requirements.

These task analysis activities have been carried out sequentially, and with different but complementary objectives, in order to progressively build confidence that the HSI was sufficient and appropriate to provide the monitoring and control capability necessary to adequately support operators in the delivery and execution of their assigned tasks and safety functions.

- FBTA (Reference 13.38) – The FBTA analysis decomposes and describes selected portions of multiple AP1000 systems that are understood to support a unitary, general function of the plant. This provides a functional perspective on plant operation that supplements the structural perspective offered by the detailed design of individual systems.

- OSA 1 (Reference 13.39) – Focuses on the operational requirements and task demands in terms of the operator actions and/or processes necessary to complete the required AP1000 control and monitoring tasks, abnormal/emergency tasks, and maintenance, testing, surveillance, and inspection tasks.

- OSA 2 (Reference 13.40) – Evaluates the adequacy of the HSI design to support the AP1000 HF program risk-important tasks by identifying and analysing task requirements, time to perform tasks, operational crew staffing and workload.

13.6.5.1 Function-Based Task Analysis (FBTA)

The purpose of the FBTA was to determine and confirm that the instrumentation, controls, alarms, and displays provided via the control systems and operator interfaces were adequate to enable the MCR operators to perform their assigned roles. The FBTA results (Reference 13.41) provide input to the detailed design of the function-based displays.

Results from the FBTA were used to feed into the TSV (Section 13.7.1) in order to:

- Obtain a completeness check on the availability of needed indications, and controls. This includes indications and controls needed for supervisory control of automated systems and manual override.

- Identify issues for tracking and resolution relating to details of plant design or operation.

13.6.5.2 Operational Sequence Analysis 1

A representative sample of plant operator tasks underwent OSA, selected on the basis of the following criteria:

- Representation of the full range of operating modes (for example, start-up, normal, shutdown, abnormal and emergency operations, transient, and low-power conditions).

- Operations including critical human actions and risk-important tasks.

- Representation of the full range of activities involved in an emergency response.

- Operations including MTIS tasks, particularly if a task is identified as risk-important.

With the aim to identify potential limitations on successful task performance that were due to the limits of human performance and capabilities, equipment or software performance and crew communications, each of the scenarios was decomposed into its constituent tasks using approved AP1000 operating procedures.

The results of the analyses of each task have been used to identify the indications, controls and alarms required by the operators and used as a key input into the display development process.

13.6.5.2.1 Criteria for Critical and Risk-Important Human Actions

The deterministic and probabilistic criteria for the identification of critical human actions (Reference 13.35) were negotiated by Westinghouse with the US NRC during development of the AP600 in the mid-1990s. They allowed credit to be taken for the improved safety of the AP600, when compared to current operating plants, and later the AP1000 due to their passive safety features and the non-reliance of ac power for 72 hours. Application of the critical human action criteria, found below, results in the identification of no such actions.

- Deterministic criteria – Any human action that is required to prevent core damage or severe release in licensing DBA.

- PSA criteria – Any one human action that, if assumed to fail, would result in a CDF greater than 1E-4 or a severe release frequency greater than 1E-5.

In order to address the intent of identifying the relevant risk significant human actions,

continued negotiation with NRC resulted in criteria for the identification of risk-important human actions, important for their contribution to CDF and large release. The criteria used to identify risk-important human actions (RIHAs) (Reference 13.35) were the following:

- Risk achievement worth (RAW) – The increase in risk that would result if a single human action were to fail. The CDF and LRF are re-quantified for each human action by setting their failure probability to 1. The RAW value is then calculated as the percentage increase in CDF or LRF due to the human error. For the baseline PSA, a human action is considered risk-important if the CDF or LRF increase is 200 percent; i.e., the RAW is > 3.0. For the "focused" PSA study (with assumed failure of non-safety mitigating features), a human action is considered risk important if the percentage increase is 100 percent; i.e., the RAW is > 2.0. Any value below these criteria is considered to be not risk-important.

- Risk reduction worth (RRW) – The decrease in risk that would result if a human action were made perfectly reliable. The CDF and LRF are re-quantified for each human action by setting their failure probability to 0. The RRW value is then calculated as the percentage decrease in CDF or LRF. For the baseline PSA study, a human action is considered risk-important if the CDF or LRF decreases by more than 10 percent; i.e., the Risk-Reduction Worth is > 1.1. For the "focused" PSA study (with assumed failure of non-safety mitigating features), a human action is considered risk-important if the percentage decrease is 5 percent; i.e., the RRW is > 1.05. Any value below these criteria is considered to be not risk-important.

(RIHAs were however identified for post-accident mitigation and for MTIS support tasks. The basis for the selection and identification of RIHAs is described in Reference 13.35.

Information collected and recorded in the OSA task step relational database included:

- Plant state data required at each step
- Source of the data (e.g., alarm, display, communication)
- Operator Action or decision to be made from the data
- Procedure Steps
- Feedback - Information that provides feedback on the adequacy of actions or decisions
- The required order of tasks, or tasks that need to be done in parallel
- Communication requirements
- Interfaces with other systems

The results of the analyses of each task (Reference 13.43) were used to identify the indications, controls, and alarms required by the operators and used as a key input into the display development process.

13.6.5.3 Operational Sequence Analysis 2

OSA-2 was undertaken on a representative set of operating scenarios that included critical human actions (none), risk-important tasks, and tasks with potential human performance concerns (e.g., anticipated high workload).

After screening the human actions identified in the PSA (Reference 13.44) on the criteria above, OSA-2 was conducted on 19 risk-important tasks and four tasks with potential

human performance concerns. The tasks with human performance concerns were selected by an expert panel on the basis that the tasks were new to control room operations (and therefore had not previously been assessed) and/or had a potentially high operator workload.

The tasks with human performance concerns included:

- Action in response to a data display and processing system failure
- Action in response to the loss of computerised procedures system (CPS)
- Technical Specification (Tech Spec) monitoring
- MCR evacuation

OSA 2 was substantially more detailed in its depth of analysis, building on the OSA 1 analysis, to evaluate the adequacy of the HSI resources available to the operator while conducting risk-important, potentially high workload, tasks. The results from OSA-2 have fed in to the design of procedures and operator training.

OSA-2 addressed four main HF areas:

- Completeness of information – to establish that the information necessary for successful task completion was available.

- Time to perform tasks – to establish that the operators were able to successfully complete tasks within the available time. The time available is based on the thermo-hydraulic calculations used in the PSA model of that time. The time taken was based on assigning to each operator-performed step in the task analysis a generic definition (e.g., check a variable, evaluate a situation, initiate a sequence, etc.) and assigning to that task step the estimated average time to complete (Reference 13.45 Table 2.2-1). Average times had been calculated from the observation of video recordings of operators executing procedure E-0 on a reactor trip or safeguards actuation using the AP1000 control room development facility and the simulator.

- Operator workload – to evaluate the effect of HSI design and task demands, including any concurrent tasks, on operator time-based workload. Time-based workload was derived from dividing time-taken by time-available and multiplying the figure by 100 to yield a percentage. Acceptable workload was considered to be between 50 and 80 percent.

- Operational crew staffing – to verify staffing assumptions. The results of the operator workload assessments and the identification of time constraints are used to review the adequacy of the staffing assumptions, HSI design, task allocation, and work organisation.

The results of OSA-2 (Reference 13.45) concluded that the design of the AP1000 plant supports the successful completion of the 19 risk-important human actions and the four tasks with human performance concerns, with no design changes necessary. The workload was considered to be acceptable for all tasks, with recommendations on operator requirements for one task.

13.6.6 HSI Design

The layout and arrangement of workstations in the MCR (see Figure 13.6) has been

informed by customer input, and by the crew organisation and shift complement described in the AP1000 Main Control Room Staff Roles and Responsibilities (Reference 13.65).

13.6.6.1 HSI Design Guidelines

The design and layout of the control and display features, presented at workstations and on equipment having hard panels or 'soft' VDUs, has been guided by two key documents produced by Westinghouse and based on international Standards, good practice guidance and operating experience.

The first of these HSI design guidance documents (Reference 13.46) is applicable to the HSI resources that are located in the OCS. The focus of the HF input is on the MCR, but the OCS also includes the TSC, the RSR, and the OSC.

The HSI resources include the plant information system, alarm system, computerised procedures, protection and safety monitoring system (PMS) display, soft controls, dedicated controls, diverse actuation system, and the wall panel information system (WPIS). The HSI design guidelines address the HSI resources that are primarily utilised by the MCR operating staff. However, additional users are also considered, such as the shift supervisors, operations management, technical, engineering, maintenance, health physics, and chemistry personnel. The HSI design guideline document includes the following HF guidance:

- Control room design
- VDU-based workstations
- Workstation and console design
- Control room equipment
- Location of controls
- Control and display design
- Alarm systems design
- Computerised procedures
- Communication facilities
- Colour-coding
- Labelling
- Closed Circuit Television Systems
- Working environment
- Display organisation and navigation

The second HSI design guidance document (Reference 13.47) is applicable to the local plant and field operations, local plant control room and operations areas, maintenance workshops, local plant maintenance tasks, and manual activities and includes the following HF aspects:

- Workstation & Console Design
- Movement of Personnel
- Manual Forces
- Location of Controls
- Control and Display Design
- Colour-coding & Labelling
- Annunciator Panels and Auditory Alarms
- Closed Circuit Television Systems
- Working Environment
- Maintainability

The guideline documents are used as a design input directly by the engineers responsible for the development of the OCS operator interfaces and the local plant areas and equipment. The guidelines are applicable across the entire AP1000 project, including peripheral areas that may not be subject to detailed HF analysis, to ensure application of best practice in HSI design, maintain consistency and avoid HF conflicts (such as inappropriate legacy transfer, misdiagnosis, etc.) within and between different operator

interfaces.

The guideline documents have also been used by HF specialists as a tool to provide a systematic means of participating in respective design reviews, and have been used as the basis for the HF design verification, which is described in Section 13.7.2 and more fully in Reference 13.42.

13.6.7 Operation and Control Centres

The objective of the control centres and HSI designs is to provide the operators with an effective means for acquiring and understanding plant data and executing actions to control the plant processes and equipment. The OCS system specification document (SSD) (Reference 13.50) describes the purpose and goals of each control centre and HSI resource, states the main design basis and the rationale supporting engineering design decisions. It covers the design of the MCR, TSC, RSR, operations support centre, local control stations, and the HSI resources (Figure 13.3). The design of each of these control centres is undertaken using the HF Engineering design process as described in the HF Engineering Program Plan (Reference 13.10).

The HF Engineering activities, such as the functional requirements analysis and allocations, FBTA, OSA-1, OSA-2, the engineering test results, operating experience reviews, HSI design guidelines, and the HRA are used by designers to produce the functional requirements, design basis, and design specifications for the individual control centres and HSI resources. The corresponding design specification documents provide greater detail. They document how the requirements as identified in the functional requirements are realised. This includes information on the means, by which the detailed HSI Design Guidelines (Reference 13.46) are applied to the design. The design specification documents typically includes layout drawings, general arrangements, and design descriptions. It is used by the designers as an input to develop the hardware and software implementation documentation, specifications, and verification test procedures.

13.6.7.1 Distributed Control and Information System (DCIS) Displays and Soft Controls

The purpose of the DCIS is to ensure that the operators' understanding of the current plant conditions, equipment, and alarm status is maintained and/or can be readily ascertained. The soft controls enable the operators to control the plant safely under normal conditions and to maintain it in a safe state under accident conditions.

The Data Display and Processing System (DDS) displays and the Plant Control system (PLS) soft controls are part of the DCIS. The displays utilise colour VDU-based workstations to present graphics displays (or mimic displays), trend displays, alarm information, etc. (e.g., Figure 13.4 – further examples of DCIS display screenshots are provided in Figures 13.7 to 13.15). Note: These 'screenshots' are provided for illustrative purposes only. No dynamic data was driving inputs to these displays so no inference to any real-world plant conditions and 'bad' magenta data should be made.)

The DDS displays include physical or system process displays (Figure 13.7), functional displays (Figure 13.8), task displays (Figure 13.9), trend displays, embedded trends, historic data displays, health displays, tagging displays, results from application programs and data processing detail displays. The displays provide dynamic indications of plant parameters and equipment status, including the detailed information required for the monitoring, planning, controlling and obtaining feedback on control actions. The DDS displays provide information on instrumented plant systems and components, including DiD and passive safety systems, functions and components, plus it includes alarm

information.

These VDU-based workstations also provide links to access other human system interfaces such as the CPS and the alarm presentation system (APS) via a windowing system.

The DDS displays provide the mechanism to access the soft controls by selecting a target area (or poke field) on a display (Figure 13.4). The means to access and display the soft controls enables the operator to view the associated graphics displays while undertaking control actions. The DDS displays and soft control displays are accessible via the VDU-based workstations on the operator's and supervisor's consoles in the MCR, although the control functionality is normally 'locked-out' at the supervisor's console.

13.6.7.2 Protection and Safety Monitoring System (PMS) Displays

The purpose of the PMS safety displays is to present information which is important to plant safety as well as provide a limited number of soft control functions. This includes Qualified Data Processing System (QDPS) visual alerts and post-accident monitoring (PAM) variables, and the Reactor Trip System (RTS) and ESF information. The QDPS is provided by the PMS. The PMS displays assist the operators during abnormal and emergency conditions in determining the safety status of the plant and determining if operator action is required to restore the function. Although primarily for use in abnormal or emergency conditions, the associated VDU-based workstations, located at the primary dedicated safety panel (PDSP) in the MCR, are continuously available. The PMS displays provide an overview of the PAM variables, critical safety function displays, RTS and ESF status displays, trends, alerts and detailed data displays. These safety VDU-based workstations are also used to perform RTS and ESF system blocks, resets, Nuclear Instrumentation System calibration functions and ESF component control (for those functions that result in onerous consequences).

The HSI aspects of the design of the PMS displays and soft controls are compatible with the DDS and PLS displays, designed to the same set of HSI/HF guidelines. Designing to the same set of HSI guidelines avoids possible operator errors or delays caused by inconsistent designs between the DDS/PLS displays and the PMS displays. In addition, much of the PMS display information is communicated (via a one-way gateway) to the DCIS and associated VDU-based workstations, where the information is presented via comparable displays.

13.6.7.3 Dedicated Controls

The fixed-position controls are located on the PDSP and the Secondary Dedicated Safety Panel (SDSP) in the MCR. Dedicated controls are also available on the remote shutdown workstation (RSW) panel located in the RSR.

These controls are dedicated to a single function or system level actuation, as typically found on traditional control panels. They provide PMS control functions, including control functions with onerous consequences. Reactor trip, turbine trip, and ESF system level actuations are accomplished using the controls on the PDSP. The ESF system level actuations, resulting in onerous consequences (e.g., automatic depressurisation system [ADS] actuation), are accomplished by actuating one of the controls on the PDSP, plus the corresponding control on the SDSP, simultaneously by two reactor operators (ROs). The RSW panel also provides the controls required for manual reactor trip and the ESF system level actuations.

13.6.7.4 Wall Panel Information System (WPIS)

The purpose of the WPIS is to provide the control room staff with a high-level understanding of the current plant and equipment status via the dynamic display of plant parameters and alarm information. The WPIS facilitates a user group comprehension of the current plant equipment and process status.

The WPIS is positioned in the MCR such that it is visible by the relevant operations personnel and the required text and graphics/symbols are legible by the operators and supervisor while seated at their respective consoles (Figure 13.6). The WPIS presents plant overview and status information, an overview of alarms, major plant parameters, trend displays, equipment and system availability. It also has the capability for the operator to present (or 'post') displays available on the console-based workstations on the WPIS. The WPIS enhances the MCR crew shared situational awareness by:

- Combining and integrating important diverse information that depicts the overall plant status
- Providing "at a glance" overview of plant status
- Identifying major changes in plant state
- Assisting in shift handover by providing a focal point for communication
- Indicate the presence of alarm conditions
- Indicate changes in plant conditions and the rate of change
- Assist in normal plant operations
- Assist in alarm, emergency, and abnormal conditions

The enhanced situational awareness that WPIS provides is particularly advantageous in fault and emergency situations when there may be higher than normal levels of workload, interaction and communication between operators in the MCR.

13.6.7.5 Alarm Presentation System (APS)

The overall purpose of the alarm system is to alert the operators to abnormal plant conditions and to provide them with an understanding of the plant status and behaviour (Reference 13.53).

The alarm system utilises the DCIS VDU-based workstations and the WPIS HSI resources as the means to present alarms and support information to the MCR operators. Alarm information is organised, managed, and presented by the APS. Examples of APS display screens are shown in Figures 13.10, 13.11, and 13.12.

In addition to the APS, the DCIS base alarm system provides detailed contextual information by integrating the alarm indications into the DDS and PLS graphics at the VDU-based workstations at the operator's and supervisor's console. This system also enables the operator to acquire detailed alarm information such as set points, current parameter values, and sorting and filtering of alarm lists.

The APS has been developed in accordance with the internationally recognised standards for the design of alarm systems, EEMUA 191 (Reference 13.51) and International Electrotechnical Commission (IEC) 62241 (Reference 13.52) and with reference to the AP1000 HSI design guidelines for alarm presentation (Reference 13.46 Section 13) where

specific guidance has been provided on the following aspects of alarm system design:

- Alarm categorisation and prioritisation
- Alarm suppression (including standing alarms)
- Minimising nuisance alarms
- Redundant alarms and logic (e.g., in certain operating modes)
- Colour coding and alarm presentation
- Alarm annunciation (visual and auditory)
- Alarm grouping
- ARPs

The APS extends the capabilities provided by the base alarm system providing additional functionality such as alarm suppression, access to alarm response procedures, and alarm grouping. As well as being available on any of the DCIS VDU based workstations on the operator consoles, APS uses the large wall-mounted WPIS to promote early detection and the fast cognitive processing of key alarms by providing fixed areas dedicated to the presentation of alarm information. The WPIS is visible and the labelling easily readable from the RO's, supervisor's and Diverse Actuation System (DAS) panel consoles. An auditory alarm signal will alert the operator to the onset of an alarm.

Alarms are viewed and responded to from the DCIS workstations using the APS as follows:

- The WPIS presents a view of alarms that allows the operators and MCR supervisor to maintain cognisance of the plant conditions at all times. The WPIS also presents a view of alarms common to all operators in the MCA that may be used for review during shift hand-over.

- The operator may use the WPIS as the primary method to identify and correlate high priority alarms and to identify situations in which multiple new alarms are present.

- The operator responds to alarms presented on the WPIS from a DCIS VDU-based workstation at the RO console through the APS support interface.

- ARPs, trend information, detailed parameter and component status information, process diagrams, and logic diagrams are all available using the DCIS VDU-based workstations and APS to assist the operator with diagnosing the alarms and undertaking the necessary compensatory actions.

The APS sorts and organises the alarms from the base alarm system into predefined chronological lists (e.g., unacknowledged alarms, alarm history, un-reset alarms, active user defined alarms, and suppressed alarms) that the operator can select to support the current operations. Any DCIS VDU-based workstation can be used to present the APS support interface and alarm lists. The following information describes key APS functionality that is available to the operators:

- The operators can acknowledge and reset alarms via a pop-up menu accessed from the APS alarm list.

- The operators can obtain information via a pop-up menu accessed from the APS alarm

list.

- The operators can sort alarms by priority, time, system, or operator work station in order to help manage alarms when multiple alarms are present.

- The operators can acknowledge groups of active alarms when presented with multiple new alarms in order to reduce alarm response task workload.

- The APS alarm lists allow the operators and MCR supervisor to be aware of plant conditions. The alarm lists also present a view of alarms that may be used for review during shift handover.

The operators perform alarm-related operations such as acknowledging and resetting alarms from the RO console. The alarm response functions may be divided between the two ROs, with each operator having responsibility for their assigned area. However, any operator assigned to the MCA will be able to monitor and remain cognisant of all alarms.

The MCR supervisor monitors the operators' alarm-related activities from the supervisor's console. Non-routine alarm-related activities such as bypassing an alarm, taking an alarm off scan, or deactivating groups of alarms when a plant function is unavailable, are performed by the operator with the concurrence of the MCR supervisor. The MCR supervisor is cognisant of all alarms and ensures that the RO responds to alarms promptly and in accordance with the ARPs.

The ARPs are electronic presentations of ARP steps, and are retrieved through hot links from the background information menus. Paper copies of the ARPs are available if the electronic versions are not available. Each alarm is provided with an associated ARP and on acknowledgement of the alarm; the operator will open the ARP and follow the procedure steps. Note that in a number of cases, the same ARP applies to more than one alarm indication.

13.6.7.6 Computerised Procedures System (CPS)

The CPS assists the operators in monitoring and controlling the execution of plant procedures. The CPS is accessible via the VDU-based workstations on the consoles in the MCR. The CPS provides navigation links to displays and associated soft controls in the Class 2 control system displays. Examples of CPS display screens are shown in Figures 13.13, 13.14, and 13.15.

The CPS guides operators through plant operating procedures, presenting the status of the procedure steps to the operator. The operators will perform all specified actions in the CPS, with supervision and monitoring from the MCR supervisor.

The CPS provides navigation links to displays in the non-safety control system. Provision of this navigation feature allows the operator to view the procedure step within the physical context of the plant, providing the detailed plant system or component status information. During the execution of emergency operating procedures, the CPS presents the status of the critical safety functions and when applicable directs the operator to the respective function restoration procedure.

In the event that the CPS is unavailable, paper procedures will be used as backup to computerised procedures. These paper procedures include all of the steps, cautions, notes, and features of the computerised procedure and are available in the MCA. In addition, if the CPS becomes unavailable, an online generation of the CPS log will be used to identify

the particular procedure step currently being executed, thereby avoiding place-losing errors in the procedure execution process.

13.6.7.7 Engineering Tests

Formal HF engineering tests were conducted and results documented to provide timely feedback during the HSI design process (References 13.15, 13.16, and 13.17). The engineering tests used rapid prototypes of the MCR consoles, panels, and operator interface designs. These tests were conducted in the AP1000 plant MCR simulator facility with qualified, licensed PWR operators, supplied from participatory utilities, undergoing realistic test scenarios. The first test was focused on the usability of the VDU-based soft controls (Reference 13.16). The second and third engineering tests addressed MCR layout and integration of the user interfaces and their operability and vulnerability to human error (References 13.17 and 13.18).

The engineering tests provided valuable feedback into the early prototype designs due to the differences in the operator interface technology from existing plants and the passive safety systems of the AP1000. The AP1000 MCR provides operator interfaces that are almost entirely comprised of soft controls and display systems (in comparison to a conventional control room layout, containing a relatively large number of dedicated fixed-position controls and displays on panels or control boards positioned around the perimeter of the MCR). The engineering tests provide data via video and digital recordings of operator actions, verbal feedback from the operator subjects and observers via questionnaires, as well as qualitative workload ratings and debriefing sessions.

13.6.7.8 Diverse Actuation System (DAS)

The DAS has been designed to address common mode software failure of the PMS in order to achieve the safety goals of the AP1000 PSA. The DAS provides an independent and diverse means of automatic and manual reactor trip actuation and a selected set of automatic and manual ESF actuations. The specific functions performed by the DAS are selected based on the AP1000 PSA evaluation (i.e., an assessment of the protection system common-mode failure probabilities combined with an event occurrence probability). The DAS is a Class 2 system.

A DAS panel is located in the MCR and comprises the controls for the manual actuation of DAS functions and fixed-position displays for a relatively small number of key parameters. The displays are sufficient for the operator to confirm that a DAS actuation has been initiated and completed. Use of this system will be infrequent, and to prevent inadvertent actuation, the panel control switches are normally kept de-energised, although the displays are continually available. The control switches are enabled from a switch located on the PDSP.

13.6.8 Main Control Room (MCR)

The purpose of the MCR is to provide a seismically qualified and habitable environment (see description of Nuclear Island Non-Radioactive Ventilation System (VBS) at PCSR Chapter 6, Section 6.8.4) for the operators and supervisors to safely, efficiently, and reliably monitor and control plant process during normal, abnormal, and accident conditions. The MCR is designated as an area that remains habitable in the event of an emergency (see description of MCR Emergency Habitability System (VES) at PCSR Chapter 6, Section 6.6.3). It supports operator performance by providing the facilities to interact with other plant personnel, while preventing distractions by non-operations personnel.

It provides a facility that supports the operators in the effective and timely execution of their assigned tasks and responsibilities. Alarms are provided to draw the operator's attention to key indications that may require operator action; displays are provided to enable the operators to determine the plant status; and control facilities are provided to allow the operators to execute control actions. It also provides an interface between plant operations and plant maintenance functions.

The MCR also incorporates the interfaces required for functions such as fire protection and radiation monitoring. In addition, the MCR contains miscellaneous items such as storage space for supplies, procedures, document storage and a drawing laydown area. A table is provided and equipped with a VDU-based workstation to allow access to the DCIS displays and soft controls by a shift manager, reactor engineer, maintenance technician, or auxiliary/field operator without disrupting control room operations. Located in the rear of the MCR are the shift supervisor's office, the operations support area, an operations work area, restrooms, and kitchen facilities.

During emergency conditions, it may be necessary for the MCR to accommodate up to eleven personnel and for the design, including VES, to support this maximum crew compliment. This maximum crew compliment may include two individuals with senior reactor operator licenses, three with RO licenses, an observer from the NRC, an observer from the plant owner's management, and one communicator. Available elsewhere in the plant are two equipment operators. This maximum MCR crew compliment would not assemble until an event occurs and the emergency plan and recall has been invoked and recalled personnel have reported to site.

13.6.9 Remote Shutdown Room (RSR)

The purpose of the RSR is to provide a facility to enable the operators to achieve and maintain safe shutdown following an evacuation of the MCR in the event that it were to become uninhabitable due to fire or smoke.

The RSR houses a single operator console that includes two DCIS VDU-based workstations – or RSW. The console has access to the same HSI resources as the workstations on the MCR reactor operator's console. The RSR is also provided with a dedicated fixed-position switch panel that includes 4 PMS VDUs (one per PMS division) providing the PMS safety displays and accompanying soft controls such as the PMS soft blocks / resets. This remote shutdown safety panel and its operator interface (PMS safety displays and controls) are similar to the MCR PDSP. The familiar design promotes reliable and efficient operator performance.

The site specific emergency plan shall address specific manning of the RSR upon evacuation of the MCR due to uncontrolled fire or smoke in the MCR. However, per the standard AP1000 plant MCR staff roles and responsibilities document (Reference 13.65), the RSR is staffed by a minimum of 1 RO and a control room senior reactor operator (SRO). This allows flexibility for the second MCR RO to immediately lead or be a member of the Fire Brigade, as possibly specified by the fire response portion of the site specific emergency plan. The site specific emergency plan shall include details for fire response, including the specifics of the fire brigade (i.e., content, responsibilities, and actions).

In the improbable event of a fire starting in the MCR that requires evacuation to the RSR, occurring simultaneously with an emergency where the site specific emergency plan invokes a full MCR complement (potentially 11 personnel), then the site emergency plan will likely direct additional personnel, not required in the RSR to achieve and maintain safe shutdown, to the OSC. The mission of the OSC is to provide a habitable area for

operations support personnel and the resources to coordinate the assignment of duties and tasks to personnel outside of the main control room and the TSC in support of plant emergency operation. Additional support personnel as they are recalled by the site specific emergency plan shall be directed to report to the TSC or to the OSC to receive further direction.

The use of the RSR will be infrequent and control capability at the RSW is normally disabled. Control capability is transferred from the MCR to the RSR via a set of control transfer switches. The RSW, consisting of 2 DCIS VDU-based workstations and a MCR PDSP-like switch panel, provides resources to physically accommodate as many as three qualified personnel to directly monitor and control the plant (i.e., one at each DCIS workstation and one at the switch panel). Additionally and as in the MCR, the control supervisor directs and supervises the actions of the ROs.

The maintenance of RSR habitability is provided by the VBS but is not served by the VES. The probable temperature and humidity profiles that might be encountered as the result of prolonged occupation of the RSR, with a subsequent loss of VBS, will be assessed as part of the ongoing RSR development for UK AP1000 design.

A detailed task analysis of the transfer to the RSR, due to a fire in the MCR, and maintenance of the plant in a safe state from the RSW, has been conducted as part of the HEA in support of the GDA submission for the Fire PSA. [

] The result of the human error task analysis of this operator action (HEPO-FI-MCREVAC) for the Fire PSA is found in Reference 13.54. [

]

13.6.10 Local Control Stations

The purpose of local control stations is to provide control and monitoring functions at selected locations outside of the MCR and the RSR for operations and maintenance personnel to carry out plant and equipment control and monitoring activities. Typically these activities are maintenance or other non-routine functions.

There are workstations that are DCIS VDU-based workstations that are connected to the DCIS network. These local DCIS workstations are provided with the displays, capabilities and soft controls required only for designated functions and do not possess general control and display capabilities.

Another type of local control station comprises dedicated fixed-position controls and/or displays. These control stations or panels are varied in size and nature. For example, they may include display meters, valve handles, switches, breakers, indicator lights, pushbuttons, emergency stop controls, electrical panels, etc. Some of these local control stations may be an integral part of an equipment package. These may comprise dedicated fixed controls and/or displays, and may include a standalone VDU-based workstation. An example would be the fuel handling machine.

An additional guidelines document supplements the HSI Design Guidelines document to address the local plant aspects. This document, (Reference 13.47) includes, for example, manual tasks associated with operating valve handles, tool laydown areas, physical access, provision of equipment, equipment labelling, etc.

Refer to section 13.6.12 for a scope description of local controls stations to be included as part of the future HF maintenance assessments to be completed during site licensing.

13.6.11 Plant Layout and Equipment Design

The HF aspects of the plant layout, room layouts and equipment design for operations will vary widely in their importance to safety and operability. Therefore, the appropriate level of HF Engineering involvement is determined on a case-by-case basis.

Design guidelines, HF checklists, and As Low As Reasonably Achievable dose checklists are employed to ensure that the design meets the requirements of a human engineered environment and to assist in ensuring that the workers exposure to radiation is minimised. The HF Engineering input has been largely limited to the application of the relevant AP1000 HSI Design Guidelines (Reference 13.46), supplemented with additional guidelines that address plant layout and equipment design (Reference 13.47). The HF considerations include equipment accessibility, lifting devices, temporary or permanent access platforms, laydown areas, labelling, and the provision of emergency equipment.

13.6.12 Maintenance and Maintainability

The HF supplemental report (Reference 13.56) provides detailed information regarding the maintainability of the AP1000 plant.

As described in Section 4.2.1 of Reference 13.10, Westinghouse adopted a tailored HF Engineering approach to determine HF analysis requirements, categorising HF Engineering areas as core, adjunct or peripheral based on such factors as the degree of human involvement in the task, the nature of the task, task complexity, required speed of operator response, and the potential safety or operational consequences of an operator error. The same framework approach was applied to maintenance to determine the level of HF involvement.

The squib valves are an example of a core maintenance area to which rigorous human factor inputs and methodologies have been applied. An extensive and detailed task analysis of the maintenance and surveillance tasks associated with the ADS Stage 4 and in-containment refuelling water storage tank (IRWST) gravity injection squib valves and the recirculation squib valves was conducted as part of the cognitive-level HEA conducted on the maintenance latent error (MLE) operator action error assessments OPR-011 and OPR-106. The task analysis and HEA pro forma for these two MLE assessments is to be found in Reference 13.54 and further reported in the AP1000 Squib Valve Safety Case (Reference 13.96).

The maintainability case activities addressed by Reference 13.56 include the following:

- Maintainability portion of the constructability, operability, maintainability, inspectability, and testability (COMIT) reviews
- HF maintenance assessment
- Human error prevention with respect to making C&I software changes

Section 3 of Reference 13.56 presents a summary of the purpose, scope, and process of the maintainability reviews and plant layout reviews conducted as part of the COMIT process. The objective of these maintainability and plant layout reviews is to ensure that the plant owner/operator is able to operate and maintain the plant in a safe and efficient manner. The

reviews determine the feasibility of accessing, removing, maintaining, testing, operating and rigging equipment. Where appropriate, changes are identified and submitted as DCPs to ensure adequate ease of maintenance tasks.

Section 4 of Reference 13.10 presents a summary of the purpose, scope, and methodology of the HF maintenance assessment. The objectives of this assessment are to ensure that the applicable HF design guidelines are appropriately applied to the design of local panels and maintenance activities, reduce the possibility of operator/maintainer injuries, avoid human errors in maintenance and local operations tasks that may create a risk to plant safety, and identify HF improvement opportunities that can readily be implemented at the design stage.

The HF maintenance assessment gives priority to local control stations and equipment that have been identified as having a potential impact on safety. The scope of the assessment is as follows:

- Risk-significant SSCs identified in Table 3.3-1 of Reference 13.35 (AP1000 Identification of Critical Human Actions and Risk Important Tasks).
- Local components involved in EOPs.
- Components\tasks associated with potential maintenance errors identified in Appendix C of Reference 13.7.
- Radwaste control room and radwaste local station, including local Ovation™ stations.
- Electrical systems, e.g., electrical rooms, motor control centres.
- C&I cabinets, e.g., component interface module (CIM).
- Other local plant control stations and equipment per the HF engineering programme on case-by-case basis, (e.g., fuel handling equipment and cranes).

As per the methodology presented in Section 4.4 of Reference 13.56, the HF maintenance assessments (local actions, maintenance activities, and associated operator interfaces) are conducted through a review against the guidelines provided by Reference 13.47. Reference 13.56 provides the results of the currently completed HF maintenance assessments. The remaining scope of the HF Maintenance assessments shall be completed during the site licensing.

Finally, Section 5 of Reference 13.56 presents a summary of human error prevention with respect to C&I software development and maintenance. Latent human errors may occur during the development and subsequent maintenance of software for complex C&I systems. Such errors are likely to affect the safety of plant operation in a number of ways. The Westinghouse HF programme, Quality Programme, and the C&I design and software V&V process all contribute to the prevention of human errors and to the identification of such errors prior to any effect on safe plant operation. Section 5 provides a summary of these programmes and processes. Also included is a description of a general process that the plant owner/operator can utilise to prevent the occurrence of human errors while making C&I system software changes.

13.6.13 Development of Procedures

The Westinghouse plant procedure writers group has developed a set of plant operating procedures for the standard AP1000 plant. The site licensee is responsible for the development of the site specific procedures to account for differences between the standard AP1000 and the Moorside site AP1000.

Several HF Engineering activities, completed as part of the HF Engineering program, have provided input to the process of determining the detailed content of plant procedures. These activities include the OER, OSA-1 and OSA-2 tasks analyses, HF engineering tests, the HRA, and the HF V&V activities. While undertaking these activities, valuable information and insights into the plant procedural content requirements are identified. In order to ensure that this procedure-related information is recorded and communicated to the plant procedure development group, an HF Engineering procedure development report has been produced (Reference 13.75).

The plant procedures writer's group developed a writer's guideline document that provides the standards for writing the AP1000 standard plant operating procedures (Reference 13.58). This procedure writer's guideline has taken account and incorporated industry RGP and regulatory standards. It defines the structure, format, style, and conventions to be used in the development of the standard AP1000 plant procedures.

The general process of procedure development includes the creation of a provisional version of the procedure that is reviewed and approved internally to Westinghouse and then issued to the procedure subcommittee of the AP1000 operations committee of the AP1000 Owner's Group (consisting of the participating domestic U.S. AP1000 utilities) for review. Westinghouse addresses the Owner's Group comments and produces the next revision of the procedure. For applicable procedures, a "walk-through" verification utilising the AP1000 simulator is completed to verify general usability of the procedure. Comments and insights from these verification walk-throughs are captured and addressed by the Westinghouse AP1000 procedures group in subsequent revisions to the procedure.

The applicable plant operating procedures are exercised and validated with the HSI during the HF ISV test (Section 13.7.3 and References 13.59 and 13.81). HEDs and HED issues relating to the design and use of procedures are captured and recorded for resolution via the HED resolution process (Section 13.7.4 and Reference 13.60).

13.6.13.1 Procedures

Utilising the procedure writer's guideline document, the Westinghouse procedure writer's group has developed the plant procedures for the standard AP1000 plant, including the following:

- Normal Operating Procedures (NOPs)
  - General Operating Procedures (GOPs); APP-GW-GJP-100s series procedures
  - System Operating Procedures (SOPs); APP-(the three letter system designator)-GJP-100's series procedures
- AOPs; APP-GW-GJP-300s series procedures
- EOPs; APP-GW-GJP-200s series procedures
  - Optimal Recovery
  - Safety Functional Restoration
- Surveillance Test Procedures (STPs); APP-GW-GJP-800s are the general, plant wide surveillance test procedures
- Maintenance procedures; APP-(the three letter system designator)-GJP-800s are the system specific surveillance procedures and maintenance procedures.
- ARPs; APP-(the three letter system designator)-GJP-400s series procedures

- SAMGs; Appendix K of UKP-GW-GGR-201 (Reference 13.84)
- Post 72-hour Operations Procedures; APP-(the three letter system designator)-GJP-720 series procedures

13.6.13.1.1 Normal Operating Procedures (NOPs)

There are two types of NOPs: GOPs and SOPs. The GOPs provide step-by-step instructions for the MCR operators to govern the transition of the plant through the plant operating modes. This set of procedures provides the instructions for moving through all modes of operation from refuelling (mode 6) to 100 percent power (mode 1). Thus, these procedures govern the plant heat-up, reactor start-up, main turbine start-up, excitation of the main generator, synchronisation to the power grid, and power escalation to 100 percent power. Similarly the GOPs include procedures that govern the reduction of power from 100 percent, normal reactor shutdown, and normal cool down and depressurisation to cold shutdown mode (mode 5) and to refuelling mode (mode 6).

A SOP exists for each plant system and provides instructions to the operators on how to align the respective system to perform its design functions. For example; the SOP for the chemical and volume control system (CVS) includes step-by-step instructions on how to establish let-down flow, how to align the system for automatic charging make-up to the RCS, and how to establish purification. The operators utilise SOPs as directed by the GOPs, AOPs, and ARPs.

13.6.13.1.2 Abnormal, Emergency Operating and Alarm Response Procedures

The AOPs provide step-by-step instructions to the MCR operators to respond to plant conditions that have deviated from normal states. These procedures are used to identify the cause of the deviation and to recover from it before the abnormality can escalate to the point where the reactor protection system and the ESFs actuation system are called into effect. In many cases, the normal entry into an AOP is from an alarm and its associated ARP.

The EOPs provide step by step instructions to the MCR operators on how to respond to plant emergency conditions. The EOPs are entered whenever a reactor trip or safeguards actuation has occurred or the plant parameters satisfy the conditions for a reactor trip or safeguards actuation. The EOPs consist of optimal plant recovery procedures and safety function functional restoration procedures. The optimal recovery procedures provide symptom-based response procedures for reactor trip, loss of reactor or secondary coolant, faulted steam generator (SG), and steam generator tube rupture (SGTR). The reactor trip procedure (E-0) is entered first, instructing the operator to manually trip the reactor as an "immediate action" (IA), even if an automatic reactor trip has occurred, and prompting the operator to verify that reactor trip has occurred and that all the safety systems have operated as required. The procedure then steps the operator through several diagnostic steps and based upon plant symptoms the operator is directed to the appropriate optimal recovery procedure. Critical safety functions are monitored through the use of logic trees during execution of the optimal recovery procedures. If a safety function is challenged at any time, the operators immediately transition to the respective function restoration procedure. Upon completion of the function restoration procedure, the operators return to the respective optimal recovery procedure.

The ARPs provide step-by-step instructions to operators on how to respond and recover from an alarm. Each alarm indication has an associated ARP. ARPs may direct the operator to transition to an AOP or NOP, as appropriate.

13.6.13.1.3 Maintenance, Test, Inspection and Surveillance (MTIS) Procedures

The STPs provide step-by-step instructions that govern the conduct of the plant Tech Spec surveillance requirement testing. The frequency of surveillance requirement testing is specified by the plant Tech Spec.

Maintenance procedures provide direction to maintenance personnel on how to conduct maintenance on the respective plant components. These also encapsulate procedures for testing, inspection and surveillance and include the following:

- Tech spec STPs
- Non-technical specification STPs
- Refuelling operational procedures
- Significant maintenance guidelines

13.6.13.1.4 Post-72 Hour Operations Procedures

Post-72 hour operating procedures direct operations to make the necessary alignments to maintain Ancillary Diesel Generators; Passive Containment Cooling; Containment Make-up; Spent Fuel Pool Cooling; and MCR Ventilation, entered when nearing the end of 72-hour's passive and battery-powered safety system installed inventory.

13.6.13.1.5 Procedure V&V

V&V of AP1000 operations procedures ensures adequacy and uniformity in documentation as required by a customer contract or regulatory guidance. Westinghouse administrative procedure APP-GW-GJP-150 specifies how to conduct V&V of operating procedures (Reference 13.101) but ultimately the V&V of procedures will be the responsibility of the owner licensee organisation, because of the specificity of operating procedures to the final, as-built, AP1000 plant, C&I and HSI design configuration and to the operating conduct, legislative and regulatory conditions of the AP1000 host nation.

Verification of procedures is performed to confirm the correctness of the procedure and to ensure that the technical aspects of the plant design are properly incorporated. Verification checks both the written accuracy through proper incorporation of information from the writer's guide (Reference 13.58) and technical accuracy through incorporation of technical plant design information and plant hardware.

Validation of procedures is an evaluation performed to determine the actions specified in the procedures can be followed by the intended users to perform activities, for which the procedure was intended. Validation checks:

- Usability of the procedure to provide sufficient, understandable information to the operator.
- Operational correctness of the procedure, compatible with plant responses, plant hardware, and the available shift manpower.
- Effectiveness of the procedure that it will work as intended.

Validation is conducted using table top, walk and talk through methods and in the AP1000 simulator using qualified personnel to perform control functions in response to scenarios for an observer/review team.

The process for V&V of procedures is an ongoing one, alongside development, enhancement and modification of the plant, C&I, and HSI design. Recent ISV trials conducted for the Standard AP1000 plant design (Reference 13.59) have resulted in the identification of a number of HEDs and HED Issues (13.82), the resolution, of which can be either wholly or partially be attributed to the modification of procedures (13.97). These amendments to procedures, along with approved DCPs, will be re-validated at plant start-up (Reference 13.61).

13.6.13.2 Severe Accident Management Guidelines (SAMGs)

The AP1000 SAMGs were developed to focus on managing the accident after core damage. The guidelines (APP-GW-GJP-5xx series) consist of three major parts. These distinct parts were defined based on in depth investigations of HF considerations, the interfaces with the AP1000 EOPs, the site Emergency Plan (*The Emergency Plan is site specific and the impact on SAMGs of a UK site Emergency Plan would need to be assessed in site licencing*); the possible high level severe accident responses, the potential positive and negative impacts of most actions after core damage, and the progression and chronology of severe accidents (Reference 13.98). SAMGs provide guidance to the MCR operators and emergency response personnel on how to respond to a plant emergency where specific plant parameters have reached a point where core damage may have occurred. The three parts consist of:

- Control Room SAMG
- TSC SAMG
- TSC Severe Challenge Response Guidelines

The Control Room SAMGs consist of two separate guidelines; the appropriate guideline is determined by the status of the TSC at the time the SAMGs are implemented.

- Severe Accident Control Room Guideline Initial Response (SACRG-1 Reference 13.99)
- Severe Accident Control Room Guideline After The TSC Is Functional (SACRG-2 Reference 13.100).

SACRG-1 is initially used by the Control Room staff during limited, rapidly developing accidents, and prior to the TCS being functional. Actions are well defined and prioritised, and presented in two column format similar to the EOPs that will be terminated on identification of core damage.

SACRG-2 is for use by the Control Room staff after the time the TSC is functional and ready to use the TSC SAMG. This guideline provides the Control Room staff with a structured set of activities for use during the time that the TSC is evaluating the plant conditions and the potential responses. This guideline is intended to foster communications between the Control Room staff and the TSC technical staff with the goal of enhancing the Control Room acceptance of the recommendations made by the TSC. Also written in a two-column format, the guideline contains instructions for:

- Monitoring support conditions for implementation of strategies.
- Monitoring the usability of instrumentation readouts being employed in TSC evaluations.
- Monitoring trends in specified key plant parameters to alert the TSC staff to

unexpected changes.

- Evaluating equipment status and availability.
- Identifying potential equipment alignments to meet the TSC accident management objectives.
- Monitoring plant status to ensure that previous actions have not resulted in an unexpected change in plant status.

A Diagnostic Flow Chart specifies the key parameters to be monitored and controlled during a severe accident. The key parameters to be monitored in the Diagnostic Flow Chart include:

- Containment water level
- RCS pressure
- Steam generator water level
- Core Temperature
- Fission product releases
- Containment pressure
- Containment hydrogen

A priority scheme for monitoring plant parameters and evaluating the need to implement a severe accident management strategy has been established, based on a detailed review of severe accident phenomena that may challenge fission product boundaries. If the value of a particular parameter is outside the range defined as a controlled, stable state, the TSC technical staff is directed to evaluate the need to implement strategies to bring the parameter within the range that defines a controlled, stable condition. The evaluation of the need to implement strategies is detailed in a set of seven Severe Accident Guidelines (SAGs). The seven SAGs are:

- SAG-1 (Inject Into Containment)
- SAG-2 (Depressurise The RCS)
- SAG-3 (Inject Into The Steam Generators)
- SAG-4 (Inject Into The RCS)
- SAG-5 (Reduce Fission Product Releases)
- SAG-6 (Control Containment Conditions)
- SAG-7 (Reduce Containment Hydrogen)

In addition, a Severe Accident Status Tree is used to diagnose ongoing fission product releases and challenges to fission product boundaries. The status tree is monitored while using the Diagnostic Flow Chart and evaluation of strategies identified by the flow chart diagnostics is ongoing. If a setpoint value in the status tree is exceeded, all other actions are terminated and a severe accident management strategy must be implemented immediately to deal with the more serious condition. The key parameters in the status tree are:

- Fission product releases
- Containment pressure

- Containment hydrogen
- Containment vacuum

The severe accident management strategies, referenced from the Severe Challenge Status Tree, are contained in a set of four Severe Challenge Guidelines (SCGs). SCGs require more urgent action so, unlike the SAGs, do not call for an evaluation of the benefits and negative impacts associated with the implementation of strategies with respect to the alternative of not implementing any strategy. Compared to the consequences of not responding to a severe challenge, the implementation of any strategy in the guidelines would be beneficial. The four SCGs are:

- SCG-1 (Mitigate Fission Product Releases)
- SCG-2 (Depressurise Containment)
- SCG-3 (Control Hydrogen Flammability)
- SCG-4 (Control Containment Vacuum)

Another important part of the APP-GW-GJP-500 series is the guidance provided to monitor long term activities after a particular strategy is implemented. This is contained in SAEG-1 (TSC Long Term Monitoring). These long-term activities range from identification of the limitations for operation of equipment put into service by the implementation of a strategy, to monitoring tank water levels to permit continued operation of equipment that is put into service to implement a strategy.

The final part of the AP1000 SAMG is the SAMG exit guideline, SAEG-2 (SAMG Termination). When selected parameters in the Diagnostic Flow Chart are less than their set-point values and stable or lowering, the plant is considered to be in a controlled, stable state. At this point, it is not expected that the plant condition will worsen and therefore, no new severe accident management strategies would be required. However, since core damage has occurred, caution should be exercised in performing some subsequent actions due to the high level of fission products possible in various plant systems and structures.

13.6.13.3 Importance of Operating Procedures

It is important to the operating philosophy of the AP1000 plant that tasks are performed in accordance with procedures and that the operators are fully knowledgeable regarding systems, components and structures. As seen in the Sections above, a complete set of procedures has been developed for all plant operating modes and for activities including maintenance, normal operation, abnormal operation and emergencies. These procedures specify how the operators will verify the proper operation of automated systems and intervene manually when needed.

13.6.14 Development of Training Programs

The development of operations training programs is the responsibility of a future licensee organisation. However, by virtue of the implementation of the HF Engineering Program Plan and completion of the HF Engineering activities, there are a number of analyses in which information is derived that is directly applicable to the process of determining the detailed content of the operations training programs. This may, for example, be in the form of identifying tasks where specific skills are required, refresher training requirements, noting where training is required for complex or demanding tasks, or instructing participants on the use of the HSI resources.

These HF Engineering activities have primarily been the OSA-1 and OSA-2 tasks analyses, engineering tests, the HRA, and the V&V analyses. While undertaking these activities, valuable information and insights into detailed operator training requirements are identified. In order to ensure that this training-related information is identified, recorded, and communicated to the group responsible for developing the training programs, an HF Engineering training program development report has been produced (Reference 13.62).

13.6.14.1 Licensed Operator Knowledge and Abilities

As a result of completing HF assessments of operator action errors (Reference 13.54) an assumption has been made that the RO and supervisor in the MCR will have passed licensing examinations (i.e., been granted a DAP certificate) and be conversant with a range of knowledge and abilities similar to those captured in NUREG-2103, "Knowledge and Abilities Catalog for Nuclear Power Plant Operators: Westinghouse AP1000 Pressurised-Water Reactors" (Reference 13.63). This provides the basis for the development of content-valid licensing examinations for ROs and SROs in the US. The examinations developed using this catalogue, along with the Operator Licensing Examination Standards for Power Reactors (Reference 13.64 NUREG-1021), will sample the topics listed in the catalogue. The catalogue is organised into six major sections: 1) Organisation of the catalogue, 2) Generic Knowledge and Ability Statements, 3) Plant Systems grouped by safety functions, 4) Emergency and Abnormal Operating Evolutions, 5) Components, and 6) Theory. This is a new Knowledge and Abilities catalogue developed specifically to address the passive nature of the Westinghouse AP1000 design.

13.6.14.2 Systematic Approach to Training (SAT)

The Westinghouse provided training utilises the INPO and WANO "Systematic Approach to Training Process (SAT)" to develop training materials for the Operations and Technical Support staff personnel. The SAT process includes the use of a Job and Task Analysis (JTA) to address operations-related technical disciplines in the AP1000 Training Program. For each technical discipline, the JTA consists of analyses and documentation to determine the knowledge and skills needed to perform the respective job. NUREG 2103, "Knowledge and Abilities Catalog for Nuclear Power Plants: Westinghouse AP1000 Pressurised Water Reactors" includes the JTA results for MCR operator candidates. This JTA forms the basis for the respective training program. The plant technical data from system/component design basis documents, system descriptions, system drawings, procedures, and safety analysis documentation is then used to produce the necessary training materials that are needed to provide the required knowledge and skills. It is assumed that the Site Licensee will use a SAT and resulting NUREG 2103, "Knowledge and Abilities Catalog for Nuclear Power Plants: Westinghouse AP1000 Pressurised Water Reactors" to develop and implement site specific training.

13.6.15 Staffing

The determination of the final and overall AP1000 staffing requirements is the responsibility of a future licensee organisation. However, the area of staffing levels, crew structures, qualifications, roles and responsibilities for the MCR is a key issue that is addressed by the HF Engineering analyses described in this HF Engineering Program Plan. The HF Engineering activities that have contributed to determining the staffing requirements for the Standard AP1000 Plant include the OER, functional requirements analysis and allocation, task analysis, HRA, the MCR and HSI design, the U.S. Code of Federal Regulations, and the HF V&V assessments.

Based on the results of the analyses conducted in this HF Engineering Program Plan, a

MCR staffing document has been produced (Reference 13.65). This describes the roles and responsibilities for each position of the operating staff in the AP1000 MCR and contributed towards the development of the AP1000 Conduct of Operations document (Reference 13.66)

For normal plant operations, the MCA and the associated HSIs have been designed based upon the following minimum MCR staffing levels (Reference 13.20, Volume 2, Chapter 10):

- One shift supervisor, holding a valid duly authorised person (DAP) certification (SRO), will be part of each shift. This individual is responsible for overall plant operation and will have an office adjacent to the MCA within the MCR. At any time, the shift supervisor may be anywhere within the plant boundary.

- One control room supervisor, holding a valid DAP certification (SRO), will be part of each shift. This individual is responsible for the direct supervision of the ROs in the MCR and their normal station is the MCA, but can be anywhere within the MCR.

- Two qualified ROs will be part of each shift. These individuals are responsible for the operations of the controls in the MCA and are normally located within the MCA. One of these ROs will be at the controls at all times, while the other is within the MCR.

- One individual qualified to provide engineering support as Shift Technical Advisor will be part of each shift. This individual will be normally located in the MCR, but can be anywhere within the plant boundary.

- Two auxiliary operators (AOs) qualified to operate equipment in the plant at local stations shall be part of each shift. These individuals will normally be located at various locations throughout the plant and take direction from the MCR operators.

For emergency operations, the MCA and the associated HSIs are being designed based upon the following maximum MCR staff levels (Reference 13.20, Volume 2, Chapter 10):

- Two individuals with appropriate DAP certificates, the shift supervisor, and the control room supervisor
- Three individuals with RO qualifications
- One engineering SQEP
- Two equipment operators
- One representative from the regulatory body
- One representative from the Plant Owner’s management
- One communications representative

13.6.15.1 Estimated AP1000 Staff Compliment

Determination of the final and overall AP1000 plant staff compliment will ultimately be the responsibility of the site licensee. The estimated or assumed UK AP1000 staff (including site staff and corporate support) is presented in Table 13-2. These 11 staffing areas include 42 detailed staffing functions. These staffing estimates are initial estimates assumed for the UK AP1000 and will be verified and validated by the licensee. The licensee shall consider site location specifics, a more detailed focus on UK regulatory

requirements, and the desired/expected organisational approaches. The personnel and their roles that are needed to man the Emergency Response Organisation, as defined by the site specific Emergency Planning documentation (also the responsibility of the site licensee), shall be drawn from the estimates above. The site specific Emergency Plan shall be considered during the verification/validation of these staffing estimates.

13.6.16 Conduct of Operations

The Conduct of Operations (Reference 13.66), which is classified as an 'Administrative Procedure' within the set of GOPs, provides the standards and guidelines to achieve a high level of performance that contributes to safe, reliable plant operations. The Conduct of Operations governs the behaviour of all operations personnel (MCR operators, field operators), no matter where in the plant they are performing actions (e.g., MCR, RSR, or local to plant).

It sets out the responsibilities of the operations personnel, which include:

13.6.16.1 Responsibilities of the Shift Manager (SM)

The SM acts as the senior management representative on shift and is responsible for the safe operation of the plant at all times. Ensures all individuals conducting business in the MCR do so with a high degree of professionalism and ensure rigorous compliance to standards and requirements. This includes an emphasis on effective use of all human performance tools. During accident situations, the SM shall return to and remain in the control room to direct and oversee the activities of control room operators.

13.6.16.2 Responsibilities of the Shift Supervisor (SS)

The SS (control room supervisor) is responsible for the following:

- Directing the actions of licensed and non-licensed operators in performing plant operations.
- Maintaining a current awareness of plant parameters.
- Ensuring alarms received are prioritised and ARPs are implemented as required.
- Implementing AOPs and EOPs when plant conditions indicate they are required.
- Ensuring a reactor operator is designated as operator at the controls (OATC).
- Being relieved by another SRO qualified as SS prior to leaving the Control Room.
- Conducting observations of plant activities.
- Ensuring Reactivity Management is the highest priority.

13.6.16.3 Responsibilities of the Control Room Reactor Operators (ROs)

The ROs are responsible for the following:

- Monitoring system status to ensure all systems are operating correctly and maintaining plant parameters within system specifications.

- If assigned as OATC, remaining within the area designated as OATC area until relieved by another RO.

- If assigned as Balance of Plant Operator maintains awareness of plant parameters and provides short term relief for the OATC.
- Taking action as necessary to prevent plant safety limits from being exceeded.
- Manually trip or shutdown the reactor, if in their judgment a situation exists that requires prompt action.
- Operating systems as directed by the SS.

13.6.16.4 Responsibilities of the Shift Technical Advisor (STA)

The STA is responsible for the following:

- Provides an oversight function to the crew during off normal conditions.
- During emergency conditions, the STA may assist the SM with oversight of crew emergency response activities while the SM is involved in the Site Specific Emergency Plan.

The Conduct of Operations further details the inherent principles and behaviours expected from an organisation displaying a good safety culture where safety is the overriding priority.

It also reminds operations personnel of their expectations and responsibilities with regards to such factors as:

- Decision making
- Operator at the Controls
- Control Room Access
- MCR Displays
- Operation of Equipment
- Skill of the Craft
- Reactivity Management
- Briefs
- Log Keeping
- Alarm Response
- Alarm Suppression
- Use of the APS
- Manual Control Of Automatic Systems
- Human Performance Tools
- Plant Announcements
- Shift Turnover

The correct and proper use of procedures:

- Procedure Adherence
- Procedure Applicability During Plant Upset Conditions
- Entry Conditions For EOPs And AOPs
- Early Actions
- CPS
- Direction To Perform Response Not Obtained (RNO) Steps
- Notes And Cautions
- Two-Column Procedures
- Continuous Actions
- Critical Safety Functions

- Hardcopy Procedures
- Adverse Containment Conditions

13.6.17 Impact of the United Kingdom Nuclear Worker on the AP1000 Design

13.6.17.1 UK Target Audience Description (TAD)

The AP1000 plant has been designed to physically accommodate the 5th percentile female to the 95th percentile male dimensions based on data initially selected for the U.S. population. A UK anthropometric data set, as well as anthropometry for the adult Chinese population, was compared with the US data set in Reference 13.67 to ensure that the dimensions applied to the AP1000 design are also appropriate for the AP1000 plant worker in the UK. A comparison of the UK and US size data (Reference 13.67, Table 4.6-1) shows the dimensions for the UK 5th percentile female to be generally larger than the US 5th-percentile female, and so encompassed by the US anthropometric data set. For the 95th percentile male, in a number of cases the dimensions for the UK male are slightly larger than for his US counterpart, but still fall within the recommended range for safe operation of controls and visibility of displays as outlined in Reference 13.46. The taller UK male worker is appropriately accommodated by the AP1000 design with respect to physical access, visual access, and design of consoles, panels, and location of controls.

As the utilities will be responsible for recruitment and selection of operators, there is no specific selection criteria developed for the AP1000 plant operators. This is also reflected in the current practices in the UK nuclear industry, which differ between companies and between sites.

Per current US practice, potential ROs are typically hired into a non-licensed operator position if they meet certain national industry selection criteria. Following selection, all licence candidates must complete a rigorous training programme, accredited by the INPO National Academy for Nuclear Training, and then must pass the NRC administered licence exam. To retain the licence, the operator must pass an annual operating exam and a biennial written exam.

There is potential for similar practices to be adopted for UK operators, to ensure that they are SQEPs for the AP1000 plant operation. However, the UK operating utilities may create alternate qualification and hiring requirements through use of the results of the formal JTA (Reference 13.68) in determining the appropriate skills to form the basis of UK national reactor operator selection criteria.

13.6.17.2 UK Nuclear Worker Stereotypes

While there has been international engineering support and participation, the AP1000 plant has been designed primarily by engineers using the characteristics and norms of US operators as the basis. To assess the compatibility of the AP1000 reactor plant design and its potential operation and maintenance by a UK workforce, Westinghouse commissioned a comparative study addressing nuclear worker norms (Reference 13.69). This study sought to address the question of whether the UK operators and maintainers work to a set of population stereotypes and norms that are counter to elements of the AP1000 reactor design, which may increase the risk of human error and negatively impact safety.

The study was conducted in two phases: Phase 1 examined identification and characterisation of nuclear worker population stereotypes in the UK and in the US. This involved a literature review and a series of workshops with subject matter experts to elicit stereotype descriptions. Phase 2 of the project compared the identified UK nuclear worker stereotypes and assessed the AP1000 reactor design against those that varied from the US

stereotype. The analysis was subject to a risk-based review to assess the impact on human error potential.

The Phase 1 study concluded that there was minimal evidence for clear population stereotypes as defined within the study, either from literature or from workshop discussions with operators and HF experts. This phase did identify characteristics of the worker population that may be adaptable subject to good design and interventions such as training. No evidence was found for national variations in population descriptions.

The Phase 2 portion of this work was a qualitative analysis of the stereotypical variations as informed by a parallel quantitative analysis. This assessment concluded that there were aspects of the AP1000 design that were likely to reduce the potential for human error and therefore the population stereotype had no impact. Some characteristics were identified where the US and UK population stereotype variation may have a negative impact on human error potential. Furthermore, a number of low- or moderate-risk areas were identified that were directly relevant to the operation of the plant and therefore were noted for future due consideration by the operating utilities. However, no risk factors were identified that pertained to the design, or changes to the design, of the AP1000 plant.

13.7 HF V&V

The function of the HF V&V activities is to demonstrate that the AP1000 design attains a high standard of HF adequacy and that it conforms to the HF principles as specified in the HF Engineering Program Plan and requirements of the HSI Design Guidelines.

The HF V&V activities include five different analyses: task support verification, design verification, integrated system validation, HED resolution verification, and plant start-up HF engineering design verification.

13.7.1 HF Task-Support Verification

Task support verification was performed in accordance with the plan (Reference 13.70) to confirm that the results of the task analyses (e.g., FBTA, OSA-1, and OSA-2) have been incorporated into the final design. The task support verification assessment includes checking that the plant status information, alarms, and the control functions required by the operators are provided by the HSI resources and are designed compliant with HF good practice. Results of the task support verification assessments are documented in the respective report (Reference 13.72). Noted deficiencies are identified in this report as HEDs. The HF HED resolution and re-verification/re-validation process is described in Section 13.7.5 below.

13.7.2 HF Design Verification

The HF design verification was performed in accordance with the plan (Reference 13.71) to verify that the design of the operations and control centres and HSI resources was done in accordance with the HSI design guidelines (References 13.46 and 13.47) to ensure that the final design meets good HF design principles. The results of the design verification are documented in Reference 13.73. Noted deficiencies are identified in this report as HEDs. The HF HED resolution and re-verification/re-validation process is described in Section 13.7.5 below.

13.7.3 HF Integrated System Validation (ISV)

The HF ISV test was executed per the ISV test plan (Reference 13.59). The HF ISV test

provides a comprehensive human performance assessment of the final design of the AP1000 plant operator interfaces based on realistic operational scenarios within the MCR engineering development AP1000 simulator. The ISV uses performance-based scenarios to determine that the integration of the HSI ensemble (i.e., the hardware, software, plant procedures, communication facilities, work environment, and operating crews) meets performance requirements and supports safe operation of the AP1000 plant. Where performance criteria are not met, HEDs are identified.

The objectives of the ISV test are listed below:

1. Establish the adequacy of the integrated HSI for achieving HF Engineering program goals – The ISV will demonstrate the capability of the AP1000 HSI to support safe, efficient, and effective operations in a wide range of plant modes and conditions, thereby meeting the goals and objectives of the HF Engineering program plan (Reference 13.10).

2. Confirm allocation of function and the structure of tasks assigned to personnel – The ISV will evaluate the capability of crews to perform, in real-time, a broad range of important tasks necessary to respond to the events specified in Section 5.1.1 of Reference 13.59. Data is collected and performance measures are assessed.

3. Validate the EOPs and associated HSI – The ISV will exercise a representative cross-section of the AP1000 EOPs to confirm that the EOPs provide an integrated network of effective and usable instructions for the response to an event, ensuring that operators can reliably bring the plant to safe shutdown conditions following abnormal and emergency events.

4. Confirm the dynamic aspects of the HSI for task accomplishment – The ISV will employ a high fidelity simulator and task environment that provides realistic appearance, behaviour, and real-time responses, so that ISV results may be generalised to actual operations.

5. Evaluate and demonstrate error tolerance to human and system failures – The ISV will employ observers and a representative range of plant operating scenarios to confirm that performance of necessary tasks is highly reliable, that human errors are minimised, and that errors or failures are manageable, should they occur.

6. Establish the adequacy of MCR staffing and of the HSI to support staff to accomplish their tasks – The ISV will assess the sufficiency of AP1000 staffing levels for properly operating the plant in a wide range of conditions, and the sufficiency of control room resources to accommodate these staffing levels and the associated staff activities.

The ISV was performed using [ ] complex performance-based scenarios challenging the integrated system of AP1000. These scenarios were performed to combine the C&I hardware, C&I software, operating plant procedures, communications facilities, and trained operating crews in a simulated AP1000 MCR. The [ ] scenarios included plant heat up and start-up from Mode 5 to 100% power, shutdown and cool down from 100% power to Mode 5, abnormal operations, and emergency operations (Reference 13.81).The ISV scenarios also included the validation of the operator performance assumptions (i.e., execution time windows) stated in the HRA portion of the PSA for those modelled human actions identified as AP1000 risk important human actions (Reference 13.35). The ISV assessed the adequacy of procedures, training, workload, work organisation, and staffing levels. Individual scenarios identify specific objectives, including shift handover, and simulated interactions (e.g., with local operators) that extend beyond the MCR. Aspects of

crew communication and coordination are addressed throughout the ISV.

Consistent with nominal AP1000 plant staffing and operations, ISV test crews consisted of four persons filling the roles of Control Room Supervisor, Reactor Operator (RO-B), Balance-of-Plant Operator (RO-A), and STA. This nominal control room staffing was sometimes increased or reduced per scenario-specific guidance for planned complications.

In situations where AO action was required, a crew member phoned the simulator instructor booth to request the actions to be taken. The limitation was made that there would only be two AOs available for local plant operations. The necessary response was then simulated or role-played according to script by the ISV Staff.

During and after each scenario different performance measures were collected, which included:

- Digital simulator recording of plant performance, obtained at a sample rate of half a second, providing an objective record of operation during the scenario and permitted objective evaluation of pass/fail criteria.

- Observer guides enabled observers to track and record crew behaviour and responses during the scenario. These data were used for both pass/fail and diagnostic criteria.

- Debriefs were conducted after post-trial questionnaires were completed. The ISV Coordinator then led a verbal post-job debrief with participants to collect their feedback about the scenario trial. Additionally, at the conclusion of the crew's participation in the ISV, a final debrief was conducted to capture overall comments. Both debriefs used the established debriefing protocols as guides to promote the free exchange of comments and observations. Feedback from the post-job debriefs was captured by the HF Observer, documented and incorporated in to the comments from the post-trial and final questionnaires.

- Video and audio recording captured the screens and operator expressions at the RO A, B, and C workstations and at the SRO workstation. This video and audio of the MCR area, RSR, and debriefing room was recorded during each scenario using the integral audio/video system.

- Questionnaires were completed by ISV subjects and observers after each scenario trial, and again at the conclusion of testing for a given crew. The questionnaires were administered by computer to facilitate ease of completion, data collection, and data processing.

Questionnaire items addressed the following measures by prompting test participants to provide both quantitative (i.e., numeric ratings) and qualitative (i.e., written comment) responses. Comparisons among scenarios, crew positions, HSI ratings, etc. were made; outliers were identified with respect to average performance and variability, and diagnostic criteria were used as applicable to each of the following:

- Situation Awareness – Rating questions for the situation awareness rating technique (SART) were included on the post-trial questionnaires as the basis for SART results.

- Workload – Rating questions for the subscales of the National Aeronautics and Space Administration (NASA) task load index (TLX) were included on the post-trial questionnaires as the basis for TLX results. (Single numeric values (TLX Omnibus) for

perceived workload during a Scenario were constructed from the self-assessed, average ratings of the six NASA TLX sub-scales – mental demand, effort, frustration level, time demand, performance and physical demand – collected on completion of each scenario).

- Anthropometric and Physiological Factors – Questions on anthropometric and physiological factors were included on the post-trial questionnaire, as a basis for ratings comparable to other HSI.

- Team Performance – Rating questions for the team performance rating technique (TPRT) were included on the post-trial questionnaires as the basis for TPRT results.

- Goal Achievement – Goal achievement questions were included on the post-trial questionnaire to solicit performance ratings and comments, as a basis for comparisons among crews and scenarios.

- Usability – Usability questions were included on the post-trial questionnaire to solicit ratings and comments on the various HSI resources; this gave a basis for comparing and evaluating the resources.

Reference 13.82 provides the results of the AP1000 standard plant HF ISV. The ISV Plan objectives were satisfied through the performance of [ ] scenarios, identifying [ ] HEDs. The integrated system performed acceptably during testing and allowed for the identification of issues and the HEDs. While these HEDs were identified, it was observed that the given plant operations were capable of being performed, necessary tasks were completed such that the health and safety of the public would not be challenged, and that the integrated system supports the safe operation of the plant. These HEDs are resolved and re-verified or re-validated per the HED resolution process as described in Section 13.7.5 below.

13.7.4 Human Engineering Discrepancy Resolution Verification

As described in Sections 13.7.1 through 13.7.3, the HF task support verification, design verification, and ISV have been completed for the standard AP1000 plant. Resultant issues or operator performance concerns have been identified in the respective reports as human error discrepancies (HEDs). The HEDs are entered into the formal HF tracking system (Section 13.5.4 and Reference 13.10 Section 4.2.5), assigned ownership, to be resolved and re-verified or re-validated.

The detailed resolution for each HED Issue is defined through a two-step process. First, a general resolution path for each HED Issue is identified. The resolution paths fall into 3 categories, as follows:

- To Be Corrected – An issue resolution that involves a design change, procedure change, training program change, or an appropriate combination of these three.

- Justify - An issue where the current approach is to justify as acceptable the Issue and respective design/procedure.

- 520 - These are issues deferred to the Plant Start-up HFE design verification as defined by APP-OCS-GEH-520, “AP1000 Plant Start-up Human Factors Engineering Design Verification Plan” (Reference 13.61). These Issues identify a physical aspect of the plant or an aspect of the Control and Instrumentation (C&I) system that can only be verified in the physical plant or actual C&I at the plant.

Second, a detailed resolution plan for each HED Issue is specified by HF and the respective engineering discipline(s). Following agreement between HF and the respective engineering discipline on the detailed resolution plan for the HED issue, the resolution is implemented (i.e., correction made), and the correction is verified or validated, as appropriate, by HF to ensure the HED issue is resolved. Once all the HED issues contributing to (mapped to) an HED are verified/validated as resolved then the HED will be closed.

Each HED issue currently has its general resolution path identified. Discussions with engineering on the detailed resolution plans (corrections) are ongoing and will not be completed for several months. The resolution plans, the implementation of the plans, and the HF verification/validation of the implementations will be documented in the HED resolution verification report (APP-OCS-GER-420, "AP1000 Human Factors Engineering Resolution Verification Report"). The completion date of this report is estimated to be late 2017.

All HEDs, identified through the execution of the HF verification and validation activities, will eventually be resolved (i.e., corrected through design change, procedure change, training program change, or combination, or justified as-is). The resolutions and their HF verification/validation shall be documented via the APP-OCS-GER-420 and APP-OCS-GER-520 reports (future). The HF ISV test results and the implemented resolutions to the HEDs and associated Issues and subsequent verifications/validations will support the HF safety case.

The resolution plan for each HED and HED issue has now been developed (Reference 13.97) and agreed with the appropriate engineering teams and the implementation of the agreed-to resolutions is now in progress.

13.7.5 Plant Start-up HF Engineering Design Verification

An HF Engineering design verification at plant start-up is planned to be executed for the UK AP1000 (Reference 13.61) once plant construction is complete and equipment is installed, although some verification activities cannot be carried out until testing and preparations for plant start-up are underway. The objectives of the plant start-up HF Engineering design verification include:

- Confirm aspects of the OCS/HSI design features that could not be evaluated in other HF V&V activities (specifically the standard plant HF design verification, task support verification, and the ISV).

- Confirm that the as-built in the plant HSIs, procedures, and training conform to the design that resulted from the AP1000 HF program.

- Confirm that all standard plant HF-related issues (including HEDs) documented in the HF Tracking System are verified as adequately addressed or resolved.

There are some aspects of the OCS/HSI design that cannot be evaluated in a simulator or by using design documentation and require the as-built plant. These aspects include lighting, noise, and ambient temperature and humidity of the MCR and RSR. These will be included in the plant start-up verification.

There are DCPs that have been approved for implementation in the standard plant following the commencement and completion of the standard plant HF design verification, task support verification, and ISV activities. In addition, relevant DCPs as the result of feedback from construction, system installation and commissioning activity at AP1000

sites in China and the US will be implemented. Such DCPs, and those that are specific to the UK AP1000 design, will require HF V&V regression. Completion of the regression analysis and activity in order to verify/validate the changed design is part of the plant start-up verification. It is assumed that completion of the UK AP1000 Plant start-up Verification is conducted by the site licensee during site licensing.

13.8 Human-Based Safety Claims (HBSCs)

The process of HFI into the design of the AP1000's SSCs (Section 13.6) and to the human operator's interface with those systems (Section 13.6.6) has been one of an exploration of how the plant works and what it does so that account can be taken of human attributes, environmental and contextual stressors to set up the conditions for operator success in the tasks they must perform.

This Section of the HF chapter identifies human failure events (HFEs) and operator action errors that may serve to impair an engineered system's ability to perform its safety function (Type-A errors) or initiate a fault (Type-B errors), or lead to an operator failing to manually recover the plant to a safe condition post-fault (Type-C errors) – Identification of operator actions important to safety (Section 13.8.1).

The IAEA defines three types of human errors that can occur and contribute throughout the development of a fault sequence (Reference 13.83). These actions are classified and defined as:

- Type-A errors: Interactions where errors in maintenance, testing, inspection or surveillance (MTIS) tasks, made before the occurrence of an initiating event, have the potential to lead to failure or unavailability of a safety related system or mitigating, DiD system when required. This type of error is also referred to as a MLE.

- Type-B errors: Interactions where errors in operation or MTIS tasks have the potential to cause an initiating event. These type of error are also referred to as "Operator-induced initiating events" (OIIEs) or "Maintenance-induced initiating events" (MIIEs).

- Type-C errors: Interactions that occur following an initiating event where errors have the potential to lead to failures of the safety systems to perform one of the required safety functions. This type of error is also referred to as a "Post-fault operator error" (PFOE).

When an operator action important to safety is identified, it is recorded in the HAD for further treatment, tracking, and analysis at an appropriate level and time (Section 13.8.1.3).

The process for identification of operator actions important to nuclear safety has taken place in two main tranches - the first prior to completion of GDA Step 4 and another for the GDA close-out phase. This also coincided with a temporary postponement of the UK's GDA process by Westinghouse between 2011 and 2015. This is only of importance here in order to explain the developments that occurred in the interim period and to explain the terminology that is being used in the rest of this sub-section to describe and to differentiate between the processes for identification and treatment of errors pre- and post-GDA Step 4.

The term 'human failure event' (HFE) is used to describe HBSCs when they have been derived and identified from the PSA, and the term 'operator action error' when they have been identified through systematic examination of the deterministic fault analysis.

Whilst there are very many errors that could be made by operators in the course of their

duties, the design of the plant means that often the consequence of those errors has little or no bearing on nuclear safety in terms of the potential for core damage, radio-active release and dose to the worker or public. The level of HEA detail and effort that a HFE or operator action error receives is in proportion to the risk presented from failure of an operator assigned task or function – Human Error Screening (Section 13.8.2).

For those HFEs and operator action errors with failure consequence exceeding the screening criteria thresholds, HEA has been conducted at an appropriate level and depth of detail.

The depth of HEA that is conducted will be dependent upon the aims of the analysis and the maturity of the design or lifecycle phase of the system at the time of the analyses. Subsequently, HEA has been conducted at different levels of detail on the pre- and post-GDA Step 4 tranches of screened-in HFEs and operator action errors. Kirwan (Reference 13.91) identifies a number of 'levels' of HEA in an "onion framework" that delve successively deeper into the errors, their causes and the subtlety and complexity of their potential impact.

Prior to 2011, some 97 HFEs and operator action errors (Appendix 13A) underwent HEA at a level described by Kirwan as "detailed."

Detailed-level HEA – aims only at the skill- and rule-based levels of behaviour, where a large number of potential errors are yielded and which, following representation, can be quantified and fed into detailed fault and event trees. It is at this level that the causes of errors, known as performance shaping factors (PSFs), and their underlying mechanisms are assessed and recorded, facilitating error-reduction analysis.

Post-2015, with the production of a new PSA model and HBSCs (Reference 13.77), and further identification of operator actions important to safety derived from other fault analysis sources, a further sample (Reference 13.92) of 20 HFEs and operator action errors (Appendix 13B) underwent HEA at a level described by Kirwan as "cognitive".

Cognitive-level HEA – considers the undesirable impacts on the system occurring as a result of mistakes and misconceptions on the part of the operator or the operating team. It is concerned with the potential for misdiagnosis, misconception, diagnostic failure or incorrect judgement to occur.

Further levels of HEA are proposed by Kirwan, but these are considered to be not analysis in more depth but errors occurring in different contextual circumstances, such as maintenance errors, rule violations, or the behaviours of operators in an organisation having a poor safety culture.

The detailed-level and the cognitive-level of HEA have been conducted and presented using a template or "pro forma" that was designed as both a guide to the analyst in the scope and content of the analysis and as a standardised presentation of the analysis data and findings in a consistent and logical format.

The detailed-level HEA pro forma can be found in References 13.7, 13.86, 13.87, 13.88, and 13.90, and the cognitive-level HEA pro forma for the HF-01 sample found in Reference 13.54. APPENDIX 13A and 0 list the source documents and assessment locations for the Detailed-level HEA and the Cognitive-level HEA, respectively. Appendix 13C provides a summary of the cognitive-level HEA results.

A significant part and purpose of conducting HEA in the GDA phase has been to

demonstrate that risk from failure of operator actions important to nuclear safety is reduced ALARP. This principle applies at all levels of risk, extending below the level that may be deemed broadly acceptable. For operator action errors that are deemed to be of lower risk, by virtue of their consequence of failure not exceeding screening criteria thresholds (Section 13.8.2 and Figure 13.5), the ALARP principle is deemed to be adequately demonstrated through compliance with modern standards RGP in the design of affected systems, equipment and the HSI, the result of optioneering design requirement solutions informed by OER, task analysis and the Conduct of Operations (Reference 13.66).

For HFEs and operator action errors where the consequence of their failure exceeds screening criteria thresholds, there has been conducted HEA at a detailed or cognitive level that affords the opportunity to propose improvements to various elements of a system's design that if implemented may demonstrably reduce the risk of failure ALARP.

This too presents another differentiation in terminology used between the detailed-level HEA and cognitive-level HEA. The scope of the detailed-level HEA did not at that time include a full and explicit consideration of the potential cognitive, internal error mechanisms that may reveal the underlying causal factor for an error to occur. Without this cognitive level of error analysis revealing potential internal error mechanisms the proposal of changes to elements of the system's design may be misdirected and therefore ineffective at reducing risk from failure ALARP. For example, there would be little value in improving task lighting if the underlying mechanism for an error were not one's ability to see information on display but that of being able to adequately comprehend what was being seen.

However, for each pro forma completed the result of detailed-level HEA, there have been "ALARP design recommendations" made by 'expert panel' review. The panel included experienced ex-licensed operators and SQEP HF practitioners, who may themselves have been considering internal cognitive decision making processes when making these ALARP design recommendations.

When changes to an element of the system's design were proposed the result of cognitive-level HEA they have been termed "Error Reducing Mechanisms" (ERMs) in order to differentiate their potentially more accurate focuses on the underlying causal factors.

13.8.1 Identification of Operator Actions Important to Safety

The process of identifying operator actions, having the potential to impact nuclear safety if omitted or conducted in error, has been systematic, comprehensive, and extensive. It has considered the requirement for operator action at all stages of the fault progression sequence, including errors of Types A, B and C. The operator action identification process has considered all normal modes of the plant's operation as well as operations in emergency and accident conditions. In addition to the systematic operator action identification processes conducted specifically for GDA (Section 13.8.1.1.2), other sources of fault analysis have been assessed, such as the various Level 1 and 2 PSA models and risk-important human actions (Section 13.8.1.1.1); fault and accident analysis and the fault schedule; internal and external hazards analyses (Section 13.8.1.1.2).

Further identification of operator actions important to safety has resulted from HF integration activities across the project, such as interviewing the technical leads and delivery managers responsible for resolution of GDA Issues that have been raised in other technical and safety areas (Section 13.8.1.2.1), and the supplementary HF review of Class 1 DCPs included in the UK AP1000 DRP for GDA (Section 13.8.1.2.2).

All HFEs and operator action errors when identified are recorded in a HAD. The HAD is an open, living repository for recording, managing and tracking operator actions important to nuclear safety for risk-proportionate HEA and ALARP substantiation (Section 13.8.1.3). The HAD will remain an effective management tool beyond GDA and into site licensing.

13.8.1.1 Identification from Fault Analysis

13.8.1.1.1 Probabilistic Safety Analysis (PSA)

The PSA provides a fully integrated model of the entire plant that can be used to examine the risk from a variety of possible initiating events (e.g., transients, loss of coolant accident [LOCAs], support system failures, etc.). The PSA consistently accounts for both the event frequency and the potential consequences from equipment failures or human errors. The model combines front-line safety systems and support systems in a manner that allows designers to identify the risk significance of important inter-system dependencies. The PSA allows designers to quantify the likelihood of "passive" and "active" failure modes, to examine the significance of single failures and multiple failures, and to determine the risk importance of "safety", "safety related" and "non-safety" systems (Reference 13.77 and 13.85).

PSAs to support new NPP designs have initially been performed on a prototype of the plant design, used early in the design process as an internal analysis tool. The PSA results are used to inform the design and any pertinent design changes. The PSA models and analyses are refined and become more complete as the design matures. During the AP1000's design lifecycle stages and over the GDA process period there have been iterations of the at-power PSA model for internal initiating events, and updates to the flood, fire and shutdown PSAs.

Updates to the PSA are required as the result of significant revisions to the AP1000 design (e.g., upgrades to the C&I architecture); the inclusion of DCPs in the DRP that impact the PSA; improvements to the thermal-hydraulic analysis basis and revised procedures. The HRA is subsequently re-analysed based on latest revisions of the AP1000's design and operation (PCSR Chapter 6) and on the most recent approved revisions of the SSD and Piping and Instrumentation Diagrams.

The at-power PSA model (Reference 13.44, 2007), used during GDA step 3, contained 72 HFEs. Screening of the 2007 PSA HFEs on the basis of their contribution to overall CDF resulted in 21 being selected for detailed HEA. The detailed-level HEA of these 21 errors are reported by 18 pro forma in Reference 13.7. An update to the at-power PSA model was conducted during GDA step 4 (Reference 13.85, 2010) to take account of performance and reliability enhancement afforded by digital C&I and soft HSIs. This update to the at-power PSA resulted in a reduction to the overall CDF and a further 7 HFEs screened-in for HEA because of the lower CDF threshold criteria. The detailed-level HEA pro forma for these 7 errors are reported in Reference 13.86.

Review and screening of the low power and shutdown (LP&SD) PSA model and for the Fire and Flood PSA identified a further 15 HFEs for detailed-level HEA. The pro forma for the 9 HFEs emanating from the LP&SD PSA are reported in Reference 13.88, and the 6 HEA pro forma for Fire and Flood HFEs in Reference 13.87.

A significant, recent, revision to the internal initiating events at-power PSA (2015) has been conducted (Chapter 10). This revision accounts for improved thermal-hydraulic analysis and revised plant procedures that in some cases identify earlier the cues for monitoring and subsequent control actions where simulator tests have resulted in the available time-windows being challenged. This revision has included a re-evaluation of the

Type A pre-initiator actions (given a 'HEPE' prefix to the event ID) and post-initiator actions (given a 'HEPO' prefix to the event ID); additionally, actions modelled in the PSA from the SAA include an 'L2' in the prefix (e.g., HEPO-L2-CNT) to indicate they are part of the Level 2 PSA, which assumes a core damage severe accident (Reference 13.77).

The HRA Guidebook (Reference 13.79) for the revised (2015) at-power PSA gives examples of the MTIS activities performed by plant operations personnel that could result in the unavailability of safety and safety-related SSCs and that have resulted in the identification of 13 (HEPE HFEs) Type A MLEs. These MTIS activities include:

- Realignment of a component or a flow path to normal operating status after completing periodic testing, inspection, or maintenance.
- Removal of jumpers or other temporary system alterations to restore the equipment back to service.
- Calibration and alignment of sensing equipment to ensure proper automatic response to emergency actuation conditions or annunciator activation.

Similarly, Reference 13.79 describes the identification of post-initiator HFEs having been performed in parallel to the PSA systems and accident sequence analyses. Through the representation of potential accident sequences in event trees, analysts identify operator actions that are required to be taken in order to mitigate an accident in accordance with the applicable procedures. As fault tree models are developed; the system analysts identify human actions that are required to place equipment in a state necessary to support the applicable success criteria. This could be an action, such as restarting a pump after a loss of off-site power or repositioning a valve to align an alternate source of water. This process has resulted in the identification of 51 (HEPO HFEs) Type C PFOEs.

These 64 HFEs have been added to the HAD in addition to the HFEs from the superseded PSA. It has not yet been determined what deltas exist or replication there is between these two sets of PSA derived HFEs; therefore, until that exercise is conducted in site-licensing, both sets will remain in the HAD.

The cognitive-level HEA, demonstrated on a sample of operator actions for GDA and reported in Reference 13.54, will be presented to PSA so that the HF team and PSA team can more accurately estimate HEPs for the site licencing phase based on detailed task analysis.

13.8.1.1.2 Design Basis Analysis (DBA)

The nature and scope of the Level 1 and 2 PSAs means that the analyses will be nuclear island and RCS boundary focused, as the source of core damage and large radioactive release, and concerned predominantly with post-fault HFEs. In order to consider more widely other types of HFE, committed earlier in the fault progression sequence, or at site locations with radioactive sources other than the core, a systematic process of human error identification (HEI) was conducted (Reference 13.7 Appendix A). This systematic identification process was executed by multi-disciplinary teams (comprising SQEP systems engineers, maintenance engineers, experienced operators, and HF analysts) using expert judgement to consider, each in turn, the events from the UK Fault Schedule (Reference 13.80), the Composite Fault List, and safety and DiD systems, by answering a set of questions (Table 13-3) designed to prompt and elicit the identification of potential Type A, B and C errors.

This systematic HEI process yielded some further 178 operator and maintainer actions having the potential to affect nuclear safety if omitted or conducted in error. These actions appear in the HAD with an "OPR" prefix to the event ID.

13.8.1.1.3 Beyond Design Basis (BDB)

One of the primary lessons learned from the accident at Fukushima Dai-Ichi was the significance of the challenge presented by a loss of nuclear safety systems following the occurrence of a beyond-design-basis external event. Extreme external events (e.g., seismic events and external flooding) beyond those accounted for in the design basis are highly unlikely but could present challenges to nuclear power plants.

BDB scenarios are by definition very rare, extreme events that could challenge the plant and the crew. The AP1000 plant is a robust, passively safe design that does not require operator action for 72 hours to ensure safety and respond to a design basis station blackout event (i.e., a total loss of ac power).

Human actions taken are directed by the respective emergency operating procedures (EOPs) and ensure optimal plant recovery. However, if the loss of ac power were to extend beyond 72 hours then human action is required to ensure continued cooling and safe shutdown of the plant.

Westinghouse has identified these actions as part of the development of the AP1000 BDB Long-Term Coping Strategy (Reference 13.84 Appendix B) and associated post-72 hour procedures. It is not feasible to identify a priori every possible set of circumstances and plant conditions that can occur in BDB situations, as is the case in severe accident scenarios that are managed via SAMGs. For this reason, the AP1000 BDB Long Term Coping Strategy outlines the objectives and lists the options available for managing the AP1000 plant during a protracted station blackout (SBO) situation.

The development of the AP1000 long-term coping strategy has resulted in 8 operator actions being added to the HAD with a "BDB" prefix to the event ID.

13.8.1.2 Identification from HFI across the AP1000 Project

The AP1000 is a large and multi-faceted socio-technical system, reliant upon human operators for its maintenance and safe operation. For this reason HF becomes a transverse topic across many of the other technical and safety-related project disciplines. In order to extend the 'reach' and integration of HF, HFI-focused activities have been conducted across the other GDA Issue areas.

13.8.1.2.1 HFI across the Other GDA Issues

Through an expert panel assessment process (Reference 13.78), conducted with the respective GDA Issue technical leads and project managers, the primary objectives of this assessment of the other GDA Issues were twofold:

- To identify and define the GDA issues requiring HF support or assessment as part of the issue resolution, and to estimate the level of HF support needed throughout the remainder of the GDA phase; and,

- To identify any claims on operator actions that were being made in safety arguments for the resolution of a GDA issue.

As a result of this expert panel assessment, 32 new operator actions have been identified and added to date that are claimed, or assumed (either implicitly or explicitly), as part of the AP1000 safety case. Each of these has been added to the HAD with an "OPR" prefix.

13.8.1.2.2 HF Review of Approved DCPs

The main objective and purpose of the HF review of DCPs was to enhance the coverage of the GDA human error identification and assessment process by:

- Identifying new operator actions required by the DCP
- Identifying current operator actions affected by the DCP
- Gathering sufficient 'metadata' to facilitate input of the identified and affected operator actions into the HAD for future, risk-proportionate, assessment.

The scope of this DCP HF review is consistent with the AP1000 DRP for the UK GDA, (Reference 13.9). The HF review focused on the identification of new operator actions or current operator actions as affected by DCPs approved by Westinghouse since the previous DRP (Rev 5).

Execution of the DCP HF review process to date (Reference 13.28) identified a further 25 claimed operator actions that have been added to the HAD with an "OPR" prefix and with event ID numbers between 251 and 275.

13.8.1.3 Human Action Database (HAD)

The operator actions important to safety that have been identified to date have been entered into the HAD. The number of actions in the HAD now numbers over 400 HFEs or potential operator action errors (Table 13-4). This number is still subject to some consolidation due to potential duplication (e.g., old and new PSA HFEs) or because of design and task-analysis latency (some actions may already have been designed out) and additions due to ongoing design review and safety substantiation activities (e.g., HFI across the other project technical and safety disciplines and GDA issues).

Many actions in the HAD have now been recorded with a basic set of action 'metadata' that describes the information necessary to make early screening predictions for future detailed HEA or to identify the low-risk actions that may be grouped by similar scenarios and ALARP arguments based on compliance with RGP.

The identification of claims made on the actions of operators is an ongoing one that will continue in parallel with the maturing design and ongoing safety substantiation. For this reason, the HAD will remain an open, living repository for newly identified operator actions important to safety and for the management and tracking of operator actions beyond GDA and in to site licensing.

13.8.2 Risk Proportionate Screening

A screening filter identifies where the major effort in the HEA should be directed. Although many tasks and actions related to system goals have been identified, not all of them will contribute significantly to overall risk if they were failed to be carried out. This may be due to the presence of diverse and reliable backup and DiD systems that adequately compensate for human errors, or because of the trivial nature of the task itself with respect to the overall level of risk involved.

In order to ensure that the 'effort' expended in conducting HEA is proportional to the risk presented from the consequence of failure in the task or action, a method of 'screening' actions for detailed assessment was devised (Figure 13.5).

Approximately 300 actions in the HAD were run through the screening criteria flow chart prior to Westinghouse's resumption of the GDA process in 2015. The HFEs from the most recent PSA (Reference 13.77) and the operator actions identified from the BDB Long-Term Coping Strategy (Reference 13.84), HF Review of DCPs (Reference 13.28) and HFI in GDA Issues (Reference 13.78) have all been added to the HAD subsequent to this first screening exercise.

The final consolidation of HAD entries, the re-screening of post-2011 actions and further cognitive-level HEA of the screened-in actions will be completed during the site licensing phase.

The results of the screening process are described in detail in Reference 13.7, Appendix A. and all the HFEs and operator actions that have been screened-in have been summarised in Appendix 13A with the operator action title and event ID; error identification source; screening node entry point and reference to the supplemental HF safety case document in which the detailed HEA pro forma can be found.

13.8.3 Human Error Analysis (HEA)

There is currently no single, totally comprehensive HEA tool that can deal effectively with skill and rule-based errors, as well as cognitive errors (misdiagnoses), rule or procedure violations, maintenance errors and management failings, and so no techniques which address the full potential impact of human error on a complex socio-technical system. There are, however, a number of HEA tools that can be integrated to provide a highly effective means of identifying a system's vulnerabilities to human error and facilitate identification of appropriately targeted changes that will reduce the risk from human failures ALARP.

13.8.3.1 Detailed-Level HEA

The use of a detailed-level HEA pro forma, executed during GDA steps 3 and 4, standardises the content and presentation of the analyses conducted for each screened-in HFE and human action error.

First, the context in which the operator action is required to be performed is described, both in terms of the operating scenario (the normal operating modes, emergency or accident conditions in which the operator is required to perform some function) and in terms of the specific sequence of events that led up to the need for action and the subsequent consequence of performing the function or conducting the action in error.

Next, the PSFs, both positive and negative, that can affect successful completion of the task are identified, as are the opportunities for the operators to rectify the error or return the plant to a safe state.

For post-fault HFEs, derived from the PSA, the 'stressors' affecting operator performance that are assumed to be present in the task scenario are listed – e.g., long or complex procedures; the time available and estimated time to complete; the cues from the HSI to prompt the appropriate operator response; team support and recovery paths – that, along with the contributory sub-tasks, have informed an estimation of the HEP using the technique for human error rate prediction.

The HEPs for maintenance latent errors going undiscovered until the affected safety or safety-related system is required has been estimated based on combinations of human error assessment and reduction technique (HEART) generic task types that account for the initial, unrevealed maintenance error and the subsequent failure of opportunities to discover the defective system, e.g., alarms, testing, inspection. The HEART-based derivation of HEPs for MLEs is described in Reference 13.7, Section A.5.2, along with the HEP modification tables that take account of the predicted time interval between the tests or maintenance activity that leaves an automatic or manually initiated system unavailable on demand and the alarm, inspection or surveillance process that may reveal its inactive state.

Finally, through a process of multi-disciplinary expert panel, consisting of systems engineers, HSI designers, procedure writers, experienced operators, PSA analysts and HF practitioners, an error reduction analysis was conducted for each HFE and operator action error that underwent detailed HEA. Informed primarily by the PSFs that were found to be important in the deterministic HEA and HRA quantification for PSA, the expert panel proposed potential ALARP design recommendations that were categorised by opportunities to, for example:

- Increase the levels of automation associated with a task to design-out the possibility of error.

- Change the design of the systems affected by the error or contributing to the probability of error by making their operation and maintenance more accessible or less complex, reducing the probability of error in use or, through the addition of sensors, improve the ability of the system to display its condition or operating status.

- Modify the HSI to improve the provision, timely identification and interpretation of system parameters important to safety or to make more intuitive the use of controls and confirmatory system feedback.

- Make improvements to the soft, administrative controls and management barriers - such as specific training objectives; procedure step sequence and presentation; job design and staffing levels - that can prevent or detect errors, reduce workload or stressful error-conducive situations.

This process has resulted in the identification of a number of ALARP design recommendation proposals, recorded in the HEA pro forma found in References 13.7, 13.86, 13.87, 13.88 and 13.90 . The detail and disposition of proposed potential ALARP design recommendations from the HEA pro forma found in Reference 13.7 is documented in Reference 13.93. Where valid ALARP improvement opportunities are found to exist, these will be further evaluated per the Westinghouse design modification and substantiation process (Reference 13.15) during site licensing.

13.8.3.2 Cognitive-Level HEA

The cognitive-level HEA considers the undesirable impacts on the system occurring as a result of mistakes and misconceptions on the part of the operator or the operating team. It is concerned with the potential occurrence of misdiagnosis, misconception, diagnostic failure or incorrect judgement.

This cognitive-level analysis process has demonstrated the application of an HEA methodology that considers the underlying mechanisms of an error and the specific PSFs at the key steps in task analysis when the error is made. In addition, where applicable, it

addresses the potential for the design of procedures and HSIs to cause misdiagnosis of a situation (Section 13.8.3.3) and also for the contribution from contextual, environmental and task design conditions to increase the potential for conditions that may cause operators to behave in violation of procedures (Sections 13.8.3.4).

HEA conducted at a level above the skill- and rule-based levels addresses the internal error mechanism and facilitates the identification and proposal of ERMs that specifically target the underlying error cause to ensure that the risk of failure is reduced ALARP. In this way, the analysis can more credibly justify an argument where, having implemented any ERMs, the risk presented from HFEs and from operator action errors is ALARP.

In order to address the cognitive mechanisms underlying HFEs and operator action errors the cognitive-level HEA process used the cognitive framework proposed in Reference 13.94. This cognitive framework was the synthesis of a comprehensive review of the relevant psychology and behavioural sciences literature to identify five macrocognitive functions: (1) detecting and noticing, (2) understanding and sense making, (3) decision making, (4) action, and (5) teamwork. For each macrocognitive function, the NUREG-2114 researchers identified the proximate causes for cognitive function failure, cognitive mechanisms underlying the failures, and factors that influence the cognitive mechanisms that may lead to human performance errors. Moreover, the research used the information from the literature to infer causal relationships and links between different types of human failures and PSFs.

Because the contextual PSFs at the time when an error occurs in a procedurally driven analysis of a task are potentially more easy to identify or to predict, the cognitive framework proposed in NUREG-2114 was essentially used in reverse for the cognitive-level HEA. If the likely PSFs were ‘known’ or could be more reliably anticipated then the causal relationship to different types of failure could be inferred. A matrix was constructed of the PSFs revealed by the literature to have the strongest influence on each of the five macrocognitive functions (Table 13-5). This in turn also directed the analyst to proposing appropriate ERMs when HEA revealed difficulty in substantiating the claimed level of human reliability or achievability of the task within the available time.

13.8.3.3 Misdiagnosis

Misdiagnosis has traditionally meant the misinterpretation by an operator of data being displayed, potentially failing to identify that the data being presented is wrong or latent, diagnosing the incorrect fault and subsequently taking a wrong or inappropriate, but procedurally driven, course of action. Since the events at Three Mile Island, lessons learned have directed the design of abnormal and emergency operating procedures to a symptom-based construct vice event-based – as is the case for AP1000 AOPs and EOPs.

In a symptom-based procedure system, as long as the operator follows the procedure as written, there is no penalty for an incorrect diagnosis. Procedural selection is not dependent upon a correct diagnosis, but instead depends upon the existing symptoms, which are identified throughout the procedure network.

When in the EOP network, if the symptoms do not match the procedure, the procedure/EOP network eventually guides the crew to the correct procedure, or back to E-0. The CPS also continually monitors plant operating parameters and provides prompts to the operators if criteria are met for entry into any EOP or Critical Safety Function Status Tree (CSFT). Furthermore, the MCR crew composition includes the STA, who monitors the CSFTs and provides expertise to aid the crew in diagnosing and responding to the event. Likewise, AOPs, which are generally entered from alarm response procedures, have

a set of "Symptoms and Entry Conditions" that the operators use to confirm that they are in the proper procedure. Operators would not proceed into a procedure based solely on the presence of one of the symptoms or entry criteria without further confirmatory checks on the status of other symptoms or entry conditions that should be present. These confirmatory checks will often utilise alternative, diverse sensors and displays so that reliance on a single data source to make a diagnostic decision is negated.

The potential for misdiagnosis of an event is further reduced through the adoption by the MCR crew of human performance (HuP) tools, as directed by the Conduct of Operations administrative procedure (Reference 13.66). In particular, those tools are used to promote a 'questioning attitude' and the practice of self-checking and peer-checking, both of which are used to augment the Stop, Think, Act, Review used prior to implementing an action.

13.8.3.4 Design Induced Violation

Rule violation occurs when a person deliberately chooses to deviate from the rules, procedures, instructions, or regulations that govern the safe operation and maintenance of a plant or equipment. In the context of HRA and assessing the potential for human error, rule violations are assumed to occur without malicious intent (sabotage is outside the scope of HRA and error assessment). Instead, HRA is concerned with the potential for plant personnel to deviate from rules or procedures for reasons including convenience (e.g., poor task design), efficiency (optimising, e.g., time saving), routine workarounds (e.g., practices that have become normal and "accepted" or ignored by management), or exceptional violations due to problem solving in unusual situations, among others. Efforts to reduce human error may not adequately address the potential for rule violations, so it is important to understand the causes of violations to be able to adequately design against them and to address the potential for violation in HEA.

13.9 Substantiation of HBSC

The HBSCs, identified as part of the DBA, PSA and SAA, have been substantiated ALARP.

The identification of operator actions important to safety and the HEA of HBSCs has furthered understanding of the human contribution to AP1000 plant safety, both in terms of its reliance on human action and the vulnerability of the plant to potential human failure events in pre-fault and post-fault situations. The substantiation of HBSCs minimises the associated risks to ALARP for the standard AP1000 plant design.

The process of identification of operator actions important to safety has been systematic and comprehensive in its coverage of:

- Plant operating conditions – all modes of operation, including normal, abnormal, emergency, and severe accident conditions.

- Stages of the fault sequence – pre-fault latent errors having the potential to leave safety and DiD systems unavailable on demand (Type-A), operator and maintenance-induced initiating events (Type-B) and actions required post-fault to return and maintain the plant to a safe state or to mitigate the consequence of fault conditions (Type-C).

- Fault analysis –PSA, DBA, BDB and post-72 hour SAA.

This has resulted in the identification of approximately 400 operator actions important to safety being recorded in the HAD, providing confidence that the role of the operator and

reliance on their actions in the maintenance of nuclear safety has been adequately assessed and understood. Some 97 of those ~400 operator actions important to safety have exceeded screening criteria thresholds and have undergone further HEA.

After risk-proportionate screening of the operator actions in the HAD, identified during GDA Steps 3 and 4, a total of 77 detailed-level HEA pro forma were completed for 101 action errors (some detailed-level HEA pro forma addressed more than one action when operator actions were similar or closely tied in a fault sequence or error progression). A breakdown of the HEA pro forma by error-type meant that 28 Type-A MLEs; 12 Type-B MIIEs and OIIEs; and 37 Type-C PFOEs, 5, of which were post-core damage, have been assessed at the detailed-level. The reporting and disposition of these detailed-level HEA pro forma is shown in Appendix 13A.

For the GDA close-out phase and for resolution of the GDA Issue HF-01, samples of 20 operator actions were assessed at a cognitive-level of HEA. The sample was selected to provide diverse coverage of plant operating conditions, fault sequence progression and fault analysis methods. This resulted in the cognitive-level assessment of a further 3 Type-A MLEs; 2 Type-B OIIEs; and 13 Type-C PFOEs, including 2 from the revised 2016 Fire PSA for GDA Issue PS-02. In support of the post-Fukushima Dai-Ichi lessons learned GDA CC-03 Issue, two operator actions identified from the BDB long-term coping strategy were also assessed using the cognitive-level HEA method. The reporting and disposition of these cognitive-level HEA pro forma is shown in Appendix 13B, and a summary schedule of the HEA findings is presented in Appendix 13C.

For specific detail substantiating an individual HBSC, the respective HEA pro forma are reported in numerous documents that comprise the HF safety case for the UK AP1000 Plant. For each operator action that has undergone HEA for GDA, the relevant HF safety case documents are referenced in Appendix 13A and Appendix 13B.

Because the sample of 20 actions that were selected for demonstration of the revised qualitative analysis method (cognitive-level HEA) were selected to provide adequate breadth of content and coverage - in terms of risk significance, fault analysis, error-type and novelty of design - they may also be seen as ‘bounding’ for similar errors and error types. The evidence accumulated to substantiate the risk of failure reduced ALARP for tasks and MTIS activities conducted within the same nuclear safety context bounded by the sample of 20 actions, may also be true for all tasks conducted in this way (i.e., in accordance with conduct of operations and the culture of safety and procedural adherence).

13.9.1 Overall Significance of HFE in the PSA

As discussed in Chapter 10, the UK AP1000 plant PSA assessed that the overall CDF is low. This frequency includes the contribution of human error, particularly post-fault human errors (Type-C) and pre-fault human errors (Type-A) relating to the MTIS e.g., misalignment of manual valves following maintenance performed at-power.

Chapter 10 addresses the relative importance of operator errors on the overall CDF. If no credit is taken for operator actions, the at-power internal events CDF is comparable with CDFs for existing Generation II reactors where credit is taken for operator actions.

Other Type-A errors are included in overall failure rates for UK AP1000 systems derived from AP1000 databases, rather than explicitly modelled in the PSA. Generally, the initiating event frequencies derived from generic operating experience reflect both component and human failure events. In general, Type-B human errors are incorporated into the initiating event frequencies.

Post-fault claims on operator action (Type-C claims) have been identified as part of the PSA. The at-power internal events actions are summarised in Chapter 10. The sampling plan included 11 risk important actions from the at-power internal events PSA model. The criteria for risk important PSA actions are discussed in Reference 13.54.

The analysis undertaken for the generic design has been proportionate to the potential nuclear safety risk and it is therefore unlikely that human error mechanisms that could significantly affect nuclear safety risk have remained unidentified for analysis and assessment. However, the HF led, cognitive-level human error and task analysis that has been conducted for the sample of 20 actions in GDA will be assessed for their impact on the estimation of HEPs that are currently in the PSA model. Cognitive-level HEA will also be performed on the remaining screened-in operator actions during the site licensing phase and used to inform the HEP estimations included in the site-specific PSA models.

13.9.1.1 Substantiation of Pre-Fault/Pre-Initiator Type-A MLE

The revised internal initiating events at-power PSA (Chapter 10) explicitly models Type-A Pre-initiators. The routine actions considered in the PRA involve restoring a component or flow path to normal configuration after completing MTIS and ensuring that the sensing equipment is correctly aligned and calibrated for automatic response to emergency actuation conditions. There are 13 Type-A HFEs (with a 'HEPE' prefix to the event ID) modelled in the PSA. One (HEPE-PCS-XVM-CL-V023) has been included in the HF-01 sample plan for HEA at a cognitive-level. Also included in the sample of 20 are two Type-A operator action errors that relate to MTIS activity on the ADS-4 and IRWST gravity injection squib valves (OPR-011), and recirculation squib valves (OPR-106).

The cognitive-level HEA pro forma for HEPE-PCS-XVM-CL-V023, OPR-106 and OPR-011 are found in Reference 13.54. Extracted from these pro forma are the evidence statements that support the argument for a claim that risk from these MTIS activities is reduced ALARP, subject to further review and disposition of the ERMs identified for consideration in the cognitive-level HEA.

- The AP1000 design and response in this scenario meets recognised RGP
- Operators will have the information and resources they need to successfully fulfil the maintenance activity.
- Plant personnel will be using human performance tools as indicated in the Conduct of Operations (Reference 13.66) sub-section 5.3.16, which include self and peer checking, three way communication, and independent and concurrent verification methods.
- Personnel performing these actions will have the correct knowledge, training, and experience needed for successful completion. Pre-job briefs will be performed, which will involve review of error traps and the application of specific human error reduction tools to avoid them.
- Given that the task is time-consuming and complex, this maintenance activity is considered to be demanding both from a cognitive perspective and from a physical perspective. Various task-support measures reduce the likelihood of error. Among these are IST engineer checks, critical step verification from SQEP engineers and the use of checklists.

From the systematic HEI process executed for GDA Step 4 (Reference 13.7 Appendix

A.2.2), 28 Type-A MLEs were screened in for detailed-level HEA. As a result of these HF assessments a number of common factors promoting successful completion of maintenance tasks on deterministically claimed safety systems were identified:

- Maintenance is performed in accordance with MTIS procedures and permits to work. These include checking for correct alignment before reinstatement.
- Before returning the plant to power after an outage, there is a full check of the operability of all deterministically claimed safety systems.
- In addition, there is a periodic check of the operability of components of these systems during operation.
- Manually operated valves that are normally closed and locked closed are the subject of two-person verification.

MTIS activities associated with risk-significant components are subject to HF assessment in accordance with the Local Panels and Maintainability Human Factors Design Guidelines (Reference 13.47). This addresses the design of MTIS tasks in order to minimise the likelihood of human failures. This document is also referenced in system and equipment specifications for procurement purposes.

For these reasons, and subject to further review and disposition of the ALARP design recommendations identified for consideration in the detailed-HEA pro forma, and by virtue of compliance with RGP in design, Westinghouse has substantiated that the risk from MTIS activity leaving deterministically claimed safety and DiD systems unavailable on demand is reduced ALARP for GDA.

13.9.1.2 Substantiation of Pre-Fault Type-B Operator or MIIE

From the systematic HEI process executed for GDA Step 4 (Reference 13.7 Appendix A.2.2), 12 Type-B OIIEs and MIIEs were screened in for detailed-level HEA. Also, included in the GDA Issue HF-01 sample plan were two Type-B OIIEs that have undergone cognitive-level HEA. These assessments identified the following evidence to support the arguments and claims that the tasks can be successfully accomplished:

- Operators will be trained and available to perform the task.
- Operators will use and follow procedures, which provide appropriate guidance for the task.
- Maintenance activities will be properly prepared, organised, and executed.
- Refuelling operations are pre-planned and undertaken in accordance with specific refuelling procedures
- Operators will have all tools and equipment necessary to perform the task, and tools and equipment are fit for purpose and appropriately maintained.
- The AP1000 plant design and response in maintenance scenarios meets recognised RGP.
- The design of the refuelling machine (RFM) reduces the potential for human error and

incorporates previous operating experience.

13.9.1.3 Substantiation of Type-C Post-Fault Operator Errors

In total, 45 Type-C post-fault operator errors underwent HEA – 32 having detailed-level HEA and 13 cognitive-level HEA.

In the event of a fault, the operators in the MCR are required and automatically prompted to follow a set of symptom-based EOPs to address any failures in automatic systems and optimally recover the plant to a stable and safe state. The HF design of the MCR and of the EOPs support a number of factors promoting successful completion of tasks that apply to all post-fault errors. These are summarised as follows:

- The Conduct of Operations governs use and verbatim adherence to procedures, operations personnel roles and responsibilities, command, control, and communication in the MCR, crew briefings and shift turnovers, HuP tools and implementation, operations management and leadership, decision making, and safety culture. The Conduct of Operation ensures a healthy nuclear safety culture of all operations personnel at the plant by describing the responsibilities and behaviour required.

- Operators will be fully trained and exercised in the use of EOPs.

- In the event of a fault, there is no requirement for the operator to make a diagnosis of the event, apart from following the steps in the symptom-based EOPs.

- EOPs will be available when needed on the CPS. Hard copies will also be available in the MCR as a backup to CPS. The CPS assists the operators in monitoring and controlling the execution of procedures. The CPS is accessible via the DCIS VDU-based workstations and provides navigation links to the relevant control system displays. The CPS automatically assesses and presents the status of each step and automatically executes parallel monitoring, alerting the operator to important plant information when it needs attention.

- Alarms are both visual and auditory and are presented on the DCIS VDU-based workstations at the RO and control room supervisor consoles. In addition, the alarms are presented at a fixed location on the wall panel information system. All alarms are conspicuous, clear in meaning and easily accessible for detailed alarm information.

- The control room supervisor and ROs will communicate directly with each other, as all are located in the MCR.

- If the STA is established, this person will provide a redundant source of advice and checking of critical safety function status to the MCR team.

13.9.2 Substantiation of HBSC in BDB and SAA

Two BDB, post 72-hour, operator actions and three PSA-derived Level 2 (post-core damage) operator actions underwent HEA at a cognitive-level, whilst 5 HFEs that were post-core damage received HEA at a detailed level.

The BDB actions involved a beyond design basis seismic event and tsunami that causes a SBO scenario exceeding 72 hours in duration, but without a concurrent reactor accident situation. Extracted from the BDB assessments are the following arguments to support the

claim that the operator tasks to extend long term coping can be carried out successfully:

- Necessary onsite equipment is available, and SSCs remain functional following the event.
- Operators necessary to conduct the task are available, both onsite and offsite.
- Operators will follow procedures, be adequately trained for the task and for the site emergency plan, have sufficient time to complete the task, and will have the necessary tools and equipment for the task.
- The site-specific emergency plan will ensure provision of care for all staff, including potable water, food, respite, personal protective equipment (PPE), medical care, and psychological care.
- The AP1000 design and response in BDB scenarios meets recognised RGP.

The three Level 2 actions all involved operator tasks post-core damage. From the cognitive level HEA conducted on these actions, the following arguments support the claim that the actions to respond to a severe accident can be completed successfully:

- Procedures have been verified to provide appropriate guidance for the task.
- Operators necessary to complete the task are available and adequately trained.
- Operators will follow procedures.
- The HSI has been verified to support the task.
- Workload is adequate and there is sufficient time to carry out the task.
- The design of the AP1000 Plant and response in this scenario meets RGP, and any discrepancies will be resolved.

13.9.3 Operator Actions with Low Risk Consequence – ALARP Justification

Whilst there are many potential errors that could be made by operators or plant staff in the course of their duties, the design of the AP1000 Plant means that often the consequences of those errors have little to no impact on nuclear safety in terms of the potential for core damage or radioactive release. This is the case for a large number of the operator actions currently in the HAD, which do not exceed the screening criteria thresholds that would be used to trigger further, more detailed, risk-proportionate, human error analysis.

The term ‘ALARP’ is used to express the concept to reduce risks SFAIRP and it is a concept that must be applied at all levels of risk, extending below the level that may be deemed broadly acceptable. In simple terms it is a requirement to take all measures to reduce risk where doing so is reasonable.

An overall ALARP justification requires a balanced argument containing elements of, (i) compliance with RGP, (ii) demonstration of optioneering, and (iii) quantitative and qualitative assessment (see section 13.2.2).

13.9.3.1 Relevant Good Practice (RGP)

The RGP element of an ALARP justification argument requires that the design solutions that are used to meet safety standards are (i) consistent with application of industry

accepted Codes, Standards and Practices in the UK, (ii) have applied the latest, proven technology, and (iii) have used applicable testing.

13.9.3.1.1 Accepted Codes, Standards and Practices

The list of HF standards and guidance (Table 13-1) that have been used to shape and inform the design of AP1000's safety and DiD systems (Section 13.6.12), the control and display HSIs (Section 13.6.6), control centres (Section 13.6.7) and the operating procedures (Section 13.6.13) were then, and remain, both internationally and industry recognised RGP. In particular the execution and management of a recognised HF Engineering programme (Reference 13.14) applied throughout the AP1000 design phases has ensured that consideration of the inherent strengths and weaknesses of the human operator have been accommodated to ensure successful execution of assigned tasks to maintain nuclear safety (Reference 13.10). The standards and guidance comprising RGP for the HFI in design have undergone an assessment of equivalency to recognised UK standards and are appropriate to the HFI activity and commensurate with the associated risks.

13.9.3.1.2 Use of Proven Technology

The recognition by workers, maintainers, operators (Section 13.6.2.2) and ultimately by the safety case of the use of proven technology, combined with an inherently safe design philosophy for AP1000 (Section 13.6.1) will contribute considerably to the safety and ease of operations and to an HF argument for risk of human failure reduced ALARP.

13.9.3.1.3 Use of Applicable Testing

RGP may be confirmed through utilisation of applicable test results in demonstrating the suitability of the design or operational practice. The progressive application of HF task-support verification (Section 13.7.1) and HF design verification (Section 13.7.2), culminating in integrated system validation tests (Section 13.7.3) provides evidence in demonstrating RGP as related to MCR and RSR HF design implementation. Such test results verify assumptions on relevant human action times through direct simulation and analysis of operator practices. This validation then establishes RGP for these assumptions.

13.9.3.2 Optioneering

The appropriate consideration of different options is an inherent part of the design and design change process. Key in the design process for HF has been the functional analysis and allocation of function process that is described and the results reported in Reference 13.32. Similarly, the DCP process and other design change driver mechanisms, such as Engineering and Design Coordination Reports and Requests for Engineering Change, incorporate opportunity for technical, operational and safety disciplines affected by a proposed design change to challenge and propose alternative solutions as a part of the acceptance or rejection decision (Reference 13.15).

13.9.3.3 Risk Assessment

A risk assessment was conducted for all of the ~400 operator actions that currently reside in the HAD as part of the screening for detailed-level and cognitive-level HEA. The level of risk presented by failure of each action was assessed against threshold criteria relating to such factors as the contribution of the failure to initiating event frequency or core damage frequency or potential effect on passive or DiD systems (Section 13.8.2 and Figure 13.5).

13.10 Conclusion

The AP1000 plant design has undergone a comprehensive and systematic programme of HF Engineering activities that together provide the evidence to support the HF basis for safety (i.e., the HF safety claims) for GDA.

- There has been a systematic, through-life, approach to HFI within the design, assessment and management of systems and processes.
- The allocation of safety actions between humans and engineered SSCs has been substantiated and validated.
- A systematic approach has been taken to identify human actions important to safety operating in normal modes and in abnormal, emergency and accident conditions.
- The administrative controls needed to keep the facility within its operating rules for normal operation or return the facility back to normal operations have been systematically identified.
- Proportionate human error analysis has been carried out for tasks important to safety.
- Workspaces in which operations and maintenance activities are conducted have been assessed to support reliable task performance.
- Suitable and sufficient user interfaces have been provided at appropriate locations to provide effective monitoring and control of the facility in all normal operating modes, fault and accident conditions.
- Procedures have been produced, verified and validated that support reliable human performance during activities that could impact on safety and a systematic approach to training assumed for operators. HF V&V activities have been completed, HEDs identified, with resolutions being identified and implemented.
- HF V&V activities have been completed, HEDs identified, with resolutions being identified and implemented.
- The staffing levels and number of competent personnel needed to operate the facility safely in all its operational states has been estimated.
- Proportionate analysis has been conducted of human actions and administrative controls that are necessary for safety as part of the DBA, PSA and SAA aspects of the safety case.
- The consideration and disposition of ERMs and ALARP design recommendations that were made in the HEA.

Further, the substantiation of human-based safety claims for GDA and the safe, efficient operation of the plant have been predicated on a number of general assumptions that will need to be adopted by a future licensee organisation or require further substantiation of alternatives. These assumptions relate to:

- Adopting a conduct of operations that governs use and verbatim adherence to procedures, defines the operations personnel their roles and responsibilities towards

effective command, control, and communication, and the use of HuP tools, where appropriate, as normal working practice.

- Having sufficient trained personnel being available to conduct operations, maintenance and safety important tasks and that the training of those personnel is based on a SAT that for licensed operators adopts a syllabus akin to that of the NUREG-2103 Knowledge and Abilities Catalog (Reference 13.63).

- Having a culture on the nuclear licensed site where operations, management and leadership see safety-first at the heart of everything they do.

The HF design of the AP1000 Plant has been based upon a set of internationally recognised Standards and Codes and on industry experience and guidance that can be deemed as RGP in the UK.

The design evolution of AP1000 is consistent with the ONR's expectations for the demonstration of ALARP with respect to new commercial reactor designs. A level of safety that is no less than a comparable facility in operation or being constructed has been demonstrated. Additionally, experiences of earlier designs and, in particular, the HF lessons learned from accidents at other NPP around the world have been considered in the design evolution of the AP1000.

Acknowledged future work in the HF safety case substantiation for GDA has been identified and will need to be further progressed during the site licensing phase. These future work areas are:

- Completion of the resolution process currently in progress for the HED and HED issues arising from the HF verification and validation activity conducted for standard AP1000 plant design.

- When appropriate, commencing the standard AP1000 plant start-up HF verification activity described in Reference 13.61.

- Complete HEA process at a cognitive-level for all screened-in, risk-significant operator actions, as demonstrated on a sample of actions for GDA. Provide the HEAs to PSA to serve as human reliability analysis input for the PSA updates to be completed during the Site Licensing.

- Complete HEA process of MTIS activity on SSCs that provide safety function

For the reasons presented above, and with acknowledgement to the aforementioned assumptions, issues and future HF substantiation areas; the role of the operator in ensuring nuclear safety is understood, and the risk to nuclear safety arising from human failure has been identified and reduced ALARP for the standard AP1000 plant design in GDA.

13.11 References

13.1 "Safety Assessment Principles for Nuclear Facilities," Rev. 0, Office for Nuclear Regulation, 2014.

13.2 "A guide to Nuclear Regulation in the UK," Office for Nuclear Regulation, October 2014.

13.3 "Assessing compliance with the law in individual cases and the use of good practice," Health and Safety Executive, Revised May 2003. http://www.hse.gov.uk/risk/theory/alarp2.htm.

13.4 ONR Technical Assessment Guide NS-TAST-GD-005, Rev. 7, "Guideline on the Demonstration of ALARP (As Low As Reasonably Practicable)," December 2015.

13.5 Health and Safety Executive Website, Risk Management Resources, "HSE principles for Cost Benefit Analysis (CBA) in support of ALARP decisions." http://www.hse.gov.uk/risk/theory/alarpcba.htm.

13.6 Westinghouse Report UKP-GW-GL-112, Rev 0, "ALARP Justification Guidance for GDA Close-Out Phase," August 2015.

13.7 Westinghouse Report UKP-GW-GL-042, Rev 1, "AP1000 Human Factors Program and Assessment for the United Kingdom," February 2010.

13.8 Westinghouse Response to RQ-AP1000-1361, NPP_JNE_000288 Enclosure 1, "Integration of HF, PSA, and Fault Studies disciplines," 27 August 2015.

13.9 Westinghouse Report UKP-GW-GL-060, Rev 10, "AP1000 Design Reference Point for UK GDA," January 2017.

13.10 Westinghouse Report APP-OCS-GBH-001, Rev. 1, "Human Factors Engineering Program Plan," April 2009.

13.11 Westinghouse Report UKP-GW-GL-144, Rev 3, "AP1000 UK Safety Categorisation and Classification of Structures, Systems and Components," January 2017.

13.12 IAEA Safety Guide NS-G-1.3, "Instrumentation and Control Systems Important to Safety in Nuclear Power Plants," 2002.

13.13 IAEA Specific Safety Requirements SSR-2/1, "Safety of Nuclear Power Plants – Design," 2012.

13.14 US NRC, NUREG-0711, Rev 2, "Human Factors Engineering Program Review Model," November 2012.

13.15 Westinghouse Procedure APP-GW-GAP-341, Rev 0, "AP1000 Plant Program Design Change Control," January 2016.

13.16 Westinghouse Report APP-OCS-T2R-020, Rev 0, "AP1000 Engineering Tests - Phase 1 Test Report," November 2006.

13.17 Westinghouse Report APP-OCS-T2R-022, Rev 0, "AP1000 Engineering Tests - Phase 2 Test Report," September 2007.

13.18 Westinghouse Report APP-OCS-T2R-030, Rev 0, "AP1000 Human Factors Engineering Tests - Phase 3 Test Report," February 2009.

13.19 Westinghouse Report APP-GW-GER-005, Rev 1, "Safe and Simple: The Genesis and Process of the AP1000 Design," August 2008.

13.20 "Advanced Light Water Reactor Utilities Requirements Document," Volumes I (Rev 2), II (Rev 8) and III (Rev 8), 1999.

13.21 "European Utility Requirements for LWR Nuclear Power Plants," Volumes 1 to 4, http://www.europeanutilityrequirements.org/Documentation/EURdocument.aspx

13.22 IAEA-TECDOC-1581, "Best Practices in Identifying, Reporting and Screening Operating Experience at Nuclear Power Plants," March 2007.

13.23 Not Used.

13.24 Westinghouse Report APP-GW-GLR-001, Rev 3, "Operational Assessment for AP1000," August 2004.

13.25 Westinghouse Report APP-GW-G1R-007, Rev A, "Operating Experience to Apply to Light Water Reactor Designs," May 2007.

13.26 Westinghouse Report GW-GJR-011, Rev 0, "Review of Nuclear Plant Operating Experience and the Application of the Design of the AP600," July 1994.

13.27 Westinghouse Report APP-OCS-GJR-001, Rev. 0 (WCAP-14645-NP, Rev 3), "Human Factors Engineering Operating Experience Review Report for the AP1000 Nuclear Power Plant," November 2006.

13.28 Westinghouse Report UKP-GW-GL-116, Rev 0, "AP1000 Supplemental Information for the Human Factors Safety Case – Review of Selected Design Change Proposals included in the 2015 Design Reference Point for GDA," October 2015.

13.29 Westinghouse Report APP-GW-GGR-100, Rev 0, "AP1000 Human Factors Multi-discipline Preliminary Design Review Report," June 2006.

13.30 Westinghouse Report APP-GW-GGR-101, Rev 0, "AP1000 Human Factors Engineering Design Review Report #2," January 2014.

13.31 Westinghouse Report APP-OCS-GGR-110, Rev 1, "AP1000 Technical Support Centre and Emergency Operations Facility Workshop," February 2008.

13.32 Westinghouse Report APP-OCS-J1-011, Rev 1, "AP600/AP1000 Functional Requirements Analysis and Function Allocation," November 2008.

13.33 IAEA TECDOC-668, "The role of automation and humans in nuclear power plants," ISSN 1011-4289," October 1992.

13.34 Office for Nuclear Regulation NS-TAST-GD-064, Rev 2, "Allocation of Function between Human and Engineered Systems," December 2014.

13.35 Westinghouse Report APP-GW-GL-011, Rev 0, "AP1000 Identification of Critical Human Actions and Risk Important Tasks," April 2006.

13.36 Westinghouse Report APP-OCS-GJR-002, Rev 1, "AP1000 Concept of Operation," February 2016.

13.37 Westinghouse Report APP-OCS-GJR-003, Rev 2, "AP1000 Main Control Room Staff Roles and Responsibilities," July 2010.

13.38 Westinghouse Report APP-OCS-J1R-100, Rev 1, "Function Based Task Analysis Methodology and Implementation for AP1000," February 2014.

13.39 Westinghouse Report APP-OCS-J1R-110, Rev 2, "AP1000 Operational Sequence Analysis 1 (OSA-1) Methodology," February 2014.

13.40 Westinghouse Report APP-OCS-J1R-210, Rev 2, "AP1000 Operational Sequence Analysis 2 (OSA-2) Implementation Plan," February 2014.

13.41 Westinghouse Report APP-OCS-J1A-030, Rev 2, "AP1000 Function-Based Task Analysis Summary Report," January 2015.

13.42 Westinghouse Report APP-OCS-GEH-020, Rev 2, "Programmatic Level Description of the AP1000 Human Factors Verification and Validation Plan," October 2003.

13.43 Westinghouse Report APP-OCS-J1R-120, Rev 6, "AP1000 Operational Sequence Analysis 1 (OSA-1) Summary Report," July 2015.

13.44 Westinghouse Report APP-GW-GL-022, Rev 8, "AP1000 Probabilistic Risk Assessment," August 2009.

13.45 Westinghouse Report APP-OCS-J1R-220, Rev 2, "AP1000 Operational Sequence Analysis 2 (OSA-2) Summary Report," September 2014.

13.46 Westinghouse Report APP-OCS-J1-002, Rev 6, "AP1000 Human System Interface Design Guidelines," July 2016.

13.47 Westinghouse Report APP-GW-GRP-001, Rev 2, "AP1000 Local Panels and Maintainability Human Factors Design Guidelines," February 2014.

13.48 Westinghouse Report APP-OCS-T5-020, Rev 0, "Engineering Test Plan for AP1000 Soft Controls," September 2005.

13.49 Westinghouse Report APP-OCS-T5-022, Rev 0, "Phase 2 Engineering Test Plan for AP1000 Control Room Integration," September 2007.

13.50 Westinghouse Report APP-OCS-J7-001, Rev. 1, "Operations and Control Centres System, System Specification Document," March 2016.

13.51 EEMUA 191, "Alarm Systems: A Guide to Design, Management and Procurement," Engineering Equipment and Materials Users' Association, 1999.

13.52 BS IEC 62241:20-4, "Nuclear Power Plants – Main Control Room – Alarm Functions and Presentation." British Standards Institution," 2004.

13.53 Westinghouse Report APP-OCS-J1-001, Rev 3, "Standard Alarm Presentation System Functional Requirements," August 2016.

13.54 Westinghouse Report UKP-GW-GL-126, Rev 0, "United Kingdom AP1000 Human Factors Qualitative Error Analysis," June 2016.

13.55 Westinghouse Report UKP-OCS-GLR-002, Rev 1, "United Kingdom AP1000 RSR Control Strategy for Class 1 Displays and Controls - ALARP Justification," December 2016.

13.56 Westinghouse Report UKP-GW-GL-074, Rev. 0, "Supplemental Information for the UK AP1000 Human Factors Safety Case – AP1000 Maintainability," December 2010.

13.57 Westinghouse Report APP-OCS-JCR-001, Rev. A, "AP1000 Local Panels and Maintainability HFE Assessment," September 2010.

13.58 Westinghouse Report APP-GW-GJP-100, Rev. 3, "Writer's Guideline for Operating Procedures," June 2015.

13.59 Westinghouse Report APP-OCS-GEH-320, Rev 6, "AP1000 Human Factors Engineering Integrated System Validation Plan," January 2015.

13.60 Westinghouse Report APP-OCS-GEH-420, Rev 2, "AP1000 Human Factors Engineering Discrepancy Process," December 2014.

13.61 Westinghouse Report APP-OCS-GEH-520, Rev 4, "AP1000 Plant Start-up Human Factors Engineering Design Verification Plan," December 2014.

13.62 Westinghouse Report APP-OCS-GER-041, Rev 0, "AP1000 the Incorporation of Human Factors Engineering into the Development of the AP1000 Plant Training Programs," November 2015.

13.63 US NRC, NUREG-2103, Draft Report for Comment, "Knowledge and Abilities Catalog for Nuclear Power Operators – Pressurized Water Reactors Westinghouse AP1000," October 2011.

13.64 US NRC, NUREG-1021, Final Report, Rev. 10, "Operator Licensing Examination Standards for Power Reactors," December 2014.

13.65 Not Used.

13.66 Administrative Procedure APP-GW-GJP-115, Rev 1, "Conduct of Operations," June 2014.

13.67 Westinghouse Report WNA-CN-00118-GEN, Rev 0, "Chinese, UK, and US Adult Population Anthropometric Data," October 2010.

13.68 Westinghouse Report APP-GJ01-GTP-001, Rev A, "AP1000 Job and Task Analysis Procedure," October 2007.

13.69 CCD Design and Ergonomics CCD/1049/REP/002/10, Version 3.0, "UK Nuclear Worker Stereotypical Representation relative to the Westinghouse AP1000 Nuclear Plant Human Factors Design – Combined Phase 1 and 2 Report," December 2010.

13.70 Westinghouse Report APP-OCS-GEH-220, Rev 4, "AP1000 Human Factors Engineering Task Support Verification Plan," January 2015.

13.71 Westinghouse Report APP-OCS-GEH-120, Rev 3, "AP1000 Human Factors Engineering Design Verification Plan," December 2014.

13.72 Westinghouse Report APP-OCS-GER-220, Rev. 1, "AP1000 Human Factors Engineering Task Support Verification Report," June 2016.

13.73 Westinghouse Report APP-OCS-GER-120, Rev 1, "AP1000 Human Factors Engineering Design Verification Report," September 2015.

13.74 Westinghouse Report APP-OCS-GLR-001, Rev 2, "AP1000 Post-Accident Risk-Important Human Actions Summary Report," December 2014.

13.75 Westinghouse Report APP-OCS-GER-031, Rev 0, "The Incorporation of Human Factors Engineering into the Development of the AP1000 Plant Procedures," November 2015.

13.76 IAEA TECDOC-1200, "Applications of probabilistic safety assessment (PSA) for nuclear power plants," ISSN 1011-4289, February 2001.

13.77 Westinghouse Report APP-PRA-GSC-321, Rev C, "AP1000 Plant At-Power Internal Events PSA, Human Reliability Analysis Notebook," July 2015.

13.78 Westinghouse Letter NPP_JNE_000737 Enclosure 1, "Status of Ongoing Human Factors Integration across GDA Issues," March 2016.

13.79 Westinghouse Report APP-PRA-GM-005, Rev C, "AP1000 Plant PSA Human Reliability Analysis Guidebook," November 2016.

13.80 Westinghouse Report UKP-GW-GLR-003, Rev 2, "AP1000 Fault Schedule for the United Kingdom," January 2017.

13.81 Westinghouse Report APP-OCS-GEH-321, Rev. 1, "Human Factors Engineering Integrated System Validation Scenario Information," January 2015.

13.82 Westinghouse Report APP-OCS-GER-320, Rev. 3, "Human Factors Engineering Integrated System Validation Report," November 2016.

13.83 International Atomic Energy Agency, IAEA, Safety Series No. 50-P-10, "Human Reliability Analysis in Probabilistic Safety Assessment for Nuclear Power Plants," Vienna, 1995.

13.84 Westinghouse Report UKP-GW-GGR-201, Rev. 1, "UK AP1000 Plant Post-Fukushima Assessment," July 2016.

13.85 Westinghouse Report UKP-GW-GLR-102, Rev 0, "UK AP1000 Probabilistic Risk Assessment Update Report," February 2010.

13.86 Westinghouse Report UKP-GW-GL-069, Rev 0, "Supplemental Information for the UK AP1000 Human Factors Safety Case as Reflecting the UK AP1000 PSA Update," November 2010.

13.87 Westinghouse Report UKP-GW-GL-070, Rev 0, "UK AP1000 Human Factors Safety Case Reflection of the UK AP1000 Fire/Flood PSA," November 2010.

13.88 Westinghouse Report UKP-GW-GL-071, Rev 0, “Supplemental Information for the UK AP1000 Human Factors Safety Case as Reflecting the UK AP1000 Low Power and Shutdown PSA,” November 2010.

13.89 Westinghouse Report UKP-GW-GL-073, Rev 0, “Supplemental Information for the UK AP1000 Human Factors Safety Case - Identified Non-Core Damage Human Errors with Possible Radioactive Release,” November 2010.

13.90 Westinghouse Report UKP-GW-GL-075, Rev 0, “Supplemental Information for the UK AP1000 Human Factors Safety Case – Additional UK Fault Schedule Faults,” December 2010.

13.91 Kirwan B., “A Guide to Practical Human Reliability Assessment,” CRC Press, ISBN 0-7484-0052-4 HB, 1994.

13.92 Westinghouse Document WEC-REG-0411N, "GDA Human Factors Sampling Plan and Substantiation," October 2015.

13.93 Westinghouse Report UKP-GW-GL-072, Rev 0, “Supplemental Information for the Human Factors Safety Case – Potential Improvements as Proposed in the ALARP Analysis,” November 2010.

13.94 US NRC, NUREG-2114, Rev 1, “Cognitive Basis for Human Reliability Analysis,” January 2016.

13.95 Westinghouse Letter NPP_JNE_000737, Enclosure 1, “Status of Ongoing Human Factors Integration across GDA Issues,” March 2016.

13.96 Westinghouse Report UKP-GW-GL-200, Rev 1, “AP1000 Squib Valve Safety Case,” December 2016.

13.97 Westinghouse Enclosure 2 RQ-AP-1000-1558, “Resolution Plans for the ISV HED Issues,” August 2016.

13.98 Westinghouse Report APP-GW-GJP-500, Rev 0, “Executive Volume for AP1000 Severe Accident Management Guidelines,” March 2015.

13.99 Westinghouse Report APP-GW-GJP-501, Rev 0, “Severe Accident Control Room Guideline Initial Response,” March 2015.

13.100 Westinghouse Report APP-GW-GJP-502, Rev 0, “Severe Accident Control Room Guideline After The TSC Is Functional,” March 2015.

13.101 Westinghouse Report APP-GW-GJP-150, Rev 1, “Operating Procedures Verification and Validation,” February 2015.

Table 13-1 Human Factors Relevant Good Practice in AP1000 design.

1	US NRC NUREG-0711 Rev 2 – Human Factors Engineering Program Review Model 2004.
2	IEEE Standard 1023-2004, "IEEE Recommended Practice for the Application of Human Factors Engineering to Systems, Equipment and Facilities of Nuclear Power Generating Stations and Other Nuclear Facilities," Institute of Electrical and Electronics Engineers, Inc., 2004.
3	BS IEC 60964, Nuclear Power Plants Control Rooms – Design, International Electrotechnical Commission, Edition 2.0, 2009.
4	ISO 11064, First Edition, Ergonomic Design of Control Centres, Parts 1 to 7. International Organization for Standardization.
5	ISO 11064-1:2000 Ergonomic Design of Control Centres: Principles of the Design of Control Centres
6	ISO 11064-2:2000 Ergonomic Design of Control Centres: Principles for the Arrangement of Control Centres
7	ISO 11064-3:1999 Ergonomic Design of Control Centres: Control Room Layout
8	ISO 11064-4:2004 Ergonomic Design of Control Centres: Layout and Dimensions of Workstations
9	ISO 11064-5:2008 Ergonomic Design of Control Centres: Displays and Controls
10	ISO 11064-6:2005 Ergonomic Design of Control Centres: Environmental Requirements for Control Centres
11	ISO 11064-7:2006 Ergonomic Design of Control Centres: Principles for the Evaluation of Control Centres
12	NUREG 0700, Rev. 2, "Human System Interface Design Review Guidance," U.S. Nuclear Regulatory Commission, May 2002
13	IEEE Standard 1289 (1998) – "IEEE Guide for the Application of Human Factors Engineering in the Design of Computer Based Monitoring and Control Displays for Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers, Inc., 1998
14	MIL-STD-1472, Rev. F, Department of Defence Design Criteria Standard: Human Engineering, U.S. Department of Defence. 23 August 1999 & change notice 1, 5 December 2003
15	BS IEC 62241 (2004) – Nuclear Power Plants – Main Control Room – Alarm Functions and Presentation
16	CEI IEC 61771 (1995) – Nuclear Power Plants – Main Control Room – Verification & Validation of Design
17	BS IEC 61839 (2000) – Nuclear Power Plants – Design of Control Rooms – Functional Analysis & Assignment
18	BS IEC 61772 (2009) – Nuclear Power Plants –Control Rooms – Application of Visual Display Units
19	BS IEC 61227 (2008) – Nuclear Power Plants – Control Rooms – Operator Controls
20	BS IEC 60965 (2009) – Nuclear Power Plants – Control Rooms – Supplementary Control Points for Reactor Shutdown without Access to the Main Control Room

Table 13-2 Estimated/Assumed UK AP1000 Staff (including site staff and corporate support)

Staffing Area	1st Unit	Total with 2nd Unit	Total with 3rd Unit
Plant Management	17	28	38
Plant Operations	77	144	201
Plant Maintenance	109	176	224
Plant Engineering	45	68	84
Plant Safety	51	77	102
Plant Licensing	2	3	4
Plant Administration	49	72	97
Environmental	2	2	3
Radiation Protection	25	37	51
Waste Management	11	18	24
Training	23	29	32
Totals	411	654	860

Table 13-3 Questions used to elicit the identification of potential operator errors

Type and Source of Error	Questions to elicit identification of potential errors
Maintenance latent errors for passive safety systems and DiD systems.	• What maintenance errors can be performed on the system or respective components that would prevent or degrade the system/component from performing its safety or mitigating function? • Use the plant Tech Specs and associated surveillance requirements as a list or required maintenance activities when answering question "a." above. • Consider improperly performed corrective maintenance when answering question "a." above. • Consider errors performed on any support systems of the respective passive safety system or DiD system that would degrade or prevent the system from performing its mitigating function. • From your extensive plant operating experience and training experience, recall and identify any human action/error that resulted in a maintenance latent error. If possible, identify the "operating experience" report and enter it into the HAD field.
Operator induced initiating events and maintenance induced initiating events from fault schedule events.	• What are the operator errors/actions that when performed would initiate the event/fault? • What are the maintenance errors that when performed would initiate the event/fault? • When answering the questions above, refer to the Fault Schedule (Reference 13.3) or to PCSR Chapter 8 and 9 to better understand the event. • Systematically consider each plant operating mode as the initial plant condition when answering the above questions. • Consider the GOPs (i.e., plant mode change procedures) when answering question "a." above. • Refer to associated plant Tech Spec surveillance requirements when answering question "b." above. • From your extensive plant operating experience and training experience, recall and identify any human action/error that resulted in an operator induced initiating event or maintenance induced initiating event. If possible, identify the "operating experience" report and enter it into the HAD field.
Post-fault operator errors from fault schedule events.	• What error can the operator make that prevents or degrades a passive safety system or a defence in depth (DiD) system from performing its mitigating function? • Refer to the appropriate EOP to identify potential operator errors during the execution of the procedure. • From your extensive plant operating experience and simulator training experience, recall and identify any human action/error performed during the execution of the appropriate EOP.

Table 13-4 Identification Source and Error Type of Human Action Database entries

Operator action or HFE identification source	Number in HAD	Type A MLE	Type B MIIE	Type B OIIE	Type C PFOE	HEA Pro forma
Early PSA HFEs (Reference 13.44 and 13.85)	72		2	2	68	21 (DL) *
New PSA HFEs (HEPE) (Reference 13.77)	13	13				1 (CL) **
New PSA HFEs (HEPO) Reference 13.77)	51				51	13 (CL)
Systematic HEI process UK AP1000 Fault Schedule (Reference 13.80)	178	77	15	73	13	44 (DL) 4 (CL)
Systematic HEI process Composite Fault List (PCSR Rev 0. 2011 Chapter 8)	41	6	11	24		10 (DL)
AP1000 BDB Long-Term Coping Strategy (Reference 13.84)	8					2 (CL)
HF Review of Class 1 DCPs in the AP1000 DRP for GDA (Reference 13.28)	25					
HFI across the other GDA Issues (Reference 13.78)	32					

* DL – Detailed-Level HEA Pro forma, ** CL – Cognitive-Level HEA Pro forma

Table 13-5 PSFs having a strong influence on macrocognitive functions

Important PSFs	Detecting and Noticing	Understanding and Sense Making	Decision Making	Action
Human System Interface (HSI) Displays	■	■		■
Knowledge / Experience / Expertise	■	■	■	■
Stress	■			
Task Load / Complexity	■			■
Procedure availability and quality		■	■	
Training		■	■	
Time pressure			■	
Divided attention				■
Leadership style and communication				

(Adapted from US NRC, NUREG-2114, Rev 1, "Cognitive Basis for Human Reliability Analysis," January 2016.)

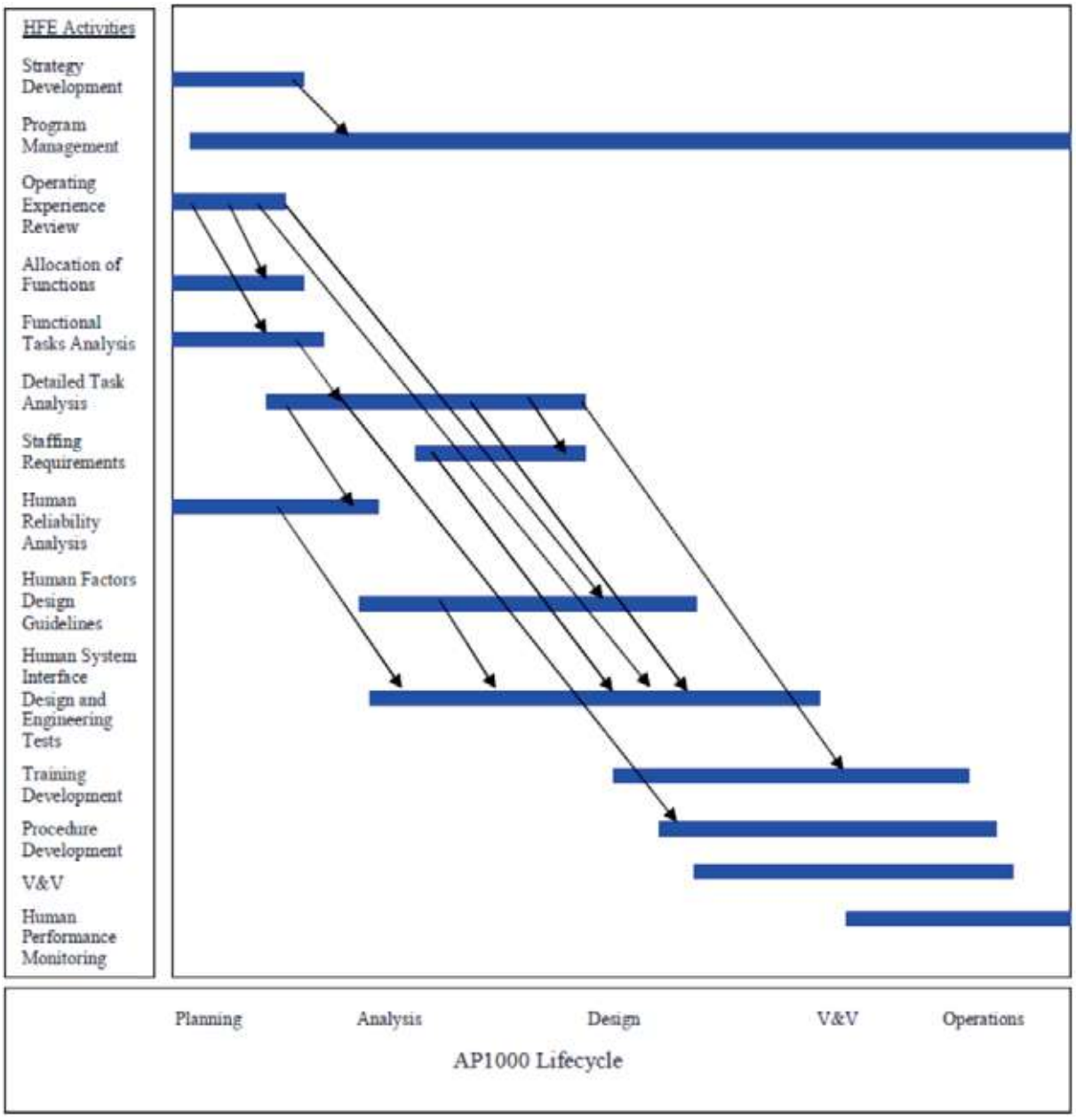


Figure 13.1. HF Engineering programme activities throughout the AP1000 design lifecycle stages

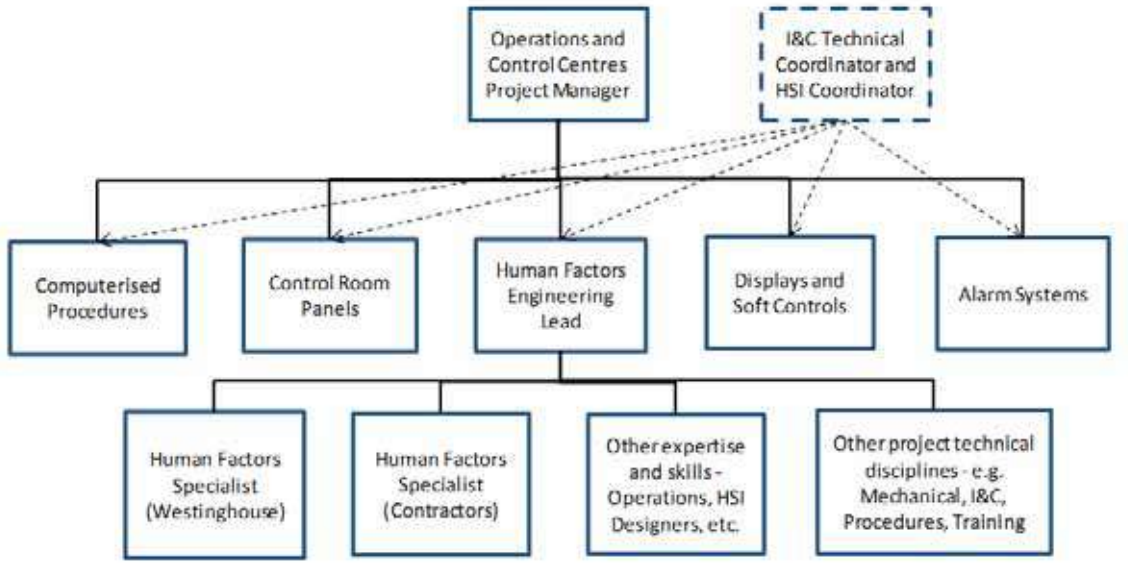


Figure 13.2. Schematic of the Human Factors Engineering Group

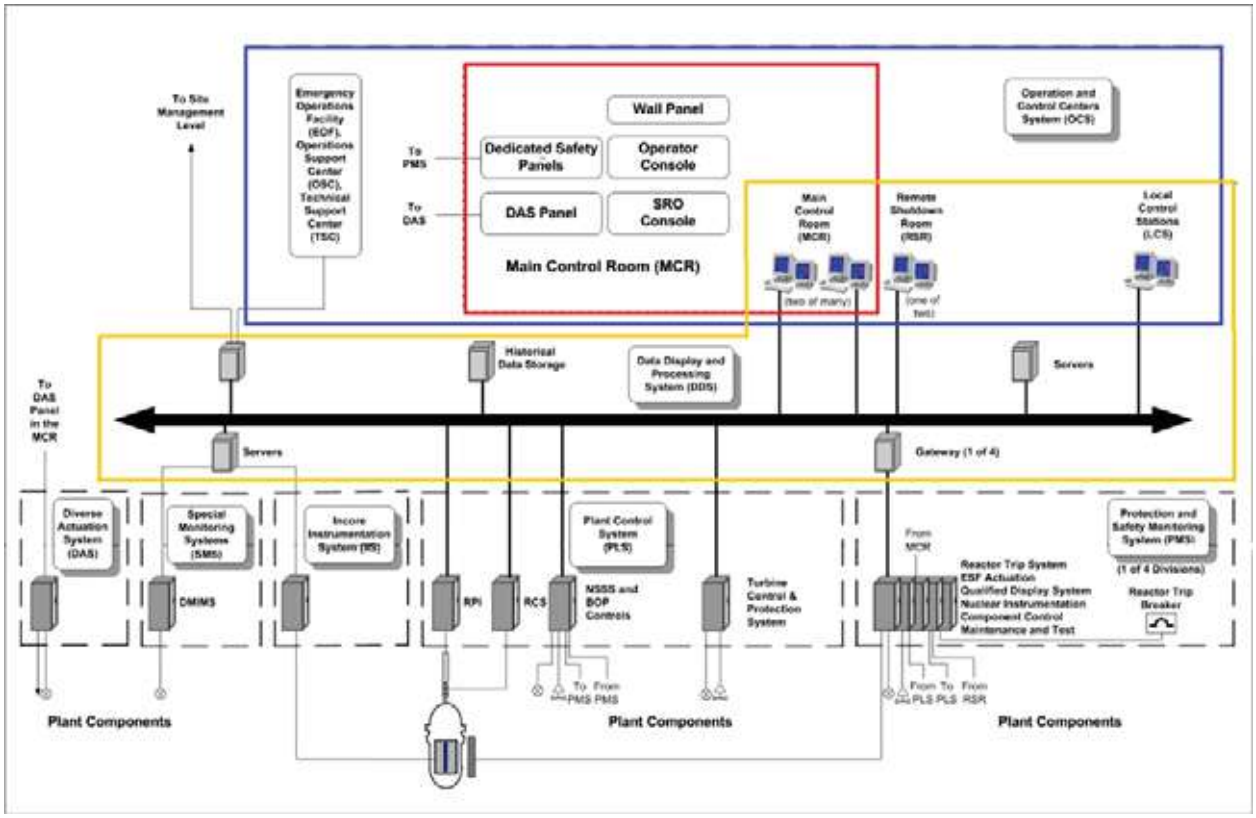


Figure 13.3. Operation and Control Centres System I&C Architecture

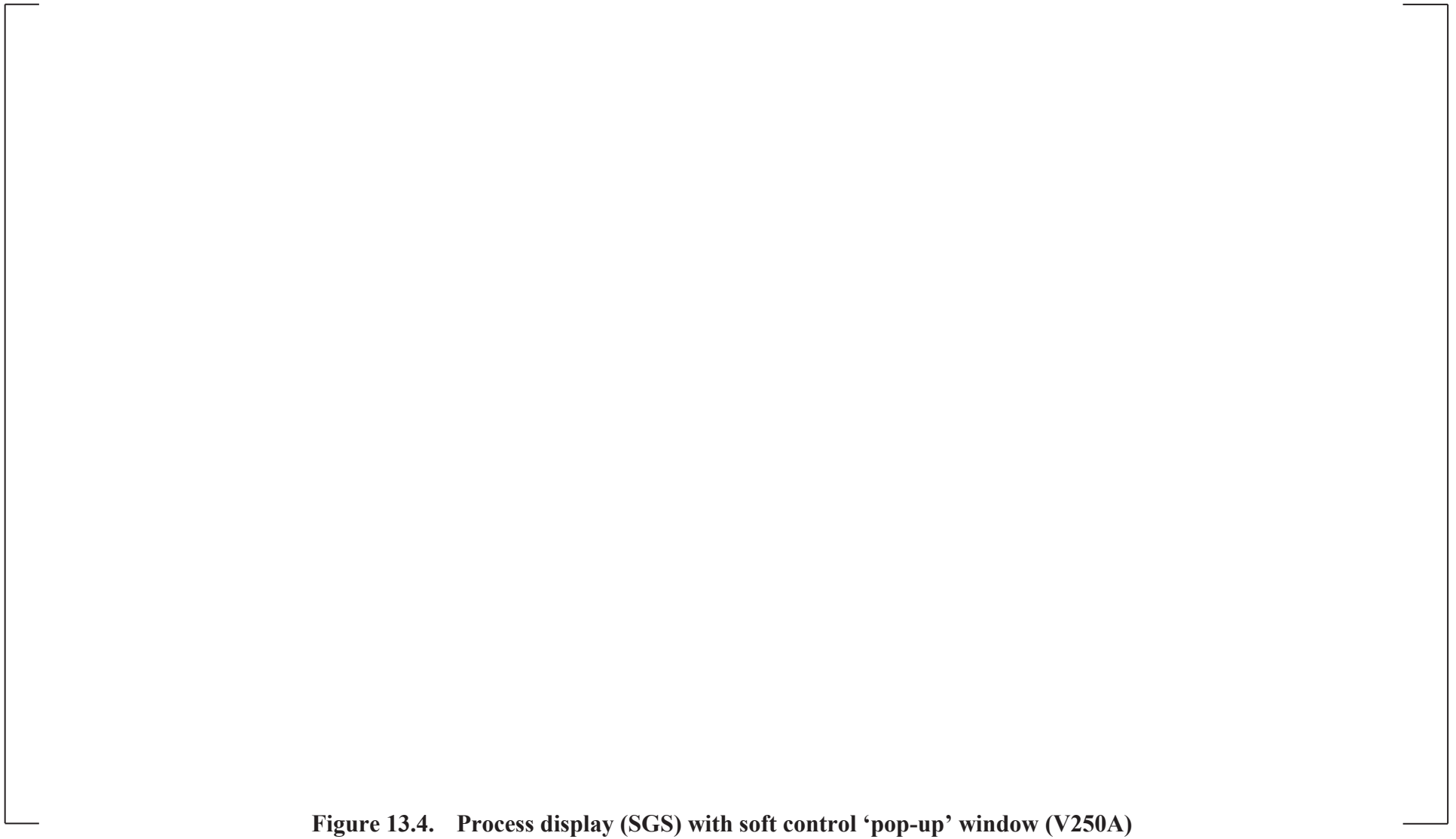


Figure 13.4. Process display (SGS) with soft control ‘pop-up’ window (V250A)

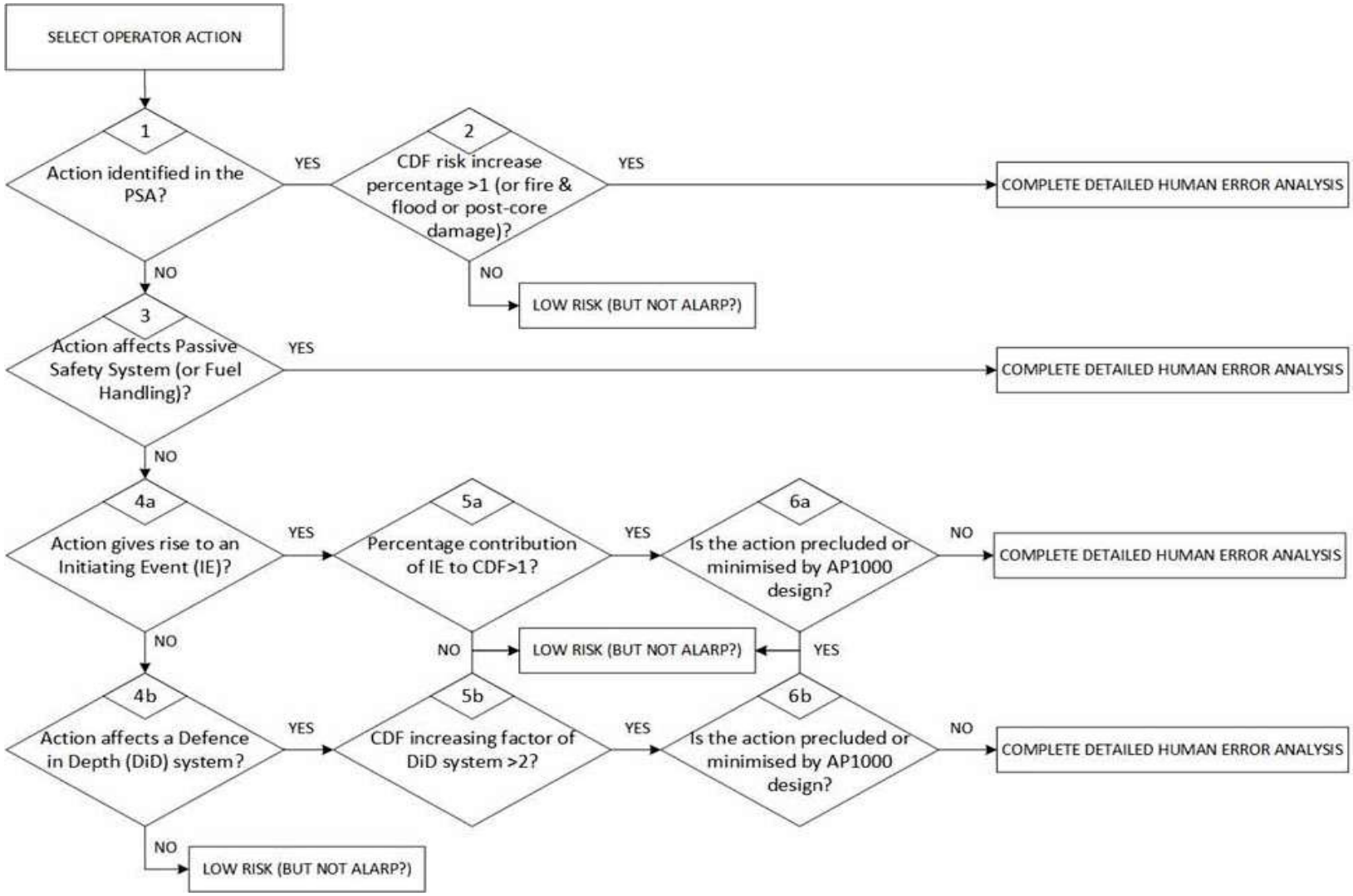


Figure 13.5. Criteria for identifying operator actions requiring detailed human error analysis

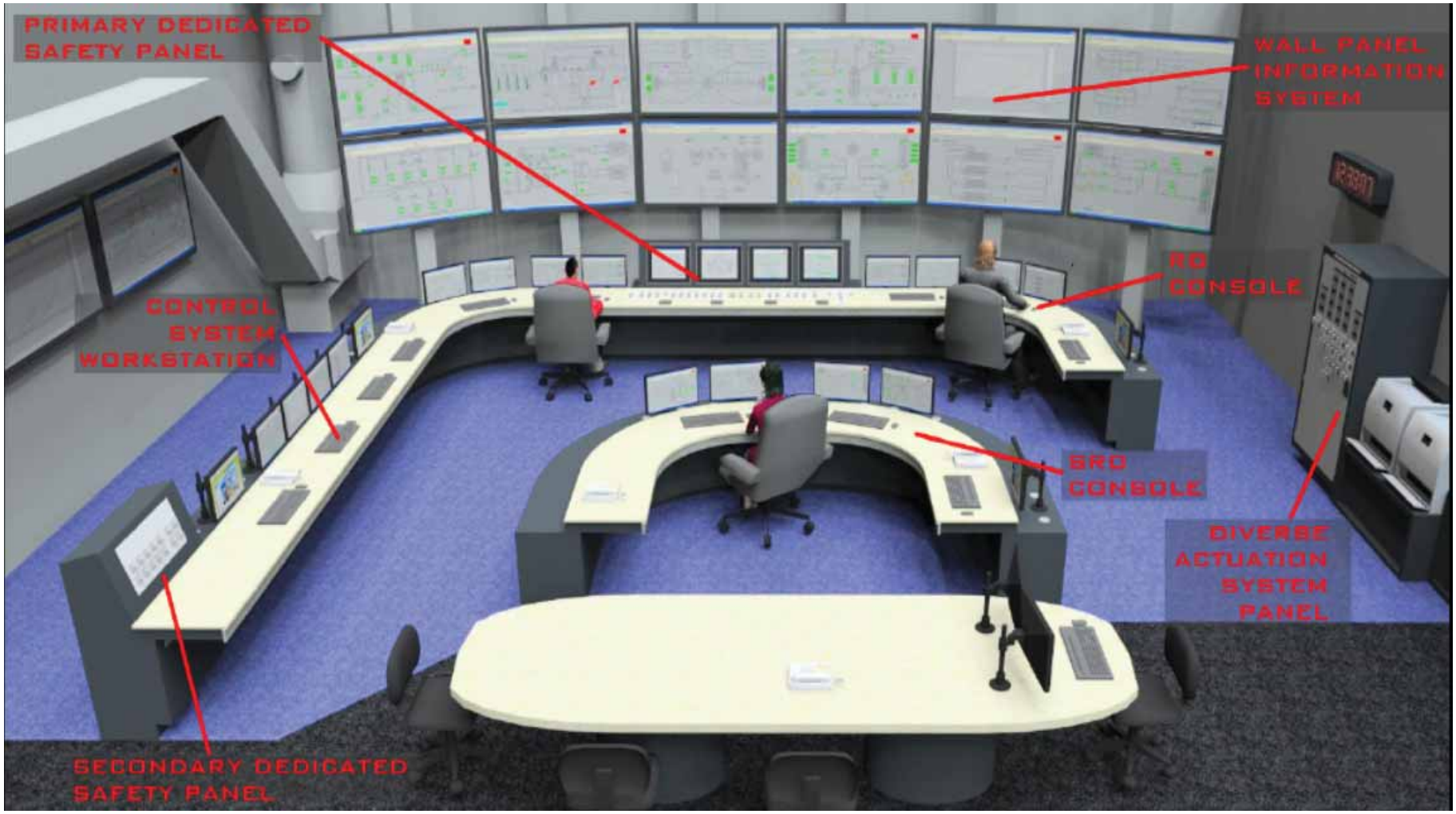


Figure 13.6. MCR Layout and Main HSI Panels

Figure 13.7. Process Display - Steam Generator System

Figure 13.8. Function Display - Steam Generator System

Figure 13.9. Task Display - Steam Generator System

Figure 13.10. Alarm Panel System – Primary Side Systems

Figure 13.11. Alarm Panel System – Secondary Side Systems

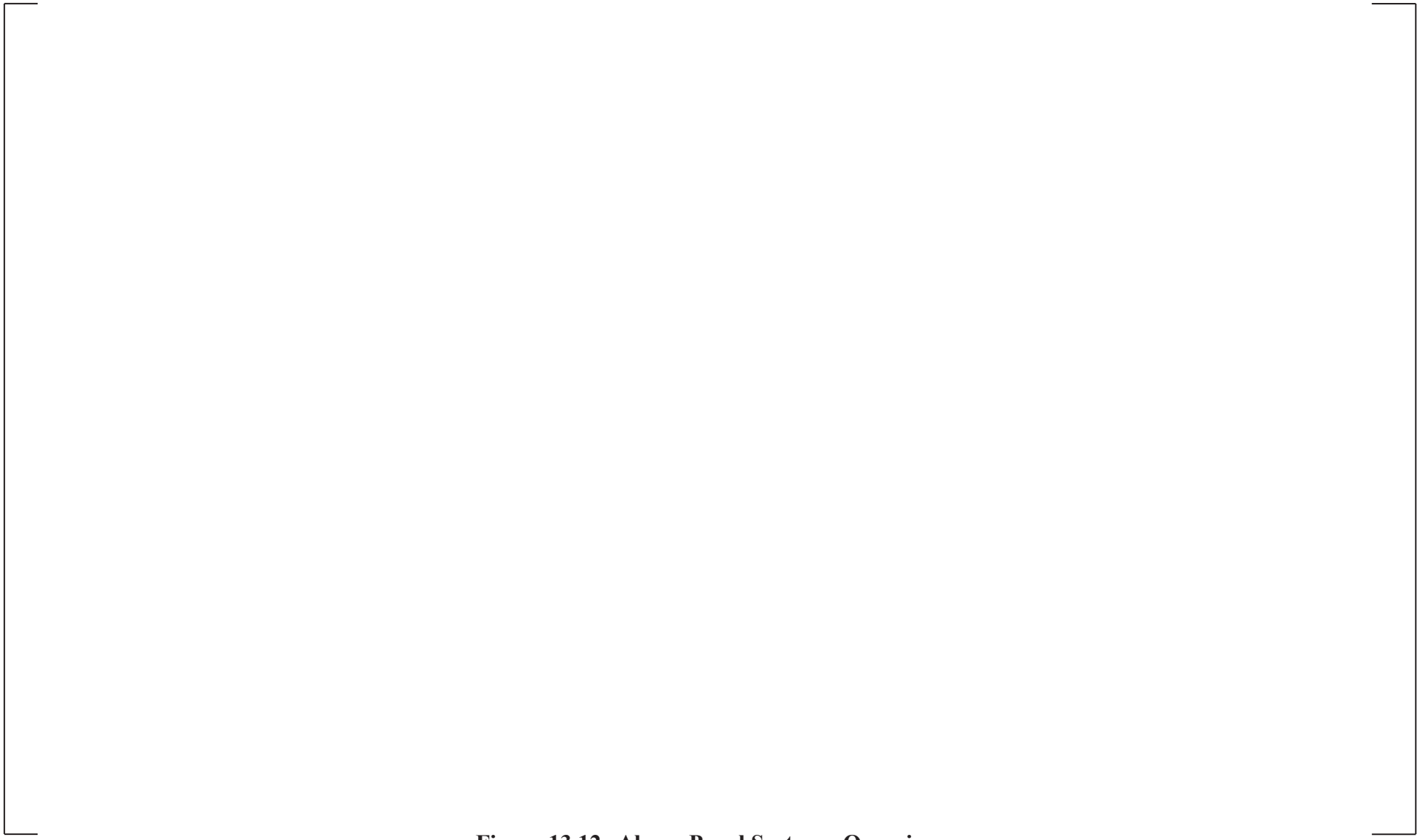


Figure 13.12. Alarm Panel System - Overview

Figure 13.13. Computerised Procedure System – AOP-304 Symptoms and Entry Conditions

Figure 13.14. Computerised Procedure System – E-0 Reactor Trip or Safeguards Actuation

Figure 13.15. Computerised Procedure System – Critical Safety Function Tree (Active Window

APPENDIX 13A DETAILED-LEVEL HEA ACTIONS

Screened-in Human Failure Events and Operator Action Errors with Detailed-Level Human Error Analysis Pro forma				
Serial No.	**Event ID**	**Human Failure Event or Operator Action Error**	**HFE or Operator Action Error Source document (Screening Node and Error Type)**	**Location of detailed HEA Pro forma**
001	ADN-MAN01 (LPM-MAN02)	Operator fails to manually actuate the Automatic Depressurisation System before core damage (Operator fails to recognise the need for RCS depressurisation during a LOCA)	at-power PSA APP-GW-GL-022 (Node 2 CDF risk increase >1%)	HF Program for the UK UKP-GW-GL-042, Rev 1, Appendix C
002	ADN-REC01 (LPM-REC01)	Operator fails to manually actuate the Automatic Depressurisation System post-core damage Operator fails to recognise need for reactor coolant system depressurisation during small LOCA	at-power PSA APP-GW-GL-022 (Node 2 Post-Core Damage)	HF Program for the UK UKP-GW-GL-042, Rev 1, Appendix C
003	ATW-MAN03	Operator fails to manually trip the reactor through Protection and Safety Monitoring System in one minute	at-power PSA APP-GW-GL-022 (Node 2 CDF risk increase >1%)	HF Program for the UK UKP-GW-GL-042, Rev 1, Appendix C
004	ATW-MAN05	Operator fails to manually trip the reactor through Protection and Safety Monitoring System in seven minutes	at-power PSA APP-GW-GL-022 (Node 2 CDF risk increase >1%)	HF Program for the UK UKP-GW-GL-042, Rev 1, Appendix C
	(CAN-MAN0S) CIC-MAN01	Operator fails to locally close manual valve CAS-V204 to isolate containment	at-power PSA APP-GW-GL-022 (Node 2 Post-Core Damage)	HF Program for the UK UKP-GW-GL-042, Rev 1, Appendix C
005	CIB-MAN00	Operator fails to Diagnose Steam Generator Tube Rupture	at-power PSA APP-GW-GL-022 (Node 2 CDF risk increase >1%)	HF Program for the UK UKP-GW-GL-042, Rev 1, Appendix C

APPENDIX 13A DETAILED-LEVEL HEA ACTIONS (cont.)

Screened-in Human Failure Events and Operator Action Errors with Detailed-Level Human Error Analysis Pro forma				
Serial No.	**Event ID**	**Human Failure Event or Operator Action Error**	**HFE or Operator Action Error Source document (Screening Node and Error Type)**	**Location of detailed HEA Pro forma**
006	CIB-MAN01	Failure to Close Main Steam Isolation valve on a Ruptured Steam Generator	at-power PSA APP-GW-GL-022 (Node 2 CDF risk increase >1%)	HF Program for the UK UKP-GW-GL-042, Rev 1, Appendix C
007	CIC-MAN01 (CAN-MANOS)	Operator fails to Isolate Containment	at-power PSA APP-GW-GL-022 (Node 2 Post-Core Damage)	HF Program for the UK UKP-GW-GL-042, Rev 1, Appendix C
008	CIT-MAN0S	Operator fails to Isolate Containment	at-power PSA APP-GW-GL-022 (Node 2 Post-Core Damage)	HF Program for the UK UKP-GW-GL-042, Rev 1, Appendix C
009	CMN-REC01	Operator fails to Actuate Core Makeup Tank	at-power PSA APP-GW-GL-022 (Node 2 Post-Core Damage)	HF Program for the UK UKP-GW-GL-042, Rev 1, Appendix C
010	CVN-MAN00	Operator fails to Align	at-power PSA APP-GW-GL-022 (Node 2 CDF risk increase >1%)	HF Program for the UK UKP-GW-GL-042, Rev 1, Appendix C
011	CVN-MAN03	Operator fails to Start Chemical and Volume Control System Pump B	at-power PSA APP-GW-GL-022 (Node 2 CDF risk increase >1%)	HF Program for the UK UKP-GW-GL-042, Rev 1, Appendix C
012	DUMP-MAN01	Operator fails to Operate Steam Dump Valves	at-power PSA APP-GW-GL-022 (Node 2 CDF risk increase >1%)	HF Program for the UK UKP-GW-GL-042, Rev 1, Appendix C

APPENDIX 13A DETAILED-LEVEL HEA ACTIONS (cont.)

Screened-in Human Failure Events and Operator Action Errors with Detailed-Level Human Error Analysis Pro forma				
Serial No.	**Event ID**	**Human Failure Event or Operator Action Error**	**HFE or Operator Action Error Source document (Screening Node and Error Type)**	**Location of detailed HEA Pro forma**
013	LPM-MAN01	Operator fails to Recognise the Need for Reactor Coolant System Depressurisation during a small LOCA or loss of high pressure heat removal system (Modes 1-5)	at-power PSA APP-GW-GL-022 (Node 2 CDF risk increase >1%)	HF Program for the UK UKP-GW-GL-042, Rev 1, Appendix C
	(LPM-MAN02) ADN-MAN01)	Operator fails to recognise the need for Reactor Coolant System depressurisation during a medium loss-of-coolant accident. (Modes 1-4)	at-power PSA APP-GW-GL-022 (Node 2 CDF risk increase >1%)	HF Program for the UK UKP-GW-GL-042, Rev 1, Appendix C
	(LPM-REC01) ADN-REC01	Operator fails to Recognise the Need for Reactor Coolant System Depressurisation during a small loss-of-coolant accident or transient with loss of the passive residual heat removal system, and successful operation of the core makeup tanks after core damage (Mode 3 – Hot Standby)	at-power PSA APP-GW-GL-022 (Node 2 Post-Core Damage)	HF Program for the UK UKP-GW-GL-042, Rev 1, Appendix C
014	REC-MANDAS	Operator fails to Diagnose of an Event Through DAS Signals or Perform an Activity by Operating DAS Controls	at-power PSA APP-GW-GL-022 (Node 2 CDF risk increase >1%)	HF Program for the UK UKP-GW-GL-042, Rev 1, Appendix C
015	REN-MAN04	Operator fails to Initiate Recirculation (LOCA and IRWST level signal failure)	at-power PSA APP-GW-GL-022 (Node 2 CDF risk increase >1%)	HF Program for the UK UKP-GW-GL-042, Rev 1, Appendix C
016	RHN-MAN01	Operator fails to Align Normal Residual Heat Removal System	at-power PSA APP-GW-GL-022 (Node 2 CDF risk increase >1%)	HF Program for the UK UKP-GW-GL-042, Rev 1, Appendix C

APPENDIX 13A DETAILED-LEVEL HEA ACTIONS (cont.)

Screened-in Human Failure Events and Operator Action Errors with Detailed-Level Human Error Analysis Pro forma				
Serial No.	**Event ID**	**Human Failure Event or Operator Action Error**	**HFE or Operator Action Error Source document (Screening Node and Error Type)**	**Location of detailed HEA Pro forma**
017	VLN-MAN01	Operator fails to Actuate Hydrogen Control System	at-power PSA APP-GW-GL-022 (Node 2 Post-Core Damage)	HF Program for the UK UKP-GW-GL-042, Rev 1, Appendix C
018	VWN-MAN01	Operator fails to Align Standby Chiller	at-power PSA APP-GW-GL-022 (Node 2 CDF risk increase >1%)	HF Program for the UK UKP-GW-GL-042, Rev 1, Appendix C
019	OPR-009 (OPR-091; OPR-092; OPR-094; OPR-095; OPR-096; OPR-097)	Incorrect maintenance leads to PRHR failing to provide a heat sink	Systematic HEI Node 3 Passive Safety System (MLE)	HF Program for the UK UKP-GW-GL-042, Rev 1, Appendix C
020	OPR-010 (OPR-127)	Maintenance error leads to CMTs failing to inject when required following reactor trip	Systematic HEI Node 3 Passive Safety System (MLE)	HF Program for the UK UKP-GW-GL-042, Rev 1, Appendix C
021	OPR-011	Maintenance error leads to ADS failing to vent RCS when required	Systematic HEI Node 3 Passive Safety System (MLE)	HF Program for the UK UKP-GW-GL-042, Rev 1, Appendix C
022	OPR-068	Mispositioned Component Interface Module (CIM) prevents control signal from reaching an actuated PMS component	Systematic HEI Node 5b CDF increasing factor of DiD system (MLE)	HF Program for the UK UKP-GW-GL-042, Rev 1, Appendix C
023	OPR-069	DC Power left de-energised to ADS valves	Systematic HEI	HF Program for the UK

APPENDIX 13A DETAILED-LEVEL HEA ACTIONS (cont.)

Screened-in Human Failure Events and Operator Action Errors with Detailed-Level Human Error Analysis Pro forma				
Serial No.	**Event ID**	**Human Failure Event or Operator Action Error**	**HFE or Operator Action Error Source document (Screening Node and Error Type)**	**Location of detailed HEA Pro forma**
			Node 3 Passive Safety System (MLE)	UKP-GW-GL-042, Rev 1, Appendix C
024	OPR-070	Outlet valve left closed erroneously on safety injection accumulator	Systematic HEI Node 3 Passive Safety System (MLE)	HF Program for the UK UKP-GW-GL-042, Rev 1, Appendix C
025	OPR-071 (OPR-074)	Accumulator levels allowed to rise to point where they are unavailable.	Systematic HEI Node 3 Passive Safety System (MLE)	HF Program for the UK UKP-GW-GL-042, Rev 1, Appendix C
026	OPR-072 (OPR-073)	Operator erroneously allows accumulators to drain to the point that not enough water available for injection	Systematic HEI Node 3 Passive Safety System (MLE)	HF Program for the UK UKP-GW-GL-042, Rev 1, Appendix C
	(OPR-073) OPR-072	Operator erroneously allows accumulator pressure to decrease too low	Systematic HEI Node 3 Passive Safety System (MLE)	HF Program for the UK UKP-GW-GL-042, Rev 1, Appendix C
	(OPR-074) OPR-071	Operator erroneously allows pressure in accumulator to go too high.	Systematic HEI Node 3 Passive Safety System (MLE)	HF Program for the UK UKP-GW-GL-042, Rev 1, Appendix C
027	OPR-079	Foreign Material is erroneously left in IRWST	Systematic HEI Node 3 Passive Safety System (MLE)	HF Program for the UK UKP-GW-GL-042, Rev 1, Appendix C
028	OPR-080	Operator incorrectly adjusts Accumulator boron concentration such that it is too low	Systematic HEI Node 3 Passive Safety System	HF Program for the UK UKP-GW-GL-042, Rev 1, Appendix C

APPENDIX 13A DETAILED-LEVEL HEA ACTIONS (cont.)

Screened-in Human Failure Events and Operator Action Errors with Detailed-Level Human Error Analysis Pro forma				
Serial No.	**Event ID**	**Human Failure Event or Operator Action Error**	**HFE or Operator Action Error Source document (Screening Node and Error Type)**	**Location of detailed HEA Pro forma**
			(MLE)	
029	OPR-081	Operator erroneously allows IRWST boron concentration to decrease below limits	Systematic HEI Node 3 Passive Safety System (MLE)	HF Program for the UK UKP-GW-GL-042, Rev 1, Appendix C
030	OPR-082	Operator allows Level in the IRWST to decrease below limits	Systematic HEI Node 3 Passive Safety System (MLE)	HF Program for the UK UKP-GW-GL-042, Rev 1, Appendix C
031	OPR-084	Foreign material left in ADS lines following maintenance	Systematic HEI Node 3 Passive Safety System (MLE)	HF Program for the UK UKP-GW-GL-042, Rev 1, Appendix C
032	OPR-085 (OPR-107; OPR-112; OPR-113)	Operator leaves IRWST outlet valve closed	Systematic HEI Node 3 Passive Safety System (MLE)	HF Program for the UK UKP-GW-GL-042, Rev 1, Appendix C
	(OPR-091) OPR-009	PRHR Heat Exchanger becomes air-bound	Systematic HEI Node 3 Passive Safety System (MLE)	HF Program for the UK UKP-GW-GL-042, Rev 1, Appendix C
	(OPR-092) OPR-009	PRHR HX not vented or refilled following maintenance	Systematic HEI Node 3 Passive Safety System (MLE)	HF Program for the UK UKP-GW-GL-042, Rev 1, Appendix C
	(OPR-094) OPR-009	Opening of PRHR outlet manual isolation valve following system maintenance is omitted	Systematic HEI Node 3 Passive Safety System	HF Program for the UK UKP-GW-GL-042, Rev 1, Appendix C

APPENDIX 13A DETAILED-LEVEL HEA ACTIONS (cont.)

Screened-in Human Failure Events and Operator Action Errors with Detailed-Level Human Error Analysis Pro forma				
Serial No.	**Event ID**	**Human Failure Event or Operator Action Error**	**HFE or Operator Action Error Source document (Screening Node and Error Type)**	**Location of detailed HEA Pro forma**
			(MLE)	
	(OPR-095) OPR-009	PRHR inlet motor operated valve left closed following maintenance	Systematic HEI Node 3 Passive Safety System (MLE)	HF Program for the UK UKP-GW-GL-042, Rev 1, Appendix C
	(OPR-096) OPR-009	Maintenance error leads to failure of a PRHR air operated outlet isolation valves to open when required	Systematic HEI Node 3 Passive Safety System (MLE)	HF Program for the UK UKP-GW-GL-042, Rev 1, Appendix C
	(OPR-097) OPR-009	Operator inadvertently closes PRHR inlet MOV PXS-V101	Systematic HEI Node 3 Passive Safety System (MLE)	HF Program for the UK UKP-GW-GL-042, Rev 1, Appendix C
033	OPR-099	Operator incorrectly executes the CMT discharge valves operability test	Systematic HEI Node 5a Initiating Event Frequency (OIIE)	HF Program for the UK UKP-GW-GL-042, Rev 1, Appendix C
034	OPR-106	Maintenance error leads to failure of Recirculation squib valves	Systematic HEI Node 3 Passive Safety System (MLE)	HF Program for the UK UKP-GW-GL-042, Rev 1, Appendix C
	(OPR-107) OPR-085	PXS-V121A/B are left closed after maintenance	Systematic HEI Node 3 Passive Safety System (MLE)	HF Program for the UK UKP-GW-GL-042, Rev 1, Appendix C
035	OPR-109	IRWST level instrumentation miscalibrated or made inoperable, preventing automatic transfer to sump recirculation	Systematic HEI Node 3 Passive Safety System (MLE)	HF Program for the UK UKP-GW-GL-042, Rev 1, Appendix C

APPENDIX 13A DETAILED-LEVEL HEA ACTIONS (cont.)

Screened-in Human Failure Events and Operator Action Errors with Detailed-Level Human Error Analysis Pro forma				
Serial No.	**Event ID**	**Human Failure Event or Operator Action Error**	**HFE or Operator Action Error Source document (Screening Node and Error Type)**	**Location of detailed HEA Pro forma**
	(OPR-112) OPR-085	Maintenance error leading to Containment sump motor operated suction valves being left closed.	Systematic HEI Node 3 Passive Safety System (MLE)	HF Program for the UK UKP-GW-GL-042, Rev 1, Appendix C
	(OPR-113) OPR-085	Maintenance error leads to check valves in containment recirculation path being unable to open	Systematic HEI Node 3 Passive Safety System (MLE)	HF Program for the UK UKP-GW-GL-042, Rev 1, Appendix C
036	OPR-115 (OPR-116)	Maintenance leads to Passive containment cooling system (PCS) motor operated outlet valves left closed	Systematic HEI Node 3 Passive Safety System (MLE)	HF Program for the UK UKP-GW-GL-042, Rev 1, Appendix C
	(OPR-116) OPR-115	Maintenance leads to Passive containment cooling System air operated valves fail to open when demanded	Systematic HEI Node 3 Passive Safety System (MLE)	HF Program for the UK UKP-GW-GL-042, Rev 1, Appendix C
037	OPR-118 (OPR-121)	Failure to maintain PCS storage tank within required temperature band.	Systematic HEI Node 3 Passive Safety System (MLE)	HF Program for the UK UKP-GW-GL-042, Rev 1, Appendix C
	(OPR-121) OPR-118	Operator fails to maintain PCS storage tank above minimum level	Systematic HEI Node 3 Passive Safety System (MLE)	HF Program for the UK UKP-GW-GL-042, Rev 1, Appendix C
038	OPR-122 (OPR-123)	Maintenance error leads to inability to monitor PCS storage tank level	Systematic HEI Node 3 Passive Safety System (MLE)	HF Program for the UK UKP-GW-GL-042, Rev 1, Appendix C
	(OPR-123)	Calibration error leads to PCS failing to actuate	Systematic HEI	HF Program for the UK

APPENDIX 13A DETAILED-LEVEL HEA ACTIONS (cont.)

Screened-in Human Failure Events and Operator Action Errors with Detailed-Level Human Error Analysis Pro forma				
Serial No.	**Event ID**	**Human Failure Event or Operator Action Error**	**HFE or Operator Action Error Source document (Screening Node and Error Type)**	**Location of detailed HEA Pro forma**
	OPR-122	on high containment pressure via PMS	Node 3 Passive Safety System (MLE)	UKP-GW-GL-042, Rev 1, Appendix C
	(OPR-127) OPR-010	Operator leaves CMT isolated following maintenance	Systematic HEI Node 3 Passive Safety System (MLE)	HF Program for the UK UKP-GW-GL-042, Rev 1, Appendix C
039	OPR-129	CMT not vented or refilled following maintenance	Systematic HEI Node 3 Passive Safety System (MLE)	HF Program for the UK UKP-GW-GL-042, Rev 1, Appendix C
040	OPR-130	Improper Latching of a Fuel Assembly	Systematic HEI Node 3 Fuel handling (OIIE)	HF Program for the UK UKP-GW-GL-042, Rev 1, Appendix C
041	OPR-131	The operator Improperly Seats the Fuel Assembly Within the Core	Systematic HEI Node 3 Fuel handling (OIIE)	HF Program for the UK UKP-GW-GL-042, Rev 1, Appendix C
042	OPR-132	Foreign Material Left Behind in the Core	Systematic HEI Node 3 Fuel handling (MLE)	HF Program for the UK UKP-GW-GL-042, Rev 1, Appendix C
	(OPR-137) OPR-174	Improper maintenance leads to Pressuriser Code Safety Valve Failing to Lift at set point pressure	Systematic HEI Node 3 Passive Safety System (MLE)	HF Program for the UK UKP-GW-GL-042, Rev 1, Appendix C
043	OPR-138	Operator fails to maintain proper boron concentration in the PXS tanks	Systematic HEI Node 3 Passive Safety System (MLE)	HF Program for the UK UKP-GW-GL-042, Rev 1, Appendix C
044	OPR-142	Master Diverse Actuation System (DAS) Disable Switch for manual DAS actuation left	Systematic HEI Node 5b CDF increasing factor of	HF Program for the UK UKP-GW-GL-042, Rev 1, Appendix C

APPENDIX 13A DETAILED-LEVEL HEA ACTIONS (cont.)

Screened-in Human Failure Events and Operator Action Errors with Detailed-Level Human Error Analysis Pro forma				
Serial No.	**Event ID**	**Human Failure Event or Operator Action Error**	**HFE or Operator Action Error Source document (Screening Node and Error Type)**	**Location of detailed HEA Pro forma**
		in disable position	DiD system (MLE)	
045	OPR-144	Operator fails to return a DAS function to its normal, ready configuration following Channel Operational Testing or Channel Calibration	Systematic HEI Node 5b CDF increasing factor of DiD system (MLE)	HF Program for the UK UKP-GW-GL-042, Rev 1, Appendix C
046	OPR-174 (OPR-137)	Maintenance error results in PZR Safety Valve incorrect opening set point (valve opens prematurely)	Systematic HEI (Node 2 CDF risk increase >1%) (MLE)	HF Program for the UK UKP-GW-GL-042, Rev 1, Appendix C
047	ATW-MAN11	Operator fails to Recognise the Need for Manual Boration	PSA Update UKP-GW-GLR-102 (Node 2 CDF risk increase >1%)	HF Safety Case as reflecting the PSA Update UKP-GW-GL-069, Rev 0, Section 6
048	CVN-MAN02	Operator fails to Align Chemical and Volume Control System	PSA Update UKP-GW-GLR-102 (Node 2 CDF risk increase >1%)	HF Safety Case as reflecting the PSA Update UKP-GW-GL-069, Rev 0, Section 6
049	HPM-MAN01	Operator fails to Diagnose Need for High Pressure Heat Removal	PSA Update UKP-GW-GLR-102 (Node 2 CDF risk increase >1%)	HF Safety Case as reflecting the PSA Update UKP-GW-GL-069, Rev 0, Section 6
050	PRI-MAN01	Operator fails to Isolate Failed Passive Residual Heat Removal Heat Exchanger	PSA Update UKP-GW-GLR-102 (Node 2 CDF risk increase >1%)	HF Safety Case as reflecting the PSA Update UKP-GW-GL-069, Rev 0, Section 6
051	PRN-MAN01	Operator fails to Align Passive Residual Heat Removal System	PSA Update UKP-GW-GLR-102 (Node 2 CDF risk increase >1%)	HF Safety Case as reflecting the PSA Update UKP-GW-GL-069, Rev 0, Section 6

APPENDIX 13A DETAILED-LEVEL HEA ACTIONS (cont.)

Screened-in Human Failure Events and Operator Action Errors with Detailed-Level Human Error Analysis Pro forma				
Serial No.	**Event ID**	**Human Failure Event or Operator Action Error**	**HFE or Operator Action Error Source document (Screening Node and Error Type)**	**Location of detailed HEA Pro forma**
052	PRN-MAN02	Operator fails to Align Passive Residual Heat Removal System	PSA Update UKP-GW-GLR-102 (Node 2 CDF risk increase >1%)	HF Safety Case as reflecting the PSA Update UKP-GW-GL-069, Rev 0, Section 6
053	PRN-MAN03	Operator fails to Align/Control Passive Residual Heat Removal System Operation	PSA Update UKP-GW-GLR-102 (Node 2 CDF risk increase >1%)	HF Safety Case as reflecting the PSA Update UKP-GW-GL-069, Rev 0, Section 6
054	CRDET	Control room operators fail to respond to the fire protection system alarms and notify	Fire PSA (Chapter 56) APP-GW-GL-022 (Node 2 Fire or Flood)	HF Safety Case as reflecting the Fire/Flood PSA UKP-GW-GL-070, Rev 0, Section 4
055	FLISM	Auxiliary personnel fail to isolate or mitigate the flood	Flood PSA (Chapter 57) APP-GW-GL-022 (Node 2 Fire or Flood)	HF Safety Case as reflecting the Fire/Flood PSA UKP-GW-GL-070, Rev 0, Section 4
056	OPA-01	Operator fails to deactivate the PMS division involved in a fire	Fire PSA (Chapter 56) APP-GW-GL-022 (Node 2 Fire or Flood)	HF Safety Case as reflecting the Fire/Flood PSA UKP-GW-GL-070, Rev 0, Section 4
057	OPA-02	Operator fails to open manual valve to sprinklers in containment	Fire PSA (Chapter 56) APP-GW-GL-022 (Node 2 Fire or Flood)	HF Safety Case as reflecting the Fire/Flood PSA UKP-GW-GL-070, Rev 0, Section 4
058	SGCCR	Security guard fails to call control room personnel	Flood PSA (Chapter 57) APP-GW-GL-022 (Node 2 Fire or Flood)	HF Safety Case as reflecting the Fire/Flood PSA UKP-GW-GL-070, Rev 0, Section 4
059	SGDTM	Security guard fails to diagnose that water is	Flood PSA (Chapter 57)	HF Safety Case as reflecting the

APPENDIX 13A DETAILED-LEVEL HEA ACTIONS (cont.)

Screened-in Human Failure Events and Operator Action Errors with Detailed-Level Human Error Analysis Pro forma				
Serial No.	**Event ID**	**Human Failure Event or Operator Action Error**	**HFE or Operator Action Error Source document (Screening Node and Error Type)**	**Location of detailed HEA Pro forma**
		leaking and fails to mitigate by opening the annex building front door	APP-GW-GL-022 (Node 2 Fire or Flood)	Fire/Flood PSA UKP-GW-GL-070, Rev 0, Section 4
060	LPM-MAN05	Operator fails to Recognise the Need for Reactor Coolant System Depressurisation	Low Power & Shutdown PSA (Chapter 54) APP-GW-GL-022	HF Safety Case as reflecting the Low Power & Shutdown PSA UKP-GW-GL-071, Section 5
061	REN-MAN02	Operator fails to Initiate Recirculation during LOCA	Low Power & Shutdown PSA (Chapter 54) APP-GW-GL-022	HF Safety Case as reflecting the Low Power & Shutdown PSA UKP-GW-GL-071, Section 5
062	RHN-MAN02/03	Operator fails to Align Normal Residual Heat Removal System	Low Power & Shutdown PSA (Chapter 54) APP-GW-GL-022	HF Safety Case as reflecting the Low Power & Shutdown PSA UKP-GW-GL-071, Section 5
063	RHN-MAN04	Operator fails to Isolate the RNS During Shutdown Conditions	Low Power & Shutdown PSA (Chapter 54) APP-GW-GL-022	HF Safety Case as reflecting the Low Power & Shutdown PSA UKP-GW-GL-071, Section 5
064	RHN-MAN05	Operator fails to Initiate Gravity Injection from IRWST via RNS Suction Line	Low Power & Shutdown PSA (Chapter 54) APP-GW-GL-022	HF Safety Case as reflecting the Low Power & Shutdown PSA UKP-GW-GL-071, Section 5
065	ZON-MAN01	Operator fails to Start the Onsite Standby Diesel Generator	Low Power & Shutdown PSA (Chapter 54) APP-GW-GL-022	HF Safety Case as reflecting the Low Power & Shutdown PSA UKP-GW-GL-071, Section 5
066	OPR-093	Maintenance error leads to inability to open RNS Isolation Valves	Systematic HEI Node 5b CDF increasing factor of	HF Safety Case as reflecting the Low Power & Shutdown PSA UKP-GW-

APPENDIX 13A DETAILED-LEVEL HEA ACTIONS (cont.)

Screened-in Human Failure Events and Operator Action Errors with Detailed-Level Human Error Analysis Pro forma				
Serial No.	**Event ID**	**Human Failure Event or Operator Action Error**	**HFE or Operator Action Error Source document (Screening Node and Error Type)**	**Location of detailed HEA Pro forma**
			DiD system (MLE)	GL-071, Section 5
067	OPR-149	Improper RNS Valve Alignment when Restoring Spent Fuel Pool System (SFS) cooling	Systematic HEI Node 5b CDF increasing factor of DiD system (MLE)	HF Safety Case as reflecting the Low Power & Shutdown PSA UKP-GW-GL-071, Section 5
068	OPR-158	Calibration error allows CVS let down to lower level below mid-loop resulting in a loss of RNS	Systematic HEI Node 5b CDF increasing factor of DiD system (MLE)	HF Safety Case as reflecting the Low Power & Shutdown PSA UKP-GW-GL-071, Section 5
069	OPR-104	Operator improperly aligns Gaseous Waste System (WGS) vent and drain valves during valve line ups	(Composite Fault List PCSR Ch. 8) Non-Core Damage Human Errors with possible Radioactive Release UKP-GW-GL-073 (OIIE)	HF Safety Case – Additional UK Fault Schedule Faults UKP-GW-GL-075 Section 5.2
070	OPR-105	Miscalibration of plant stack radiation monitor	(Composite Fault List PCSR Ch. 8) Non-Core Damage Human Errors with possible Radioactive Release UKP-GW-GL-073 (MIIE)	HF Safety Case – Additional UK Fault Schedule Faults UKP-GW-GL-075 Section 5.2
071	OPR-108	Incorrect alignment of Liquid Waste System (WLS) vent and drain valves	(Composite Fault List PCSR Ch. 8) Non-Core Damage Human Errors with possible Radioactive Release UKP-GW-GL-073 (MIIE)	HF Safety Case – Additional UK Fault Schedule Faults UKP-GW-GL-075 Section 5.2
072	OPR-110	Misoperation of the Liquid Radwaste discharge valve V223	(Composite Fault List PCSR Ch. 8) Non-Core Damage Human Errors with possible Radioactive Release UKP-GW-GL-073 (OIIE)	HF Safety Case – Additional UK Fault Schedule Faults UKP-GW-GL-075 Section 5.2

APPENDIX 13A DETAILED-LEVEL HEA ACTIONS (cont.)

Screened-in Human Failure Events and Operator Action Errors with Detailed-Level Human Error Analysis Pro forma				
Serial No.	**Event ID**	**Human Failure Event or Operator Action Error**	**HFE or Operator Action Error Source document (Screening Node and Error Type)**	**Location of detailed HEA Pro forma**
073	OPR-111	Calibration of Liquid Radwaste Discharge Radiation Monitor (RE229)	(Composite Fault List PCSR Ch. 8) Non-Core Damage Human Errors with possible Radioactive Release UKP-GW-GL-073 (OIIE)	HF Safety Case – Additional UK Fault Schedule Faults UKP-GW-GL-075 Section 5.2
074	OPR-193	Failure to recognise high tank level (Liquid Waste) and stop transfer pump operation.	(Composite Fault List PCSR Ch. 8) Non-Core Damage Human Errors with possible Radioactive Release UKP-GW-GL-073 (OIIE)	HF Safety Case – Additional UK Fault Schedule Faults UKP-GW-GL-075 Section 5.2
075	OPR-204	Operator places fuel assembly in wrong core location	(Composite Fault List PCSR Ch. 8) Additional UK Fault Schedule Faults UKP-GW-GL-075 (OIIE)	HF Safety Case – Additional UK Fault Schedule Faults UKP-GW-GL-075 Section 5.1
076	OPR-209	Polar Crane operator violates safe load path and inadvertently drops heavy load onto top of the core resulting in core damage	(Composite Fault List PCSR Ch. 8) Additional UK Fault Schedule Faults UKP-GW-GL-075 (OIIE)	HF Safety Case – Additional UK Fault Schedule Faults UKP-GW-GL-075 Section 5.1
077	OPR-210	Polar Crane fails following "two-blocking" event with heavy load drop onto reactor core	(Composite Fault List PCSR Ch. 8) Additional UK Fault Schedule Faults UKP-GW-GL-075 (OIIE)	HF Safety Case – Additional UK Fault Schedule Faults UKP-GW-GL-075 Section 5.1
078	OPR-213	Improper latching of fuel assembly results in dropped fuel in spent fuel pool	(Composite Fault List PCSR Ch. 8) Additional UK Fault Schedule Faults UKP-GW-GL-075 (OIIE)	HF Safety Case – Additional UK Fault Schedule Faults UKP-GW-GL-075 Section 5.1

APPENDIX 13B COGNITIVE HEA-LEVEL ACTIONS

Sample Human Failure Events and Operator Action Errors with Cognitive-Level Human Error Analysis Pro forma				
Serial #	**Event ID**	**Human Failure Event or Operator Action Error**	**Human Error Identification Source**	**Location of cognitive error HEA Pro forma**
01	BDB-005*	Operators provide makeup to the PCCWST and SFP from the PCCAWST with the offsite pump	BDB Long-Term Coping Strategy UKP-GW-GGR-201	UK AP1000 Plant Post-Fukushima Assessment UKP-GW-GGR-201
02	BDB-006*	Operators provide makeup to the SFP by gravity drain from the PCCWST	BDB Long-Term Coping Strategy UKP-GW-GGR-201	UK AP1000 Plant Post-Fukushima Assessment UKP-GW-GGR-201
03	HEPE-PCS-XVM-CL-V023	PCS manual valve PCS-PL-V023 unintentionally left closed. (Type-A MLE)	AP1000 Plant PSA Human Reliability Analysis Guidebook APP-PSA-GM-005, Rev B.	UK AP1000 HF Qualitative Error Analysis UKP-GW-GL-126
04	HEPO-ADS4-C1	Operator fails to depressurise the RCS with ADS stage 4 on low CMT level	AP1000 Plant PSA Human Reliability Analysis Guidebook APP-PSA-GM-005, Rev B.	UK AP1000 HF Qualitative Error Analysis UKP-GW-GL-126
05	HEPO-COG-CONT	Operator fails to diagnose high containment pressure	AP1000 Plant PSA Human Reliability Analysis Guidebook APP-PSA-GM-005, Rev B.	HF Qualitative Assessment of the HF-01 Sample UKP-GW-GL-126
06	HEPO-COG-CORECOOLING	Operator fails to diagnose inadequate core cooling (post core damage)	AP1000 Plant PSA Human Reliability Analysis Guidebook APP-PSA-GM-005, Rev B.	UK AP1000 HF Qualitative Error Analysis UKP-GW-GL-126
07	HEPO-FI-ADSDIS	Operator fails to open breakers to prevent spurious ADS Stage 4 actuation	Fire PSA	UK AP1000 HF Qualitative Error Analysis UKP-GW-GL-126
08	HEPO-FI-MCREVAC	Main control room evacuation due to fire	Fire PSA	UK AP1000 HF Qualitative Error Analysis UKP-GW-GL-126

APPENDIX 13B COGNITIVE HEA-LEVEL ACTIONS (cont.)

Sample Human Failure Events and Operator Action Errors with Cognitive-Level Human Error Analysis Pro forma				
Serial #	**Event ID**	**Human Failure Event or Operator Action Error**	**Human Error Identification Source**	**Location of cognitive error HEA Pro forma**
09	HEPO-INJ	Operator fails to actuate IRWST injection	AP1000 Plant PSA Human Reliability Analysis Guidebook APP-PSA-GM-005, Rev B.	UK AP1000 HF Qualitative Error Analysis UKP-GW-GL-126
10	HEPO-L2-CAVFLD	Operator fails to flood RV cavity for IVR on loss of core cooling cue. (post core damage)	AP1000 Plant PSA Human Reliability Analysis Guidebook APP-PSA-GM-005, Rev B.	UK AP1000 HF Qualitative Error Analysis UKP-GW-GL-126
11	HEPO-L2-CNT	Operator fails to manually isolate containment (post core damage)	AP1000 Plant PSA Human Reliability Analysis Guidebook APP-PSA-GM-005, Rev B.	UK AP1000 HF Qualitative Error Analysis UKP-GW-GL-126
12	HEPO-L2-H2I	Operator fails to manually actuate hydrogen ignitors (post core damage)	AP1000 Plant PSA Human Reliability Analysis Guidebook APP-PSA-GM-005, Rev B.	UK AP1000 HF Qualitative Error Analysis UKP-GW-GL-126
13	HEPO-OFILL	Operator fails to isolate ruptured SG (on High-3 NR SG level—PMS backup)	AP1000 Plant PSA Human Reliability Analysis Guidebook APP-PSA-GM-005, Rev B.	UK AP1000 HF Qualitative Error Analysis UKP-GW-GL-126
14	HEPO-PRHR-GT	Operator fails to actuate PRHR during an event without a Safeguards signal	AP1000 Plant PSA Human Reliability Analysis Guidebook APP-PSA-GM-005, Rev B.	UK AP1000 HF Qualitative Error Analysis UKP-GW-GL-126
15	HEPO-RNSINJ	Operator fails to align RNS for injection	AP1000 Plant PSA Human Reliability Analysis Guidebook APP-PSA-GM-005, Rev B.	UK AP1000 HF Qualitative Error Analysis UKP-GW-GL-126
16	HEPO-RRWSTISO	Operator fails to isolate IRWST recirculation following spurious recirculation actuation	AP1000 Plant PSA Human Reliability Analysis Guidebook APP-PSA-GM-	UK AP1000 HF Qualitative Error Analysis

APPENDIX 13B COGNITIVE HEA-LEVEL ACTIONS (cont.)

Sample Human Failure Events and Operator Action Errors with Cognitive-Level Human Error Analysis Pro forma				
Serial #	**Event ID**	**Human Failure Event or Operator Action Error**	**Human Error Identification Source**	**Location of cognitive error HEA Pro forma**
			005, Rev B.	UKP-GW-GL-126
17	OPR-011	Maintenance error leads to failure of ADS Stage 4 and IRWST gravity injection squib valves (Type-A MLE)	Systematic HEI Node 3 Passive Safety System	UK AP1000 HF Qualitative Error Analysis UKP-GW-GL-126
18	OPR-099	Operator incorrectly executes the CMT discharge valves operability test (Type-B OIIE)	Systematic HEI Node 5a Initiating Event Frequency	UK AP1000 HF Qualitative Error Analysis UKP-GW-GL-126
19	OPR-106	Maintenance error leads to failure of recirculation squib valves (Type-A MLE)	Systematic HEI Node 3 Passive Safety System	UK AP1000 HF Qualitative Error Analysis UKP-GW-GL-126
20	OPR-131	Operator improperly seats the fuel assembly within the core (Type-B OIIE)	Systematic HEI Node 3 Fuel handling	UK AP1000 HF Qualitative Error Analysis UKP-GW-GL-126

APPENDIX 13C COGNITIVE-HEA ACTIONS SUMMARY SCHEDULE

Human Error Analysis Sample - Summary Schedule	
Human Action Identifier	**BDB-005**
Location (s) of Action	This is a manual valve lineup that will be performed at several locations. Room 00304, Room 00371 Room 12213, Room 12211 Room 12306, Room 12354, Room 12351
Person(s) Performing Action	Licensed Reactor Operator 1 Local Equipment (auxiliary) Operator
Task	Operator conducts post-72 hour operation of Containment Cooling
Tools/Equipment	PCCWST level, PCS-LT010/011 PCCAWST level, PCS-LT037 SFP Level, SFS-LT019B/C SFP Emergency Makeup Flow rate, PCS-FIT039 PCS Recirculation Pump Discharge Flow rate, PCS-FIT030
SSC	Passive Containment Cooling System (PCS) Spent Fuel Pool (SFP)
Error Description	Operator fails to refill the PCCWST and / or the SFP or fails to adjust flow to the containment distribution buckets.
Performance Shaping Factors	Training Communication Availability of tools

APPENDIX 13C COGNITIVE-HEA ACTIONS SUMMARY SCHEDULE (cont.)

Human Error Analysis Sample - Summary Schedule	
Error Mechanism	Communication errors; these will be combated by the use of 3 way communication and reinforced with training. Local operators may feel under pressure to establish PCCWST and SFP makeup quickly if site clearance and arrival of the temporary pump were delayed, resulting in missing or short-cutting PCS component alignment precondition checks prior to connecting and starting pump. However, this assessment assumes that the offsite equipment arrives within 24 hours, and given that there will be enough people to handle the high workload of site clean-up and recovery, it is not expected that there will be motivation to take short cuts.
Consequence	Failure of Containment Cooling
Recovery	There are no procedural based recovery opportunities due to the simple nature of the actions required of the operators. However, suction and discharge hose connection failure would likely be revealed immediately to local operator in vicinity of temporary pump with recovery opportunity before pump damage or containment and/or SFP overheating. The failure to establish flow due to PCS component alignment may not be revealed until PCCWST level low indications and established in time before containment and SFP temperature rise
Error Likelihood	The likelihood of unrecovered error is considered to be low, given the assumptions made in the assessment. The action consists of simple, manual tasks, the operators conducting the task will have clear objectives and procedures, have plenty of time, and will not have high workload. This action is judged to be feasible and likely to be performed successfully. The operators will have been trained on and know how to operate the equipment needed to complete this action. The procedures are straight forward. Given the assumptions made in this assessment, it is expected that operators will be able to complete this task successfully. It is assumed that offsite equipment will arrive in a timely manner, the plant is able to clear a path to the PCCAWST and the connection flanges, there is sufficient SQEP to perform the task, that the operators will have clear objectives and procedures, and that there is enough time to complete this action.
Corrective Action / Recommendation	1) Supply two hoses with the off-site pump. One terminating at both ends with male connectors and one terminating at both ends with female connectors. Then make the PCCAWST outlet and pump suction connectors both male and the Pump discharge and Class 1 PCS flange both female. Hoses cannot then be cross-connected. 2) The specification of the self-powered, off-site pump should include a requirement for local panel and connection task-lighting to reduce risk of error in night-time operation.

Human Action Identifier	BDB-006
Location (s) of Action	This is a manual valve line up that will be performed at several locations. Room 12351, Room 12701, Room 12553,
Person(s) Performing Action	Local Equipment (auxiliary) Operator
Task	Operator makes up to the SFP by gravity drain from the PCCWST
Tools/Equipment	SFS-LT019B (SFP Lvl B) SFS-LT019C (SFP Lvl C)
SSC	Passive Containment Cooling System (PCS) Spent Fuel Pool (SFP) Passive Containment Cooling Water Storage Tank (PCCWST)
Error Description	Failure to refill the spent fuel pool post 72 hours
Performance Shaping Factors	HSI Design; Training; Communication; Stress; Time Pressure
Error Mechanism	Communication errors; these will be combated by the use of 3 way communication and reinforced with training.
Consequence	Inadequate mass of water in SFP. Failure of proper MCR communication with LO could lead to uncovering of fuel in the SFP.
Recovery	There are no procedural based recovery opportunities due to the simple nature of the task required of the operators. There are two knowledge based recovery opportunities that could occur at the end of this action; there is a flow indicator after valve V0045, which, if the operator checks, could indicate insufficient/no flow or, the MCR crew could notice the level changes of the PCCWST and/or SFP are not what is expected with successfully established flow.
Error Likelihood	The likelihood of unrecovered error is considered to be low, given the assumptions made in the assessment. The action consists of simple, manual tasks, the operators conducting the task will have clear objectives and procedures, have plenty of time, and will not have high workload. This action is judged to be feasible and likely to be performed successfully. The operators will have been trained on and know how to operate the equipment needed to complete this action. The procedures are straight forward. Given the assumptions made in this

APPENDIX 13C COGNITIVE-HEA ACTIONS SUMMARY SCHEDULE (cont.)

Human Error Analysis Sample - Summary Schedule	
	assessment, it is expected that operators will be able to complete this task successfully.
Corrective Action / Recommendation	To reduce the risk to operators in navigating to room 12701, the procedure will be updated to provide alternative means of directing operators to take certain routes from room 12351 to room 12701 during a SBO.
Human Action Identifier	**HEPE-PCS-XVM-CL-V023**
Location (s) of Action	Valve/Piping Penetration Room 12306
Person(s) Performing Action	Local Equipment (auxiliary) Operator
Task	Operators complete a valve cycling test of the PCS Manual Valve PCS-PL-V023 (Recirculation Return Isolation)
Tools/Equipment	PCS-FT030
SSC	Passive Containment Cooling System (PCS)
Error Description	PCS Manual Valve PCS-V023 unintentionally left closed.
Performance Shaping Factors	HSI Design Training Task Complexity Procedures
Error Mechanism	Population stereotypes dictate the expectancies of certain control behaviours (e.g., one expects that when a valve is turned counter clockwise, flow will increase). Violating population stereotypes can lead to errors. The valves will be controlled based on population stereotypes, and any plant worker dispatched to align valves will be trained in their operation. Retention of motor skills is influenced by several factors associated with practice including amount of practice and practice schedule; the AO will be well practiced in opening valves.

APPENDIX 13C COGNITIVE-HEA ACTIONS SUMMARY SCHEDULE (cont.)

Human Error Analysis Sample - Summary Schedule	
	Manual control issues will be reduced by designing the valves to be opened within the human physiological limitations or providing tools to do so. The valves involved in this action are manual valves and thus designed to be operated manually. There is no time pressure and the tasks are simple (open/close manual valves).
Consequence	If the recirculation isolation valve is closed no recirculation is possible (chemistry concern). Failure to open valve PCS-PL-V023 would result in the inability to recirculate through the 2 recirculation pumps (PCS-MP 01A and PCS-MP 01B), recirculation heater (PCS-MB 01), and chemical addition tank (PCS-MT 02), removing an alternate source for PCS cooling to the PCS distribution bucket.
Recovery	The auxiliary operator could identify that the valve PCS-PL-V023 was unintentionally left in closed position when initialling on Passive Containment Cooling System Valve Stroke Test (APP-PCS-GJP-806) Attachment 2 step 5.11 that the valve PCS-PL-V023 was opened. The auxiliary operator could identify that the valve PCS-PL-V023 was unintentionally left in closed position when initialling and circling it is open on Passive Containment Cooling System Valve Stroke Test (APP-PCS-GJP-806) Attachment 5 regarding step 5.11 that the valve PCS-PL-V023 is open. The independent verifier could identify that the valve PCS-PL-V023 was unintentionally left in closed position when initialling on Passive Containment Cooling System Valve Stroke Test (APP-PCS-GJP-806) Attachment 2 step 5.11 that the valve PCS-PL-V023 was opened. Step 5.18 for procedure APP-PCS-GJP-806 requires the PCCWST be placed in recirculation via procedure APP-PCS-GJP-101, which requires the starting up of the recirculation pumps (PCS-MP 01A and PCS-MP 01B), which would result in a low flow indication from APP-PCS-FT-030, which would cause an automatic trip of the recirculation pumps and heater (PCS-MB 01) to prevent damage. An auxiliary operator would be dispatched to identify any valves out of normal position.
Error Likelihood	This is a routine action that the AOs will perform hundreds of times. Provided the AOs are following procedures as they are required to do, they will be initialling and having an independent verifier initialling that the valve PCS-PL-V023 is left open at the ending of the procedure, a low workload, and they have been trained to test valves, it is expected that operators will be able to complete this task successfully. The likelihood of unrecovered error of this action is very low. See Chapter 10 for the PSA quantification of the HEP for this action.

APPENDIX 13C COGNITIVE-HEA ACTIONS SUMMARY SCHEDULE (cont.)

Human Error Analysis Sample - Summary Schedule	
Corrective Action / Recommendation	None
Human Action Identifier	**HEPO-ADS4-C1**
Location (s) of Action	Main Control Room (MCR)
Person(s) Performing Action	Main Control Room Crew
Task	Operator depressurises the RCS using the ADS Stage 4 valves.
Tools/Equipment	RCS-V004A/B/C/D
SSC	Reactor Coolant System (RCS)
Error Description	Operator fails to depressurise the RCS with the ADS Stage 4 on low CMT level.
Performance Shaping Factors	Procedures; Training; HSI Design; Task Complexity; Attention
Cognitive Processes	Detect CMT Narrow Range Level (less than 61.9%). Understand the significance of the CMT Narrow Range Level. Detect that ADS stage 4 has not actuated automatically. Understand the significance of ADS Stage 4 not actuating. Determine the correct actions to take in this situation. Actuate ADS Stage 4 using manual back-up PMS switches.
Consequence	The purpose of opening the ADS stage 4 valves is to depressurise the RCS sufficiently to allow for gravity injection of the IRWST. With only the stage 1 to 3 valves open the RCS pressures may be too high to support gravity injection. If ADS stage 4 is not successfully actuated within the 15-minute time window, irreversible core damage is expected to happen at 36 minutes after the cue.

APPENDIX 13C COGNITIVE-HEA ACTIONS SUMMARY SCHEDULE (cont.)

Human Error Analysis Sample - Summary Schedule	
Recovery	There is a CMT lower narrow range level alarm on PMS if the operator fails to see the cue of low CMT level. Operators may diagnose why cooling does not happen at the expected rate and realise that ADS stage 4 has not been actuated. At that time the action can be completed
Error Likelihood	This assessment indicates that this action is feasible within the PSA time window. It is not likely that errors will occur as the operators are trained in this scenario, the interface provides cues, alarms, and indications that are clear and unambiguous, the task steps are clearly guided by procedures, and the procedures are assessed to be of high quality. The likelihood of unrecovered failure of this action is low; see Chapter 10 for the PSA quantification of the HEP for this action.
Corrective Action / Recommendation	None aside from resolution of HED issues associated with this action.
Human Action Identifier	**HEPO-COG-CONT**
Location (s) of Action	MCR
Person(s) Performing Action	MCR crew
Task	Operator diagnoses high containment pressure when the pressure reaches or exceeds 59 PSIG.
Tools/Equipment	PCS-PT005, PCS-PT006, PCS-PT007, PCS-PT008 PCS-PT012, PCS-PT013, PCS-PT014
SSC	PCS
Error Description	Operator fails to diagnose high containment pressure when the pressure reaches or exceeds 59 PSIG.
Performance Shaping Factors	Procedures Training HSI Design

APPENDIX 13C COGNITIVE-HEA ACTIONS SUMMARY SCHEDULE (cont.)

Human Error Analysis Sample - Summary Schedule	
	Task Complexity Attention Stress Staff Structure
Cognitive Processes	Detection, recognition and understanding of the containment pressure alarms, diagnosing high containment pressure.
Consequence	There will be no consequences unless PMS and DAS also fail, as either PMS or DAS will actuate Containment Cooling
Recovery	There is an alarm High-2 Containment pressure when the pressure reaches 6.2 psig, There are four (PCS-PT005/6/7/8) priority alarms and the outlet valves to the Passive Containment Cooling Water Storage Tank (PCCWST) will automatically open. In addition there will be peer checks.
Error Likelihood	Unrecovered failure of this action is considered very unlikely. It is unlikely that the operator will either fail to detect high containment pressure, nor understand the significance as the containment pressure and the status of the Containment CSF is present on many interfaces including the WPIS. In addition, procedures guide the operator to look for and assess this parameter, procedural adherence is a requirement, the operator is trained to diagnose high containment pressure, and the monitoring of the critical safety functions is likely to be the dedicated task of the STA. Peer checking will add another line of defence. See PCSR Chapter 10 for the PSA quantification of the HEP for this action.
Corrective Action / Recommendation	None
Human Action Identifier	**HEPO-COG-CORE COOLING**
Location (s) of Action	MCR
Person(s) Performing Action	MCR Crew

APPENDIX 13C COGNITIVE-HEA ACTIONS SUMMARY SCHEDULE (cont.)

Human Error Analysis Sample - Summary Schedule	
Task	Diagnosis of inadequate core cooling in a large loss of coolant (LOCA) accident scenario.
Tools/Equipment	5th hottest CETs (Red and Orange path) Sub-Cooling Margin (Orange path)
SSC	Reactor System (RXS)
Error Description	Operator fails to diagnose inadequate core cooling
Performance Shaping Factors	Procedures; Training; Staff Structure; HSI design; Task Complexity; Attention ;Stress
Cognitive Processes	Detection of CET, understanding of what high CET means, diagnosis of inadequate core cooling
Consequence	Core cooling is required to prevent core damage. The consequence of the operator failing to diagnose inadequate core cooling is that they would not enter procedure FR-C.1 "Response to Inadequate Core Cooling". This could mean that actions in FR-C.1 may not be implemented (e.g., turning on the hydrogen igniters or flooding the reactor cavity). This could lead to a reactor vessel failure and a molten core concrete interaction
Recovery	This is a time sensitive action. Completing this action after the available time window may not be effective but will not have a negative impact.
Error Likelihood	Having considered the potential errors, it is considered NOT likely that this action would fail. It is directed by procedures in a rigorous fashion and the task is a fundamental part of the operators' training. Clear indications are present on the interface, and the STA is dedicated to the task of monitoring the CSFs. See Chapter 10 for the PSA quantification of the HEP for this action.
Corrective Action / Recommendation	Further research should be conducted to determine if it is beneficial to provide a means of alerting the operators to a recent red path condition on the critical safety function trees, which may have reverted back to an orange path. This would beneficial to alleviate the possibility in which the plant conditions could oscillate, across the boundary, of a red and orange path, before an operator notices. However care must be taken to ensure a solution does not create worse errors.

APPENDIX 13C COGNITIVE-HEA ACTIONS SUMMARY SCHEDULE (cont.)

Human Error Analysis Sample - Summary Schedule	
	Resolution of HED issues associated with this action.
Human Action Identifier	**HEPO-F1-ADSDIS**
Location (s) of Action	Auxiliary Building I&C Room 12213
Person(s) Performing Action	Equipment (auxiliary) operators
Task	Operator opens breakers to prevent spurious ADS Stage 4 actuation. A fire in a PMS Division cabinet in one of the Class 1E I&C Rooms requires that the Operator takes action to remove power from the safeguards actuation circuits to prevent spurious actuation of the Stage 4 Automatic Depressurisation System (ADS) Squib Valves.
Tools/Equipment	ECS-EC-121-2M (Div A Battery Charger Bkr) ECS-EC-121-2C (Div A Regulating Xfmr Bkr)
SSC	Main AC Power System (ECS) Fire Protection System (FPS) PMS
Error Description	Failure to remove power to the affected PMS Division I&C cabinet through de-energising the battery bus by isolating the batteries and isolating the affected I&C cabinets.
Performance Shaping Factors	Audible and visual Fire Alarm cues in the MCR Symptom-based Fire Response procedures presented on CPS Communication between MCR crew and Auxiliary Operators
Cognitive Processes	Correctly read Fire panel. Execute desired action correctly communicate correct fire location. Information recall – working memory and attention – Step 7 - Implement the correct attachment for fire response.

APPENDIX 13C COGNITIVE-HEA ACTIONS SUMMARY SCHEDULE (cont.)

Human Error Analysis Sample - Summary Schedule	
	Team communication –Local (auxiliary) operators correctly perceive information from MCR about breaker location or identification Execute required response/action – Local (auxiliary) operators open the correct breakers
Consequence	The consequence of failure to de-energise a PMS Division ADS4 cabinet within 30 minutes of a fire in an I&C room is the possibility of spurious actuation of the ADS4 Squib Valves. However this would require that fire-induced hot shorts generate sequential 'arming' and 'firing' signals, emanating from separate I&C cabinets, within a short time-window (i.e., if a 'firing' signal does not follow 'arming' signal within a certain time then the system will 're-set', requiring that another, time-dependant, sequential arming and firing signal sequence is spuriously generated).
Recovery	Failure in the MCR to communicate to site and to the fire brigade the correct area/zone or room affected by a fire may first be revealed to them by local site personnel who are evacuating or by first-responders attending the area/zone or room reporting that no fire is evident. Failure of the local (auxiliary) operators to open the correct breakers for the fire affected Division PMS cabinet would be revealed primarily by the relevant Division safety display monitor on the PDSP in the MCR not going dark and no audible and visual PMS alarm on the APS as expected. There is also likely to be an unexpected alarm coincident with the local (auxiliary) operators reporting the breakers open.
Error Likelihood	The likelihood of unrecovered failure of this action is considered to be very low. See Chapter 10 for the PSA quantification of the HEP for this action.
Corrective Action / Recommendation	1) Reinstate manual reactor trip in Revision 3 of AOP-305 2) The list of rooms on pages 2-3 of Attachment 2 AOP-305 (Rev 2) are presented sequentially (except for the 50xxx rooms that appear in the middle of the list of 40xxx rooms) in 4 columns. Each column extends over both pages. Normal reading and page scanning expectation is to go from top to bottom of column 1 on page 1 and then to top of column 2 on page 1, etc. Currently, Attachment 2 lists the room numbers and attachment cross-reference sequentially in columns from top of column 1 on page 1 to the bottom of column 1 on page 2 and back to the top of column 2 on page 1, etc. Presentation of look-up tables in this way increases search times for the attachment cross-reference and the probability of making cross-referencing errors.

APPENDIX 13C COGNITIVE-HEA ACTIONS SUMMARY SCHEDULE (cont.)

Human Error Analysis Sample - Summary Schedule	
	Resolution of HED issues associated with ISV Scenario 5 OPA-1 action
Human Action Identifier	**HEPO-FI-MCREVAC**
Location (s) of Action	MCR (Fire Zone 1242 AF 01).
Person(s) Performing Action	MCR Crew
Task	Main control room evacuation due to fire Temporary evacuation of the Main Control Room (MCR) is required because the outbreak of a fire and smoke in the MCR is making the MCR uninhabitable. The operators evacuate to the Remote Shutdown Workstations (RSW) located in the Remote Shutdown Room (RSR) on the floor below to establish and maintain safe shutdown conditions until the MCR can be made habitable again.
Tools/Equipment	RSW Transfer Switch Panel Self -Contained Breathing Apparatus (SCBA) can prolong the time available to operators to conduct operations in the MCR before becoming uninhabitable.
SSC	Operation and Control Centres System (OCS)
Error Description	Failure to evacuate MCR and transfer control to the RSR to establish and maintain safe shutdown.
Performance Shaping Factors	Human System Interface and System Response Workplace and Workstation Adequacy Training Task and Work Load
Cognitive Processes	Detect fire/smoke in the MCR, understand its significance, knowledge of procedure to follow, follow procedure
Consequence	Reactor at power with no one in the control room.
Recovery	Reactor can be tripped from RSR.

APPENDIX 13C COGNITIVE-HEA ACTIONS SUMMARY SCHEDULE (cont.)

Human Error Analysis Sample - Summary Schedule	
Error Likelihood	The likelihood of unrecovered failure of this action is considered very low. No credible failure paths were identified for this task/action. Failure to identify an alarm and source of the fire causing the alarm were not deemed credible when a fire emanates from an MCR that is permanently occupied by trained, licenced operators. See PCSR Chapter 10 for the PSA quantification of the HEP for this action.
Corrective Action / Recommendation	The site Licensee shall define policies and procedures to respond to an on-site fire during Site Licensing. There will be a room designated as an 'assembly area' for fire fighters. This may contain lockers for the on-shift fire-fighter's clothing and kit with a changing, forming-up and briefing area and direct communication with the MCR. There will be portable, hand-held devices available to facilitate communication between the MCR and the Fire Fighting crew and with locally dispatched auxiliary operators having a range sufficient to cover all fire assembly points, fire areas/zones and rooms containing nuclear safety important SSCs. Doors to rooms that contain systems, equipment and components providing or supporting a nuclear safety, security or power generation function and that are not frequently or routinely occupied will be normally locked and only accessible to duly authorised and appropriately qualified and trained personnel. Resolution of HED issues associated with this ISV Scenario 7 action.
Human Action Identifier	**HEPO-INJ**
Location (s) of Action	MCR
Person(s) Performing Action	MCR Crew
Task	Actuate IRWST injection
Tools/Equipment	PXS-V123A/B PXS-V125A/B PXS-V121A/B

APPENDIX 13C COGNITIVE-HEA ACTIONS SUMMARY SCHEDULE (cont.)

Human Error Analysis Sample - Summary Schedule	
SSC	Passive Core Cooling System (PXS)
Error Description	Operator fails to actuate IRWST injection
Performance Shaping Factors	Procedures Training HSI design Task Complexity Attention
Cognitive Processes	Detect that IRWST injection has not actuated automatically (procedurally prompted). Detect that PMS IRWST injection has failed (procedurally directed). Correctly execute DAS IRWST injection, a simple manual task (procedurally directed). Confirm that IRWST injection was performed correctly. Follow procedures
Consequence	If operator fail to open the In-containment Refuelling Water Storage Tank (IRWST) injection valves manually from the Diverse Actuation System (DAS) Panel and nothing further is attempted then core damage would occur. However, the chances that the nuclear operators would attempt nothing else are highly unlikely from a human action standpoint as strict adherence to procedures and peer checking is expected per Conduct of Operations. Additionally in APP-GW-GJP-201 (E0, Step 5) the implementation of [Site specific procedure (Event Classification] occurs. This action notifies the Technical Support Centre and Emergency off-site facility which will be aware of any undue changes or issues from the Main Control Room (MCR). Additionally the alignment and injection of RNS is attempted to negate core damage.
Recovery	Peer checking is part of the Conduct of Operations, as is SRO supervision and the practice of crew briefs, any of which, could recover a failure of this action. The PRA does not credit recovery for this step. Recovery actions are available in FR-C.1 (Response to Inadequate Core Cooling) but this is after core damage and therefore only appropriate to be credited in the Level 2 PRA.
Error Likelihood	Unrecovered failure of this action is very unlikely. It is not likely that errors will occur as the operators are

APPENDIX 13C COGNITIVE-HEA ACTIONS SUMMARY SCHEDULE (cont.)

Human Error Analysis Sample - Summary Schedule	
	trained in this scenario, the interface provides cues and indications that are clear and unambiguous, the task steps are clearly guided by procedures, and the procedures are assessed to be of high quality. See PCSR Chapter 10 for the PSA quantification of the HEP for this action.
Corrective Action / Recommendation	None aside from resolution of HED issues associated with this action.
Human Action Identifier	**HEPO-L2-CAVFLD**
Location (s) of Action	MCR
Person(s) Performing Action	MCR Crew
Task	Operators recognise the need and manually open the containment recirculation valves to flood the reactor cavity after core damage in a large loss of coolant accident (LOCA) scenario with indications of inadequate core cooling.
Tools/Equipment	PXS-V117A, PXS-V118A, PXS-V120A PXS-V117B, PXS-V118B, PXS-V120B
SSC	RCS
Error Description	Operator fails to flood RV cavity for IVR on loss of core cooling cue
Performance Shaping Factors	Procedures Training HSI design Task Complexity Attention Stress

APPENDIX 13C COGNITIVE-HEA ACTIONS SUMMARY SCHEDULE (cont.)

Human Error Analysis Sample - Summary Schedule	
Cognitive Processes	Detect CET higher than 1200F, recognise CSFT red path, follow procedures, recognise the need for reactor cavity flooding, execute the reactor cavity flood correctly, and confirm flood occurred successfully.
Consequence	Since there is already core damage, the consequences are vessel damage, if water is not released around the vessel to help lower the temperature.
Recovery	Step 3 in FR-C.1 directs the operators to Actuate Safeguards. If the operators had already actuated safeguards, technically the need to “initiate reactor cavity flooding” should not be needed as the plant’s passive safety features should already be in effect.
Error Likelihood	The likelihood of unrecovered failure of this action is considered to be low. While the action involves higher workload and stress, the HSI design, procedures, task complexity, and training will drive this action towards success. While the initial conditions of this action are different from those of scenario 12 for the ISV, the action of interest was performed successfully in all trials, which shows that it is possible for operators to complete this action. This combined with the majority of the PSFs leading to success of the action; it seems unlikely that a human error will occur to prevent this action from being successfully completed. See PCSR Chapter 10 for the PSA quantification of the HEP for this action.
Corrective Action / Recommendation	None aside from the resolution of the HED issue (ISV-51 and Issue ID ISV-07-07) associated with this task.
Human Action Identifier	**HEPO-L2-CNT**
Location (s) of Action	MCR
Person(s) Performing Action	Local Equipment (auxiliary) Operator
Task	Operator manually isolates containment
Tools/Equipment	Containment isolation valves
SSC	Containment System (CNS)

APPENDIX 13C COGNITIVE-HEA ACTIONS SUMMARY SCHEDULE (cont.)

Human Error Analysis Sample - Summary Schedule	
Error Description	Operator fails to manually isolate containment
Performance Shaping Factors	Procedures, Training, HSI Design, Attention, Stress
Cognitive Processes	Follow procedures, successfully ensure all containment isolation valves are closed, confirm with peer check.
Consequence	Since there is already core damage, the consequences could be a release associated with the accident progression provided additional actions to prevent this are not taken.
Recovery	Step 7 of FR.C-1 will also have the operators perform this action (manual containment isolation), which the operators will reach if they transition out of E-0 via the Foldout Page. If the operators did transition out of E-0 but failed to perform this action (manual containment isolation), they could, depending on the failure, be directed to "Return To Procedure And Step In Effect" (as in F-0 Step 7), which allows them to reach Step 13 of E-0.
Error Likelihood	The likelihood of unrecovered failure of this action is considered to be very low. While the level of stress the operator is experiencing is a negative PSF, the HSI design, procedures, task complexity, and training will drive this action towards success. While the initial conditions of this action are different from those of scenario 17 for the ISV, the action of interest was performed successfully in all trials, which shows that it is possible for operators to complete this action. This combined with the majority of the PSFs leading to success of the action; it seems unlikely that a human error will occur to prevent this action from being successfully completed. See PCSR Chapter 10 for the PSA quantification of the HEP for this action.
Corrective Action / Recommendation	None aside from resolution of HED issues associated with manual isolation of containment action in ISV Scenario 17.
Human Action Identifier	**HEPO-L2-H2I**
Location (s) of Action	MCR
Person(s) Performing Action	Licenced Reactor Operator 2

APPENDIX 13C COGNITIVE-HEA ACTIONS SUMMARY SCHEDULE (cont.)

Human Error Analysis Sample - Summary Schedule	
Task	Operator manually actuates the hydrogen igniters in a large loss (LOCA) of coolant scenario.
Tools/Equipment	VLS-AE001/2/3
SSC	Containment Hydrogen Control System (VLS)
Error Description	Operator fails to manually actuate hydrogen ignitors
Performance Shaping Factors	Training, HSI Design, Task Complexity, Attention, Time Pressure, Procedures
Cognitive Processes	Follow procedures, recognise that PLS actuation of hydrogen igniters failed, successfully actuate hydrogen igniters via DAS, and confirm hydrogen igniter actuation. Operators already know they are in a core damage scenario and have initiated reactor cavity flooding, so the significance and importance of this task are fully understood.
Consequence	The PSA assumes containment failure once the hydrogen level reaches detonation conditions.
Recovery	There is an alarm when the hydrogen concentration reaches 3%. In Severe Accident Control Room Guideline (SACRG-1), APP-GW-GJP-501, Rev 0, in Step 5 the text states "Determine if Hydrogen Igniters should be in service: 5a) Check hydrogen concentration (less than 10%), 5b) Turn on both groups of Hydrogen Igniters. If the hydrogen igniters fail then the Response Not Obtained (RNO) column 5b) instructs the operator to Actuate DAS Containment Hydrogen Igniters.
Error Likelihood	Unrecovered failure of this action is considered to be of very low likelihood. Turning on the hydrogen igniters is a simple task and there is the potential for recovery if the operator initially fails to carry out the task. The main PSFs are workload and stress but the procedures give sufficient guidance to allow us to deduce that this failure is unlikely. See Chapter 10 for the PSA quantification of the HEP for this action.
Corrective Action / Recommendation	None aside from the resolution of the HEDs associated with RIHAs VLN-MAN01 and DAS-VLN-MAN01 actions in ISV Scenario 17.
Human Action Identifier	**HEPO-OFILL**

APPENDIX 13C COGNITIVE-HEA ACTIONS SUMMARY SCHEDULE (cont.)

Human Error Analysis Sample - Summary Schedule	
Location (s) of Action	MCR
Person(s) Performing Action	MCR Crew
Task	Operator successfully isolates RCS makeup flow from CVS and SFW flow prior to ruptured Steam Generator overfill.
Tools/Equipment	SGS-LT001-1-MED, SGS-LT011-1-MED SGS-LT005-1-MED, SGS-LT013-1-MED
SSC	Protection and Safety Monitoring System (PMS)
Error Description	Operator fails to isolate ruptured SG (on High-3 NR SG level—PMS backup)
Performance Shaping Factors	Audible and visual Alarm cues in the MCR, HSI Design Training; Procedures; Time Pressure; Communication; Workload
Cognitive Processes	Detect ruptured SG NR level above 72.8%, recognise and understand the significance of failure of isolation of the ruptured SG, follow procedures, make correct decisions, successfully execute manual valve closures. Operators will have already diagnosed the situation as a SGTR event, and will be watching ruptured SG NR level.
Consequence	The operator failure to isolate RCS makeup flow from CVS and SFW flow to the ruptured SG without ADS manual actuation could lead to steam generator overfill, potentially resulting in Containment-bypass sequences and a significant increase in the offsite radiological consequences. If the primary-to-secondary leakage continues for a significant time, the Steam Generator may become filled and water may enter the steamline. If the leakage continues, Containment is bypassed and fluid may be released through the secondary side safety valves to the atmosphere. Moreover, due to the presence of water, these valves may not be capable of reclosing and will remain stuck open.
Recovery	A SRO/STA review on operators' actions could potentially help them identifying the error in recognising the ruptured SG overfill and the error in failing to isolate SFW and CVS before the ruptured SG NR level reaches

APPENDIX 13C COGNITIVE-HEA ACTIONS SUMMARY SCHEDULE (cont.)

Human Error Analysis Sample - Summary Schedule	
	95% of span. The available time for this human action is deemed short, as it is based on the bounding PSA scenario. However, even if that PSA bounding scenario occurs, E 3 foldout page criteria for ADS will be met sooner in the scenario evolution: operators will manually actuate ADS, thus lengthening the time window. It has to be noted that in case of both Ruptured SG isolation and SFW/CVS isolation failure, core damage can be prevented by RCS depressurisation via the ADS valves and IRWST or RNS injection/recirculation. This has been demonstrated in ISV test Scenario 15 results, as the MCR crews prevented SG overfill by depressurising the RCS using ADS stage 1-3 (RIHA ADF MAN01) that terminated the filling of the ruptured SG before overfilling instead of isolating RCS makeup flow from CVS and SFW flow to the ruptured SG. The depressurisation of the RCS terminates the primary-to-secondary leakage and prevents a Steam Generator overfill event. HEPO OFILL may not be recovered this way, but SG overfill is successfully prevented.
Error Likelihood	The likelihood of unrecovered failure of this action is considered to be low. Workload, stress and time pressure have been identified as negative PSFs, but a good HSI design, knowledge/experience/training and clear procedures have been identified as positive PSFs, reducing the likelihood of error. Given that this action is a backup of PMS automatic isolations and that it is required after the failure when attempting to isolate the ruptured SG, the likelihood of requiring MCR crew to perform this action is already reduced. Moreover, it is not likely that this error will occur given that the operators are trained in this scenario, the interface provides clear indication of the status of the ruptured SG NR level, the task steps are guided specifically by symptom-based procedures, and SRO surveillance is provided. See Chapter 10 for the PSA quantification of the HEP for this action.
Corrective Action / Recommendation	In the previous revision (Rev. 5) of EOP E-3, which was used for the PSA HRA (as documented in HRA Notebook, APP-PRA-GSC-321 Rev. C), the verification of the ruptured SG level (i.e., Check Ruptured SG(s) Narrow Range Level – LESS THAN 82%) was positioned in Step 6, right after the SG isolation actions from the Main Steam line and from ruptured SG drains (E 3 Steps 3 through 5). It was just a “check” step. Currently, this step has been transformed into a “continuous/monitor” step and its set point has been lowered, from 82% of span to 72.8% of span. However, this step has been moved from Step 6 to Step 17. Therefore, in order to make sure that the timely, automatic PMS isolation of RCS makeup flow from CVS and SFW flow to the ruptured SG has occurred, it is recommended to move current Step 17 so that it is encountered by the MCR crew at an earlier stage in the procedure. Resolution of HED issues associated with RIHA CIB-MAN01 in ISV Scenario 15 and isolation of ruptured SG as part of ISV Scenario 14.

Human Action Identifier	HEPO-PRHR-GT
Location (s) of Action	MCR
Person(s) Performing Action	MCR crew
Task	Operator manually actuates PRHR after automatic actuation failure post reactor trip without safeguards actuation.
Tools/Equipment	PXS-PRHT, PRHRHX Outlet Temp Filtered PXS-FT49A/B, PRHR HX Flow
SSC	PXS
Error Description	Operator fails to actuate Passive Residual Heat Removal (PRHR) during an event without a Safeguards signal
Performance Shaping Factors	HSI Design Training Communication
Cognitive Processes	Monitoring of the CSFT, recognition and understanding of a heat sink red path, following procedures, communicate within the MCR crew, manually actuate PRHR.
Consequence	Failure of this task could ultimately result in damage to the core.
Recovery	The EOP ES-0.1 Reactor Trip Response procedure is being performed concurrently with monitoring of Critical Safety Functions (EOP F-0) and will eventually (Step 25 RNO) instruct the operator to throttle PRHR although this may not occur in the time to core damage postulated by the PSA.
Error Likelihood	The likelihood of unrecovered failure of this task is considered to be very low. Given the positive impact of the PSFs, the training and experience levels of the operators, the presence of the STA in monitoring the CSFTs, the procedurally driven resolution method, and modern standards HSI design, this task is deemed to be achievable in

APPENDIX 13C COGNITIVE-HEA ACTIONS SUMMARY SCHEDULE (cont.)

Human Error Analysis Sample - Summary Schedule	
	the available time. See PCSR Chapter 10 for the PSA quantification of the HEP for this action.
Corrective Action / Recommendation	None
Human Action Identifier	**HEPO-RNSINJ**
Location (s) of Action	MCR
Person(s) Performing Action	MCR Crew
Task	Operator aligns the normal residual heat removal (RNS) for injection from the cask loading pit (CLP).
Tools/Equipment	SFS-LT022 RNS-FT001A/B
SSC	RNS
Error Description	Operator fails to align RNS for injection
Performance Shaping Factors	Procedures, Training, HSI design
Cognitive Processes	
Consequence	RNS is a support system and although it would be helpful to use it, if it is not possible, there is no safety consequence. RNS failure does not lead to core damage but rather is used as DiD.
Recovery	There is no real recovery for RNS. Peer checking is provided. SRO also provides supervision. From the PRA standpoint no recovery was credited for this step. Recovery actions are available in FR-C.1 (Response to Inadequate Core Cooling) but this is after core damage.
Error Likelihood	The likelihood of unrecovered failure of this action is considered to be low. Due to a design change, any actuation of ADS (automatic or manual) always transitions to ES 1.3 and ADS Stages 1-3 Actuation Response.

APPENDIX 13C COGNITIVE-HEA ACTIONS SUMMARY SCHEDULE (cont.)

Human Error Analysis Sample - Summary Schedule	
	The most current procedures have been changed to reflect the DCP. Due to the DCP and updated procedure changes PRA issued a revised set of critical human action steps to HF for the Human Action HEPO-RNSINJ. Although the actions were relatively simple, the operators were required to transition to several procedures to complete the action. The workload was considered medium, although the action was not complicated. The PRA time window for HEPO-RNSINJ was 24 minutes, developed prior to the design change. The HF analysis time for the human action was 30.97. However, in the ISV trials for Scenario 11 all four crews completed the action and two of the four crews did meet the PRA time of 24 minutes. Based on this assessment it seems unlikely that a human error will occur to prevent this action from being successfully completed. It should also be noted that the PSA time window has been calculated using conservative considerations. The PSA time window calculated was based on the upper bound of a MLOCA break size. This time window would be significantly longer for smaller and more likely break sizes. A modified time window based on a smaller break size and consideration for procedures improvements are also anticipated to result in a time window that can be achieved. See PCSR Chapter 10 for the PSA quantification of the HEP for this action.
Corrective Action / Recommendation	None aside from the resolution of ISV issues related to alignment of RNS from CLP and then from IRWST to the RCS from ISV Scenario 11.
Human Action Identifier	**HEPO-RRWSTISO**
Location (s) of Action	MCR
Person(s) Performing Action	MCR crew
Task	Operator successfully isolates IRWST recirculation following spurious IRWST recirculation squib valve(s) actuation.
Tools/Equipment	PXS-V117A/B; PXS-LT054 & PXS-LT055
SSC	PXS
Error Description	Operator fails to isolate IRWST recirculation following spurious recirculation actuation

APPENDIX 13C COGNITIVE-HEA ACTIONS SUMMARY SCHEDULE (cont.)

Human Error Analysis Sample - Summary Schedule	
Performance Shaping Factors	Training, HSI Design, Stress, Time Pressure, Task Complexity
Cognitive Processes	Detect and understand the IRWST level and Containment Sump Level High alarms and the associated level indications, follow procedures, successfully close PXS valves.
Consequence	The operator failure of isolating the IRWST inventory leakage into the Containment floodable region would render the IRWST unavailable. In consequence, IRWST passive injection and PRHR long term cooling can no longer be considered available as mitigation means: IRWST would not contain enough water inventory for passive injection and the PRHR heat exchanger would not be operable as the IRWST water level is below the required level for its correct operation. The unavailability of the IRWST inventory would leave operators with only the secondary side heat removal systems to be used for the mitigation of this event (MFW and SFW systems).
Recovery	Various alarms will appear in the MCR indicating a leak into the Containment floodable region and the IRWST level alarm will help the identification of the leakage. Peer/supervisor check is expected.
Error Likelihood	The likelihood of unrecovered failure of this action is considered to be very low. The likelihood of not recognising the IRWST leak is low: IRWST level alarms will be triggered, Containment sump alarms will be triggered, progressively showing the IRWST level drop and Containment flooding. Error of omission (action not attempted) is considered low as the main error mechanisms linked to this type of error is related to misdiagnosis and non-expectation of cues. Despite this fact, the ample available time reduces the probability of failing the action. For the accomplishment of this human action, a few indicators in MCR are required to identify and diagnose the event, the stress level is low, there is not a significant time pressure, the task is simple and only a single control action is to be performed. See PCSR Chapter 10 for the PSA quantification of the HEP for this action.
Corrective Action / Recommendation	Within seconds of the initiating event, the WLS Containment sump level alarm is received. Alarm Response Procedure APP-WLS-GJP-401, is used to treat this alarm. It directs the operator to AOP-340 “Response to a RCS Leak”. This procedure does not mitigate the faulted PXS recirculation condition because it directs the operators to look for a RCS leak only. The ALARP discussion has identified a recommended procedure change of both ARP-APP-WLS-GJP-401 and AOP-340 in order to include indications of other types of leaks that could occur in fluid systems located in Containment, apart from a RCS leak.

APPENDIX 13C COGNITIVE-HEA ACTIONS SUMMARY SCHEDULE (cont.)

Human Error Analysis Sample - Summary Schedule	
	Repetitive steps have been identified in Alarm Response Procedure used to accomplish the Containment Recirculation line isolation, APP-PXS-GJP-401. The associated instructions for the primary cue, level transmitters PXS-LT054 and PXS-LT055, direct the operator to close Containment Recirculation isolation MOVs per Step 3. Similar instructions are repeated in steps 4 and 6. Moreover, instructions for PXS LT054 and PXS LT055 are not exactly the same although they are redundant level transmitters. The ALARP discussion has identified a recommended a simplification of level transmitters PXS-LT054 and PXS-LT055A related procedure steps, including identical steps for both transmitters.
Human Action Identifier	**OPR-011**
Location (s) of Action	Rooms 11206, 11300, 12206, and 11207
Person(s) Performing Action	Local Equipment (auxiliary) Operator
Task	Operators maintain ADS stage 4 and IRWST injection valves and return them to service.
Tools/Equipment	1. Static Protector Plug(s) 2. Hand held, Battery Powered, Digital Volt Meter 3. Keys for ILC cabinets A01, A03, B01, B04, C01, C02, D01 and D04 4. Keys for the following cabinets: • DAS-JD-001 (Processor Cab 1) • DAS-JD-003 (Squib Valve Cab) • PMS-JD-SVCA01 (Squib Valve Controller Cab Div A) • PMS-JD-SVCB01 (Squib Valve Controller Cab Div B) • PMS-JD-SVCC01 (Squib Valve Controller Cab Div C) • PMS-JD-SVCD01 (Squib Valve Controller Cab Div D)
SSC	ADS

APPENDIX 13C COGNITIVE-HEA ACTIONS SUMMARY SCHEDULE (cont.)

Human Error Analysis Sample - Summary Schedule	
Error Description	Maintenance error leads to failure of ADS Stage 4 and IRWST gravity injection squib valves
Performance Shaping Factors	Team Work, Communication, Time Pressure, Tooling and PPE, Access, Training, HSI design, Procedures
Cognitive Processes	Correctly determine which tests are required for which valves, correctly and unambiguously record outcomes of tests and inspections, apply correct levels of force when connecting or disconnecting electrical connecters at the valve, correctly reconnect the cabling from PMS/DAS SVCs to the squib valve igniters after installation in the pipeline, correctly restore PMS/DAS SVC to service, correctly and completely perform visual inspections of the valves, detect and understand the significance of any fault in the valve, follow procedures, apply proper force to components during disassembly and reassembly, remove, disassemble, and reassemble items in the correct order, apply the correct text, properly handle squib valve cartridges, ensure proper hoist connections, properly use the hoist, properly disconnect the valve from the flanges, properly perform electrical continuity checks, use properly calibrated tools (e.g., multimeter), correctly record measurements, proper communication amongst team members. Work planning and use of checklists and human performance fundamentals is of primary importance for this task.
Consequence	Failure to successfully complete specific maintenance tasks may result in a failure of the squib valves to actuate. This could potentially lead to one of the four flow paths required to vent the RCS not functioning. In this eventuality, the three remaining flow paths that are unaffected would be sufficient to depressurise the RCS to allow the IRWST to drain to the RCS. In addition to this ADS stage 1-3 will be sufficient to depressurise the RCS providing further redundancy for this system. Failure of IRWST injection valves to actuate would result in failure to inject the contents of the IRWST into the RCS or failure to place the RCS and Containment sump on recirculation. In this eventuality, the three remaining flow paths that are unaffected would be sufficient to inject the IRWST into the RCS.
Recovery	Co-worker peer review, Independent Verification (when indicated by the procedure) and Concurrent Verification (when indicated by the procedure) performed by SQEP engineers
Error Likelihood	The likelihood of unrecovered failure of this action is considered to be low, due to the training, work planning, collective recognition of the safety significance of the squib valves, use of procedures and checklists, peer checks, and independent verification. A number of recommendations for improvements to this task are identified below. An HEP for this action will not be calculated until site licensing.

APPENDIX 13C COGNITIVE-HEA ACTIONS SUMMARY SCHEDULE (cont.)

Human Error Analysis Sample - Summary Schedule	
Corrective Action / Recommendation	1) Since IRWST Injection squib valves (i.e., PXS-V123A/B, PXS-V125A/B) need to be removed in order to access and maintain the Containment Recirculation Squib valves (i.e., PXS-V1183A/B, PXS-V120A/B), it is recommended to include in APP-PXS-GJP-804 procedure a statement in "precautions and limits" section alerting the operator that the activity he/she is about to perform could require the removal of other squib valves. 2) There is the potential for the IST engineer to make a selection error and chose either wrong valves to be tested and / or chose the wrong tests to be undertaken on the right valves and vice versa. There is no IV identified for the test selection process in the current revision (i.e., Rev. 0) of the MTIS procedure and therefore, including IV of the test selection process is raised as a suggested improvement from this assessment. 3) There also exists the possibility for an administration error to occur when undertaking the maintenance activities locally either at the valves location in-situ or on the Maintenance Floor. Therefore, it is recommended to add a verification step during the results recording process to ensure that the documented results are correct and comprehensible for other maintenance operators. 4) It is recommended that the Site specific Maintenance procedure includes all IVs and CVs as instructed in the current MTIS procedure (APP-PXS GJP-804, Rev. 0) as well as including all Vendor's Manual (APP PV70 VMM 001, Rev. 1) recommendations, cautions and documentations requirements for critical steps. Moreover, it is also recommended that the site licensee's maintenance procedure will include a step to check the CIMs LEDs indications to ensure proper restoration. 5) Since both IRWST injection and Containment Recirculation squib valves need to be maintained at least once every two years for all valves on a rotational basis, it is recommended to adapt the site specific maintenance schedule to synchronise the maintenance activities requiring valves removal for those pairs of IRWST injection and Containment Recirculation squib valves located one above the other at the same time. 6) In order to prepare the working area in the PXS room, transporting all required tools and equipment, it is recommended to use the personnel hatch versus the equipment hatch itself, as this will avoid transportation/handling of equipment on top of the IRWST injection squib valves, which could damage them. 7) The current maintenance procedure (APP-PXS-GJP-804, Rev. 0) provides checklists to follow when undertaking maintenance activities. The checklists do not contain a high degree of detail. Moreover, the

APPENDIX 13C COGNITIVE-HEA ACTIONS SUMMARY SCHEDULE (cont.)

Human Error Analysis Sample - Summary Schedule	
	In-Service Inspection Data Sheet, where results are recorded requires the maintenance operator to circle a box to record if the test was Satisfactory or not ("SAT/UNSAT" box). Circling this box may easily be completed in a manner that may not be clear to another operator and it is likely that this particular design element of the checklist could increase the likelihood of a latent maintenance error. A redesign of this element of the checklist is recommended in order to avoid misinterpretation of the results. 8) In order to minimise the risk of omitting or forgetting to reconnect the PMS/DAS SVCs cabling after maintenance and reinstallation, it is recommended that the Site specific Maintenance procedure includes an IV step to check that the electrical connection has been properly restored to the squib valves igniters. 9) The time taken to remove the worst case valves is currently unknown. Further assessment is required to understand if the time available during maintenance is sufficient to enable the maintenance operators to complete this task. 10) It is recommended to study the feasibility of fitting the hydraulic system to the flange studs located closest to the room wall in order to ensure proper valve removal from the pipeline. 11) It is recommended to study the feasibility of removing the IRWST injection valves flange studs with the current room layout.
Human Action Identifier	**OPR-099**
Location (s) of Action	Rooms: 12305, 12304, 12301, and MCR
Person(s) Performing Action	Local Equipment (auxiliary) Operator
Task	Operator executes the CMT discharge valves operability test.
Tools/Equipment	PXS-V002A/B; PXS-V014A/B; PXS-V015A/B PMS-MTCD01; PMS-MTCB01; PMS-JD-ILCA01
SSC	Core Makeup Tank (CMT)
Error Description	Operator incorrectly executes the CMT discharge valves operability test

APPENDIX 13C COGNITIVE-HEA ACTIONS SUMMARY SCHEDULE (cont.)

Human Error Analysis Sample - Summary Schedule	
Performance Shaping Factors	Procedures, HSI Design, Task Complexity, Attention, Task Preparation, Time Pressure, Training
Cognitive Processes	Follow procedures, select the correct valve, correctly use independent verification, correctly close the valves, and return them to proper alignment.
Consequence	Failure to close the CMT inlet isolation first and opening the CMT discharge isolation valves results in the flow of highly borated and cooler CMT fluid into the reactor coolant. Failing to close the CMT discharge isolation extends the time period, during which the fluid injection would continue, and therefore the severity of the consequences. If not identified and corrected promptly an automatic reactor trip will result. Safeguards actuation occurs about 3 minutes or less after both CMT valves are left open.
Recovery	Peer check and independent verifier signature for the critical subtasks are opportunities for recovery. The plant transient initiated by inadvertent CMT flow would result in multiple alarms in the MCR. Such alarms would be expected to include Control Rod Motion audible, Pressuriser Level Low alarms, CMT High Temperature alarms, Steam line Pressure Low alarms and Cold Leg temperature low alarms. The operator or the control room supervisor would be expected to investigate and correct the cause of these alarms.
Error Likelihood	The likelihood of unrecovered failure of this task is considered to be low. Workload is considered low, as no other actions are required to be performed before this one. Stress level is also considered to be low as this is a maintenance action. Time pressure is not significant, as this is a maintenance action with no time requirements. All of the valves linked to failure of this action have valve positions indications in the MCR, leading to successful completion. An HEP for this action will not be calculated until site licensing.
Corrective Action / Recommendation	None
Human Action Identifier	**OPR-106**
Location (s) of Action	Rooms 11206, 11300, 12206, and 11207
Person(s) Performing Action	Local Equipment (auxiliary) Operator
Task	Operators maintain Containment Recirculation squib valves and return them to service.

APPENDIX 13C COGNITIVE-HEA ACTIONS SUMMARY SCHEDULE (cont.)

Human Error Analysis Sample - Summary Schedule	
Tools/Equipment	1. Static Protector Plug(s) 2. Hand held, Battery Powered, Digital Volt Meter 3. Keys for ILC cabinets A01, A03, B01, B04, C01, C02, D01 and D04 4. Keys for the following cabinets: • DAS-JD-001 (Processor Cab 1) • DAS-JD-003 (Squib Valve Cab) • PMS-JD-SVCA01 (Squib Valve Controller Cab Div A) • PMS-JD-SVCB01 (Squib Valve Controller Cab Div B) • PMS-JD-SVCC01 (Squib Valve Controller Cab Div C) • PMS-JD-SVCD01 (Squib Valve Controller Cab Div D)
SSC	PXS
Error Description	Maintenance error leads to failure of recirculation squib valves
Performance Shaping Factors	Communication, Time Pressure, Training, Access, HSI Design, Procedures
Cognitive Processes	Correctly determine which tests are required for which valves, correctly and unambiguously record outcomes of tests and inspections, apply correct levels of force when connecting or disconnecting electrical connecters at the valve, correctly reconnect the cabling from PMS/DAS SVCs to the squib valve igniters after installation in the pipeline, correctly restore PMS/DAS SVC to service, correctly and completely perform visual inspections of the valves, detect and understand the significance of any fault in the valve, follow procedures, apply proper force to components during disassembly and reassembly, remove, disassemble, and reassemble items in the correct order, apply the correct text, properly handle squib valve cartridges, ensure proper hoist connections, properly use the hoist, properly disconnect the valve from the flanges, properly perform electrical continuity checks, use properly calibrated tools (e.g., multimeter), correctly record measurements, proper communication amongst team members. Work planning and use of checklists and human performance fundamentals is of primary importance for this task.

APPENDIX 13C COGNITIVE-HEA ACTIONS SUMMARY SCHEDULE (cont.)

Human Error Analysis Sample - Summary Schedule	
Consequence	Failure to successfully complete this test would render unavailable the Containment Recirculation squib valves undergoing maintenance. This unavailability reduces the capabilities for the establishment long term recirculation from the Containment sump to the Reactor when required for the mitigation of certain accidents. As the IRWST Injection squib valves will be removed to perform a full maintenance on the Containment Recirculation squib valves, the potential for a common cause failure during maintenance on both types of valves may occur, potentially rendering unavailable IRWST Injection valves as well. This is initially limited to the valves being worked on during that particular outage.
Recovery	Co-worker peer review, Independent Verification (when indicated by the procedure) and Concurrent Verification (when indicated by the procedure) performed by SQEP engineers
Error Likelihood	The likelihood of unrecovered failure of this action is considered to be low, due to the training, work planning, collective recognition of the safety significance of the squib valves, use of procedures and checklists, peer checks, and independent verification. A number of recommendations for improvements to this task are identified below. An HEP for this action will not be calculated until site licensing.
Corrective Action / Recommendation	As per OPR-011
Human Action Identifier	**OPR-131**
Location (s) of Action	Containment
Person(s) Performing Action	Refuelling SRO
Task	The operator seats the fuel assembly within the Reactor Vessel (RV).
Tools/Equipment	PPE – full body coveralls will be worn by the SROs during normal refuelling operations.
SSC	Fuel Handling and Refuelling System (FHS)
Error Description	Operator improperly seats the fuel assembly within the core.

APPENDIX 13C COGNITIVE-HEA ACTIONS SUMMARY SCHEDULE (cont.)

Human Error Analysis Sample - Summary Schedule	
Performance Shaping Factors	Communication; Time Pressure; Training; PPE; HSI Design; Procedures
Cognitive Processes	Select proper operational mode for the refuelling machine, ensure interlocks are operational, follow procedures, detect fuel assembly position on the interlock display, and ensure fuel assembly is properly seated before releasing from the refuelling machine gripper.
Consequence	If the FA is improperly seated onto the RV assembly support floor and guide pins AND is erroneously released by the RFM or the operator it could move from its vertically upright position impacting the side of the RV vessel or another FA. This could potentially damage the FA (or the one impacted) resulting in a release of radioactive material. At this point the SRO would contact the Main Control Room (MCR) to sound the containment evacuation alarm and suspend refuelling activities. Ultimately, this error would potentially lead to an increased outage time for the plant.
Recovery	Concurrent Verification occurs throughout the refuelling process and SROs are able to check each other's actions and key system status indicators e.g., interlock displays throughout the process.
Error Likelihood	The likelihood of unrecovered failure of this task is considered to be extremely low. The refuelling SROs are SQEP, are fit for duty and are highly trained and experienced in undertaking refuelling activities. The HSI is designed according to good RGP and AP1000 HF guidelines. There are also numerous safety related interlocks that prevent an SRO from releasing a fuel assembly into the RV if it is not properly seated within the RV. The workload of the crew is deemed to be medium and no significant negative performance shaping factors have been identified that will increase the likelihood of human error in this scenario. Based on the positive influence of the PSFs, the prevention and recovery mechanisms, as well as the training and SQEP levels of the SRO crew, this scenario, during normal operations is deemed extremely unlikely. However, during recovery operations i.e., a major PLC malfunction the likelihood of a human error based failure increases.

APPENDIX 13C COGNITIVE-HEA ACTIONS SUMMARY SCHEDULE (cont.)

Human Error Analysis Sample - Summary Schedule	
	This increase in risk can be mitigated by introducing IV during the crucial stage of inserting a FA into the RV when operating in this mode. This has been identified as an improvement. An HEP for this action will not be calculated until site licensing.
Corrective Action / Recommendation	Site specific procedures specifically identify the points, at which IV should occur, if the SROs put the FA down in the RV in interlock override mode

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

None.

LIST OF ABBREVIATIONS AND ACRONYMS

ac	alternating current
ADS	automatic depressurisation system
ALARP	as low as reasonably practicable
ANSIS	AP1000 reliability programme for non-Class 1 systems with safety importance
ATWT	anticipated transient without trip
BSL	basic safety level
BSO	basic safety objective
C&I	control and instrumentation
CCF	common-cause failure
CCS	component cooling water system
CDF	core damage frequency
CI	containment isolation
CIV	containment isolation valve
CVS	chemical and volume control system
DAS	diverse actuation system
DB	design basis
DF	decontamination factor
D-RAP	design reliability assurance programme
DVI	direct vessel injection
ECF	early containment failure
ESF	engineered safety feature
GDA	generic design assessment
HEPA	high-efficiency particulate air
HVAC	heating, ventilation, and air conditioning
HX	heat exchanger
IC	intact containment
ICRP	International Committee on Radiological Protection
IRWST	in-containment refuelling water storage tank
ISLOCA	interfacing system loss-of-coolant accident
IVR	in-vessel retention
LLOCA	large loss-of-coolant accident
LOCA	loss-of-coolant accident
LRF	large release frequency
MOV	motor-operated valve
ONR	Office for Nuclear Regulation
OPRAA	operational phase reliability assurance activities
O-RAP	operational reliability assurance programme
PCS	passive containment cooling system
PCSR	Pre-Construction Safety Report
PMS	protection and safety monitoring system
PRA	probabilistic risk assessment
PRHR	passive residual heat removal
PSA	probabilistic safety assessment
PWR	pressurised water reactor
PXS	passive core cooling system
RAP	reliability assurance programme
RC	release category
RCP	reactor coolant pump

LIST OF ABBREVIATIONS AND ACRONYMS (cont.)

RCS	reactor coolant system
RNS	normal residual heat removal system
RV	reactor vessel
SAMDA	severe accident mitigation design alternative
SAP	safety assessment principle
SFP	spent fuel pool
SFS	spent fuel pool cooling system
SFW	startup feedwater
SG	steam generator
SGTR	steam generator tube rupture
SSC	system, structure, or component
SWS	service water system
UK	United Kingdom
US	United States
VAS	radiologically controlled area ventilation system
VES	main control room emergency habitability system
VFS	containment air filtration system

14 AP1000 PLANT ALARP EVALUATION

14.1 Introduction

This chapter summarises and consolidates the results and conclusions of the following fault analysis and hazards safety case chapters in Volume 3 of the AP1000 Pre-Construction Safety Report (PCSR):

- Fault and Accident Analysis (Chapter 8)
- Internally initiated faults (Chapter 9)
- Probabilistic safety assessment (PSA) (Chapter 10)
- Internal hazards (Chapter 11)
- External hazards (Chapter 12)
- Human factors (Chapter 13)

Each of the above preceding chapters has its own results and conclusions, but there are some overall results and conclusions for the AP1000 plant design that are better suited to be discussed collectively. This collective presentation allows for an assessment of the AP1000 design against the requirement that the risks from its operation should be ALARP.

The results and conclusions of the fault and accident analyses demonstrate that the dose and frequency targets given in the Office for Nuclear Regulation (ONR) safety assessment principles (SAPs) (Reference 14.2) are met by the design and operation of the plant, and that the risks associated with plant operation are ALARP. These demonstrations are the subject of the rest of this chapter.

Section 14.2 discusses the classification and categorisation of systems, structures, or components (SSCs) identified in the various chapters of the fault and accident analysis and the claims made on them. These claims lead to requirements placed on the individual SSCs in terms of performance, reliability, separation and segregation, seismic withstand, and other survivability requirements. These requirements are the starting point for the engineering substantiation that is the subject of Volume 4.

Section 14.3 discusses the limits and conditions cited in the various chapters of the fault and accident analysis.

Section 14.4 lists the emergency instructions and operator actions identified in the fault and accident analyses. The corresponding operator errors (the failure of operators to fulfil these actions) are analysed in Chapter 13, which also contains a human factors as low as reasonably practicable (ALARP) assessment.

Section 14.5 is a compilation of information from the preceeding chapters of this volume to provide comparisons with the public and worker risk targets from the ONR SAPs that apply to the safety case as a whole.

Section 14.6 summarises the risk-reduction and ALARP arguments for the AP1000 plant, compiled from various sources. These sources demonstrate implementation of numerous design enhancesments over the life of the AP1000 design program. The implementation of the identified measures leads to the conclusion that, in the areas of severe accidents and human errors, the risks from the AP1000 plant are ALARP.

Section 14.7 provides an assessment to demonstrate that the total plant risk has been lowered to the point that it is very difficult to identify further cost-effective risk reduction measures.

The overall conclusion of this chapter is that risk-reduction and ALARP assessments have been carried out systematically and comprehensively to a sufficient degree to demonstrate that the risks associated with the AP1000 design and operation are considered to be ALARP.

14.2 Requirements on Systems, Structures, and Components from the Fault and Accident Analysis

The safety case developed in this volume of the PCSR identifies a number of SSCs as being important for safety. The categorisation and classification of the SSC is determined using the methodology in Section 5.2. The classification of SSCs defines the quality requirements placed on those SSCs during design, manufacture, and through life.

For the faults discussed in Chapter 9, the performance of the identified SSCs is analysed, and the analysis in the safety case confirms that these performance requirements are adequate for design basis (DB) targets to be met.

Generic component failure data parameters from Table 10-34 and Table 10-35 are used as an input to the AP1000 plant PSA discussed in Chapter 10. The engineering substantiation in Chapters 15 through 23 provides evidence that the design supports those assumptions.

In addition to performing their assumed safety functions, each SSC has to perform its function in the environment created by the events they are designed to mitigate. For example, SSCs designed to mitigate the consequences of a loss-of-coolant accident (LOCA) must be able to provide the required functionality in the elevated temperature and humidity associated with a LOCA. The environmental requirements for SSCs in normal and abnormal conditions are discussed in Section 5.8.

In addition to the above, there are also requirements driven by internal and external hazards evaluations, including separation, segregation, and seismic capacity. These requirements are derived from the internal hazards assessment (Chapter 11) and the external hazards assessment (Chapter 12).

14.3 Limits and Conditions Identified in the Safety Case

The limits and conditions identified or implied by the design basis accident analyses in Chapter 9 are presented in Reference 14.4. Section 5.6 and Reference 14.3 describe the process for the development of limits and conditions.

14.4 Emergency Actions Identified in the Safety Case

In some DB and other accidents, there is sometimes a requirement that operators should perform certain actions, either to manually initiate or realign a safety system (for example, manually activating CMT injection) or for their own protection (for example, to evacuate a particular area upon the activation of an area activity alarm).

In all of these cases, the required operator action is the subject of written operator procedures, supported by appropriate training and review. . Human Factors has been involved in the development of plant normal, abnormal, and emergency operating procedures, as described in Chapter 13, and Human Factors will continue to be involved in the development of site-specific procedures and procedure revisions to ensure error-likely situations are identified and mitigated.

The design basis accident analyses presented in Chapter 9 require a limited number of such operator actions. These operator actions have been entered into the Human Factors Human

Action Database (HAD), which is described in Chapter 13. The HAD is an open, living repository for recording, managing, and tracking operator actions important to nuclear safety. During site licensing, actions in the HAD will be screened for risk significance, and actions identified as risk significant will receive risk-proportionate human error analysis via the methodology established during GDA.

14.5 Comparison with Public and Worker Targets

14.5.1 Introduction

The SAPs (Reference 14.2) give a number of dose targets relating to normal operation, to fault sequences, and to societal risk. Targets 1, 2, and 3 relate to normal operation and as such are addressed separately in Chapter 24.

The dose targets relating to fault sequences are as follows:

- Target 4 – Design basis faults sequences, any person
- Target 5 – Individual risk of death from accidents, any person on the site
- Target 6 – Frequency dose targets for any single accident, any person on the site
- Target 7 – Individual risk to people off the site from accidents
- Target 8 – Frequency dose targets for an individual facility, any person off the site
- Target 9 –Total risk of more than 100 deaths

Each target defines a basic safety level (BSL) and a basic safety objective (BSO). It is relevant good practise that any new facility should meet the BSOs wherever possible. The BSO is a benchmark that reflects modern nuclear safety standards and expectations. In all cases, new facilities should meet the BSLs and demonstrate that risks are ALARP.

The comparison with Target 4 uses the results of the DB assessment given in Chapter 9 for all faults. The comparison with the probabilistic targets (Targets 5 to 9) uses the results of the PSA presented in Chapter 10 and is supplemented by additional probabilistic assessments cited in Chapters 8 and 9 as necessary. During GDA, the PSA work used to demonstrate meeting the SAP Targets is focused on the internal events at-power modelling. During site licensing, this comparison would be expanded to include various other models, including the low power and shutdown PSA, seismic PSA, maintenance activities, and the spent fuel pool PSA.

14.5.2 Comparison with SAP Targets

14.5.2.1 Target 4 – Design Basis Faults Sequences, Any Person

Target 4 gives a set of targets for the effective dose received by any person from a DB fault sequence. The targets are:

Onsite

BSL: 20 mSv for initiating event frequencies exceeding 10^{-3}/yr
200 mSv for initiating event frequencies between 10^{-3}/yr and 10^{-4}/yr
500 mSv for initiating event frequencies less than 10^{-4}/yr and 10^{-5}/yr

BSO: 0.1 mSv

Offsite

BSL: 1 mSv for initiating event frequencies exceeding 10^{-3}/yr
10 mSv for initiating event frequencies between 10^{-3}/yr and 10^{-4}/yr
100 mSv for initiating event frequencies less than 10^{-4}/yr and 10^{-5}/yr

BSO: 0.01 mSv

Chapter 9 demonstrates that these targets are met for DB fault sequences. Most fault analyses support the BSOs; however, there are some limited events that are above the BSO but support the BSL with a conservative amount of margin. Some of the largest radiological consequences would be further refined during site licensing and would be expected to be reduced, as discussed in Chapter 9.

14.5.2.2 Target 5 – Individual Risk of Death from Accidents, Any Person on the Site

Target 5 gives an individual risk of death for a person on the site from the sum total of accidents on the site. The individual risk of death is given as follows:

- BSL 10^{-4}/yr
- BSO 10^{-6}/yr

A risk figure for core damage releases can be conservatively derived from the Level 1 PSA results for comparison with this target, using a risk factor of 1, i.e., equating the total frequency of core damage with the risk of death to some worst-located individual onsite. This is clearly conservative because not all events with core damage will result in a release from the containment (as demonstrated by the Level 2 PSA results), and not all releases will result in high enough doses to cause death. Chapter 10 gives this frequency as 8.4E-07/yr, which is the total core damage frequency (CDF) for at-power internal events, internal flooding, and internal fire. The BSO is achieved even making this conservative assumption.

14.5.2.3 Target 6 – Frequency Dose Targets for Any Single Accident – Any Person on the Site

Target 6 gives targets for predicted frequency for any single accident on the site that could give an effective dose to a person on the site as follows:

Effective Dose (mSv)	Predicted Frequency per Annum	
	BSL	BSO
2-20	10^{-1}	10^{-3}
20-200	10^{-2}	10^{-4}
200-2000	10^{-3}	10^{-5}
>2000	10^{-4}	10^{-6}

On the same basis as for Target 5, a conservative derivation can be made of the frequency of accidents resulting in greater than 2000 mSv to the most exposed individual, by equating this to the CDF. As noted for Target 5, the total CDF for at-power internal events, internal flooding, and internal fire is 8.4E-07/yr, which therefore achieves the BSO for this dose band of Target 6. This simplified derivation assumes that no sequences without core damage can cause a dose to any person onsite of greater than 2000 mSv.

14.5.2.4 Target 7 – Individual Risk to People Off the Site from Accidents

Target 7 gives an individual risk of death for a person off the site from the sum total of accidents on the site. The individual risk of death is given as follows:

- BSL 10-4/yr
- BSO 10-6/yr

The sum of the large release frequency (LRF) for at-power internal events, at-power internal flooding and at-power internal fire is 7.4E-8/yr. Since the dose to the reference individual from any large release is calculated to be well above 20,000 mSv, the risk of death is effectively one, so large releases contribute 7.4E-8/yr towards the risk of death. . This gives a conservative total risk estimate of 743E-8/yr, more than an order of magnitude below the BSO for this target.

A cruder but more demonstrably conservative approach is to use the same principle as with Target 5, and to note that the risk from releases following core damage is bounded by the CDF of 4.6E-7, which is below the BSO.

14.5.2.5 Target 8 –Frequency Dose Targets for an Individual Facility – Any Person Off the Site

Target 8 gives targets for predicted frequency for any single accident on the site that could give an effective dose to a person off the site as follows:

Effective Dose (mSv)	Predicted Frequency per Annum	
	BSL	BSO
0.1-1	1	10^{-2}
1-10	10^{-1}	10^{-3}
10-100	10^{-2}	10^{-4}
100-1000	10^{-3}	10^{-5}
>1000	10^{-4}	10^{-6}

Section 10.23 compares Target 8 BSO with the CDF and LRF values for the at-power PSA results (Internal Events, Internal Flooding, and Internal Fire). Section 10.23 demonstrates margin to the Target 8 BSO.

14.5.2.6 Target 9 – Total Risk of More than 100 Deaths

Target 9 is the societal risk target for the total risk of 100 or more fatalities:

- BSL 10^{-5}/yr
- BSO 10^{-7}/yr

The total risk of 100 or more deaths is not a parameter directly calculated in the DB or PSA analysis. Furthermore, this parameter will be highly site-specific and cannot be calculated precisely in a generic assessment. Nevertheless, a simplified assessment can be made that assumes that all large releases will result in more than 100 fatalities, either immediate or eventual, and no other events (including all events outside the reactor, since the

inventory of radioactive material is very small elsewhere) will result in that number of fatalities. In this case, the LRF approximates to the total risk of 100 or more deaths. Section 10.23 demonstrates margin to the Target 9 BSO.

14.5.3 Conclusion of Comparison with Public and Worker Targets

This section has brought together the results of various analyses to provide a comparison with the dose and risk targets given in the SAPs. The results show that in most cases the calculated doses and risks are below the BSO of the relevant frequency and dose band target. In the small number of cases where this is not so, the doses or risks are still below the BSL with margin.

During site licensing, these targets would need to be evaluated once again to incorporate additional probabilistic and deterministic evaluations that have not yet been completed, such as the spent fuel pool PSA, maintenance activities and faults, as well as additional aspects of the reactor PSA, such as the low power and shutdown model. Generally speaking, the additional PSA models are expected to contribute less to the total CDF and LRF than the existing at-power models, and as such would not compromise the demonstration of meeting the risk targets. Additionally, many of the maintenance and spent fuel pool activities to be evaluated are not driven by plant-specific unique features, and as such would reflect the same results as existing operating units which support these risk targets, and may be slightly better if reflecting more recent relevant good practice.

14.6 Assessment That Risks Are As Low As Reasonably Practicable

This section uses the results of the fault and accident assessment chapters in addition to information from other chapters of the PCSR to demonstrate that there are no further reasonably practicable improvements to the AP1000 design that could be implemented and therefore the overall plant risk has been reduced ALARP.

The discussion of ALARP begins with relevant good practice. The AP1000 design has evolved through the use of proven fuel and major reactor component designs, including reactor vessel (RV), reactor internals, control rod drive mechanisms, reactor coolant pumps (RCPs), steam generators (SGs), and pressuriser. Proven major components reduce the chance of leakage or failures that would affect normal plant operation, possibly resulting in plant transients or forced outages with their associated impact on safety system challenges and occupational radiation exposures. Innovative design solutions have been used to reduce the complexity of engineered safety systems to make them significantly more reliable than those used in the previous generations of pressurised water reactor (PWRs). The use of Class 2 systems to provide defence in depth is also a best practice. These features of the AP1000 design are discussed in detail in Chapter 6 of this PCSR.

Chapter 5 summarises the codes and standards used for SSCs of each class. The relevant chapters of Volume 4 – Engineering Substantiation give further details of codes and standards used in the design of the AP1000 plant and justify the claim that these codes and standards demonstrate conformance with relevant good practice in their respective areas, and that they are met by the design:

- Chapter 16, Civil Engineering
- Chapter 17, Mechanical Engineering
- Chapter 18, Essential Electrical Systems
- Chapter 19, Control and Instrumentation
- Chapter 20, Structural Integrity

- Chapter 21, Reactor Chemistry
- Chapter 22, Fuel System, Nuclear and Thermal Hydraulic Design
- Chapter 23, Containment and Nuclear Ventilation Systems

The discussion of ALARP continues by examining options for reasonably practicable measures to reduce risk. This section reviews major design decisions taken during the evolution of the design from the previous generation of PWRs, giving a brief explanation of why certain features were selected and others were rejected, to demonstrate that the evolution process has resulted in a sufficiently optimised design from the point of view of safety.

Following this, the section discusses a number of exercises that have been carried out to identify potential risk reduction measures. These exercises constitute a systematic and comprehensive approach to risk reduction.

The ALARP assessment for the AP1000 design presented therefore consists of a number of inputs from different phases of the development and assessment of the design. Many of these exercises have been aimed at overall risk reduction and optioneering, and may not have included explicit risk-reward evaluations in the United Kingdom (UK) context of ALARP, but they have led to many risk-reduction measures being incorporated into the design that contribute to achieving an overall plant risk judged to be ALARP.

In this section, risk-reduction and ALARP arguments for the AP1000 plant are compiled from various sources:

- Review of major design decisions
- Use of PSA to inform the AP1000 design
- Severe accident mitigation design alternative (SAMDA) process
- Reliability assurance programmes
- Fault and hazard analysis
- Changes implemented in the UK specific design
- Human factors ALARP assessment
- ALARP issues raised in the GDA process

The final part of the ALARP assessment is to evaluate the options identified in terms of cost and benefit to show that the cost of any further improvements to the design would be grossly disproportionate to the risk reduction achievable.

14.6.1 Review of Major Design Decisions

A discussion of major design decisions dating back to the earlier AP600 design and its development into the AP1000 design is contained in Appendix 6A. In that discussion, the advantages and disadvantages of a number of design alternatives are reviewed with an assessment of their contribution to overall risk reduction.

These design choices fall under the following headings:

- Residual heat removal
- Containment design
- Control room systems
- Primary system design
- Duty systems

Additionally, Section 9.8.3 provides a detailed description of AP1000 design features specifically to address plant safety during shutdown modes.

Many of the options considered under the above headings were considered as part of the development of the AP600 design; however, the conclusions of those exercises apply equally to the AP1000 plant and the design choices have been carried over to its design. More detailed consideration of the major design choices and the rationale for them is presented in Appendix 6A. Addtionally, this information is detailed in Reference 14.1.

Westinghouse developed the AP1000 design to have an electric power production capability comparable with existing nuclear power stations but with a level of risk more than an order of magnitude lower than the best reactors currently operating. Current nuclear power stations have achieved an acceptable level of risk by evolving ever-increasing complexity with respect to their engineered safety features (ESFs), but this complexity is subject to the law of diminishing returns. If those same approaches (i.e., additional complexity) are taken to the extreme when developing a new design, very low levels of risk might be achievable; however, it would be at a price so high that it is no longer economical to build the nuclear power station.

Westinghouse has taken an alternative approach in designing the AP1000 plant. The complexity of the design is reduced by making the ESFs passive rather than active to the maximum degree feasible, thereby achieving a very high level of reliability and a simplified design. The basic design uses the concepts of inherent safety, fault tolerance, passive safety features, and defence in depth to produce a design that has significantly lower risks than earlier PWR designs.

14.6.2 Use of PSA to Inform the Design

The plant PSA was used throughout the AP1000 design program to review a number of areas to gain insight into risk-significant issues, leading to the implementation of a number of risk-reduction measures that significantly contribute to risk being ALARP for the plant as a whole. Appendix 10A provides historical information which specifically examined the following groups of design features:

- Design Improvements Introduced as a Result of the AP600 Design PSA
- Review of Defence-in-Depth Systems
- AP1000 Design Enhancements Implemented Based on PSA Insights

The total plant core damage and large release frequencies incorporating the examined design enchancements are demonstrated to support all applicable SAP Targets, as discussed in detail in Section 14.5. As such, the PSA was an invaluable tool in the development of the AP1000 plant design, and its use and overall results and conclusions support the claim of the overall plant risks being reduced ALARP.

14.6.3 Severe Accident Mitigation Design Alternatives Process

The SAMDA process was a United States (US) national programme specifically aimed at assessing candidate design alternatives to reduce the risk from severe accidents. As part of this process, an evaluation of candidate modifications to the design was conducted to evaluate the potential for such modifications to provide significant and practical improvements in the radiological risk profile. This process is entirely consistent with the ONR SAP (Reference 14.2) requirement to use severe accident analysis to consider further risk-reducing measures.

The process used for identifying and selecting candidate design alternatives included a review of SAMDAs evaluated for other plant designs. Several alternative designs evaluated previously for other plants were excluded from the present evaluation because they have already been incorporated or because they were not applicable to the AP1000 design. These include the following:

- Hydrogen ignition system (Already incorporated)
- Reactor cavity flooding system (Already incorporated)
- Reactor Coolant System (RCS) depressurisation (Already incorporated)
- RV exterior cooling (Already incorporated)
- RCP seal cooling (AP1000 uses sealless pumps)

Candidate design alternatives were selected based upon those evaluated for other plant designs as well as suggestions from design personnel. Additional candidate design alternatives were selected based upon an assessment of the plant PSA results. The following 15 design alternatives were finally selected for further evaluation:

- Diverse containment recirculation valves
- RNS located inside the containment
- Self-actuating containment isolation valves (CIVs)
- Improved reliability of the diverse actuation system (DAS)
- Diverse in-containment refuelling water storage tank (IRWST) injection valves
- SG safety valve flow directed to the IRWST
- SG shell-side passive heat removal system
- Chemical and volume control system (CVS) upgraded to mitigate small LOCAs
- Ex-vessel core catcher
- Secondary containment filtered ventilation
- Passive containment spray
- Filtered containment vent
- Increase of SG secondary side-pressure capacity
- High-pressure containment design
- Active high-pressure safety injection system

Two design changes additional to those identified in the SAMDA process were also considered for inclusion in the AP1000 design:

- Larger accumulators
- Larger fourth-stage ADS valves

14.6.3.1 Results of the Severe Accident Mitigation Design Alternative Process

An evaluation of these alternatives was performed using a bounding methodology, such that the potential benefit of each alternative is conservatively maximised. As part of this process, it was assumed that each alternative performs beyond expectations and completely eliminates the corresponding severe accident sequence. In addition, the capital cost estimates for each alternative were intentionally biased on the low side to maximise the risk-reduction benefit. This approach maximises the potential benefits associated with each alternative.

The results for the AP1000 plant show that despite the significant conservatism employed in the evaluation, only one of the alternatives evaluated (diverse containment recirculation valves) provides risk reductions that are cost-beneficial. A second (improved reliability of the DAS) was rejected in the SAMDA process but has subsequently been included in the UK design to increase availability during maintenance.

The results also show that even a conceptual "ideal SAMDA", one that reduces the total plant radiological risk to zero, would not be cost-effective. This is due primarily to the already low-risk profile of the AP1000 design.

14.6.3.2 Diverse Containment Recirculation Valves

The SAMDA alternative consists of changing the containment recirculation valve design so that two out of the four lines use diverse valves. In the AP600 design, each of the four lines contained a squib valve, two of the lines contained check valves, and the other two lines contained motor operated valves (MOVs). To provide diversity, the squib valves in two of the lines would be made diverse, thereby reducing the frequency of core melt by eliminating the common-cause failure (CCF) of the containment recirculation.

The four AP600 plant recirculation squib valves were of the "low-pressure" type and were a part of a single common-cause group. In the AP1000 plant, two of these valves that are in series with non-return valves are designated to be of the "high-pressure" type, in a common-cause group with the same design of valves on the IRWST injection lines. Thus, the CCF mode that fails the four recirculation lines in the AP600 plant is eliminated and replaced with the product of two CCF modes, one applicable to the group of six high-pressure squib valves and the other to the two low-pressure squib valves. This design change reduces the likelihood of recirculation failure.

To estimate the benefit from this SAMDA, the core damage sequences resulting from a failure of containment recirculation are assumed to be averted. Core damage sequences resulting from failure of containment recirculation correspond to PSA CDF at long term following failure of water recirculation to the RV after successful gravity injection.

14.6.3.3 Improved Reliability of the Diverse Actuation System

This potential design improvement consists of improving the reliability of the DAS, which actuates ESFs and allows the operator to monitor the plant status. The design change would add a third C&I cabinet and a third set of DAS instruments to allow the use of two-out-of-three logic instead of two-out-of-two logic.

This design improvement was rejected in the SAMDA process but has since been incorporated in the UK design to prevent a single failure from causing actuation during maintenance operations. This is considered best practice.

14.6.3.4 Potential Design Improvements Not Taken forward in the Severe Accident Mitigation Design Alternative Process

Table 14-1 gives the capital cost estimates in US dollars and UK pounds for each rejected alternative assessed in the SAMDA process. A dollar/pound exchange rate of 1.5 has been assumed. Each design alternative is discussed in turn and the argument given as to why the risk-reduction benefit is not commensurate with the capital cost.

Locate the Normal Residual Heat Removal System inside the Containment

This potential design improvement consists of placing the entire RNS and piping inside the containment pressure boundary. Doing so would prevent containment bypass due to ISLOCAs of the RNS. In previous PSAs of current-generation nuclear power plants, the ISLOCA is the leading contributor to plant risk because of large offsite consequences. A failure of the valves that isolate the low-pressure RNS from the high-pressure RCS causes the RNS to overpressurise and fail, releasing reactor coolant outside the containment, where it cannot be recovered for recirculation cooling of the core. The result is core damage and the direct release of fission products outside the containment.

In the AP1000 plant, the design of the RNS is already substantially enhanced over that of currently operating PWR plants: the AP1000 plant is designed with a higher design pressure and an additional isolation valve is provided. In the AP1000 plant PSA, no ISLOCAs contribute significantly to the CDF (Chapter 10), therefore, locating the RNS of the AP1000 plant inside the containment would provide virtually no risk-reduction benefit and so was not investigated further in terms of its cost.

Self-Actuating Containment Isolation Valves

This potential design improvement consists of improved containment isolation provisions on all normally open containment penetrations. The category of "normally open" is limited to normally open pathways to the environment during power and shutdown conditions, excluding closed systems inside and outside the containment, such as the RNS and CCS.

The design alternative would be either to add a self-actuating valve or to enhance the existing isolation valve inside containment to provide for self-actuation in the event that containment conditions indicate a severe accident. Conceptually, the design would be either an independent valve or an appendage to an existing fail-closed valve that would respond to post-accident ambient conditions within the containment: for example, a fusible link would melt in response to elevated ambient temperatures and close the valve.

The benefits of this potential design alternative are evaluated by generously assuming that it eliminates the containment isolation failure release category. This does not include induced containment failures that occur at the time of the accident, such as in cases of vessel rupture or anticipated transient without trip (ATWT). Thus, the component of the LRF and the component of collective dose due to failure of containment isolation events can each be set to zero. This potential design alternative ameliorates the consequences of a core damage event but has no effect on reducing its frequency. Given the low contribution of containment isolation failure to the LRF (approximately 5% of the total, Chapter 10), there is an ALARP case for not including this potential design alternative.

Improved Reliability of the Diverse Actuation System

This improvement consisting of improving the reliability of DAS by adding a third division of the control and instrumentation (C&I) system allowing for 2 out of 3 actuation logic rather than 2 out of 2 was rejected in the US SAMDA process but is included in the UK design. For additional information, please see Chapter 19.

Diverse In-Containment Refuelling Water Storage Tank Injection Valves

This potential design improvement consists of changing the IRWST injection valve designs so that two of the four lines use diverse valves. Each of the four lines is currently isolated by

a squib valve in series with a non-return valve. To provide diversity, the valves in two of the lines would be provided by a different vendor.

For the non-return valves, alternate vendors are available; however, it is questionable if non-return valves from different vendors would be sufficiently different to be considered diverse unless the type of non-return valve was changed from the current swing disk check to another type. The swing disk type is preferred for this application and other types are considered to be less reliable.

Squib valves are specialised valve designs for which there are few vendors. A vendor might not be willing to design, qualify, and build a reasonable squib valve design for this AP1000 plant application, given that they would only supply two valves per plant. As a result, this potential design improvement is not really practicable because of the uncertain availability of a second squib valve supplier and the uncertain reliability of another non-return valve type.

The cost estimate for this potential design improvement assumes, however, that a second squib valve vendor does exist and that this vendor provides only the two diverse IRWST squib valves.

The cost impact does not include the additional first-time engineering and qualification testing that would be incurred by the second vendor. Such costs would be expected to be up to or even exceeding £1M.

This change would reduce the frequency of core melt by eliminating the CCF of the IRWST injection.

The contribution to CDF from failure of IRWST injection valves is 8.1E-8/yr during power operation (see Chapter 10) and 3.3E-8/yr at shutdown (Chapter 10). Given the costs above, there is an ALARP case for not including this potential design alternative.

Steam Generator Safety Valve Flow Directed to the In-Containment Refuelling Water Storage Tank

This potential design improvement consists of providing all the piping and valves required for redirecting the flow from the SG safety and relief valves to the IRWST. An alternate, lower-cost option of this potential design improvement consists of redirecting only the first-stage safety valve to the IRWST. This system would prevent or reduce fission product release from bypassing the containment in the event of an SGTR event.

The cost-benefit analysis for this design alternative is essentially the same as for the diverse IRWST injection valves with the same conclusion that there is an ALARP case for not including it.

Steam Generator Shell-Side Passive Heat Removal System

This potential design improvement consists of providing a passive safety-significant heat removal system to the secondary side of the SGs. The system would provide closed-loop cooling of the secondary side using natural circulation and stored water cooling.

This would prevent a loss of primary heat sink in the event of a loss of starup feedwater (SFW) and the passive residual heat removal (PRHR) heat exchanger (HX). A perfect secondary heat removal system would eliminate transients from each of the release categories. To evaluate the benefit of this potential design improvement, the frequencies of all

the transient sequences are subtracted from the overall frequency of each of the release categories and the risk is recalculated.

Chemical and Volume Control System Upgraded to Mitigate Small Loss-of-Coolant Accidents

The current design of the CVS for the AP1000 plant is capable of supplying pressurised water at a rate sufficient to keep the reactor core covered in the event of an RCS leak of a magnitude within the very small LOCA category. The CVS can provide sufficient makeup of the reactor coolant in the event of a failure of a small line of 0.97 cm (3/8 inch) or less. Only one CVS pump would be needed for this duty.

The CVS is regarded as an active duty system, which supports normal operations, and acts as a first line of defence to reduce the unnecessary actuation and operation of the safety systems. The AP1000 plant includes several active systems that provide defence-in-depth capabilities for RCS makeup and decay heat removal. These active systems are the first line of defence to reduce challenges to the passive systems in the event of plant transients.

The potential design-improvement-proposed system is intended to enhance its capability so that it could intervene following a small or intermediate LOCA, such as would result from an RCS leak or a tube leak within the PRHR HX, to keep the core covered during such LOCAs.

This increase in capability would be achieved by means of the following SAMDA enhancements:

- Connections provided from the IRWST containment recirculation to the CVS
- A second line added from the CVS makeup pumps to the RCS

A perfect, upgraded CVS is assumed to prevent core damage in the following release categories: RCS leak, PRHR HX tube ruptures, small LOCA, and intermediate LOCA. The CVS is assumed to have perfect support systems (power supply and component cooling) and to work in all situations regardless of the CCFs of other systems.

Ex-Vessel Core Catcher

This potential design improvement consists of designing a structure in the containment cavity or using a special concrete or coating that will inhibit core-concrete interaction even if the debris bed dries out. A perfect core catcher would prevent core-concrete interaction for all cases; however, the AP1000 plant incorporates a wet cavity design in which ex-vessel cooling is used to maintain the core debris in the vessel to prevent ex-vessel phenomena such as core-concrete interaction. Consequently, containment failure due to core-concrete interaction is not considered in detail for the AP1000 plant large-release PSA.

For cases in which RV flooding fails, it is assumed that containment failure would occur due to ex-vessel steam explosion or core-concrete interaction. This containment failure is assumed to be an early containment failure (ECF) (due to ex-vessel steam explosion) even though core-concrete interaction and basemat melt-through would be a late containment failure. To conservatively estimate the risk reduction of an ex-vessel core catcher, this design change is assumed to eliminate the ECF release category.

Secondary Containment Filtered Ventilation

This potential design improvement consists of providing the middle and lower annulus of the secondary concrete containment with a passive annulus filter system for filtration of elevated

releases. The passive filter system would be operated by drawing a partial vacuum on the middle annulus through charcoal and high-efficiency particulate air (HEPA) filters. The partial vacuum is drawn by a diffusion pump with motive flow from compressed gas tanks.

The secondary containment would then reduce particulate fission product release from any failed containment penetrations (containment isolation (CI) failure). To evaluate the benefit from such a system, this design change is assumed to eliminate the CI release category.

Passive Containment Spray

This potential design improvement involves adding a passive safety-significant spray system and all associated piping and support systems to the AP1000 plant containment.

A passive containment spray system would result in risk benefits in the following ways:

- Scrubbing of fission products could be done, primarily for CI failures.
- Assuming appropriate timing, containment spray could be used as an alternate means of flooding the RV and debris-quenching should vessel failure occur.
- Containment spray could also be used to control containment pressure for cases in which the passive containment cooling system (PCS) has failed.

To envelop these potential risk benefits, the risk-reduction evaluation will assume that containment sprays are perfectly effective for each of these benefits with the exception of fission product scrubbing for containment bypass. Thus, the risk reduction can be conservatively estimated by assuming that all release categories except containment bypass are eliminated.

Filtered Containment Vent

This potential design improvement consists of placing a filtered containment vent and all associated piping and penetrations into the AP1000 plant containment design. The filtered vent could be used to vent the containment to prevent catastrophic overpressure failure, and it would also provide filtering capability for source term release. With respect to the AP1000 plant PSA, the possible scenario in which the filtered vent could result in risk reduction would be late containment overpressure failures. Other containment overpressure failures occur because of dynamic severe accident phenomena, such as hydrogen burn and steam explosion.

The late containment failures for the AP1000 plant are failures of the PCS. Analyses have indicated that for scenarios with PCS, air cooling might limit the containment pressure to less than the ultimate pressure; however, for the large-release PRA, failure of the PCS is assumed to result in containment failure based on an adiabatic heatup.

To conservatively consider the risk reduction of a filtered vent, the use of a filtered vent to preclude a late containment failure will be evaluated. A decontamination factor (DF) of 1000 will conservatively be assumed for each PRA Level-1 accident classification, even though it is realised that the dose due to noble gases will not be impacted by the filtered vent because 100 percent of the noble gas fission products will still be released. The risk reduction is therefore equal to the DF assumed because the PRA CDF accident classification frequencies do not change.

Increase of Steam Generator Secondary Side Pressure Capacity

This potential design improvement consists of increasing the design pressure of the SG secondary side and safety valve setpoint to the degree that an SGTR will not cause the secondary system safety valve to open. The design pressure would have to be increased sufficiently so that the combined heat capacity of the secondary system inventory and the PRHR system could reduce the RCS temperature to below T_{sat} for the secondary design pressure.

Although specific analysis would have to be performed, it is estimated that the design pressure would have to be increased by tens of bar (several hundred psi). This design would also prevent the release of fission products that bypass the containment via the SGTR.

High-Pressure Containment Design

This potential design improvement consists of using the massive high-pressure containment design in which the design pressure of the containment is approximately 20 bar (300 psi) for the AP1000 plant containment.

The massive containment design has a passive containment cooling feature much like the AP1000 plant containment. The high design pressure is considered only for prevention of containment failures due to severe accident phenomena, such as steam explosions and hydrogen detonation. A perfect high-pressure containment design would reduce the probability of containment failures but would not reduce the frequency or magnitude of the release from an unisolated containment (containment isolation failure or containment bypass). To estimate the risk reduction of a high-pressure containment design, this design is assumed to eliminate the containment failure release categories. This design change was not incorporated since it is judged that the likely cost is disproportionate to the risk reduction that would be achieved.

Active High-Pressure Safety Injection System

This potential design improvement consists of adding a safety-significant active high-pressure safety injection pump and all associated piping and support systems to the AP1000 design. A perfect high-pressure safety injection system would prevent core melt for all events except excessive LOCA and ATWT. To estimate the risk reduction, therefore, only the contributions to vessel rupture and ATWT need to be considered. Including an active high-pressure safety injection system would contravene the fundamental design objective of the AP1000 plant that all safety systems should be passive. It would require a high-pressure safety injection pump or pumps and all associated piping, ac power supplies, and support systems. All equipment would have a high safety classification. This would be very expensive and would not provide any significant risk reduction; therefore, this design change was not incorporated.

Larger Accumulators

Increasing the size of the accumulators would result in a significant increase in cost that would be greater than the cost threshold established by the perfect SAMDA evaluation. To have any benefit in the PRA, the accumulators would have to be increased in size sufficiently to change the large LOCA success criteria from two of two accumulators to one of two accumulators.

Westinghouse estimates that the accumulator tanks would have to be increased in size from 56 to 112 m^3 (2000 to 4000 ft^3) and the hardware costs associated with this change would be significant. Such a size increase would also likely result in a change to the design of the direct vessel injection (DVI) piping subsystem.

Note that the most recent large LOCA analysis shows that the current accumulator size can in fact prevent core melt using only one accumulator, so this change should not be considered.

The design of this piping system was established early in the AP1000 plant design program, and any change in the DVI piping would result in significant piping reanalysis of the DVI piping. Westinghouse estimates the redesign costs associated with the changes in hardware and piping redesign to be significantly greater than the cost threshold established for the perfect SAMDA discussed above; therefore, this design change was not incorporated.

Larger Fourth-Stage Automatic Depressurisation System Valves

Increasing the size of the fourth-stage ADS valves would result in a significant increase in cost associated with redesigning the AP1000 plant loop piping and fourth-stage piping configuration. The AP1000 plant ADS valves were already increased in size compared with the AP600 plant valves by more than the ratio of the power uprate of the AP1000 plant. To have any benefit in the PRA, the fourth-stage ADS valves would have to be increased in size sufficiently to change the LOCA success criteria from three of four valves to two of four valves.

To accommodate such a change, Westinghouse estimates that the fourth-stage ADS valves would have to increase in size from 356 to 457 mm (14 to 18 inches); the associated piping would also increase accordingly. In addition, the common fourth-stage inlet piping that connects to the hot leg would have to increase in size from 457 to at least 508 mm (18 to 20 inches). This would require a significant redesign of the squib valve and would also result in redesign of the ADS stage 4 piping, which in turn would impact the design of the reactor coolant loop piping.

Such a redesign would require Westinghouse to perform additional confirmatory testing of the passive core cooling system (PXS) to verify that the behaviour of the passive safety systems was not adversely impacted. Westinghouse estimates the cost of this change to be significantly higher than the cost threshold of the perfect SAMDA. This design change was therefore not incorporated.

14.6.4 Reliability Assurance Programmes

The AP1000 plant reliability assurance programme (RAP) described in Chapter 5 represents a dual-stage approach to the design and operation of the AP1000 plant to provide increased confidence in plant reliability and the corresponding safety of the public. The first stage of the RAP is the design stage, referred to as the design reliability assurance programme (D-RAP). The second stage of the RAP is referred to as the operational reliability assurance programme (O-RAP).

The AP1000 plant D-RAP is implemented as an integral part of the AP1000 design process to provide confidence that reliability is designed into the plant and that the important reliability assumptions made as part of the AP1000 plant PSA will remain valid throughout its lifetime.

Reliability of AP1000 plant SSCs will be ensured by applying operational phase reliability assurance activities (OPRAAs), which are contained in various operating plant programmes.

The OPRAAs comprise site administrative, maintenance, operational, and testing programmes to enhance operational phase reliability throughout the designed plant life.

In addition to this, the AP1000 plant designers have systematically reviewed the reliability of SSCs other than the Class 1 systems, particularly those providing defence in depth. This programme, the AP1000 reliability programme for non-Class 1 systems with safety importance (ANSIS), has systematically reviewed the availability controls relevant to these Class 2 SSCs to ensure their reliability in operation.

These programmes are primarily aimed at the reliability of SSCs throughout the plant life. This systematic approach to reliability contributes to risk minimisation and is a contribution to the overall ALARP argument.

14.6.5 Changes Implemented in the UK Design

As part of licensing the AP1000 plant in the UK, a number of design alternatives have been incorporated for the UK AP1000 design. The ALARP implications of these changes are discussed in the relevant chapters of the PCSR.

14.6.6 As Low As Reasonably Practicable Conclusions

The design philosophy for the AP1000 has been to take the best of the proven design features from the previous generation of PWRs and to substantially improve the safety through the use of innovative passive engineered safety systems with defence in depth provided by more traditional systems. This approach constitutes good practice and has led to a design whose risks are very low.

Further, it is clear that the designers of the AP1000 plant have systematically sought ways of further reducing risk during every phase of development from the original AP600 concept to the fully developed AP1000 design. Risk reduction has been an intimate and natural part of the design and risk evaluation process.

The designers have also used appropriate analysis tools such as the accident analyses, PSA and severe accident assessments to systematically identify potential risk-reduction measures, many of which have been implemented in the design on the basis that they are the ALARP option or that they constitute good practice.

During the course of the development of this PCSR, systematic fault studies have been performed, beginning with a systematic, auditable, and comprehensive identification of faults followed by systematic DB and probabilistic assessments. For each fault analysed, further ALARP measures were sought, and specific implementation of changes are noted throughout Chapter 9. The total plant risk has been lowered to the point that it has become very difficult to find further cost-effective plant improvements, especially since the benefit threshold is so low.

The conclusion from this section is that risk-reduction and ALARP assessments have been carried out systematically and comprehensively to the point that there are no further reasonably practicable improvements that could be implemented and, therefore, risk has been reduced ALARP.

14.7 Summary of AP1000 Plant ALARP Assessment

This chapter ssynthesises the results and conclusions from the internally initiated faults (Chapter 9), PSA (Chapter 10), internal and external hazards assessments (Chapters 11 and

12), and the human factors assessments (Chapter 13). These assessments have identified the SSCs that are important for safety and the requirements placed upon them by the safety case in terms of performance and reliability.

Operator actions identified in the DB analysis (Chapter 9) or the PSA (Chapter 10) are collected into the HAD, screened for risk significance, and for a sample of actions, analysed for human error potential as discussed in Chapter 13.

With all these identifications in place, the results of the various analyses have been compared with the dose and risk targets given in the ONR SAPs. The results show that in most cases the calculated doses and risks are below the BSO of the relevant frequency and dose band target. In the small number of cases where this is not so, the doses or risks are still below the BSL with adequate margin.

Finally, this chapter has brought together the various ALARP assessments, including historical and individual ALARP evaluations coming from the fault and hazard analyses, to demonstrate that the risks from the AP1000 design and operation are ALARP.

14.8 References

14.1 Westinghouse Report APP-GW-GER-005, Rev. 1, "Safe and Simple: The Genesis and Process of the AP1000 Design," August 2008.

14.2 "Safety Assessment Principles for Nuclear Facilities," Rev. 0, Office for Nuclear Regulation, 2014.

14.3 Westinghouse Report UKP-GW-GL-500, Rev. 0, "AP1000 UK Limits and Condition Process Description," December 2015.

14.4 Westinghouse Report UKP-GW-GL-501, Rev. 0, "AP1000 UK Generic Technical Specifications," January 2016.

Table 14-1 Estimated Costs of Improvement Options

	Estimated Cost of the Design Alternatives	US $	£
1	Locate the RNS inside the containment.	Virtually no risk-reduction benefit and so was not investigated further in terms of its cost	
2	Self-actuating CIVs	$33,000	£22,000
3	Improved reliability of the DAS	$470,000	£313,000
4	Diverse IRWST injection valves	$570,000	£380,000
5	SGTR safety valve flow directed to the IRWST	$620,000	£413,000
6	SGTR shell-side passive heat removal system	$1,300,000	£867,000
7	CVS upgraded to mitigate small LOCAs	$1,500,000	£1,000,000
8	Ex-vessel core catcher	$1,660,000	£1,110,000
9	Secondary containment filtered ventilation	$2,200,000	£1,470,000
10	Passive containment spray	$3,900,000	£2,600,000
11	Filtered containment vent	$5,000,000	£3,330,000
12	Increase of SGTR secondary-side pressure capacity	$8,200,000	£5,470,000
13	High-pressure containment design	$50,000,000	£33,300,000
14	Active high-pressure safety injection system	Extremely expensive, also contravenes a fundamental design objective	
15	Larger accumulators	Significant increase in cost	
16	Larger fourth-stage ADS valves	Significant increase in cost	

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

None.

LIST OF ABBREVIATIONS AND ACRONYMS

ac	alternating current
ACI	American Concrete Institute
ADS	automatic depressurisation system
AISC	American Institute of Steel Construction
AMCA	Air Movement and Control Association
API	American Petroleum Institute
ANSI	American National Standards Institute
ASME	American Society of Mechanical Engineers
ASS	auxiliary steam supply system
BAST	boric acid storage tank
BDS	steam generator blowdown system
C&I	control and instrumentation
C-I	(Seismic) Category I
C-II	(Seismic) Category II
CAGI	Compressed Air and Gas Institute
CAS	compressed air system
CCS	component cooling water system
CDS	condensate system
CES	condenser tube cleaning system
CFS	turbine island chemical feed system
CMS	condenser air removal system
CMT	core make-up tank
CNS	containment system
CPS	condensate polishing system
CRDM	control rod drive mechanism
CSA	control support area
Ctmt	containment
CVS	chemical and volume control system
CWP	cask washdown pit
CWS	circulating water system
DAS	diverse actuation system
DBA	design basis accident
DB	design basis
dc	direct current
DOS	standby diesel and auxiliary boiler fuel oil system
DTS	demineralised water treatment system
DVI	direct vessel injection
DWS	demineralised water transfer and storage system
ECS	main ac power system
EDS	Class 2 dc and uninterruptible power supply system
EFS	communication systems
EGS	grounding and lightning protection system
EHS	special process heat tracing system
ELS	plant lighting system
EMIT	examination, maintenance, inspection, and testing
EQS	cathodic protection system
ESF	engineered safety feature
FHS	fuel handling and refuelling system
FPS	fire protection system
FTC	fuel transfer canal

LIST OF ABBREVIATIONS AND ACRONYMS (cont.)

FW	feedwater
FWS	main and startup feedwater system
GNS	general non-safety
GRCA	gray rod cluster assembly
GSS	gland seal system
HCS	generator hydrogen and CO2 system
HDS	heater drain system
HEPA	high-efficiency particulate air
HL	hot leg
HP	high pressure
HSS	hydrogen seal oil system
HVAC	heating, ventilation and air conditioning
HX	heat exchanger
IDS	class 1E dc and UPS system
IHP	integrated head package
IIS	in-core instrumentation system
IPSTAC	investment protection short-term availability controls
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronic Engineers
ILRT	integrated leak rate test
IRC	inside reactor containment
IRWST	in-containment refuelling water storage tank
LOCA	loss-of-coolant accident
LOS	main turbine and generator lube oil system
MC	metal containment
MCR	main control room
M/f Std	manufacturer's standard
MFCV	main feedwater control valve
MFW	main feedwater
MHS	mechanical handling system
MSIV	main steam isolation valve
MSR	moisture separator reheater
MSS	main steam system
MTS	main turbine system
NEC	Nuclear Energy Code
NEMA	National Electrical Manufacturers Association
NFPA	National Fire Protection Association
NNS	non-nuclear seismic
OCS	operation and control centre system
ORC	outside reactor containment
PAMS	post-accident monitoring system
PCCAWST	passive containment cooling ancillary water storage tank
PCCWST	passive containment cooling water storage tank
PCS	passive containment cooling system
PCSR	Pre-Construction Safety Report
PGS	plant gas system
PLS	plant control system
PMS	protection and safety monitoring system
PORV	power operated relief valve
PRHR	passive residual heat removal
PSS	primary sampling system

LIST OF ABBREVIATIONS AND ACRONYMS (cont.)

PWS	potable water system
PXS	passive core cooling system
RAP	reliability assurance programme
RC	release category
RCCA	rod cluster control assembly
RCDT	reactor coolant drain tank
RCP	reactor coolant pump
RCS	reactor coolant system
RHX	regenerative heat exchanger
RNS	normal residual heat removal system
RMS	radiation monitoring system
RV	reactor vessel
RVLIS	reactor vessel level instrumentation system
RWS	raw water system
RXS	reactor system
SAP	safety assessment principle
SES	plant security system
SDS	sanitary drainage system
SFP	spent fuel pool
SFS	spent fuel pool cooling system
SFW	startup feedwater
SG	steam generator
SGS	steam generator system
SMACNA	Sheet Metal and Air Conditioning Contractors' National Association
SMS	special monitoring system
SSC	system, structure, or component
SSE	safe shutdown earthquake
SSS	secondary sampling system
SWS	service water system
TCS	turbine building closed cooling water system
TDS	turbine island vents, drains, and relief system
TEMA	Tubular Exchange Manufacturers Association
TOS	main turbine control and diagnostics system
TVS	closed circuit television system
UK	United Kingdom
UL	Underwriters Laboratories
UPS	uninterruptible power supplies
VAS	radiologically controlled area ventilation system
VBS	nuclear island nonradioactive ventilation system
VCS	containment recirculation cooling system
VES	main control room emergency habitability system
VFS	containment air filtration system
VHS	health physics and hot machine shop HVAC system
VLS	containment hydrogen control system
VRS	radwaste building HVAC system
VTS	turbine building ventilation system
VUS	containment leak rate test system
VWS	central chilled water system
VXS	annex/auxiliary building nonradioactive ventilation system
VYS	hot water heating system

LIST OF ABBREVIATIONS AND ACRONYMS (cont.)

VZS	diesel generator building heating and ventilation system
WGS	gaseous radwaste system
WLS	liquid radwaste system
WR	wide range
WRS	radioactive waste drain system
WSS	solid radwaste system
WWS	waste water system
ZAS	main generator system
ZBS	excitation and voltage regulation system
ZOS	onsite standby power system
ZVS	excitation and voltage regulation system

15 ENGINEERING SUBSTANTIATION

15.1 Introduction

The purpose of Volume 4 of the Pre-Construction Safety Report (PCSR) is to provide the evidence that the systems making up the AP1000 standard design meet the requirements placed on them by the safety case presented in other parts of the PCSR.

This chapter lists the sources of claims on systems, structures, or components (SSCs) in the safety case and the requirements on SSC performance that are implied by them. The chapter then introduces the chapters of Volume 4, which provide evidence that the SSCs identified in the fault assessments (Volume 3) can meet the requirements arising from the claims made on them in the safety case.

These requirements come from the following sources:

- Performance requirements from the transient analysis performed as part of the design basis (DB) assessment
- Survivability and operability requirements arising from the need to operate in normal plant environmental conditions and the environmental conditions following a design basis accident (DBA)
- Reliability requirements from the probabilistic assessment of DB faults and the probabilistic safety assessment
- Separation and segregation requirements from the internal hazards assessment
- Seismic qualification requirements arising from the external hazards assessment
- Quality requirements for design, manufacturing, installation, commissioning, maintenance, and testing
- Durability requirements related to expected plant service life

The purpose of the engineering substantiation volume is to provide the evidence that these requirements are met by the SSCs as designed and by the way they are tested and maintained throughout the life of the plant.

The requirements on the SSCs from the safety case are detailed in the engineering schedule (Reference 15.1) and summarised in the tables in Appendix 15A. These tables will be further developed during site-specific licensing to form the basis of the maintenance schedule.

15.2 Performance Requirements

The transient analysis performed as part of the DB assessment to demonstrate that system limits such as departure from nucleate boiling ratio or pressuriser level are not exceeded assumes that the various systems claimed in the analysis, whether as the principal means of providing each safety function or as the alternate means (in the case of frequent faults) or SSCs providing defence in depth, meet certain performance requirements. These performance requirements will depend on the safety function being provided but will be given in terms of physical parameters such as flow rate, fluid pressure, fluid capacity, or reactivity worth.

15.3 Survivability and Operability Requirements

Chapter 5 provides an overview of the equipment qualification requirements for defined SSCs. Equipment qualification requirements are based on design requirements and location of the SSC within the plant. For SSCs that are required to operate following a DBA, the defined SSCs must be able to perform their intended function in the environmental conditions corresponding to their location following an accident. These requirements are implemented through a defined environmental qualifications programme.

15.4 Reliability Requirements

Accident sequences are discussed in Chapter 8. The frequency of the sequence is the initiating event frequency multiplied by the probabilities of failure of each of the SSCs making up the sequence.

The demonstration that reliability requirements are met involves the use of analysis or operational data plus assessment of dependent failures (common-cause failures). Section 5.9 discusses equipment reliability in more detail.

15.5 Separation and Segregation Requirements

Selected systems identified in the safety case have redundant equipment to meet single-failure criteria. Where survivability of the redundant equipment is threatened by such events as internal hazards, protection is achieved by providing the appropriate level of separation or segregation of the redundant equipment. Reference 15.3 defines the separation criteria for SSCs.

15.6 Seismic Qualification

Chapter 5 provides an overview of seismic categorisation. Certain SSCs identified in the safety case are required to operate after a seismic design basis event. Class 1 SSCs are classified as seismic Category I (C-I), which implies the requirement that the SSC does not fail and it can perform its intended function after a design basis earthquake.

Other SSCs are not required to operate during or after a design basis earthquake but do have the requirement to retain their structural integrity. Such SSCs are designated as seismic Category II (C-II).

Where the failure of an SSC in a design basis earthquake has the capacity to adversely affect a Class 1 SSC or incapacitate a plant operator in the control room, there is a higher requirement on its structural integrity. Such SSCs are referred to as seismic C-II/C-I and apply seismic C-II requirements.

Seismic qualification substantiates the seismic withstand of SSCs appropriate to their seismic classification. Reference 15.2 defines the seismic design criteria that apply to SSCs that must be seismically designed.

15.7 Quality Requirements

The classification methodology described in Chapter 5 is the means used to capture the safety significance of SSCs. This has implications for the standard of design, manufacturing, construction, maintenance, and testing to be used, and the appropriate codes and standards become requirements on the corresponding SSCs.

15.8 Durability Requirements

The design life of the AP1000 plant is 60 years. Many components will have to be repaired or replaced during the lifetime of the plant; however, this is not possible for some SSCs, particularly civil structures. For these, the necessity of retaining structural integrity or functionality over a 60-year lifetime will place requirements on the design, construction, or maintenance of the SSC. Both pre-operational and in-service inspection and testing requirements are defined to support the defined reliability claims on SSCs.

15.9 Substantiation

Substantiation of the claims made on SSCs in the safety case involves providing arguments and evidence to show that the design and operation of SSCs meet the requirements that come from normal operations and the safety case as described above.

For convenience in this PCSR, this substantiation is given by engineering discipline in the remaining chapters of this volume.

15.9.1 Civil Engineering

In Chapter 16, the claims made on the AP1000 plant civil structures are substantiated. This includes normal and abnormal (accident) loads and loading from design basis earthquakes and other external hazards.

15.9.2 Mechanical Engineering

In Chapter 17, the claims made on the AP1000 plant mechanical systems are substantiated. In particular, the claims made on the performance and reliability of the Class 1 protection systems and the Class 2 systems claimed as defence in depth are substantiated.

15.9.3 Electrical Systems

In Chapter 18, the claims made on the Class 1 and standby Class 2 electrical systems in terms of loading and reliability are substantiated, along with claims on normal alternating current systems during normal operation.

15.9.4 Control and Instrumentation

In Chapter 19, the claims made on the Class 1 protection system, the Class 2 diverse actuation system (DAS), the Class 2 functionality provided by part of the normal operations control system, and other control and instrumentation systems are substantiated.

15.9.5 Structural Integrity

In Chapter 20, the structural integrity classification and supporting claims for plant components are defined. The chapter primarily focuses on components with the potential to have a structural integrity classification of High Safety Significant or High Integrity.

15.9.6 Reactor Chemistry

In Chapter 21, the claims made on primary circuit chemistry in relation to reactivity control, primary circuit activity levels, corrosion resistance, and prevention of stress corrosion cracking are substantiated. Also, the corresponding claims on the secondary (steam raising) system are also substantiated.

15.9.7 Fuel Design

In Chapter 22, the claims made on the fuel design relating to performance in accident conditions such as clad ballooning and pellet-clad interactions are substantiated.

15.9.8 Containment and Ventilation

In Chapter 23, the claims made in relation to radioactivity retention and containment by the containment and ventilation systems are substantiated.

15.10 References

15.1 Westinghouse Report UKP-GW-GL-144, Rev. 3, "AP1000 UK Safety Categorisation and Classification of Systems, Structures, and Components," January 2017.

15.2 Westinghouse Report APP-GW-G1-003, Rev. 6, "AP1000 Seismic Design Criteria," August 2011.

15.3 Westinghouse Report APP-GW-P1-002, Rev. 1, "AP1000 General Layout Criteria," April 2015.

APPENDIX 15A
ENGINEERING SCHEDULE

The DB analysis presented in Chapter 9 identifies the SSCs required to provide the safety functions necessary to meet the DB requirement that the DB targets (SAP Target 4) should be met, and that adequate diversity should be provided for each safety function. The analysis also identifies SSCs provided in the design to achieve defence in depth.

The classification scheme given in Chapter 5 for SSCs is used to identify those SSCs that play an important part in ensuring nuclear safety. This in turn helps to define the quality requirements placed on those SSCs during design and manufacture, and through life. In particular, the safety class of a given SSC can be used to determine which codes, standards, and seismic design considerations are appropriate to the design and manufacture of that SSC, and to specify examination, maintenance, inspection, and testing (EMIT) regimes for that SSC.

Further, for each SSC identified in the safety case, transient and other analyses lead to performance requirements and reliability requirements that will be appropriate to the importance of the SSC to safety.

This appendix lists the AP1000 SSCs claimed in the safety case, principally in Chapter 9, Fault and Accident Analysis. The safety function and category provided by each SSC is given along with its safety classification. The listing corresponds to the list given in Reference 15A.1.

Table 15A-1 contains the categorisation and classification of the AP1000 mechanical SSCs.

Table 15A-2 contains the categorisation and classification of the AP1000 electrical SSCs.

Table 15A-3 contains the categorisation and classification of the AP1000 control and instrumentation (C&I) SSCs.

Table 15A-4 contains the categorisation and classification of the AP1000 structural SSCs.

These tables will be developed as the safety case is developed to a site-specific PCSR, and will eventually contain a complete set of requirements for each SSC, and form the basis of the maintenance schedule.

15A.1 Reference

15A.1 Westinghouse Report, UKP-GW-GL-144, Rev. 3, “AP1000 UK Safety Categorisation and Classification of Systems, Structures, and Components,” January 2017.

Table 15A-1. AP1000 UK Categorisation and Classification of Mechanical SSCs

Tag Number	Description	AP1000 Class	Seismic Category	Principal Design Code	UK Safety Category	Safety Function(s) Provided by the SSC	UK Safety Class	Justification of the Safety Class
Auxiliary Steam Supply System (ASS) Location: Turbine Building								
System components are Class E					GNS	No nuclear safety implications.	GNS	SSCs are not designed or considered in the application of a safety function.
Steam Generator Blowdown System (BDS) Location: Turbine Building								
BDS-PL-V009	Discharge to WLS Vent	D	NNS	ASME B16.34	B	Preventing the release of radioactive waste material from onsite radioactive waste systems	2	Principal means of fulfilling the safety function
BDS-PL-V037	Discharge to WLS Valve	D	NNS	ASME B16.34	B	Preventing the release of radioactive waste material from onsite radioactive waste systems	2	Principal means of fulfilling the safety function
BDS-PL-V046	WWS Contained Flow Connection	D	NNS	ASME B16.34	B	Preventing the release of radioactive waste material from onsite radioactive waste systems	2	Principal means of fulfilling the safety function
–	BDS Purification Loop	E	NNS	Industry Std	C	Provides long-term support of a Category A safety function.	3	The BDS contributes to the control of steam generator secondary cycle water chemistry by removal of the blowdown flow from the secondary side of each steam generator during normal operation.
Balance of system components are Class E					GNS	No nuclear safety implications.	GNS	SSCs are not designed or considered in the application of a safety function.
Compressed Air System (CAS) Location: Various								
CAS-PL-V014	Instrument Air Supply Outside Containment Isolation	B	I	ASME III-2	A	Prevention of the release of radioactive material from the containment.	1	The isolation valves are the principal means of providing containment isolation.
CAS-PL-V015	Instrument Air Supply Inside Containment Isolation	B	I	ASME III-2				
CAS-PL-V027	Containment Penetration Test Connection Isolation	B	I	ASME III-2				
CAS-PL-V204	Service Air Supply Outside Containment Isolation	B	I	ASME III-2				
CAS-PL-V205	Service Air Supply Inside Containment Isolation	B	I	ASME III-2				
CAS-PL-V219	Containment Penetration Test Connection Isolation	B	I	ASME III-2				
CAS-PY-C02	Containment Instrument Air Inlet Penetration	B	I	ASME III, MC	A	Prevention of the release of radioactive material from the containment.	1	Each containment penetration provides a principal means of maintaining containment integrity.
CAS-PY-C03	Containment Service Air Inlet Penetration	B	I	ASME III, MC				
	Instrument Air Subsystem	E	NNS	Industry Std	C	Removal of nuclear heat from the reactor coolant during normal operation.	3	The CAS contributes to the removal of nuclear heat from the reactor coolant by: 1) supporting operation of power generation valve functions (e.g., MFCV modulation) and 2) positioning Class 1 valves in their power generation state to support continued power operation (e.g., PRHR and CMT discharge valves).
Balance of system components are Class E					GNS	No nuclear safety implications.	GNS	SSCs are not designed or considered in the application of a safety function.

Table 15A-1. AP1000 UK Categorisation and Classification of Mechanical SSCs (cont.)

Tag Number	Description	AP1000 Class	Seismic Category	Principal Design Code	UK Safety Category	Safety Function(s) Provided by the SSC	UK Safety Class	Justification of the Safety Class
Component Cooling Water System (CCS) Location: Auxiliary Building and Turbine Building								
CCS-ME-01A/B	Heat Exchangers, CCS and SWS Side	D	NNS	ASME VIII	A	Removing the nuclear core decay (or residual) heat from the reactor coolant during normal operations and accident conditions (includes those SSCs that provide the heat sink for the removal of decay heat from the reactor coolant).	2	CCS is a heat sink for the RNS, which is a defence in depth decay heat removal system.
CCS-MP-01A/B	Pumps	D	NNS	Hydraulic Institute Stds				
CCS-MT-01A/B	Tanks	D	NNS	ASME VIII				
–	RNS Cooling subsystem	D	NNS	ANSI B31.1				
–	SFS Cooling subsystem	D	NNS	ANSI B31.1	A	Maintaining spent fuel integrity such that significant radioactive releases do not occur (as a result of impacts or overheating).	2	CCS is a heat sink for the SFS, which is a defence in depth spent fuel cooling system.
CCS-PL-V200	CCS Containment Isolation Valve – Inlet Line ORC	B	I	ASME III-2	A	Maintaining the integrity of the containment; thereby minimising the release of radioactive material from the containment.	1	The isolation valves are the principal means of fulfilling the safety function.
CCS-PL-V201	CCS Containment Isolation Valve – Inlet Line IRC	B	I	ASME III-2				
CCS-PL-V207	CCS Containment Isolation Valve – Outlet Line IRC	B	I	ASME III-2				
CCS-PL-V208	CCS Containment Isolation Valve – Outlet Line ORC	B	I	ASME III-2				
CCS-PL-V209	Containment Isolation Valve Test Connection – Outlet Line	B	I	ASME III-2				
CCS-PL-V214	CCS Supply Containment Isolation – IRC	C	I	ASME III-3				
CCS-PL-V215	CCS Supply Containment Isolation Valve Test Connection – IRC	C	I	ASME III-3				
CCS-PL-V216	Containment Leak Test Outlet Line – IRC	C	I	ASME III-3				
CCS-PL-V217	Containment Isolation Valve V207 Body Test Connection Valve	C	I	ASME III-3				
CCS-PL-V270	CCS IRC Relief Valve	C	I	ASME III-3				
CCS-PL-V271	CCS IRC Relief Valve	C	I	ASME III-3				
CCS-PL-V220	CCS Containment Isolation Relief Valve	B	I	ASME III-2				
CCS-PL-V257	Containment Isolation Valve Test Connection – Inlet Line	B	I	ASME III-2				
CCS-PY-C01	Containment Supply Header Penetration	B	I	ASME III, MC	A	Maintaining the integrity of the containment; thereby minimising the release of radioactive material from the containment.	1	Each containment penetration provides a principal means of maintaining containment integrity.
CCS-PY-C02	Containment Return Header Penetration	B	I	ASME III, MC				

Table 15A-1. AP1000 UK Categorisation and Classification of Mechanical SSCs (cont.)

Tag Number	Description	AP1000 Class	Seismic Category	Principal Design Code	UK Safety Category	Safety Function(s) Provided by the SSC	UK Safety Class	Justification of the Safety Class
Component Cooling Water System (CCS) Location: Auxiliary Building and Turbine Building (cont.)								
Balance of system components are Class D & E					C	The balance of the system provides Category C functions such as: • Removing nuclear heat from the reactor coolant during normal operation (including providing a heat sink for those systems involved in the removal of heat from the reactor coolant during normal operation). Failure of this function would result in a short-term power manoeuvre, thus affecting nuclear safety. • Support plant reactivity control during normal operation. • Providing long-term support of Category A or B functions.	3	The CCS provides cooling to equipment that supports normal power operation, whether by removing nuclear heat (cooling of the RCP for example), controlling the reactivity (cooling of the CVS letdown HX for example), or providing long-term support of Category A or B functions (WLS RCDT HX, for example).
Condensate System (CDS) Location: Turbine Building								
–	Feedwater Heaters	E	NNS	ASME Section VIII	C	Removing nuclear heat from the reactor during normal operations. Failure of this function can result in a short-term power manoeuvre, thus affecting safety.	3	The feedwater heaters provide required heat removal and thermal efficiency improvements to support normal power operation. If a tube leak occurs in a feedwater heater, the heater train is bypassed and power must be reduced.
CDS-ME-05	Deaerator	E	NNS	ASME Section VIII	C	Removing nuclear heat from the reactor during normal operations.	3	Mechanical failure of deaerator internal components could create a blockage of suction lines from the deaerator to feedwater pump. This would cause the deaerator level to rise above the allowable level.
–	Condensers	E	NNS	ASME Section VIII	C	Removing nuclear heat from the reactor during normal operations. Failure of this function can result in a short-term power manoeuvre, thus affecting safety.	3	The main condenser must accommodate the steam loads and drain flows specified for normal power operation. On a significant tube leak in a condenser shell, the bank of tubes containing the leak would have to be isolated resulting in a reduction in power.
–	Feedwater Heater Drain Coolers	E	NNS	ASME Section VIII	C	Removing nuclear heat from the reactor during normal operations. Failure of this function can result in a short-term power manoeuvre, thus affecting safety.	3	If a tube leak occurs in a drain cooler, the heater train is bypassed and power must be reduced.
System components are Class E					GNS	No nuclear safety implications.	GNS	SSCs are not designed or considered in the application of a safety function.
Condenser Tube Cleaning System (CES) Location: Turbine Building								
System components are Class E					GNS	No nuclear safety implications.	GNS	SSCs are not designed or considered in the application of a safety function.
Turbine Island Chemical Feed System (CFS) Location: Turbine Building								
–	CFS Chemical Distribution Package	E	NNS		C	Provide long-term support of Category A functions.	3	The CFS injects chemicals into selected plant secondary systems to maintain control of the secondary water chemistry. This includes chemistry control of SWS, which performs Category A functions.
Balance of system components are Class E					GNS	No nuclear safety implications.	GNS	SSCs are not designed or considered in the application of a safety function.

Table 15A-1. AP1000 UK Categorisation and Classification of Mechanical SSCs (cont.)

Tag Number	Description	AP1000 Class	Seismic Category	Principal Design Code	UK Safety Category	Safety Function(s) Provided by the SSC	UK Safety Class	Justification of the Safety Class
Condenser Air Removal System (CMS) Location: Turbine Building								
–	Condenser Vacuum Breakers	E	NNS	ANSI 16.34	GNS	No nuclear safety implications.	GNS	SSCs are not designed or considered in the application of a safety function.
Balance of system components are Class D					C	Control of levels of radioactivity released to the environment.	3	The CMS and the gland seal system (GSS) discharge into the turbine island vents, drains and relief system (TDS). The exhaust from the TDS into the turbine island vent is continuously monitored for radiation. No credit is taken for absorption of noble gases along the release pathway during steam generator tube rupture.
Containment System (CNS) Location: Containment								
CNS-MV-01	Containment Vessel	B	I	ASME III, MC	A	Prevention of the release of radioactive material from the containment.	1	The containment vessel, the hatches, and the spare penetrations must not leak, in order to maintain containment integrity. These SSCs provide the principal means of providing this safety function.
CNS-MY-Y01	Equipment Hatch	B	I	ASME III, MC				
CNS-MY-Y02	Maintenance Hatch	B	I	ASME III, MC				
CNS-MY-Y03	Personnel Hatch – 110.744 m (135′-3″)	B	I	ASME III, MC				
CNS-MY-Y04	Personnel Hatch – 102.184 m (107′-2″)	B	I	ASME III, MC				
–	Spare Containment Penetrations	B	I	ASME III, MC	A	Prevention of the release of radioactive material from the containment.	1	Each containment penetration provides a principal means of maintaining containment integrity.
Condensate Polishing System (CPS) Location: Turbine Building								
–	Condensate Polishing Loop	E	NNS	M/f Std	C	Provides long-term support of a Category A safety function.	3	The CPS helps maintain a noncorrosive environment within the CDS, FWS, and SGS to meet the plant water chemistry guidelines.
Balance of system components are Class E					GNS	No nuclear safety implications.	GNS	SSCs are not designed or considered in the application of a safety function.
Chemical and Volume Control System (CVS) Location: Containment, Auxiliary Building, and Annex Building								
CVS-ME-01	CVS Regenerative Heat Exchanger	D	NNS	ASME VIII/ TEMA	C	Control of the level of radioactivity within the reactor coolant.	3	The CVS purification function provides a means for control of the radioactivity contained within the reactor coolant.
CVS-ME-02	CCS Letdown Heat Exchanger	D	NNS	ASME VIII/ TEMA				
CVS-MP-01A/B	Pumps	D	NNS	Hydraulic Institute Stds	A	Maintaining reactor coolant inventory. Controlling subcritical reactivity of the fuel in the reactor core during normal operation and accident conditions.	2	The CVS makeup pumps provide a supplemental source of RCS inventory makeup. This function is contained with the RAP and is considered important to safety. The CVS makeup pumps provide coolant to the pressuriser spray line.
CVS-MT-01	Boric Acid Storage Tank	D	NNS	API 650				

Table 15A-1. AP1000 UK Categorisation and Classification of Mechanical SSCs (cont.)

Tag Number	Description	AP1000 Class	Seismic Category	Principal Design Code	UK Safety Category	Safety Function(s) Provided by the SSC	UK Safety Class	Justification of the Safety Class
Chemical and Volume Control System (CVS) Location: Containment, Auxiliary Building, and Annex Building (cont.)								
CVS-MT-02	Boric Acid Batching Tank	E	NNS	ASME VIII	C	Provide long-term support of Category A or B functions	3	Provides support for the BAST which performs a Category A function.
CVS-MT-03	Chemical Mixing Tank	E	NNS	ASME VIII	C	Provide long-term support of Category A or B functions	3	Contains hydrazine solution required to provide a 10 ppm concentration in a cold, water solid RCS for scavenging oxygen.
CVS-MT-05	Air Intrusion Prevention Tank	D	NNS	ASME VIII	B	Prevention of the release of radioactive waste material from onsite storage facilities	2	This tank is used with the radioactive waste processing system for pre-shutdown operations. This system is designed to prevent the release of radiation.
–	Demineralisers	D	NNS	ASME VIII	C	Control of the level of radioactivity within the reactor coolant.	3	The CVS purification function provides a means for control of the radioactivity contained within the reactor coolant. This function is not subject to increased availability controls and is not important to safety.
–	Filters	D	NNS	ASME VIII				
–	Valves Providing CVS AP1000 Equipment Class D Function	D	NNS	ANSI 16.34	A	Maintaining reactor coolant inventory.	2	The CVS makeup pumps provide a supplemental source of RCS inventory makeup. This function is contained with the RAP and is considered important to safety.
CVS-PL-V001	RCS Purification Stop	A	I	ASME III-1	A	Prevention of the release of radioactive material through the boundary of the RCS.	1	These valves provide the principal means of isolating the CVS from the RCS.
CVS-PL-V002	RCS Purification Stop	A	I	ASME III-1				
CVS-PL-V003	RCS Purification Stop	C	I	ASME III-3				
CVS-PL-V030	Cation Bed Control Valves	D	NNS	ASME B16.34	C	Removal of nuclear heat from the reactor coolant during normal operation. Control of radioactivity to support normal power operation.	3	The CVS cation bed is used weekly to remove specific chemical contribution in the coolant to maintain compliance with chemistry control guidelines for the coolant. Failure of these valves will result in a potential impact to power production.
CVS-PL-V040	Resin Flush IRC Isolation	B	I	ASME III-2	A	Prevention of the release of radioactive material from the containment.	1	The isolation valves are the principal means of fulfilling the safety function.
CVS-PL-V041	Resin Flush ORC Isolation	B	I	ASME III-2				
CVS-PL-V042	Flush Line Containment Isolation Relief	B	I	ASME III-2				
CVS-PL-V045	Letdown Containment Isolation IRC	B	I	ASME III-2				
CVS-PL-V046	Letdown Pressure Instrument Root	B	I	ASME III-2				
CVS-PL-V047	Letdown Containment Isolation ORC	B	I	ASME III-2				
CVS-PL-V058	Letdown Line Thermal Relief Valve	B	I	ASME III-2	A	Maintaining the integrity of containment.	1	This valve protects the containment boundary between the inboard and outboard containment isolation valves on the CVS letdown line from thermal overpressurisation.
CVS-PL-V059	Letdown Isolation Valve for WLS RCDT	D	NNS	ASME B16.34	C	Removal of nuclear heat from the reactor coolant during normal operation.	3	Flow path is required to support degasification of the reactor coolant to support normal plant operation.
CVS-PL-V065	H2/Zinc Addition IRC Shutoff Valve	C	I	ASME III-3	A	Prevention of the release of radioactive material from the containment.	1	The isolation valves are the principal means of fulfilling the safety function.

Table 15A-1. AP1000 UK Categorisation and Classification of Mechanical SSCs (cont.)

Tag Number	Description	AP1000 Class	Seismic Category	Principal Design Code	UK Safety Category	Safety Function(s) Provided by the SSC	UK Safety Class	Justification of the Safety Class
Chemical and Volume Control System (CVS) Location: Containment, Auxiliary Building, and Annex Building (cont.)								
CVS-PL-V067	CVS Makeup Return Line Bypass Check Valve	A	I	ASME III-3	A	Maintaining the integrity of the reactor coolant system pressure boundary.	1	The makeup return line spring-assisted check valve functions to protect the RHX from overpressure due to thermal expansion. If a leak were to occur upstream of this valve, it would remain closed to preserve reactor coolant pressure boundary and therefore performs a safety-related function.
CVS-PL-V080	RCS Purification Return Line Check Valve	C	I	ASME III-3	A	Prevention of the release of radioactive material through the boundary of the RCS.	1	These valves provide the principal means of isolating the CVS from the RCS.
CVS-PL-V081	RCS Purification Return Line Stop Valve	A	I	ASME III-1				
CVS-PL-V082	RCS Purification Return Line Check Valve	A	I	ASME III-1				
CVS-PL-V084	Auxiliary Pressuriser Spray Line Isolation	A	I	ASME III-1				
CVS-PL-V085	Auxiliary Pressuriser Spray Line	A	I	ASME III-1				
CVS-PL-V090	Makeup Line Containment Isolation	B	I	ASME III-2	A	Prevention of the release of radioactive material from the containment. Control of core reactivity during normal operation and accident conditions.	1	The isolation valves are the principal means of fulfilling the safety function. Provides a principal means of isolation of dilution flow to reduction of RCS boron concentration.
CVS-PL-V091	Makeup Line Containment Isolation	B	I	ASME III-2				
CVS-PL-V092	Zinc Injection Containment Isolation ORC	B	I	ASME III-2	A	Prevention of the release of radioactive material from the containment.	1	The isolation valves are the principal means of fulfilling the safety function.
CVS-PL-V094	Zinc Injection Containment Isolation IRC	B	I	ASME III-2				
CVS-PL-V095	Zinc Injection Cont Isolation Test Connection Valve	C	I	ASME III-3				
CVS-PL-V096	Zinc Injection Containment Isolation Test Connection	B	I	ASME III-2				
CVS-PL-V100	Makeup Line Containment Isolation Relief	B	I	ASME III-2				
CVS-PL-V115	Makeup Pump Suction Header 3-way Blend Valve	D	NNS	ASME B16.34	C	Removal of nuclear heat from the reactor coolant during normal operation.	3	Failure of this valve will result in boration of the primary coolant and a reduction in plant power generation.
CVS-PL-V136A	Demineralised Water System Isolation	C	I	ASME III-3	A	Control of core reactivity during normal operation and accident conditions.	1	Provides a principal means of isolation of dilution flow to reduction of RCS boron concentration.
CVS-PL-V136B	Demineralised Water System Isolation	C	I	ASME III-3				
CVS-PL-V215	Hydrogen Injection Containment Isolation Test Valve IRC	C	I	ASME III-3	A	Prevention of the release of radioactive material from the containment.	1	The isolation valves are the principal means of fulfilling the safety function.
CVS-PL-V216	Hydrogen Injection Containment Isolation Test Connection Valve IRC							
CVS-PL-V217	Hydrogen Injection Containment Isolation Check IRC	B	I	ASME III-2	A	Prevention of the release of radioactive material from the containment.	1	The isolation valves are the principal means of fulfilling the safety function.

Table 15A-1. AP1000 UK Categorisation and Classification of Mechanical SSCs (cont.)

Tag Number	Description	AP1000 Class	Seismic Category	Principal Design Code	UK Safety Category	Safety Function(s) Provided by the SSC	UK Safety Class	Justification of the Safety Class
CVS-PL-V218	Hydrogen Injection Containment Isolation Test Connection							
Chemical and Volume Control System (CVS) Location: Containment, Auxiliary Building, and Annex Building (cont.)								
CVS-PL-V219	Hydrogen Injection Containment Isolation ORC							
–	Zinc Addition Equipment	E	NNS	-	C	Controlling the level of radioactivity within the reactor coolant.	3	The CVS provides a means of adding liquid zinc acetated solution to the RCS to reduce the potential of crud-induced power shifts and radiation fields.
–	Hydrogen Addition Equipment	E	NNS	-	C	Provide long-term support of Category A or B functions.	3	The CVS provides hydrogen to the RCS during normal operations to eliminate free oxygen and minimise corrosion of the fuel and primary surfaces.
CVS-PY-C01	Demineraliser Resin Flush Line Containment Penetration	B	I	ASME III, MC	A	Prevention of the release of radioactive material from the containment.	1	Each containment penetration provides a principal means of maintaining containment integrity.
CVS-PY-C02	Letdown Line Containment Penetration	B	I	ASME III, MC				
CVS-PY-C03	Makeup Line Containment Penetration	B	I	ASME III,MC				
CVS-PY-C04	Zinc Injection Line Containment Penetration	B	I	ASME III-MC				
CVS-PY-C05	Hydrogen Add Line Containment Penetration	B	I	ASME III, MC				
–	Remaining Class D CVS SSCs	D	NNS	ASME B16.34	C	Control of the level of radioactivity within the reactor coolant.	3	The CVS purification function provides a means for control of the radioactivity contained within the reactor coolant. This function is not subject to increased availability controls and is not important to safety.
Balance of system components are Class E					GNS	No nuclear safety implications.	GNS	SSCs are not designed or considered in the application of a safety function.
Circulating Water System (CWS) Location: Turbine Building and Pump Intake Structure								
System components are Class E					GNS	No nuclear safety implications.	GNS	SSCs are not designed or considered in the application of a safety function.
Standby Diesel Fuel Oil System (DOS) Location: Diesel Generator Building and Yard								
–	Fuel Oil Transfer Package	D	NNS	M/f Std	A	Removal of decay heat from the reactor coolant during normal operation and accident conditions.	2	The onsite diesel generators have been identified as important to safety. These SSCs provide standby power for supplementary decay heat removal functions. This does not represent the principal means of decay heat removal.
–	Fuel Oil Storage Tanks	D	NNS	API 650				
–	Fuel Oil Day Tanks	D	NNS	ASME VIII				
–	Valves Providing DOS AP1000 Equipment Class D Function	D	NNS	ANSI 16.34				
–	Ancillary Diesel Generator Fuel Tank	D	Note 2	ASME VII	B	Reducing the probability of requiring the use of offsite SSCs to maintain Category A safety functions after 72 hours following an accident.	2	The ancillary diesel generators and fuel tanks reduce the probability that offsite SSCs would be needed to support post 72 hour actions required to maintain safe shutdown.
Balance of system components are Class E					GNS	No nuclear safety implications.	GNS	SSCs are not designed or considered in the application of a safety function.

Table 15A-1. AP1000 UK Categorisation and Classification of Mechanical SSCs (cont.)

Tag Number	Description	AP1000 Class	Seismic Category	Principal Design Code	UK Safety Category	Safety Function(s) Provided by the SSC	UK Safety Class	Justification of the Safety Class
Demineralised Water Treatment System (DTS) Location: Turbine Building								
–	Primary Demineralisation Package	E	NNS	-	C	Provide long-term support of Category A or B functions.	3	The DTS receives treated water from RWS, processes this water to remove ionic impurities, and provides demineralised water to the DWS, which performs Category A functions.
–	Secondary Primary Demineralisation Package	E	NNS	-				
Balance of system components are Class E					GNS	No nuclear safety implications.	GNS	SSCs are not designed or considered in the application of a safety function.
Demineralised Water Transfer and Storage System (DWS) Location: Various								
–	Condensate Storage Tanks	D	NNS	API 650	A	Removal of decay heat from the reactor coolant during normal operation and accident conditions.	2	DWS supplies a water source for the SFW pumps, which serve to remove decay heat after reactor trip.
–	Valves Providing DWS AP1000 Equipment Class D Function	D	NNS	ANSI 16.34				
DWS-PL-V241	DWS Containment Penetration Thermal Relief Valve	C	I	ASME III-3	A	Prevention of the release of radioactive material from the containment	1	The isolation valves are the principal means of fulfilling the safety function.
DWS-PL-V244	Demineralised Water Supply Containment Isolation – Outside	B	I	ASME III-2	A	Prevention of the release of radioactive material from the containment.	1	These valves isolate the DWS piping that penetrates the containment barrier. This containment flow path is normally locked closed, and it is only opened when demineralised water is required inside containment.
DWS-PL-V245	Demineralised Water Supply Containment Isolation – Inside	B	I	ASME III-2				
DWS-PL-V248	Containment Penetration Test Connection Isolation	B	I	ASME III-2				
DWS-PY-C01	Containment Demineralised Water Supply Penetration	B	I	ASME III, MC	A	Prevention of the release of radioactive material from the containment.	1	Each containment penetration provides a principal means of maintaining containment integrity.
Balance of system components are Class E					C	Provide long-term support to Category A or B safety functions.	C	The DWS provides initial fill and makeup to the primary side RCS through the CVS. The DWS contains equipment to deoxygenate demineralised water and condensate. The DWS provides initial fill and makeup to the spent fuel pool through the CVS. The DWS provides water to humidifiers in the HVAC systems.

Table 15A-1. AP1000 UK Categorisation and Classification of Mechanical SSCs (cont.)

Tag Number	Description	AP1000 Class	Seismic Category	Principal Design Code	UK Safety Category	Safety Function(s) Provided by the SSC	UK Safety Class	Justification of the Safety Class
Fuel Handling and Refuelling System (FHS) Location: Containment and Auxiliary Building								
FHS-FH-01	Refuelling Machine	D	II	AISC	A	Protecting against internal/external hazards that would directly and inevitably result in loss of one of the other Category A safety functions.	2	The water in the spent fuel pool and designated makeup sources provide the principal means of protecting the spent fuel against damage. However, all handling systems are significant contributors to this protection: they are not allowed to fail and damage safety-related equipment.
FHS-JL-01	Refuelling Machine Control Panel	D	II	M/f Std				
FHS-FH-02	Fuel Handling Machine	D	II	AISC				
FHS-FH-04	New Fuel Elevator	D	II	AISC				
FHS-FH-05	Fuel Transfer System	D	II	AISC				
FHS-JL-03	Fuel Transfer System Control Panel Inside Containment	D	II	M/f Std				
FHS-JL-04	Fuel Transfer System Control Panel Outside Containment	D	II	M/f Std				
FHS-FH-52	Spent Fuel Assembly Handling Tool	D	II	AISC				
FHS-FS-01	New Fuel Storage Rack	D	I	M/f Std	A	Controlling subcritical reactivity of the fuel in the reactor core and the spent nuclear fuel in the spent fuel pool and associated structures during normal operations and accident conditions.	2	This SSC is a significant contributor to the cooling and reactivity control of the spent fuel. Principal means of performing these functions are associated with the spent fuel pool and the coolant contained within.
FHS-FS-06	In-containment Fuel Storage Rack	D	I	M/f Std	A	Controlling subcritical reactivity of the fuel in the reactor core and the spent nuclear fuel in the spent fuel pool and associated structures during normal operations and accident conditions.	2	This SSC is a significant contributor to the cooling and reactivity control of the spent fuel. Principal means of performing these functions are associated with the pit and the coolant contained within.
FHS-FS-21 FHS-FS-22 FHS-FS-23 FHS-FS-24 FHS-FS-25 FHS-FS-26 FHS-FS-27 FHS-FS-28	Spent Fuel Storage Rack	D	I	M/f Std	A	Controlling subcritical reactivity of the fuel in the reactor core and the spent nuclear fuel in the spent fuel pool and associated structures during normal operations and accident conditions. Maintaining spent fuel integrity such that significant radioactive releases do not occur (as a result of impacts or overheating).	2	This SSC is a significant contributor to the cooling and reactivity control of the spent fuel. Principal means of performing these functions are associated with the spent fuel pool and the coolant contained within.
FHS-MT-01	Spent Fuel Pool	C	I	ACI 349	A	Controlling subcritical reactivity of the fuel in the reactor core and the spent nuclear fuel in the spent fuel pool and associated structures during normal operations and accident conditions. Maintaining spent fuel integrity such that significant radioactive releases do not occur (as a result of impacts or overheating).	1	Spent fuel pool represents the principal means of providing this safety function.

Table 15A-1. AP1000 UK Categorisation and Classification of Mechanical SSCs (cont.)

Tag Number	Description	AP1000 Class	Seismic Category	Principal Design Code	UK Safety Category	Safety Function(s) Provided by the SSC	UK Safety Class	Justification of the Safety Class
Fuel Handling and Refuelling System (FHS) Location: Containment and Auxiliary Building (cont.)								
FHS-MT-02	Fuel Transfer Canal	C	I	ACI 349	A	Maintaining spent fuel integrity such that significant radioactive releases do not occur (as a result of impacts or overheating). Removing decay heat from the reactor coolant during normal operation and accident conditions (including providing a heat sink for those systems involved in the removal of heat from the reactor coolant during normal operation and accident conditions).	1	These SSCs provide for maintaining inventory of coolant in the spent fuel pool to provide cooling and reactivity control of the spent fuel. Additionally, the cask loading pit provides an alternate suction source for the cooling water to various support systems. Therefore, integrity of these volumes is considered a principle function.
FHS-MT-03	Refuelling Cavity	C	I	ACI 349				
FHS-MT-05	Spent Fuel Cask Loading Pit	C	I	ACI 349				
FHS-MT-06	Spent Fuel Cask Washdown Pit	C	I	ACI 349				
FHS-MY-Y01	Spent Fuel Transfer Gate	C	I	M/f Std				
FHS-MY-Y02	Spent Fuel Cask Loading Pit Gate	C	I	M/f Std				
FHS-MY-Y03	Permanent Cavity Seal Ring	C	I	M/f Std				
FHS-PL-V001	Fuel Transfer Tube Isolation Valve	C	I	ASME III-3				
FHS-PL-V001	Fuel Transfer Tube Isolation Valve	C	I	ASME III-3	A	Maintaining the integrity of the containment; thereby minimising the release of radioactive material from the containment.	1	Each containment penetration provides a principal means of maintaining containment integrity.
FHS-FT-01	Fuel Transfer Tube	B	I	ASME III Class MC				
FHS-PY-B01	Fuel Transfer Tube Blind Flange	B	I	ASME III-2				
Balance of system components are Class E					GNS	No nuclear safety implications.	GNS	Does not contribute to maintaining nuclear safety as determined by the safety case.
Fire Protection System (FPS) Location: Various								
FPS-PL-V045	PCS to FPS Isolation Valve	F	NNS	ANSI B16.34	C	Ensures proper firefighting and sprinkler system supply from seismically qualified source and allows maintenance of PCS and/or FPS.	3	This normally open valve ensures Non-RCA side of Auxiliary Building is supplied with adequate supply of firefighting and sprinkler operation.
FPS-PL-V050	Fire Water Containment Supply Isolation – Outside	B	I	ASME III-2	A	Prevention of the release of radioactive material from the containment.	1	The isolation valves are the principal means of maintaining containment isolation.
FPS-PL-V051	Fire Water Containment Test Connection Isolation	B	I	ASME III-2				
FPS-PL-V052	Fire Water Containment Supply Isolation – Inside	B	I	ASME III-2				
FPS-PL-V702	FPS Containment Penetration Thermal Relief Valve	C	I	ASME III-3	A	Prevention of the release of radioactive material from the containment.	1	The isolation valves are the principal means of fulfilling the safety function.
FPS-PY-C01	Fire Protection Containment Penetration	B	I	ASME III, MC	A	Prevention of the release of radioactive material from the containment.	1	Each containment penetration provides a principal means of maintaining containment integrity.
FPS-PL-V441	Auxiliary Connection to CCS Isolation	D	NNS	ANSI B16.34	C	Provide long-term support of a Category A or B safety function.	3	This connection allows a fire protection standpipe to furnish water to cool a normal residual heat removal pump and heat exchanger following a fire that disables the normal CCS cooling function.
FPS-MS-01A/B	Fire Protection Pump Package Units	F	NNS	M/f Std	B	Function that provides a backup to a Category A safety function.	3	The fire protection pumps provide an alternative means to provide cooling water to multiple sources such as the PCCWST, the spent fuel pool, and the RNS heat exchangers.
–	Automatic sprinklers for SWS pumps, CCS pumps, and startup feedwater pumps	G	NNS	-	GNS	No nuclear safety implications.	GNS	Protection from internal hazards is train-separation where required based on risk-analysis.

Table 15A-1. AP1000 UK Categorisation and Classification of Mechanical SSCs (cont.)

Tag Number	Description	AP1000 Class	Seismic Category	Principal Design Code	UK Safety Category	Safety Function(s) Provided by the SSC	UK Safety Class	Justification of the Safety Class
Fire Protection System (FPS) Location: Various (cont.)								
–	Containment standpipe and suppression system components. Includes all FPS components inside reactor containment with the exception of those used for containment isolation and containment spray	F	NNS	ANSI B31.1	GNS	No nuclear safety implications.	GNS	SSCs are not designed or considered in the application of a safety function.
–	Auxiliary Building Standpipe and Non-1E Equipment Penetration Room Preaction Sprinkler System Components	F	NNS	ANSI B31.1	GNS	No nuclear safety implications.	GNS	SSCs are not designed or considered in the application of a safety function.
Balance of system components are Class E, F, and G					GNS	No nuclear safety implications.	GNS	SSCs are not designed or considered in the application of a safety function.
Main and Startup Feedwater System (FWS) Location: Turbine Building								
FWS-MP-03A/B	Startup Feedwater Pumps	D	NNS	Hydraulic Institute Standards	A	Removal of decay heat from the reactor coolant during normal operation and accident conditions (including providing a heat sink for those systems involved in the removal of heat from the reactor coolant during normal operation and accident conditions).	2	The SFW pumps provide a mode of decay heat removal using steam dump to the atmosphere or the main condenser. These pumps are included in the RAP and are important to safety.
–	Valves Providing SFW AP1000 Equipment Class D Function	D	NNS	ANSI 16.34				
FWS-MS-01A/B/C	Main Feedwater Pump Packages (Includes Main Feedwater Pump, Main Feedwater Booster Pump, Speed Increaser, and associated Lube Oil equipment)	E	NNS	Hydraulic Institute Standards	C	Removing nuclear heat from the reactor during normal operations.	3	The main feedwater pumps provide the motive power for main feedwater flow.
FWS-ME-06A/B	6th Stage Feedwater Heaters	E	NNS	ASME Section VIII	C	Removing nuclear heat from the reactor during normal operations.	3	The feedwater heaters provide required heat removal and thermal efficiency improvements to support normal power operation.
FWS-ME-07A/B	7th Stage Feedwater Heaters	E	NNS	ASME Section VIII	C			
–	Valves and instrumentation supporting normal power operation of the AP1000 MFW function	E	NNS	Mfg. Std	C	Removing nuclear heat from the reactor during normal operations.	3	The main feedwater function supports continued normal plant operation and removal of power operation nuclear heat.
Balance of main and startup feedwater system components are Class E					GNS		GNS	
Gland Seal System (GSS) Location: Turbine Building								
System components are Class D					C	Removing nuclear heat from the reactor during normal operations. Failure of this function can result in a short-term power manoeuvre, thus affecting safety.	3	The GSS is a system necessary for power generation and can affect the availability of the AP1000 generating unit since it is a vital part of maintaining main condenser vacuum and backpressure on the main turbine during plant operation.
Generator Hydrogen and CO2 Systems (HCS) Location: Turbine Building								
System components are Class E					GNS	No nuclear safety implications.	GNS	SSCs are not designed or considered in the application of a safety function.

Table 15A-1. AP1000 UK Categorisation and Classification of Mechanical SSCs (cont.)

Tag Number	Description	AP1000 Class	Seismic Category	Principal Design Code	UK Safety Category	Safety Function(s) Provided by the SSC	UK Safety Class	Justification of the Safety Class
Heater Drain System (HDS) Location: Turbine Building								
HDS-MP-01A/B	MSR Shell Drain Pumps	E	NNS	Hydraulic Institute	C	These components are important to power production reliability. Failure of this component would result in a short-term power manoeuvre, thus affecting nuclear safety.	3	If there is a loss of function in a MSR shell drain pump, 50% of the MSR shell drain to the deaerator is lost which will result in a reduction in power production.
–	MSR Shell Drain Tank Normal Drain Path Control Valves	E	NNS	ANSI B16.34	C	These components are important to power production reliability. Failure of this component would result in a short-term power manoeuvre, thus affecting nuclear safety.	3	If one of these valves failed to a closed position during full power operation, 50% of the MSR shell drain is lost.
–	Feedwater Heater Drain Path Control Valves	E	NNS	ANSI B16.34	C	These components are important to power production reliability. Failure of this component would result in a short-term power manoeuvre, thus affecting nuclear safety.	3	If one of these valves failed to a closed position during full power operation, 50% of the MSR shell drain is lost.
–	MSR 2nd Stage Reheater Drain Tank Normal Drain Path Control Valves	E	NNS	ANSI B16.34	C	These components are important to power production reliability. Failure of this component would result in a short-term power manoeuvre, thus affecting nuclear safety.	3	If one of these valves failed to a closed position during full power operation, 50% of the MSR shell drain is lost.
Balance of system components are Class E					GNS	No nuclear safety implications.	GNS	SSCs are not designed or considered in the application of a safety function.
Hydrogen Seal Oil System (HSS) Location: Turbine Building								
System components are Class E					GNS	No nuclear safety implications.	GNS	SSCs are not designed or considered in the application of a safety function.
In-core Instrumentation System (IIS) Location: Containment								
–	IIS Guide Tubes	A	I	ASME III-1	A	Prevention of the release of radioactive material through the boundary of the RCS.	1	Provides the principal means of fulfilling the safety function.
–	Thimble assemblies	B	I	M/f Std	B	Instrumentation used to monitor Category A safety functions (but not required to facilitate actuation).	1	The thimble assemblies provide the structure for mounting of the in-core instrumentation channels. The individual channels are classified separately.
Main Turbine and Generator Lube Oil System (LOS) Location: Turbine Building								
System components are Class E					GNS	No nuclear safety implications.	GNS	SSCs are not designed or considered in the application of a safety function.
Mechanical Handling System (MHS) Location: Various								
MHS-MH-01	Containment Polar Crane	C	I	NUREG-0554 supplemented by ASME NOG-1	A	Maintaining spent fuel integrity such that significant radioactive releases do not occur (as a result of impacts or overheating). Preventing the release of radioactive material through the boundary of the RCS.	1	Provides the principal means of fulfilling the safety function. The polar crane protects against load drops on the RCS or on any irradiated fuel assemblies, regardless of location in the transfer canal or vessel.
MHS-MH-02	Cask Handling Crane	C	I	NUREG-0554 supplemented by ASME NOG-1	A	Maintaining spent fuel integrity such that significant radioactive releases do not occur (as a result of impacts or overheating).	1	Provides the principal means of fulfilling the safety function.

Table 15A-1. AP1000 UK Categorisation and Classification of Mechanical SSCs (cont.)

Tag Number	Description	AP1000 Class	Seismic Category	Principal Design Code	UK Safety Category	Safety Function(s) Provided by the SSC	UK Safety Class	Justification of the Safety Class
Mechanical Handling System (MHS) Location: Various (cont.)								
MHS-MH-05	Equipment Hatch Hoist	C	I	NUREG-0554 supplemented by ASME NOG-1	A	Prevention of the release of radioactive material through the boundary of the RCS.	1	Provides the principal means of fulfilling the safety function.
MHS-MH-06	Maintenance Hatch Hoist	C	I	NUREG-0554 supplemented by ASME NOG-1				
MHS-MH-16	Filter Cask Portable Handling Device	D	NNS	M/f Std	B	Preventing the release of radioactive waste material from onsite radioactive waste systems.	3	The filter cask provides the principal means of fulfilling the safety function. The filter cask portable handling device is a significant contributor to the safety function.
Balance of system components are Class E					GNS	No nuclear safety implications.	GNS	Does not contribute to maintaining nuclear safety as determined by the safety case.
Main Steam System (MSS) Location: Turbine Building								
–	Moisture Separator Reheaters (MSR)	E	NNS	ASME Section VII	C	This component is important to power production reliability. Single failure of an MSR during power operation will result in a reduction in plant power production.	3	If an MSR reheater section must be taken out of service due to a tube leakage, plant power production must be reduced per turbine generator vendor requirements. A tube leak in the MSR is not expected to cause low-pressure turbine parameters to reach the trip setpoint before operator action can be taken to isolate the reheater section.
MSS-PL-V001 MSS-PL-V002 MSS-PL-V003 MSS-PL-V004 MSS-PL-V005 MSS-PL-V006	Turbine Bypass Control Valves	E	NNS	M/f Std	C	Remove nuclear heat from the reactor coolant during normal operation. If one or more of these valves are failed to the closed position and unable to be opened, the plants availability to survive a full load rejection without a reactor trip is challenged, thus affecting nuclear safety.	3	Single failure of a turbine bypass control valve during power operation could result in a reactor trip. The valves are credited as back-up to the MSIVs, and the valves are required to prevent a reactor trip during a Level A transient.
MSS-PL-V015A/B	MSR 2nd Stage Reheat Supply Steam Isolation Valves	E	NNS	M/f Std	C	Remove nuclear heat from the reactor coolant during power operation. Failure of either of these valves to their closed position during power operation will result in a loss of reheat steam to 2nd stage of the MSR, which will result in a reduction in plant power per turbine generator vendor requirements.	3	V015A/B valves are fail-closed, air-operated valves that serve as isolation valves in the 2nd stage MSR reheat steam supply. These valves are also credited as backup to the MSIVs.
–	Extraction Non-Return Valves	E	NNS	M/f Std	C	Remove nuclear heat from the reactor coolant. Failure of the air assist on one of these valves would push the valve to a partially closed position during power operation which may cause a small reduction in plant power.	3	These valves are partially closed, air-assisted check valves in the extraction steam supply lines to the FW heaters and 1st Stage MSRs. Single valve failure may result in a reduction in plant power production.
–	Main Steam Delivery Valves and Piping	E	NNS	-	C	Removing nuclear heat from the reactor coolant during normal operation.	3	The MSS delivers steam from the SGS to the MTS and to and from the moisture separator reheaters during normal operation.
Balance of system components are Class E					GNS	No nuclear safety implications.	GNS	SSCs are not designed or considered in the application of a safety function.

Table 15A-1. AP1000 UK Categorisation and Classification of Mechanical SSCs (cont.)

Tag Number	Description	AP1000 Class	Seismic Category	Principal Design Code	UK Safety Category	Safety Function(s) Provided by the SSC	UK Safety Class	Justification of the Safety Class
Main Turbine System (MTS) Location: Turbine Building								
MTS-MG-01	High-Pressure Turbine	E	NNS	M/f Std	C	This component is important to power production reliability. Failure of this component would result in a short-term power manoeuvre, thus affecting nuclear safety.	3	Failure of high-pressure turbine will result in immediate unit trip
–	Low-Pressure Turbines	E	NNS	M/f Std	C	This component is important to power production reliability. Failure of this component would result in a short-term power manoeuvre, thus affecting nuclear safety.	3	Failure of low-pressure turbine will result in immediate unit trip.
MTS-PL-V001A/B MTS-PL-V003A/B	Turbine Main Stop Valves	E	NNS	M/f Std	C	These components are important to power production reliability. Failure of this component would result in a short-term power manoeuvre, thus affecting nuclear safety.	3	Single valve failure will result in a reduction in plant power if not remedied. The failure of this valve to operate on demand requires a plant shutdown if not remedied within 72 hours.
MTS-PL-V002A/B MTS-PL-V004A/B	Turbine Control Valves	E	NNS	M/f Std	C	These components are important to power production reliability. Failure of this component would result in a short-term power manoeuvre, thus affecting nuclear safety.	3	Single valve failure will result in a reduction in plant power if not remedied. The failure of this valve to operate on demand requires a plant shutdown if not remedied within 72 hours.
–	Turbine Reheat Stop Valve	E	NNS	M/f Std	C	These components are important to power production reliability. Failure of this component would result in a short-term power manoeuvre, thus affecting nuclear safety.	3	Single valve failure will result in a reduction in plant power if not remedied.
–	Turbine Intercept Valves	E	NNS	M/f Std	C	These components are important to power production reliability. Failure of this component would result in a short-term power manoeuvre, thus affecting nuclear safety.	3	Single valve failure will result in a reduction in plant power if not remedied.
Balance of system components are Class E					GNS	No nuclear safety implications.	GNS	SSCs are not designed or considered in the application of a safety function.
Passive Containment Cooling System (PCS) Location: Containment Shield Building and Auxiliary Building								
PCS-EH-02	Ancillary Water Storage Tank Heater	D	NNS	M/f Std.	B	Reduce the probability of requiring the use of offsite SSCs to maintain Category A safety functions after 72 hours following an accident.	3	Supports the operation of a Class 2 component (PCS-MT-05). This component reduces the probability that offsite SSCs would be needed to support post 72 hour actions.
PCS-MT-01	Passive Containment Cooling Water Storage Tank	C	I	ACI 349	A	Maintaining the integrity of the containment; thereby minimising the release of radioactive material containment.	1	Provides the principal means of fulfilling the safety function.
PCS-MT-03	Water Distribution Bucket	C	I	M/f Std				
PCS-MT-04	Water Collection Troughs	C	I	M/f Std				
PCS-MY-Y01 PCS-MY-Y02 PCS-MY-Y03 PCS-MY-Y04 PCS-MY-Y05	PCS Water Storage Tank Screens	C	I	M/f Std				
PCS-MT-05	Passive Containment Cooling Ancillary Water Storage Tank	D	II	API 650	B	Reduce the probability of requiring the use of offsite SSCS to maintain Category A safety functions after 72 hours following an accident.	2	Provides the principal means of fulfilling the safety function. This component reduces the probability that offsite SSCs would be needed to support post 72 hour actions.

Table 15A-1. AP1000 UK Categorisation and Classification of Mechanical SSCs (cont.)

Tag Number	Description	AP1000 Class	Seismic Category	Principal Design Code	UK Safety Category	Safety Function(s) Provided by the SSC	UK Safety Class	Justification of the Safety Class
Passive Containment Cooling System (PCS) Location: Containment Shield Building and Auxiliary Building (cont.)								
PCS-MT-06	PCCWST Leak Chase Collection Pot	D	NNS	ASME VIII, Div. 1	B	Functions that continuously monitor the availability of Category A safety functions for proper operation or to alert control room staff of their failures.	2	Collects leakage from PCCWST weld seam channels and penetration sleeves. Provides the principal means of fulfilling the safety function.
PCS-PL-V001A	PCCWST Isolation	C	I	ASME III-3	A	Prevention of the release of radioactive material from the containment.	1	Provides the principal means of fulfilling the safety function.
PCS-PL-V001B	PCCWST Isolation	C	I	ASME III-3				
PCS-PL-V001C	PCCWST Isolation	C	I	ASME III-3				
PCS-MP-01A	PCS Recirculation Pump	D	Note 2	Hydraulic Institute Standards	B	Reduce the probability of requiring the use of offsite SSCs to maintain Category A safety functions after 72 hours following an accident.	2	Long-term support of post-accident heat removal has been evaluated as important to safety. This component reduces the probability that offsite SSCs would be needed to support post 72 hour actions.
PCS-MP-01B	PCS Recirculation Pump	D	Note 2	Hydraulic Institute Standards				
PCS-MT-02	Chemical Addition Tank	D	II	ASME VIII, Div. 1				
PCS-MB-01	Recirculation Heater	D	II	ASME VIII, Div. 1				
PCS-PL-V002A	PCCWST Series Isolation	C	I	ASME III-3	A	Maintaining the integrity of the containment; thereby minimising the release of radioactive material from the containment.	1	Provides the principal means of fulfilling the safety function.
PCS-PL-V002B	PCCWST Series Isolation	C	I	ASME III-3				
PCS-PL-V002C	PCCWST Series Isolation	C	I	ASME III-3				
PCS-PL-V005	PCCWST Supply to FPS Isolation Valve	C	I	ASME III-3	B	Maintaining Category A safety functions after 72 hours following an accident.	2	Provides the principal means of fulfilling the safety function.
PCS-PL-V009	Spent Fuel Pool Emergency Makeup Isolation Valve	C	I	ASME III-3	A	Maintaining spent fuel integrity such that significant radioactive releases do not occur (as a result of impacts or overheating).	1	Provides the principal means of fulfilling the safety function.
PCS-PL-V010A	Flow Transmitter FT001 Root Valve	C	I	ASME III-3	A	Maintaining the integrity of the containment; thereby minimising the release of radioactive material from the containment.	1	Provides the principal means of fulfilling the safety function.
PCS-PL-V010B	Flow Transmitter FT001 Root Valve							
PCS-PL-V011A	Flow Transmitter FT002 Root Valve							
PCS-PL-V011B	Flow Transmitter FT002 Root Valve							
PCS-PL-V012A	Flow Transmitter FT003 Root Valve							
PCS-PL-V012B	Flow Transmitter FT003 Root Valve							
PCS-PL-V013A	Flow Transmitter FT004 Root Valve							
PCS-PL-V013B	Flow Transmitter FT004 Root Valve							
PCS-PL-V014	Chemical Addition Tank Discharge Outlet Valve	D	Note 2	ANSI B16.34	B	Reduce the probability of requiring the use of offsite SSCs to maintain Category A safety functions after 72 hours following an accident.	2	Long-term support of post accident heat removal has been evaluated as important to safety. This component reduces the probability that offsite SSCs would be needed to support post 72 hour actions.
PCS-PL-V015	Water Bucket Makeup Line Drain Valve	C	I	ASME III-3	B	Maintaining Category A safety functions after 72 hours following an accident.	2	Long-term support of post accident heat removal has been evaluated as important to safety.

Table 15A-1. AP1000 UK Categorisation and Classification of Mechanical SSCs (cont.)

Tag Number	Description	AP1000 Class	Seismic Category	Principal Design Code	UK Safety Category	Safety Function(s) Provided by the SSC	UK Safety Class	Justification of the Safety Class
Passive Containment Cooling System (PCS) Location: Containment Shield Building and Auxiliary Building (cont.)								
PCS-PL-V016	PCCWST Drain Isolation Valve	C	I	ASME III-3	A	Maintaining the integrity of the containment; thereby minimising the release of radioactive material from the containment.	1	Flow path provided to support system maintenance.
PCS-PL-V004	Recirc Pump Header Heater Bypass Isolation Valve	D	Note 2	ANSI B16.34	B	Reduce the probability of requiring the use of offsite SSCs to maintain Category A safety functions after 72 hours following an accident.	2	Long-term support of post-accident heat removal has been evaluated as important to safety. This component reduces the probability that offsite SSCs would be needed to support post 72 hour actions.
PCS-PL-V006A	Recirc Pump A Suction Line Drain Valve							
PCS-PL-V006B	Recirc Pump B Suction Line Drain Valve							
PCS-PL-V007A	Recirc Pump A Discharge Line TV Valve							
PCS-PL-V007B	Recirc Pump B Discharge Line TV Valve							
PCS-PL-V008	Recirc Pump Suction Header Line TV Valve							
PCS-PL-V017	Chemical Addition Tank Vent Isolation Valve							
PCS-PL-V018	Recirculation Pump Throttle Valve							
PCS-PL-V019	Chemical Addition Tank Fill Isolation Valve							
PCS-PL-V020	Water Bucket Makeup Line Isolation Valve	C	I	ASME-III	B	Maintaining Category A safety functions after 72 hours following an accident.	2	Long-term support of post accident heat removal has been evaluated as important to safety.
PCS-PL-V021	PCCWST to Recirculation Pump Suction Isolation Valve	D	Note 2	ANSI B16.34	B	Reduce the probability of requiring the use of offsite SSCs to maintain Category A safety functions after 72 hours following an accident.	2	Flow path provided to support system maintenance. Valve closed position required to ensure system Cat. A or B flow path is preserved. This component reduces the probability that offsite SSCs would be needed to support post 72 hour actions.
PCS-PL-V022	Chemical Addition Tank Drain Isolation Valve	D	Note 2	ANSI B16.34	B	Reduce the probability of requiring the use of offsite SSCs to maintain Category A safety functions after 72 hours following an accident.	2	Flow path provided to support system maintenance. Valve closed position required to ensure system Cat. A or B flow path is preserved. This component reduces the probability that offsite SSCs would be needed to support post 72 hour actions.
PCS-PL-V023	PCS Recirculation Return Isolation	C	I	ASME III-3	A	Maintaining the integrity of the containment; thereby minimising the release of radioactive material from the containment.	1	Long-term support of post-accident heat removal has been evaluated as important to safety. This valve is located in the seismically qualified makeup line to PCS water distribution bucket.
PCS-PL-V024	Recirc Heater Drain Valve	D	Note 2	ANSI B16.34	B	Reduce the probability of requiring the use of offsite SSCs to maintain Category A safety functions after 72 hours following an accident.	2	Valves utilised for maintenance. This component reduces the probability that offsite SSCs would be needed to support post 72 hour actions.
PCS-PL-V025	Pressure Transmitter PT031 Root Isolation Valve	D	Note 2	ANSI B16.34				
PCS-PL-V026	Makeup To Dist Bucket Isolation Valve	C	I	ASME-III	A	Maintaining containment integrity and spent fuel integrity.	1	Long-term support of post accident heat removal has been evaluated as important to safety.

Table 15A-1. AP1000 UK Categorisation and Classification of Mechanical SSCs (cont.)

Tag Number	Description	AP1000 Class	Seismic Category	Principal Design Code	UK Safety Category	Safety Function(s) Provided by the SSC	UK Safety Class	Justification of the Safety Class
Passive Containment Cooling System (PCS) Location: Containment Shield Building and Auxiliary Building (cont.)								
PCS-PL-V028A	Recirc Pump A Discharge Line Drain	D	Note 2	ANSI B16.34	B	Reduce the probability of requiring the use of offsite SSCs to maintain Category A safety functions after 72 hours following an accident.	2	Valves utilised for maintenance. This component reduces the probability that offsite SSCs would be needed to support post 72 hour actions.
PCS-PL-V028B	Recirc Pump B Discharge Line Drain	D	Note 2	ANSI B16.34				
PCS-PL-V029	PCCWST Isolation Valve Leakage Detection Drain	C	I	ASME III-3	A	Maintaining the integrity of the containment; thereby minimising the release of radioactive material from the containment.	1	Provides the principal means of fulfilling the safety function.
PCS-PL-V030	PCCWST Isolation Valve Leakage Detection Cross-connect Valve	C	I	ASME III-3				
PCS-PL-V031A	Level Transmitter LT 016 & 010 Root Isolation Valve	C	I	ASME III-3	A	Maintaining the integrity of the containment; thereby minimising the release of radioactive material from the containment.	1	Provides the principal means of fulfilling the safety function.
PCS-PL-V031B	Level Transmitter LT 015 & 011 Root Isolation Valve	C	I	ASME III-3				
PCS-PL-V033	Recirculation Pump Suction from Long Term Makeup Isolation Valve	C	I	ASME III-3	A	Maintaining containment integrity and spent fuel integrity.	1	Long-term support of post accident heat removal has been evaluated as important to safety
PCS-PL-V035A	Recirculation Pump Suction Isolation Valve	D	Note 2	ANSI B16.34	B	Reduce the probability of requiring the use of offsite SSCs to maintain Category A safety functions after 72 hours following an accident.	2	Long-term support of post-accident heat removal has been evaluated as important to safety. This component reduces the probability that offsite SSCs would be needed to support post 72 hour actions.
PCS-PL-V035B	Recirculation Pump Suction Isolation Valve	D	Note 2	ANSI B16.34				
PCS-PL-V036A/B	Recirculation Pump Discharge Check Valve	D	Note 2	ANSI B16.34				
PCS-PL-V037	PCCAWST Discharge Isolation Valve	D	Note 2	ANSI B16.34				
PCS-PL-V038	PCCAWST Drain Isolation Valve	D	Note 2	ANSI B16.34				
PCS-PL-V039	PCCWST Long-Term Makeup Check Valve	C	I	ASME III-3	A	Maintaining containment integrity and spent fuel integrity.	1	Long-term support of post accident heat removal has been evaluated as important to safety
PCS-PL-V040	Recirculation Pump Suction from PCCAWST Isolation Valve	D	Note 2	ANSI B16.34	B	Reduce the probability of requiring the use of offsite SSCs to maintain Category A safety functions after 72 hours following an accident.	2	Long-term support of post-accident heat removal has been evaluated as important to safety. This component reduces the probability that offsite SSCs would be needed to support post 72 hour actions.
PCS-PL-V041	PCCAWST Recirculation Return Line Isolation Valve	D	Note 2	ANSI B16.34				
PCS-PL-V042	PCCWST Long Term Makeup Isolation Drain Valve	C	I	ASME III-3	A	Maintaining containment integrity and spent fuel integrity.	1	Long-term support of post accident heat removal has been evaluated as important to safety
PCS-PL-V043	PCCAWST Recirculation Return Line Drain Isolation Valve	D	Note 2	ANSI B16.34	B	Reduce the probability of requiring the use of offsite SSCs to maintain Category A safety functions after 72 hours following an accident	3	Flow path supports recirculation of PCCAWST only and is not used for PCS makeup flow. This component reduces the probability that offsite SSCs would be needed to support post 72 hour actions.
PCS-PL-V044	PCCWST Long Term Makeup Connection Isolation	C	I	ASME III-3	A	Maintaining containment integrity and spent fuel integrity.	1	Long-term support of post accident heat removal has been evaluated as important to safety
PCS-PL-V045	Emergency Makeup to the Spent Fuel Pool Isolation Valve	C	I	ASME III-3	A	Maintaining spent fuel integrity such that significant radioactive releases do not occur.	1	Provides the principal means of fulfilling the safety function.
PCS-PL-V046	PCCWST Recirculation Return Isolation Valve	C	I	ASME III-3	A	Maintaining containment integrity and spent fuel integrity.	1	Long-term support of post accident heat removal has been evaluated as important to safety

Table 15A-1. AP1000 UK Categorisation and Classification of Mechanical SSCs (cont.)

Tag Number	Description	AP1000 Class	Seismic Category	Principal Design Code	UK Safety Category	Safety Function(s) Provided by the SSC	UK Safety Class	Justification of the Safety Class
Passive Containment Cooling System (PCS) Location: Containment Shield Building and Auxiliary Building (cont.)								
PCS-PL-V047A	Recirculation A Discharge Isolation Valve	D	Note 2	ANSI B16.34	B	Reduce the probability of requiring the use of offsite SSCs to maintain Category A safety functions after 72 hours following an accident.	2	Long-term support of post-accident heat removal has been evaluated as important to safety. This component reduces the probability that offsite SSCs would be needed to support post 72 hour actions.
PCS-PL-V047B	Recirculation B Discharge Isolation Valve	D	Note 2	ANSI B16.34				
PCS-PL-V048	Recirculation Pump Fire Suction Isolation Valve	D	II	ANSI B16.34	B	Protecting against internal/external hazards that could, as part of a sequence of failures, result in loss of one of the safety functions, for example preventing fire spread such that all normally operating systems and safety systems delivering a specific function could be compromised.	3	Provides alternate fire water makeup source from PCCAWST.
PCS-PL-V049	Emergency Makeup to the Spent Fuel Pool Drain Isolation Valve	C	I	ASME III-3	A	Maintaining spent fuel integrity such that significant radioactive releases do not occur (as a result of impacts or overheating).	1	Provides the principal means of fulfilling the safety function.
PCS-PL-V050	Recirc Heater Discharge to SFS Pool Isolation Valve	C	I	ASME III-3				
PCS-PL-V051	Spent Fuel Pool Emergency Makeup Lower Isolation	C	I	ASME III-3				
PCS-PL-V052	Spent Fuel Pool Emergency Makeup Isolation Valve	C	I	ASME III-3				
PCS-PL-V053	Recirculation Heater Relief Valve	D	Note 2	ANSI B16.34	B	Reduce the probability of requiring the use of offsite SSCs to maintain Category A safety functions after 72 hours following an accident.	2	Principal means of fulfilling safety function. This component reduces the probability that offsite SSCs would be needed to support post 72 hour actions.
PCS-PL-V060A/B	Shutoff Valve for Leakage Sensor	C	I	ASME III-3	A	Maintaining containment integrity.	1	Sensor for PCCWST Isolation Valve Leakage Level
PCS-PL-V070	FPS Isolation Valve	F	NNS	ANSI B16.34	C	Isolates the FPS Yard Main from Non-RCA Auxiliary Building Standpipe and Sprinkler System, which limits the flood volume. Piping provides the primary safety protection.	3	Limit the amount of flood volume and isolated yard main to protect batteries during all plant modes.
PCS-PL-V100	Temporary Containment Washdown Isolation Valve	D	Note 2	ANSI B16.34	B	Reduce the probability of requiring the use of offsite SSCs to maintain Category A safety functions after 72 hours following an accident.	2	Flow path provided to support system maintenance. Valve closed position required to ensure system Cat. A or B flow path is preserved. This component reduces the probability that offsite SSCs would be needed to support post 72 hour actions.
PCS-PL-V301	PCCWST Recirculation Drain Valve	D	Note 2	ANSI B16.34	B	Reduce the probability of requiring the use of offsite SSCs to maintain Category A safety functions after 72 hours following an accident.	2	Provides the principal means of fulfilling the safety function. This component reduces the probability that offsite SSCs would be needed to support post 72 hour actions.
PCS-PL-V302	FPS Supply Drain Valve	F	NNS	MSS SP-80	GNS	No nuclear safety implication.	GNS	SSCs are not designed or considered in the application of a safety function.
PCS-PL-V303	Recirc Header Discharge to SFS Pool Vent Isolation Valve	C	I	ASME III-3	A	Maintaining spent fuel integrity such that significant radioactive releases do not occur (as a result of impacts or overheating).	1	Provides the principal means of fulfilling the safety function.
PCS-PL-V304	Recirc Header Discharge to SFS Pool Vent Isolation Valve	C	I	ASME III-3	A	Maintaining spent fuel integrity such that significant radioactive releases do not occur (as a result of impacts or overheating).	1	Provides the principal means of fulfilling the safety function.

Table 15A-1. AP1000 UK Categorisation and Classification of Mechanical SSCs (cont.)

Tag Number	Description	AP1000 Class	Seismic Category	Principal Design Code	UK Safety Category	Safety Function(s) Provided by the SSC	UK Safety Class	Justification of the Safety Class
Passive Containment Cooling System (PCS) Location: Containment Shield Building and Auxiliary Building (cont.)								
PCS-PL-V305	PCCWST Recirculation Return Drain Isolation Valve	C	I	ASME III-3	A	Maintaining containment integrity and spent fuel integrity.	1	Provides the principal means of fulfilling the safety function.
PCS-PL-V306	PCCAWST Supply Line Vent Valve	D	Note 2	ANSI B16.34	B	Reduce the probability of requiring the use of offsite SSCs to maintain Category A safety functions after 72 hours following an accident.	2	Provides the principal means of fulfilling the safety function. This component reduces the probability that offsite SSCs would be needed to support post 72 hour actions.
-	Leak Chase Penetration Sleeve Isolation for level instruments	D	NNS	ANSI B16.34	B	Functions which monitor the availability of a Category A safety function.	2	Provides the principal means of fulfilling the safety function.
PCS-PL-V414	PCCWST Leak Chase Channel Isolation	D	NNS	ANSI B16.34	B	Functions which monitor the availability of a Category A safety function.	2	Provides the principal means of fulfilling the safety function.
-	Leak Chase Collection Pot Isolation Valves	D	NNS	ANSI B16.34	B	Functions which monitor the availability of a Category A safety function.	2	Provides the principal means of fulfilling the safety function.
PCS-PL-V500	PCCAWST Makeup Line Isolation Valve	D	Note 2	ANSI B16.34	B	Reduce the probability of requiring the use of offsite water to maintain Category A safety functions after 72 hours following an accident.	2	This component reduces the probability that offsite water would be needed to support post 72 hour to 7 day actions.
PCS-PY-B01	Spent Fuel Pool Emergency Makeup Isolation	C	I	ASME III-3	A	Maintaining spent fuel integrity such that significant radioactive releases do not occur (as a result of impacts or overheating).	1	Provides the principal means of fulfilling the safety function.
–	Containment Pressure Instrument Line Penetration	B	I	ASME III-MC	A	Prevention of the release of radioactive material from the containment.	1	Each containment penetration provides a principal means of maintaining containment integrity.
Balance of system components are Class E					GNS	No nuclear safety implications.	GNS	SSCs are not designed or considered in the application of a safety function.
Plant Gas Systems (PGS) Location: Various								
System components are Class E					GNS	No nuclear safety implications.	GNS	SSCs are not designed or considered in the application of a safety function.
Primary Sampling System (PSS) Location: Containment and Auxiliary Building								
-	Corrosion Product Sample Filter and Boron Concentration Monitoring Package	D	NNS	M/f Std	B	Prevention of the release of radioactive waste material from onsite storage facilities.	3	The PSS sample handling SSCs are designed to contain and control radioactive fluids and direct them to WLS.
PSS-MS-01	Grab Sample Unit	D	NNS	M/f Std				
PSS-MS-02	Sample Cooler Rack	D	NNS	M/f Std				
PSS-ME-01A/B	Sample Cooler	D	NNS	ANSI B31.1				
–	Equipment Providing PSS AP1000 Equipment Class D Function	D	NNS	M/f Std				
–	Valves Providing PSS AP1000 Equipment Class D Function	D	NNS	ANSI 16.34				
PSS-MT-01 PSS-MT-02 PSS-MT-03	Sample Flask, Sample Expansion Tanks	D	NNS	49 CFR Part 178	B	Prevention of the release of radioactive waste material from onsite storage facilities.	3	The PSS sample handling SSCs are designed to contain and control radioactive fluids.
PSS-MT-13 through MT-18	Sample Tanks	D	NNS	49 CFR Part 178				

Table 15A-1. AP1000 UK Categorisation and Classification of Mechanical SSCs (cont.)

Tag Number	Description	AP1000 Class	Seismic Category	Principal Design Code	UK Safety Category	Safety Function(s) Provided by the SSC	UK Safety Class	Justification of the Safety Class
Primary Sampling System (PSS) Location: Containment and Auxiliary Building (cont.)								
PSS-MT-04	PSS Panel Drains Sump Tank	D	NNS	M/f Std.	B	Prevention of the release of radioactive waste material from onsite storage facilities.	3	The PSS sample handling SSCs are designed to contain and control radioactive fluids.
PSS-MT-11	Diluted Liquid Sample Tank	D	NNS	M/f Std.				
PSS-MT-12	Undiluted Degassed Depressed Liquid Sample Tank	D	NNS	M/f Std.				
PSS-PL-V001A	Hot Leg 1 Sample Isolation	B	I	ASME III-2				
PSS-PL-V001B	Hot Leg 2 Sample Isolation	B	I	ASME III-2				
PSS-PL-V003	Pressurizer Liquid Isolation	B	I	ASME III-2				
PSS-PL-V005A/B/C/D	PXS CMT Sample Isolation	B	I	ASME III-2				
PSS-PL-V013	RCS Pressurizer Sample Isolation Valve	B	I	ASME III-2				
PSS-PL-V014A/B	RCS Hot Leg 1 Sample Isolation Valve	B	I	ASME III-2				
PSS-PL-V016A/B/C/D	PXS CMT Sample Isolation	B	I	ASME III-2				
PSS-PL-V004A/B	PXS Accumulator Sample Isolation	C	I	ASME III-3				
PSS-PL-V012A	Liquid Sample Isolation Valve	C	I	ASME III-3				
PSS-PL-V015A/B	PXS Accumulator Sample Isolation Valve	C	I	ASME III-3				
PSS-PL-V008	Containment Isolation Valves	B	I	ASME III-2	A	Maintaining the integrity of the containment; thereby minimising the release of radioactive material from the containment.	1	Provides the principal means of fulfilling the safety function.
PSS-PL-V010A/B	Liquid Sample Line Cont Isolation Valve – IRC	B	I	ASME III-2				
PSS-PL-V011A/B	Liquid Sample Line Cont Isolation Valve – ORC	B	I	ASME III-2				
-	Liquid Sample Line Cont Isolation Valve – IRC	B	I	ASME III-2				
-	Liquid Sample Line Cont Isolation Valve – ORC	B	I	ASME III-2				
PSS-PL-V023	Sample Return Line Cont Isolation ORC	B	I	ASME III-2				
PSS-PL-V024	Sample Return Line Cont Isolation IRC	B	I	ASME III-2				
PSS-PL-V046	Air Sample Line Cont Isol ORC	B	I	ASME III-2				
PSS-PY-C01 PSS-PY-C02 PSS-PY-C03 PSS-PY-C04	Containment Penetrations	B	I	ASME III, MC				

Table 15A-1. AP1000 UK Categorisation and Classification of Mechanical SSCs (cont.)

Tag Number	Description	AP1000 Class	Seismic Category	Principal Design Code	UK Safety Category	Safety Function(s) Provided by the SSC	UK Safety Class	Justification of the Safety Class
Primary Sampling System (PSS) Location: Containment and Auxiliary Building (cont.)								
PSS-PL-V012B	Liquid Sample Check Valves	C	I	ASME III-3	A	Maintaining the integrity of the RCS pressure boundary; including mitigating RCS overpressure during normal operations and accident conditions.	1	Provides the principal means of fulfilling the safety function.
PSS-PL-V076A/B	Containment Testing Boundary Isolation Valves	C	I	ASME III-3				
PSS-PL-V082 PSS-PL-V083 PSS-PL-V086	Containment Isolation Test Connection Isolation Valves	C	I	ASME III-3				
PSS-PL-V085	Containment Isolation Test Connection Isolation Valve	B	I	ASME III-2	A	Maintaining the integrity of the reactor coolant system pressure boundary; including mitigating reactor coolant system overpressure during normal operations and accident conditions.	1	Provides the principal means of fulfilling the safety function.
–	Containment Testing Boundary Isolation Valves	D	NNS	ANSI B16.34	C	Provide long-term support for Category A o r B function.	3	Provides the principal means of fulfilling the safety function.
–	Containment Isolation Test Vent Isolation Valves	D	NNS	ANSI B16.34				
PSS-MP-27	Sample Pump	D	NNS	ANSI B31.1	B	Functions that continuously monitor the availability of Category A safety functions for proper operation or to alert control room staff of their failures.	3	Does not provide the principal means of fulfilling the safety function. The high alarm alerts the operator of a pressure boundary leak in the RCS which exceeds 0.11 m^3/hr (0.5 gpm) at 20% reactor power.
PSS-PY-Y01/Y02	RCS Hot Leg 1/2 Sample Line Delay Coil	C	I	ASME III, MC	B	Controlling levels of radioactivity released to the environment.	2	Provides the principal means of fulfilling the safety function. Reduces potential personnel exposure from the sample line fluid before it exits containment.
PSS-MY-Y05	Delay Coil Assembly	C	I	ASME III, MC	B	Controlling levels of radioactivity released to the environment.	2	Provides the principal means of fulfilling the safety function. Reduces potential personnel exposure from the sample line fluid before it exits containment.
Balance of system components are Class E					GNS	No nuclear safety implications.	GNS	SSCs are not designed or considered in the application of a safety function.
Potable Water System (PWS) Location: Various								
PWS-PL-V418	PWS MCR Isolation Valve	C	I	ASME III-3	A	Maintaining habitability of the main control room.	1	The isolation valves are the principal means of isolating the main control room envelope during main control room emergency habitability system (VES) operation.
PWS-PL-V420	PWS MCR Isolation Valve	C	I	ASME III-3				
PWS-PL-V498	PWS MCR Vacuum Relief	C	I	ASME III-3				
Balance of system components are Class E					GNS	No nuclear safety implications.	GNS	SSCs are not designed or considered in the application of a safety function.

Table 15A-1. AP1000 UK Categorisation and Classification of Mechanical SSCs (cont.)

Tag Number	Description	AP1000 Class	Seismic Category	Principal Design Code	UK Safety Category	Safety Function(s) Provided by the SSC	UK Safety Class	Justification of the Safety Class
Passive Core Cooling System (PXS) Location: Containment								
PXS-ME-01	Passive Residual Heat Removal Heat Exchanger	A	I	ASME III-1	A	Removal of decay heat from the reactor coolant during normal operation and accident conditions (including providing a heat sink for those systems involved in the removal of heat from the reactor coolant during normal operation and accident conditions).	1	Provides the principal means of fulfilling the safety function.
PXS-MT-01A	Accumulator Tank A	C	I	ASME III-3	A	Maintaining reactor coolant inventory. Control of core reactivity during normal operation and accident conditions.	1	Provides the principal means of fulfilling the safety function.
PXS-MT-01B	Accumulator Tank B	C	I	ASME III-3				
PXS-MT-02A	Core Makeup Tank (CMT) A	A	I	ASME III-1	A	Maintaining reactor coolant inventory. Control of core reactivity during normal operation and accident conditions.	1	Provides the principal means of fulfilling the safety function.
PXS-MT-02B	Core Makeup Tank B	A	I	ASME III-1				
PXS-MT-03	In-Containment Refuelling Water Storage Tank (IRWST)	C	I	ACI 349/AISC N690	A	Maintaining reactor coolant inventory. Control of core reactivity during normal operation and accident conditions. Maintaining spent fuel subcritical.	1	Provides the principal means of fulfilling the safety function.
PXS-MT-04	IRWST Gutter	C	I	M/f Std	A	Removal of decay heat from the reactor coolant during normal operation and accident conditions (including providing a heat sink for those systems involved in the removal of heat from the reactor coolant during normal operation and accident conditions).	1	Provides the principal means of fulfilling the safety function.
PXS-MW-01A	Reactor Coolant Depressurisation Sparger A	C	I	ASME III-3	A	Protecting against internal/external hazards that would directly and inevitably result in loss of one of the other Category A safety functions.	1	Provides the principal means of fulfilling the safety function.
PXS-MW-01B	Reactor Coolant Depressurisation Sparger B	C	I	ASME III-3				
PXS-MY-Y01A	IRWST Screen A	C	I	M/f Std	A	Maintaining reactor coolant inventory. Maintaining spent fuel integrity such that significant radioactive releases do not occur (as a result of impacts or overheating).	1	Provides the principal means of fulfilling the safety function.
PXS-MY-Y01B	IRWST Screen B	C	I	M/f Std				
PXS-MY-Y01C	IRWST Screen C	C	I	M/f Std.				
PXS-MY-Y02A	Containment Recirculation Screen A	C	I	M/f Std	A	Maintaining reactor coolant inventory.	1	Provides the principal means of fulfilling the safety function.
PXS-MY-Y02B	Containment Recirculation Screen B	C	I	M/f Std				
PXS-MY-Y03A	Type 1 pH Adjustment Basket A	C	I	M/f Std	A	Prevention of the release of radioactive material from the containment.	1	Provides the principal means of fulfilling the safety function.
PXS-MY-Y03B	Type 1 pH Adjustment Basket B	C	I	M/f Std				
PXS-MY-Y04A	Type 2 pH Adjustment Basket C	C	I	M/f Std				
PXS-MY-Y04B	Type 2 pH Adjustment Basket D	C	I	M/f Std				

Table 15A-1. AP1000 UK Categorisation and Classification of Mechanical SSCs (cont.)

Tag Number	Description	AP1000 Class	Seismic Category	Principal Design Code	UK Safety Category	Safety Function(s) Provided by the SSC	UK Safety Class	Justification of the Safety Class
Passive Core Cooling System (PXS) Location: Containment (cont.)								
-	CMT Upper and Lower Level Standpipes	A	I	ASME III-3	A	Maintaining reactor coolant inventory. Control of core reactivity during normal operation and accident conditions.	1	Provides the principal means of fulfilling the safety function.
-	Type I IRWST Hood Steam Vent Covers	C	I	M/f Std.	A	Maintaining reactor coolant inventory. Control of core reactivity during normal operation and accident conditions.	1	Provides the principal means of fulfilling the safety function.
-	IRWST SG Wall Vent Covers	C	I	M/f Std.	A	Maintaining reactor coolant inventory. Control of core reactivity during normal operation and accident conditions.	1	Provides the principal means of fulfilling the safety function.
-	IRWST Overflow Weir Covers	C	I	M/f Std.	A	Maintaining reactor coolant inventory. Control of core reactivity during normal operation and accident conditions.	1	Provides the principal means of fulfilling the safety function.
-	Downspout Screens	C	I	M/f Std.	A	Maintaining reactor coolant inventory. Control of core reactivity during normal operation and accident conditions.	1	Provides the principal means of fulfilling the safety function.
PXS-PL-V002A	CMT A Inlet Isolation	A	I	ASME III-1	A	Prevention of the release of radioactive material through the boundary of the RCS. Maintaining reactor coolant inventory. Control of core reactivity during normal operation and accident conditions.	1	Provides the principal means of fulfilling the safety function.
PXS-PL-V002B	CMT B Inlet Isolation	A	I	ASME III-1				
PXS-PL-V010A	CMT A Upper Sample	B	I	ASME III-2	A	Prevention of the release of radioactive material through the boundary of the RCS.	1	Provides the principal means of fulfilling the safety function. Flow from this flow path is reduced by the use of a flow restrictor. This valve represents the first point of flow isolation.
PXS-PL-V010B	CMT B Upper Sample	B	I	ASME III-2				
PXS-PL-V011A	CMT A Lower Sample	B	I	ASME III-2				
PXS-PL-V011B	CMT B Lower Sample	B	I	ASME III-2				
PXS-PL-V012A	CMT A Drain	A	I	ASME III-1	A	Prevention of the release of radioactive material through the boundary of the RCS.	1	Provides the principal means of fulfilling the safety function.
PXS-PL-V012B	CMT B Drain	A	I	ASME III-1				
PXS-PL-V013A	CMT A Discharge Manual Isolation	A	I	ASME III-1	A	Prevention of the release of radioactive material through the boundary of the RCS. Maintaining reactor coolant inventory. Control of core reactivity during normal operation and accident conditions.	1	Provides the principal means of fulfilling the safety function.
PXS-PL-V013B	CMT B Discharge Manual Isolation	A	I	ASME III-1				
PXS-PL-V014A	CMT A Discharge Isolation	A	I	ASME III-1				
PXS-PL-V014B	CMT B Discharge Isolation	A	I	ASME III-1				
PXS-PL-V015A	CMT A Discharge Isolation	A	I	ASME III-1				
PXS-PL-V015B	CMT B Discharge Isolation	A	I	ASME III-1				
PXS-PL-V016A	CMT A Discharge Check	A	I	ASME III-1				
PXS-PL-V016B	CMT B Discharge Check	A	I	ASME III-1				
PXS-PL-V017A	CMT A Discharge Check	A	I	ASME III-1				

Table 15A-1. AP1000 UK Categorisation and Classification of Mechanical SSCs (cont.)

Tag Number	Description	AP1000 Class	Seismic Category	Principal Design Code	UK Safety Category	Safety Function(s) Provided by the SSC	UK Safety Class	Justification of the Safety Class
Passive Core Cooling System (PXS) Location: Containment (cont.)								
PXS-PL-V017B	CMT B Discharge Check	A	I	ASME III-1				
PXS-PL-V019A	RNS Discharge DVI Line A Drain	B	I	ASME III-2	A	Prevention of the release of radioactive material through the boundary of the RCS	1	Provides the principal means of fulfilling the safety function.
PXS-PL-V019B	RNS Discharge DVI Line B Drain	B	I	ASME III-2				
PXS-PL-V020A	IRWST Injection Line A Drain	B	I	ASME III-2				
PXS-PL-V020B	IRWST Injection Line B Drain	B	I	ASME III-2				
PXS-PL-V021A	Accumulator A Nitrogen Makeup/Vent	C	I	ASME III-3	A	Maintaining the integrity of the reactor coolant pressure boundary, including mitigating over.	1	The accumulators are normally isolated from the nitrogen supply by these valves. The valves are pressure boundary valves.
PXS-PL-V021B	Accumulator B Nitrogen Makeup/Vent	C	I	ASME III-3				
PXS-PL-V022A	Accumulator A Pressure Relief	C	I	ASME III-3				
PXS-PL-V022B	Accumulator B Pressure Relief	C	I	ASME III-3				
PXS-PL-V023A	Accumulator A Pressure Transmitter B Isolation	C	I	ASME III-3	A	Maintaining the integrity of the reactor coolant pressure boundary.	1	Provides the principal means of fulfilling the safety function.
PXS-PL-V023B	Accumulator B Pressure Transmitter B Isolation	C	I	ASME III-3				
PXS-PL-V024A	Accumulator A Pressure Transmitter A Isolation	C	I	ASME III-3				
PXS-PL-V024B	Accumulator B Pressure Transmitter A Isolation	C	I	ASME III-3				
PXS-PL-V025A	Accumulator A Sample	C	I	ASME III-3	A	Maintaining the integrity of the reactor coolant pressure boundary.	1	Provides the principal means of fulfilling the safety function.
PXS-PL-V025B	Accumulator B Sample	C	I	ASME III-3				
PXS-PL-V026A	Accumulator A Drain	C	I	ASME III-3	A	Maintaining reactor coolant inventory. Control of core reactivity during normal operation and accident conditions.	1	Provides the principal means of fulfilling the safety function.
PXS-PL-V026B	Accumulator B Drain	C	I	ASME III-3				
PXS-PL-V027A	Accumulator A Discharge Isolation	C	I	ASME III-3				
PXS-PL-V027B	Accumulator B Discharge Isolation	C	I	ASME III-3				
PXS-PL-V028A	Accumulator A Discharge Check	A	I	ASME III-1				
PXS-PL-V028B	Accumulator B Discharge Check	A	I	ASME III-1				
PXS-PL-V029A	Accumulator A Discharge Check	A	I	ASME III-1				
PXS-PL-V029B	Accumulator B Discharge Check	A	I	ASME III-1				
PXS-PL-V030A	CMT A Highpoint Vent	B	I	ASME III-2	A	Prevention of the release of radioactive material through the boundary of the RCS.	1	Provides the principal means of fulfilling the safety function. Flow from this flow path is reduced by the use of a flow restrictor. This valve represents the first point of flow isolation.
PXS-PL-V030B	CMT B Highpoint Vent	B	I	ASME III-2				
PXS-PL-V031A	CMT A Highpoint Vent	B	I	ASME III-2				
PXS-PL-V031B	CMT B Highpoint Vent	B	I	ASME III-2				
PXS-PL-V033A	Accumulator A Check Valve Drain	B	I	ASME III-2				
PXS-PL-V033B	Accumulator B Check Valve Drain	B	I	ASME III-2				

Table 15A-1. AP1000 UK Categorisation and Classification of Mechanical SSCs (cont.)

Tag Number	Description	AP1000 Class	Seismic Category	Principal Design Code	UK Safety Category	Safety Function(s) Provided by the SSC	UK Safety Class	Justification of the Safety Class
Passive Core Cooling System (PXS) Location: Containment (cont.)								
PXS-PL-V042	Nitrogen Supply Containment Isolation ORC	B	I	ASME III-2	A	Prevention of the release of radioactive material from the containment.	1	Provides the principal means of fulfilling the safety function.
PXS-PL-V043	Nitrogen Supply Containment Isolation IRC	B	I	ASME III-2				
PXS-PL-V052	Accumulator Nitrogen Containment Penetration TC	B	I	ASME III-2	A	Prevention of the release of radioactive material from the containment.	1	Provides the principal means of fulfilling the safety function.
PXS-PL-V080A	CMT A WR Level Isolation	B	I	ASME III-2	A	Maintaining the integrity of the reactor coolant pressure boundary.	1	Provides the principal means of fulfilling the safety function.
PXS-PL-V080B	CMT B WR Level Isolation	B	I	ASME III-2				
PXS-PL-V081A	CMT A WR Level Isolation	B	I	ASME III-2				
PXS-PL-V081B	CMT B WR Level Isolation	B	I	ASME III-2				
PXS-PL-V082A	CMT A Upper Level A Isolation 1	A	I	ASME III-3	A	Maintaining the integrity of the reactor coolant pressure boundary.	1	Provides the principal means of fulfilling the safety function.
PXS-PL-V082B	CMT B Upper Level A Isolation 1	A	I	ASME III-3				
PXS-PL-V083A	CMT A Upper Level A Isolation 2	A	I	ASME III-3				
PXS-PL-V083B	CMT B Upper Level A Isolation 2	A	I	ASME III-3				
PXS-PL-V084A	CMT A Upper Level A Vent	B	I	ASME III-2				
PXS-PL-V084B	CMT B Upper Level A Vent	B	I	ASME III-2				
PXS-PL-V085A	CMT A Upper Level A Drain	B	I	ASME III-2				
PXS-PL-V085B	CMT B Upper Level A Drain	B	I	ASME III-2				
PXS-PL-V086A	CMT A Upper Level B Isolation 1	A	I	ASME III-3				
PXS-PL-V086B	CMT B Upper Level B Isolation 1	A	I	ASME III-3				
PXS-PL-V087A	CMT A Upper Level B Isolation 2	A	I	ASME III-3				
PXS-PL-V087B	CMT B Upper Level B Isolation 2	A	I	ASME III-3				

Table 15A-1. AP1000 UK Categorisation and Classification of Mechanical SSCs (cont.)

Tag Number	Description	AP1000 Class	Seismic Category	Principal Design Code	UK Safety Category	Safety Function(s) Provided by the SSC	UK Safety Class	Justification of the Safety Class
Passive Core Cooling System (PXS) Location: Containment (cont.)								
PXS-PL-V088A	CMT A Upper Level B Vent	B	I	ASME III-2	A	Maintaining the integrity of the reactor coolant pressure boundary.	1	Provides the principal means of fulfilling the safety function.
PXS-PL-V088B	CMT B Upper Level B Vent	B	I	ASME III-2				
PXS-PL-V089A	CMT A Upper Level B Drain	B	I	ASME III-2				
PXS-PL-V089B	CMT B Upper Level B Drain	B	I	ASME III-3				
PXS-PL-V092A	CMT A Lower Level A Isolation 1	A	I	ASME III-3				
PXS-PL-V092B	CMT B Lower Level A Isolation 1	A	I	ASME III-3				
PXS-PL-V093A	CMT A Lower Level A Isolation 2	A	I	ASME III-3				
PXS-PL-V093B	CMT B Lower Level A Isolation 2	A	I	ASME III-2				
PXS-PL-V094A	CMT A Lower Level A Vent	B	I	ASME III-2				
PXS-PL-V094B	CMT B Lower Level A Vent	B	I	ASME III-2				
PXS-PL-V095A	CMT A Lower Level A Drain	B	I	ASME III-2				
PXS-PL-V095B	CMT B Lower Level A Drain	B	I	ASME III-2				
PXS-PL-V096A	CMT A Lower Level B Isolation 1	A	I	ASME III-3				
PXS-PL-V096B	CMT B Lower Level B Isolation 1	A	I	ASME III-3				
PXS-PL-V097A	CMT A Lower Level B Isolation 2	A	I	ASME III-3				
PXS-PL-V097B	CMT B Lower Level B Isolation 2	A	I	ASME III-3				
PXS-PL-V098A	CMT A Lower Level B Vent	B	I	ASME III-2				
PXS-PL-V098B	CMT B Lower Level B Vent	B	I	ASME III-2				
PXS-PL-V099A	CMT A Lower Level B Drain	B	I	ASME III-2				
PXS-PL-V099B	CMT B Lower Level B Drain	B	I	ASME III-2				
PXS-PL-V101	PRHR HX Inlet Isolation	A	I	ASME III-1	A	Removal of decay heat from the reactor coolant during normal operation and accident conditions (including providing a heat sink for those systems involved in the removal of heat from the reactor coolant during normal operation and accident conditions). Prevention of the release of radioactive material through the boundary of the RCS.	1	Provides the principal means of fulfilling the safety function.
PXS-PL-V102A	PRHR HX Inlet Head Vent	B	I	ASME III-2	A	Prevention of the release of radioactive material through the boundary of the RCS.	1	Provides the principal means of fulfilling the safety function. Flow from this flow path is reduced by the use of a flow restrictor. This valve represents the first point of flow isolation.
PXS-PL-V102B	PRHR HX Inlet Head Drain	B	I	ASME III-2				
PXS-PL-V103A	PRHR HX Outlet Head Vent	B	I	ASME III-2				
PXS-PL-V103B	PRHR HX Outlet Head Drain	B	I	ASME III-2				

Table 15A-1. AP1000 UK Categorisation and Classification of Mechanical SSCs (cont.)

Tag Number	Description	AP1000 Class	Seismic Category	Principal Design Code	UK Safety Category	Safety Function(s) Provided by the SSC	UK Safety Class	Justification of the Safety Class
Passive Core Cooling System (PXS) Location: Containment (cont.)								
PXS-PL-V104A	PRHR HX Flow Transmitter A Isolation	B	I	ASME III-2	A	Maintaining the integrity of the reactor coolant pressure boundary.	1	Provides the principal means of fulfilling the safety function.
PXS-PL-V104B	PRHR HX Flow Transmitter B Isolation	B	I	ASME III-2				
PXS-PL-V105A	PRHR HX Flow Transmitter A Isolation	B	I	ASME III-2				
PXS-PL-V105B	PRHR HX Flow Transmitter B Isolation	B	I	ASME III-2				
PXS-PL-V106	Containment Recirc Line A Vent 1	C	I	ASME III-3	A	Maintaining reactor coolant inventory.	1	Provides the principal means of fulfilling the safety function.
PXS-PL-V107	Containment Recirc Line A Vent 2	C	I	ASME III-3				
PXS-PL-V108A	PRHR HX Control	A	I	ASME III-1	A	Removal of decay heat from the reactor coolant during normal operation and accident conditions (including providing a heat sink for those systems involved in the removal of heat from the reactor coolant during normal operation and accident conditions). Prevention of the release of radioactive material through the boundary of the RCS.	1	Provides the principal means of fulfilling the safety function.
PXS-PL-V108B	PRHR HX Control	A	I	ASME III-1				
PXS-PL-V109	PRHR HX/RCS Return Isolation	A	I	ASME III-1				
PXS-PL-V111A	PRHR HX Highpoint Vent	B	I	ASME III-2	A	Prevention of the release of radioactive material through the boundary of the RCS.	1	Provides the principal means of fulfilling the safety function. Flow from this flow path is reduced by the use of a flow restrictor. This valve represents the first point of flow isolation.
PXS-PL-V111B	PRHR HX Highpoint Vent	B	I	ASME III-2				
PXS-PL-V113	PRHR HX Pressure Transmitter Isolation	B	I	ASME III-2	A	Maintaining the integrity of the reactor coolant pressure boundary.	1	Provides the principal means of fulfilling the safety function.
PXS-PL-V115A	Cont Recirc Line A Highpoint Drain Valve 1	C	I	ASME III-3				
PXS-PL-V115B	Cont Recirc Line B Highpoint Drain Valve 1	C	I	ASME III-3				
PXS-PL-V116A	Cont Recirc Line A Highpoint Drain Valve 2	C	I	ASME III-3				
PXS-PL-V116B	Cont Recirc Line B Highpoint Drain Valve 2	C	I	ASME III-3				
PXS-PL-V117A	Containment Recirculation A Isolation	C	I	ASME III-3	A	Maintaining reactor coolant inventory.	1	Provides the principal means of fulfilling the safety function.
PXS-PL-V117B	Containment Recirculation B Isolation	C	I	ASME III-3				
PXS-PL-V118A	Containment Recirculation A Isolation	C	I	ASME III-3				
PXS-PL-V118B	Containment Recirculation B Isolation	C	I	ASME III-3				
PXS-PL-V119A	Containment Recirculation A Check	C	I	ASME III-3				
PXS-PL-V119B	Containment Recirculation B Check	C	I	ASME III-3				
PXS-PL-V120A	Containment Recirculation A Isolation	C	I	ASME III-3				
PXS-PL-V120B	Containment Recirculation B Isolation	C	I	ASME III-3				
PXS-PL-V121A	IRWST Line A Isolation	C	I	ASME III-3				
PXS-PL-V121B	IRWST Line B Isolation	C	I	ASME III-3				

Table 15A-1. AP1000 UK Categorisation and Classification of Mechanical SSCs (cont.)

Tag Number	Description	AP1000 Class	Seismic Category	Principal Design Code	UK Safety Category	Safety Function(s) Provided by the SSC	UK Safety Class	Justification of the Safety Class
Passive Core Cooling System (PXS) Location: Containment (cont.)								
PXS-PL-V122A	IRWST Injection A Check	A	I	ASME III-1	A	Maintaining reactor coolant inventory. Prevention of the release of radioactive material through the boundary of the RCS.	1	Provides the principal means of fulfilling the safety function.
PXS-PL-V122B	IRWST Injection B Check	A	I	ASME III-1				
PXS-PL-V123A	IRWST Injection A Isolation	A	I	ASME III-1				
PXS-PL-V123B	IRWST Injection B Isolation	A	I	ASME III-1				
PXS-PL-V124A	IRWST Injection A Check	A	I	ASME III-1				
PXS-PL-V124B	IRWST Injection B Check	A	I	ASME III-1				
PXS-PL-V125A	IRWST Injection A Isolation	A	I	ASME III-1				
PXS-PL-V125B	IRWST Injection B Isolation	A	I	ASME III-1				
PXS-PL-V126A	IRWST Injection Check Test	C	I	ASME III-3	A	Maintaining reactor coolant inventory.	1	Provides the principal means of fulfilling the safety function.
PXS-PL-V126B	IRWST Injection Check Test	C	I	ASME III-3				
PXS-PL-V127	IRWST Injection Line A Drain Valve	C	I	ASME III-3				
PXS-PL-V128A	IRWST Injection Check Test	A	I	ASME III-1	A	Maintaining reactor coolant inventory. Prevention of the release of radioactive material through the boundary of the RCS.	1	Provides the principal means of fulfilling the safety function.
PXS-PL-V128B	IRWST Injection Check Test	A	I	ASME III-1				
PXS-PL-V129A	IRWST Injection Check Test	A	I	ASME III-1				
PXS-PL-V129B	IRWST Injection Check Test	A	I	ASME III-1				
PXS-PL-V130A	IRWST Gutter Bypass A Isolation	C	I	ASME III-3	A	Removal of decay heat from the reactor coolant during normal operation and accident conditions (including providing a heat sink for those systems involved in the removal of heat from the reactor coolant during normal operation and accident conditions).	1	Provides the principal means of fulfilling the safety function.
PXS-PL-V130B	IRWST Gutter Bypass B Isolation	C	I	ASME III-3				
PXS-PL-V131A	IRWST Injection Line A Drain Line	B	I	ASME III-2	A	Maintaining the integrity of the reactor coolant pressure boundary.	1	Provides the principal means of fulfilling the safety function.
PXS-PL-V131B	IRWST Injection Line B Drain Line	B	I	ASME III-2				
PXS-PL-V132A	IRWST Injection Line A Drain Line	B	I	ASME III-2				
PXS-PL-V132B	IRWST Injection Line B Drain Line	B	I	ASME III-2				
PXS-PL-V133A	IRWST Injection Line A Vent Valve	B	I	ASME III-2				
PXS-PL-V133B	IRWST Injection Line B Vent Valve	B	I	ASME III-2				
PXS-PL-V134A	IRWST Injection Line A Vent Valve	B	I	ASME III-2				
PXS-PL-V134B	IRWST Injection Line B Vent Valve	B	I	ASME III-2				
PXS-PL-V135A	IRWST Injection Line A Vent Valve	B	I	ASME III-2				
PXS-PL-V135B	IRWST Injection Line B Vent Valve	B	I	ASME III-2				
PXS-PL-V149	RNS Suction Pump Drain Line	C	I	ASME III-3				

Table 15A-1. AP1000 UK Categorisation and Classification of Mechanical SSCs (cont.)

Tag Number	Description	AP1000 Class	Seismic Category	Principal Design Code	UK Safety Category	Safety Function(s) Provided by the SSC	UK Safety Class	Justification of the Safety Class
Passive Core Cooling System (PXS) Location: Containment (cont.)								
PXS-PL-V150A	IRWST Level Transmitter A Isolation	C	I	ASME III-3	A	Instrumentation and control systems required to automatically actuate or provide manual actuation (where this is the only means of actuation) for SSCs delivering other Category A functions.	1	Provides the principal means of fulfilling the safety function.
PXS-PL-V150B	IRWST Level Transmitter B Isolation	C	I	ASME III-3				
PXS-PL-V150C	IRWST Level Transmitter C Isolation	C	I	ASME III-3				
PXS-PL-V150D	IRWST Level Transmitter D Isolation	C	I	ASME III-3				
PXS-PL-V151A	IRWST Wide Range Level Transmitter A Isolation	C	I	ASME III-3				
PXS-PL-V151B	IRWST Wide Range Level Transmitter B Isolation	C	I	ASME III-3				
PXS-PL-V151C	IRWST Wide Range Level Transmitter C Isolation	C	I	ASME III-3				
PXS-PL-V151D	IRWST Wide Range Level Transmitter D Isolation	C	I	ASME III-3				
PXS-PL-V161A	IRWST Lower. Narrow Range Level Transmitter A Isolation	C	I	ASME III-3	A	Instrumentation and control systems required to automatically actuate or provide manual actuation (where this is the only means of actuation) for SSCs delivering other Category A functions.	1	Provides the principal means of fulfilling the safety function.
PXS-PL-V161B	IRWST Lower. Narrow Range Level Transmitter B Isolation	C	I	ASME III-3				
PXS-PL-V161C	IRWST Lower. Narrow Range Level Transmitter C Isolation	C	I	ASME III-3				
PXS-PL-V161D	IRWST Lower. Narrow Range Level Transmitter D Isolation	C	I	ASME III-3				
PXS-PL-V162A	IRWST Lower. Narrow Range Level Transmitter A Ref. Leg Isolation	C	I	ASME III-3				
PXS-PL-V162B	IRWST Lower. Narrow Range Level Transmitter B Ref. Leg Isolation	C	I	ASME III-3				
PXS-PL-V162C	IRWST Lower. Narrow Range Level Transmitter C Ref. Leg Isolation	C	I	ASME III-3				
PXS-PL-V162D	IRWST Lower. Narrow Range Level Transmitter D Ref. Leg Isolation	C	I	ASME III-3				
PXS-PL-V170A	PRHR Flow Transmitter A Vent	B	I	ASME III-2	A	Instrumentation and control systems required to automatically actuate or provide manual actuation (where this is the only means of actuation) for SSCs delivering other Category A functions.	1	Provides the principal means of fulfilling the safety function.
PXS-PL-V170B	PRHR Flow Transmitter B Vent	B	I	ASME III-2				
PXS-PL-V171A	PRHR Flow Transmitter A Vent	B	I	ASME III-2				
PXS-PL-V171B	PRHR Flow Transmitter B Vent	B	I	ASME III-2				

Table 15A-1. AP1000 UK Categorisation and Classification of Mechanical SSCs (cont.)

Tag Number	Description	AP1000 Class	Seismic Category	Principal Design Code	UK Safety Category	Safety Function(s) Provided by the SSC	UK Safety Class	Justification of the Safety Class
Passive Core Cooling System (PXS) Location: Containment (cont.)								
PXS-PL-V201A	Accumulator A Leak Test	B	I	ASME III-2	A	Maintaining the integrity of the reactor coolant pressure boundary.	1	Provides the principal means of fulfilling the safety function.
PXS-PL-V201B	Accumulator B Leak Test	B	I	ASME III-2				
PXS-PL-V202A	Accumulator A Leak Test	C	I	ASME III-3				
PXS-PL-V202B	Accumulator B Leak Test	C	I	ASME III-3				
PXS-PL-V205A	RNS Discharge Leak Test	B	I	ASME III-2				
PXS-PL-V205B	RNS Discharge Leak Test	B	I	ASME III-2				
PXS-PL-V206	RNS Discharge Leak Test	C	I	ASME III-3				
PXS-PL-V207A	RNS Suction Leak Test	B	I	ASME III-2				
PXS-PL-V207B	RNS Suction Leak Test	B	I	ASME III-2				
PXS-PL-V208A	RNS Suction Leak Test	B	I	ASME III-2				
PXS-PL-V217	PXS Leak Test Line Isolation	D	NNS	ANSI B3 1.1	C	Provide long-term support of Category A or B functions.	3	These flow paths are used to support long-term function of the PXS by allowing the required testing of PXS valves.
PXS-PL-V221	Test Header to IRWST	D	NNS	ANSI B3 1.1				
PXS-PL-V230A	CMT A Fill Isolation	B	I	ASME III-2	A	Maintaining the integrity of the reactor coolant pressure boundary.	1	Provides the principal means of fulfilling the safety function.
PXS-PL-V230B	CMT B Fill Isolation	B	I	ASME III-2				
PXS-PL-V231A	CMT A Fill Check	B	I	ASME III-2				
PXS-PL-V231B	CMT B Fill Check	B	I	ASME III-2				
PXS-PL-V232A	Accumulator A Fill/Drain Isolation	C	I	ASME III-3				
PXS-PL-V232B	Accumulator B Fill/Drain Isolation	C	I	ASME III-3				
PXS-PL-V250A	CMT A Check Valve Test	A	I	ASME III-1	A	Maintaining the integrity of the reactor coolant pressure boundary.	1	Provides the principal means of fulfilling the safety function.
PXS-PL-V250B	CMT B Check Valve Test	A	I	ASME III-1				
PXS-PL-V251A	CMT A Check Valve Test	A	I	ASME III-1				
PXS-PL-V251B	CMT B Check Valve Test	A	I	ASME III-1				
PXS-PL-V252A	CMT A Check Valve Test	A	I	ASME III-1				
PXS-PL-V252B	CMT B Check Valve Test	A	I	ASME III-1				
PXS-PY-C01	Nitrogen Makeup Containment Penetration	B	I	ASME III, MC	A	Prevention of the release of radioactive material from the containment.	1	Provides the principal means of fulfilling the safety function.
PXS-PY-E01	DVI-B Inline Expansion Joint	C	I	ASME III-3	A	Maintaining reactor coolant inventory, core cooling.	1	Provides the principal means of fulfilling the safety function.
PXS-PY-R01A	Core Makeup Tank A Orifice	A	I	ASME III-1	A	Maintaining reactor coolant inventory. Control of core reactivity during normal operation and accident conditions.	1	Provides the principal means of fulfilling the safety function.
PXS-PY-R01B	Core Makeup Tank B Orifice	A	I	ASME III-1	A	Maintaining reactor coolant inventory. Control of core reactivity during normal operation and accident conditions.	1	Provides the principal means of fulfilling the safety function.

Table 15A-1. AP1000 UK Categorisation and Classification of Mechanical SSCs (cont.)

Tag Number	Description	AP1000 Class	Seismic Category	Principal Design Code	UK Safety Category	Safety Function(s) Provided by the SSC	UK Safety Class	Justification of the Safety Class
Passive Core Cooling System (PXS) Location: Containment (cont.)								
PXS-PY-R02A	Accumulator Tank A Orifice	C	I	ASME III-3	A	Maintaining reactor coolant inventory. Control of core reactivity during normal operation and accident conditions	1	Provides the principal means of fulfilling the safety function.
PXS-PY-R02B	Accumulator Tank B Orifice	C	I	ASME III-3	A	Maintaining reactor coolant inventory. Control of core reactivity during normal operation and accident conditions.	1	Provides the principal means of fulfilling the safety function.
PXS-PY-R04A	Core Makeup Tank A to RCDT	B	I	ASME III-2	A	Maintaining reactor coolant inventory. Control of core reactivity during normal operation and accident conditions.	1	Provides the principal means of fulfilling the safety function.
PXS-PY-R04B	Core Makeup Tank A to RCDT	B	I	ASME III-2	A	Maintaining reactor coolant inventory. Control of core reactivity during normal operation and accident conditions.	1	Provides the principal means of fulfilling the safety function.
PXS-PY-R05	PXS Leak Test Subsystem Orifice	D	NNS	ASME B31.1	C	Provide long-term support of Category A or B functions.	3	Supports operation of Class 1 and Class 2 SSCs.
Balance of system components are Class E					GNS	No nuclear safety implications.	GNS	SSCs are not designed or considered in the application of a safety function.
Reactor Coolant System (RCS) Location: Containment								
RCS-MB-01	Steam Generator 1	A	I	ASME III-1	A	Maintaining the integrity of the RCS pressure boundary; including mitigating RCS overpressure during normal operations and accident conditions. Removing decay heat from the reactor coolant during normal operation and accident conditions (including providing a heat sink for those systems involved in the removal of heat from the reactor coolant during normal operation and accident conditions).	1	Provides the principal means of fulfilling the safety function of maintaining the integrity of the RCS pressure. The RCS function of decay heat removal is not a principal means of satisfying the safety function.
RCS-MB-02	Steam Generator 2	A	I	ASME III-1				
RCS-MP-01A	SG 1 Reactor Coolant Pump	A	I	ASME III-1	A	Maintaining the integrity of the RCS pressure boundary; including mitigating RCS overpressure during normal operations and accident conditions. Removing decay heat from the reactor coolant during normal operation and accident conditions (including providing a heat sink for those systems involved in the removal of heat from the reactor coolant during normal operation and accident conditions).	1	Provides the principal means of fulfilling the safety function of maintaining the integrity of the RCS pressure. Pump coast down time is credited within design basis analysis. The RCS function of decay heat removal is not a principal means of satisfying the safety function.
RCS-MP-01B	SG 1 Reactor Coolant Pump	A	I	ASME III-1				
RCS-MP-02A	SG 2 Reactor Coolant Pump	A	I	ASME III-1				
RCS-MP-02B	SG 2 Reactor Coolant Pump	A	I	ASME III-1				
RCS-MV-01	Reactor Vessel	A	I	ASME III-1	A	Maintaining the integrity of the RCS pressure boundary; including mitigating RCS overpressure during normal operations and accident conditions.	1	Provides the principal means of fulfilling the safety function.
RCS-MV-02	Pressuriser	A	I	ASME III-1	A	Maintaining the integrity of the RCS pressure boundary; including mitigating RCS overpressure during normal operations and accident conditions. Mitigating reactor coolant overpressure during normal operation and accident conditions.	1	Provides the principal means of fulfilling the safety function.

Table 15A-1. AP1000 UK Categorisation and Classification of Mechanical SSCs (cont.)

Tag Number	Description	AP1000 Class	Seismic Category	Principal Design Code	UK Safety Category	Safety Function(s) Provided by the SSC	UK Safety Class	Justification of the Safety Class
Reactor Coolant System (RCS) Location: Containment (cont.)								
–	Pressuriser heaters	A/D	NNS	ASME III-1 ANSI B31.1	A/C	Maintain integrity of the RCS boundary. Maintaining the RCS pressure in the operating band. Since the control of RCS pressure during normal operation prevents reactor trips and the actuation of Category A and Category B functions, these normally operating duty systems are recognised as being important to safety.	1/3	The pressuriser heaters sheath is part of the RCS boundary. This is the heaters only class 1 function. The heaters are configured in 5 groups. A control group is sized to accommodate steady-state heat losses. Backup heater capacity is provided to produce the minimum heat required to maintain subcooled RCS pressure during standby operations.
–	SG Shells	B	I	ASME III-1	A	Maintaining the integrity of the RCS pressure boundary; including mitigating RCS overpressure during normal operations and accident conditions. Removing of decay heat from the reactor coolant during normal operation and accident conditions (including providing a heat sink for those systems involved in the removal of heat from the reactor coolant during normal operation and accident conditions).	1	Provides the principal means of fulfilling the safety function for the release of radioactive material from the containment. The SG shell function of decay heat removal is not a principal means of satisfying the safety function.
–	SG Channel Head Divider Plates	B	I	ASME III-1	A	Maintaining the integrity of the RCS pressure boundary; including mitigating RCS overpressure during normal operations and accident conditions.	1	Provides the principal means of fulfilling the safety function.
–	SG Tube Bundle Support Assemblies	C	I	ASME III, NG	A	Protecting against internal/external hazards that would directly and inevitably result in loss of a principal means to fulfil one of the other Category A safety functions	1	Provides the principal means of fulfilling the safety function.
–	SG Steam Flow Limiting Venturies	B	I	ASME III, NG	A	Maintaining the integrity of the containment; thereby minimising the release of radioactive material from the containment.	1	Provides the principal means of fulfilling the safety function.
–	SG Feedwater Distribution Ring Supports	B	I	ASME III, NG	A	Protecting against internal/external hazards that would directly and inevitably result in loss of a principal means to fulfil a Category A safety function. Removing decay heat from the reactor coolant during normal operation and accident conditions (including providing a heat sink for those systems involved in the removal of heat from the reactor coolant during normal operation and accident conditions).	1	Provides the principal means of fulfilling the safety function of protecting against internal/external hazards that would directly and inevitably result in loss of a principal means to fulfil a Category A safety function. The SG feedwater distribution ring support function of decay heat removal is not a principal means of satisfying the safety function.
RCS-PL-V001A	First Stage ADS	A	I	ASME III-1	A	Removing decay heat from the reactor coolant during normal operation and accident conditions (including providing a heat sink for those systems involved in the removal of heat from the reactor coolant during normal operation and accident conditions). Preventing the release of radioactive material through the boundary of the RCS.	1	Provides the principal means of fulfilling the safety function.
RCS-PL-V001B	First Stage ADS	A	I	ASME III-1				
RCS-PL-V002A	Second Stage ADS	A	I	ASME III-1				
RCS-PL-V002B	Second Stage ADS	A	I	ASME III-1				
RCS-PL-V003A	Third Stage ADS	A	I	ASME III-1				
RCS-PL-V003B	Third Stage ADS	A	I	ASME III-1				
RCS-PL-V004A	Fourth Stage ADS	A	I	ASME III-1				
RCS-PL-V004B	Fourth Stage ADS	A	I	ASME III-1				
RCS-PL-V004C	Fourth Stage ADS	A	I	ASME III-1				
RCS-PL-V004D	Fourth Stage ADS	A	I	ASME III-1				

Table 15A-1. AP1000 UK Categorisation and Classification of Mechanical SSCs (cont.)

Tag Number	Description	AP1000 Class	Seismic Category	Principal Design Code	UK Safety Category	Safety Function(s) Provided by the SSC	UK Safety Class	Justification of the Safety Class
Reactor Coolant System (RCS) Location: Containment (cont.)								
RCS-PL-V005A	Pressuriser Safety Valve	A	I	ASME III-1	A	Maintaining the integrity of the RCS pressure boundary.	1	Provides the principal means of fulfilling the safety function.
RCS-PL-V005B	Pressuriser Safety Valve	A	I	ASME III-1				
RCS-PL-V007A	ADS Test Valve	B	I	ASME III-2	A	Maintaining the integrity of the RCS pressure boundary.	1	Provides the principal means of fulfilling the safety function.
RCS-PL-V007B	ADS Test Valve	B	I	ASME III-2				
RCS-PL-V007C	ADS Test Valve	B	I	ASME III-2				
RCS-PL-V010A	ADS Discharge Header A Vacuum Relief	C	I	ASME III-3	A	Protecting against internal/external hazards that would directly and inevitably result in loss of one of the other Category A safety functions.	1	Hydrodynamic/wet load mitigation.
RCS-PL-V010B	ADS Discharge Header B Vacuum Relief	C	I	ASME III-3	A	Protecting against internal/external hazards that would directly and inevitably result in loss of one of the other Category A safety functions.	1	Hydrodynamic/wet load mitigation.
RCS-PL-V011A/B RCS-PL-V012A/B RCS-PL-V013A/B RCS-PL-V014A/B/C/D	ADS Isolation Valves	A	I	ASME III-1	A	Removing decay heat from the reactor coolant during normal operation and accident conditions (including providing a heat sink for those systems involved in the removal of heat from the reactor coolant during normal operation and accident conditions). Maintaining the integrity of the RCS pressure boundary.	1	Provides the principal means of fulfilling the safety function.
–	Instrument Root Valves	B	I	ASME III-2	A	Maintaining the integrity of the RCS pressure boundary.	1	Provides the principal means of fulfilling the safety function.
–	Sample Isolation Valves	B	I	ASME III-2	A	Maintaining the integrity of the RCS pressure boundary.	1	Provides the principal means of fulfilling the safety function. Flow from this flow path is reduced by the use of a flow restrictor. This valve represents the first point of flow isolation.
RCS-PL-V103	PRHR HX Line Reclosable Connection Isolation Valve	B	I	ASME III-2				
RCS-PL-V108A	Hot Leg 1 Sample Isolation	B	I	ASME III-2	A	Maintaining the integrity of the reactor coolant system pressure boundary.	1	Provides the principal means of fulfilling the safety function.
RCS-PL-V108B	Hot Leg 2 Sample Isolation	B	I	ASME III-2	A	Maintaining the integrity of the reactor coolant system pressure boundary.	1	Provides the principal means of fulfilling the safety function.
RCS-PL-V110A	Pressuriser Spray Valve	A	I	ASME III-1	A	Maintaining the integrity of the RCS pressure boundary.	1	Provides the principal means of fulfilling the safety function.
RCS-PL-V110B	Pressuriser Spray Valve	A	I	ASME III-1				
RCS-PL-V111A	Pressuriser Spray Block Valve	A	I	ASME III-1	A	Maintaining the integrity of the RCS pressure boundary.	1	Provides the principal means of fulfilling the safety function.
RCS-PL-V111B	Pressuriser Spray Block Valve	A	I	ASME III-1				
RCS-PL-V120	Reactor Vessel Flange Leakoff	D	NNS	MSS SP-105	B	Prevention of the release of radioactive waste material from onsite storage facilities.	3	These valves comprise a portion of the reactor vessel flange leakoff detection subsystem to detect and monitor seal leakage.
RCS-PL-V121	Reactor Vessel Flange Leakoff	D	NNS	MSS SP-105				
RCS-PL-V122A	Reactor Vessel Flange Leakoff	D	NNS	ANSI B16.34				
RCS-PL-V122B	Reactor Vessel Flange Leakoff	D	NNS	ANSI B16.34				

Table 15A-1. AP1000 UK Categorisation and Classification of Mechanical SSCs (cont.)

Tag Number	Description	AP1000 Class	Seismic Category	Principal Design Code	UK Safety Category	Safety Function(s) Provided by the SSC	UK Safety Class	Justification of the Safety Class
Reactor Coolant System (RCS) Location: Containment (cont.)								
RCS-PL-V150A	Reactor Vessel Head Vent	A	I	ASME III-1	A	Preventing the release of radioactive material through the boundary of the RCS. Mitigating reactor coolant overpressure during normal operation and accident conditions	1	Provides the principal means of fulfilling the safety function. Opens during pressuriser water solid operation.
RCS-PL-V150B	Reactor Vessel Head Vent	A	I	ASME III-1				
RCS-PL-V150C	Reactor Vessel Head Vent	A	I	ASME III-1				
RCS-PL-V150D	Reactor Vessel Head Vent	A	I	ASME III-1				
RCS-PL-V204	Pressuriser Manual Vent	A	I	ASME III-1	A	Maintaining the integrity of the RCS pressure boundary; including mitigating RCS overpressure during normal operations and accident conditions.	1	Provides the principal means of fulfilling the safety function.
RCS-PL-V205	Pressuriser Manual Vent	A	I	ASME III-1				
RCS-PL-V210A	Pressuriser Spray Bypass	B	I	ASME III-2	A	Protecting against internal/external hazards that would directly and inevitably result in loss of a principal means to fulfil a Category A safety functions. Maintaining the integrity of the RCS pressure boundary; including mitigating RCS overpressure during normal operations and accident conditions.	1	Provides the principal means of fulfilling the safety function (nozzle protection). Flow from this flow path is reduced by the use of a flow restrictor. This valve represents the first point of flow isolation.
RCS-PL-V210B	Pressuriser Spray Bypass	B	I	ASME III-2				
RCS-PL-V232	Manual Head Vent	C	I	ASME III-3	A	Protecting against internal/external hazards that would directly and inevitably result in loss of a principal means to fulfil a Category A safety functions.	1	Provides the principal means of fulfilling the safety function.
RCS-PL-V233	Head Vent Isolation	C	I	ASME III-3				
RCS-PL-V241	ADS Valve Discharge Header Drain Isolation	C	I	ASME III-3	A	Protecting against internal/external hazards that would directly and inevitably result in loss of a principal means to fulfil Category A safety functions.	1	Provides the principal means of fulfilling the safety function.
RCS-PL-V242	ADS Valve Discharge Header Drain Check	D	NNS	ANSI 16.34	B	Preventing the release of radioactive waste material from onsite storage facilities.	3	This valve is used to route ADS discharge fluid to the RCDT and WLS. Therefore, its function is the retention of radioactive liquid wastes.
RCS-PL-V260A	RCP 1A Vent	A	I	ASME III-1	A	Maintaining the integrity of the RCS pressure boundary; including mitigating RCS overpressure during normal operations and accident conditions.	1	Provides the principal means of fulfilling the safety function.
RCS-PL-V260B	RCP 1B Vent	A	I	ASME III-1				
RCS-PL-V260C	RCP 2A Vent	A	I	ASME III-1				
RCS-PL-V260D	RCP 2B Vent	A	I	ASME III-1				
RCS-PL-V261A	RCP 1A Drain	A	I	ASME III-1				
RCS-PL-V261B	RCP 1B Drain	A	I	ASME III-1				
RCS-PL-V261C	RCP 2A Drain	A	I	ASME III-1				
RCS-PL-V261D	RCP 2B Drain	A	I	ASME III-1				

Table 15A-1. AP1000 UK Categorisation and Classification of Mechanical SSCs (cont.)

Tag Number	Description	AP1000 Class	Seismic Category	Principal Design Code	UK Safety Category	Safety Function(s) Provided by the SSC	UK Safety Class	Justification of the Safety Class
Reactor Coolant System (RCS) Location: Containment (cont.)								
RCS-PL-V262A	RCP 1A Flywheel Cooling Purge Supply	A	I	ASME III-1	A	Maintain integrity of the reactor coolant system boundary. This allows a connection within the thermal barrier of the RCP for an external purge water system to be attached during plant outages in order to keep any particulate from entering the motor housing.	1	Provides the principal means of fulfilling the safety function.
RCS-PL-V262B	RCP 1B Flywheel Cooling Purge Supply	A	I	ASME III-1				
RCS-PL-V262C	RCP 2A Flywheel Cooling Purge Supply	A	I	ASME III-1				
RCS-PL-V262D	RCP 2B Flywheel Cooling Purge Supply	A	I	ASME III-1				
RCS-PL-V263A	RCP 1A Flywheel Cooling Purge Discharge	A	I	ASME III-1				
RCS-PL-V263B	RCP 1B Flywheel Cooling Purge Discharge	A	I	ASME III-1				
RCS-PL-V263C	RCP 2A Flywheel Cooling Purge Discharge	A	I	ASME III-1				
RCS-PL-V263D	RCP 2B Flywheel Cooling Purge Discharge	A	I	ASME III-1				
RCS-PY-B01	ADS Hydrostatic Test Spectacle Flange	C	I	ASME III-3	A	Maintaining reactor coolant inventory. Maintaining the integrity of the reactor coolant system pressure boundary; including mitigating reactor coolant system overpressure during normal operations and accident conditions.	2	Permits hydrotesting of piping downstream of ADS. Permits pulling a vacuum on the RCS.
RCS-PY-B02	ADS Hydrostatic Test Spectacle Flange	C	I	ASME III-3				
RCS-PY-B03	RCS Vacuum Pump Suction Spectacle Blind	C	I	ASME III-3				
RCS-PY-B04	RCS Vacuum Ejector Package Suction Spectacle Blind	C	I	ASME III-3				
RCS-PY-K03	Safety Valve Discharge Chamber Rupture Disk	C	I	ASME III-3	A	Maintaining the integrity of the RCS pressure boundary; including mitigating RCS overpressure during normal operations and accident conditions. Preventing the release of radioactive waste material from onsite storage facilities (Cat. B).	1	Provides the principal means of fulfilling the safety function.
RCS-PY-K04	Safety Valve Discharge Chamber Rupture Disk	C	I	ASME III-3				
RCS-PY-R01A	Reactor Vessel Head Vent Flow Orifice A	C	I	ASME III-3	A	Removing the nuclear core decay (or residual) heat from the reactor coolant during normal or accident conditions.	1	Provides the principal means of fulfilling the safety function.
RCS-PY-R01B	Reactor Vessel Head Vent Flow Orifice B	C	I	ASME III-3	A	Removing the nuclear core decay (or residual) heat from the reactor coolant during normal or accident conditions.	1	Provides the principal means of fulfilling the safety function.
RCS-PY-Y01A	Pressurizer Level Reference Leg L225A Flex Hose	B	I	ASME III-2	A	Preventing the release of radioactive material through the boundary of the reactor coolant system.	1	Provides the principal means of fulfilling the safety function.
RCS-PY-Y01B	Pressurizer Level Reference Leg L225B Flex Hose	B	I	ASME III-2	A	Preventing the release of radioactive material through the boundary of the reactor coolant system.	1	Provides the principal means of fulfilling the safety function.
RCS-PY-Y01C	Pressurizer Level Reference Leg L225C Flex Hose	B	I	ASME III-2	A	Preventing the release of radioactive material through the boundary of the reactor coolant system.	1	Provides the principal means of fulfilling the safety function.
RCS-PY-Y01D	Pressurizer Level Reference Leg L225D Flex Hose	B	I	ASME III-2	A	Preventing the release of radioactive material through the boundary of the reactor coolant system.	1	Provides the principal means of fulfilling the safety function.
Balance of system components are Class E					C	Supports the RCS function of removing nuclear heat from the reactor coolant during normal operation.	3	Provides the principal means of fulfilling the safety function.

Table 15A-1. AP1000 UK Categorisation and Classification of Mechanical SSCs (cont.)

Tag Number	Description	AP1000 Class	Seismic Category	Principal Design Code	UK Safety Category	Safety Function(s) Provided by the SSC	UK Safety Class	Justification of the Safety Class
Normal Residual Heat Removal System (RNS) Location: Containment and Auxiliary Building								
RNS-ME-01A	Normal Residual Heat Removal Heat Exchanger A (Tube Side)	C	I	ASME III-3	A	Maintaining the integrity of the RCS boundary. Removal of decay heat from the reactor coolant during normal operation and accident conditions.	1	RNS pressure boundary is considered Class 1 in order to address inter-system LOCA concerns. The RNS function of decay heat removal is not a principal means of satisfying the safety function. Non-pressure retaining portions of the RNS, supporting the decay heat removal function, are treated as Class 2 SSCs.
RNS-ME-01B	Normal Residual Heat Removal Heat Exchanger B (Tube Side)	C	I	ASME III-3				
RNS-MP-01A	Residual Heat Removal Pump A	C	I	ASME III-3				
RNS-MP-01B	Residual Heat Removal Pump B	C	I	ASME III-3				
RNS-PL-V001A	RNS HL Suction Isolation – Inner	A	I	ASME III-1	A	Removal of decay heat from the reactor coolant during normal operation and accident conditions (including providing a heat sink for those systems involved in the removal of heat from the reactor coolant during normal operation and accident conditions). Prevention of the release of radioactive material through the boundary of the RCS.	1	Provides the principal means of fulfilling the safety function.
RNS-PL-V001B	RNS HL Suction Isolation – Inner	A	I	ASME III-1				
RNS-PL-V002A/B	RNS HL Suction Isolation Valves	A	I	ASME III-1	A	Preventing the release of radioactive material through the boundary of the RCS. Removing decay heat from the reactor coolant during normal operation and accident conditions (including providing a heat sink for those systems involved in the removal of heat from the reactor coolant during normal operation and accident conditions).	1	RNS pressure boundary is considered Class 1 in order to address inter-system LOCA concerns. The RNS function of decay heat removal is not a principal means of satisfying the safety function. Non-pressure retaining portions of the RNS, supporting the decay heat removal function, are treated as Class 2 SSCs.
–	RCS Pressure Boundary Thermal Relief Valves	B	I	ASME III-2	A	Preventing the release of radioactive material through the boundary of the RCS.	1	Provides the principal means of fulfilling the safety function. Flow from this flow path is reduced by the use of a flow restrictor. This valve represents the first point of flow isolation.
–	RCS Pressure Boundary Thermal Relief Isolation Valves	B	I	ASME III-2				
RNS-PL-V005A	RNS Pump A Suction Isolation	C	I	ASME III-3	A	Preventing the release of radioactive material through the boundary of the RCS. Removing decay heat from the reactor coolant during normal operation and accident conditions (including providing a heat sink for those systems involved in the removal of heat from the reactor coolant during normal operation and accident conditions).	1	RNS pressure boundary is considered Class 1 in order to address inter-system LOCA concerns. The RNS function of decay heat removal is not a principal means of satisfying the safety function. Non-pressure-retaining portions of the RNS, supporting the decay heat removal function, are treated as Class 2 SSCs.
RNS-PL-V005B	RNS Pump B Suction Isolation	C	I	ASME III-3				
RNS-PL-V006A	RNS HX A Outlet Flow Control	C	I	ASME III-3				
RNS-PL-V006B	RNS HX B Outlet Flow Control	C	I	ASME III-3				
RNS-PL-V007A	RNS Pump A Discharge Isolation	C	I	ASME III-3				
RNS-PL-V007B	RNS Pump B Discharge Isolation	C	I	ASME III-3				
RNS-PL-V008A	RNS HX A Bypass Flow Control	C	I	ASME III-3				
RNS-PL-V008B	RNS HX B Bypass Flow Control	C	I	ASME III-3				
RNS-PL-V010	RNS Discharge Containment Isolation Valve Test	C	I	ASME III-3	A	Preventing the release of radioactive material through the boundary of the RCS.	1	Flow path provided to support system maintenance. Valve closed position required to ensure system Cat. A or B flow path is preserved.
RNS-PL-V011A/B	RNS Discharge Containment Isolation Valve – ORC	B	I	ASME III-2	A	Preventing the release of radioactive material through the boundary of the RCS. Removing decay heat from the reactor coolant during normal operation and accident conditions (including providing a heat sink for those systems involved in the removal of heat from the reactor coolant during normal operation and accident conditions).	1	RNS pressure boundary is considered Class 1 in order to address intersystem LOCA concerns. The RNS function of decay heat removal is not a principal means of satisfying the safety function. Non-pressure-retaining portions of the RNS, supporting the decay heat removal function, are treated as Class 2 SSCs.

Table 15A-1. AP1000 UK Categorisation and Classification of Mechanical SSCs (cont.)

Tag Number	Description	AP1000 Class	Seismic Category	Principal Design Code	UK Safety Category	Safety Function(s) Provided by the SSC	UK Safety Class	Justification of the Safety Class
Normal Residual Heat Removal System (RNS) Location: Containment and Auxiliary Building (cont.)								
RNS-PL-V012	RNS Discharge Containment Isolation Valve Test Connection ORC	B	I	ASME III-2	A	Preventing the release of radioactive material through the boundary of the RCS.	1	Provides the principal means of fulfilling the safety function
RNS-PL-V013A/B	RNS Discharge Containment Isolation – IRC	B	I	ASME III-2	A	Preventing the release of radioactive material through the boundary of the RCS. Removing decay heat from the reactor coolant during normal operation and accident conditions (including providing a heat sink for those systems involved in the removal of heat from the reactor coolant during normal operation and accident conditions).	1	RNS pressure boundary is considered Class 1 in order to address intersystem LOCA concerns. The RNS function of decay heat removal is not a principal means of satisfying the safety function. Non-pressure-retaining portions of the RNS, supporting the decay heat removal function, are treated as Class 2 SSCs.
RNS-PL-V014	RNS Discharge Containment Isolation Valve Test Connection	C	I	ASME III-3	A	Preventing the release of radioactive material through the boundary of the RCS.	1	Provides the principal means of fulfilling the safety function.
RNS-PL-V015A/B RNS-PL-V017A/B	RNS Discharge RCS Pressure Boundary Valves	A	I	ASME III-1	A	Preventing the release of radioactive material through the boundary of the RCS. Removing decay heat from the reactor coolant during normal operation and accident conditions (including providing a heat sink for those systems involved in the removal of heat from the reactor coolant during normal operation and accident conditions).	1	RNS pressure boundary is considered Class 1 in order to address inter-system LOCA concerns. The RNS function of decay heat removal is not a principal means of satisfying the safety function. Non-pressure retaining portions of the RNS, supporting the decay heat removal function, are treated as Class 2 SSCs.
RNS-PL-V016	RNS Discharge Containment Penetration Isolation Valves Test	C	I	ASME III-3	A	Preventing the release of radioactive material through the boundary of the RCS. Removing decay heat from the reactor coolant during normal operation and accident conditions (including providing a heat sink for those systems involved in the removal of heat from the reactor coolant during normal operation and accident conditions).	1	RNS pressure boundary is considered Class 1 in order to address inter-system LOCA concerns. The RNS function of decay heat removal is not a principal means of satisfying the safety function. Non-pressure-retaining portions of the RNS, supporting the decay heat removal function, are treated as Class 2 SSCs.
RNS-PL-V021A/B	RNS HL Suction Pressure Relief	B	I	ASME III-2	A	Preventing the release of radioactive material through the boundary of the RCS. Mitigation of reactor coolant overpressure during normal operation and accident conditions.	1	Provides the principal means of fulfilling the safety function.
RNS-PL-V022A/B	RNS Suction Header Containment Isolation – ORC	B	I	ASME III-2	A	Preventing the release of radioactive material through the boundary of the RCS. Removing decay heat from the reactor coolant during normal operation and accident conditions (including providing a heat sink for those systems involved in the removal of heat from the reactor coolant during normal operation and accident conditions).	1	RNS pressure boundary is considered Class 1 in order to address inter-system LOCA concerns. The RNS function of decay heat removal is not a principal means of satisfying the safety function. Non-pressure retaining portions of the RNS, supporting the decay heat removal function, are treated as Class 2 SSCs.
RNS-PL-V023A/B	RNS Suction from IRWST – Containment Isolation	B	I	ASME III-2	A	Preventing the release of radioactive material through the boundary of the RCS. Removing decay heat from the reactor coolant during normal operation and accident conditions (including providing a heat sink for those systems involved in the removal of heat from the reactor coolant during normal operation and accident conditions).	1	RNS pressure boundary is considered Class 1 in order to address inter-system LOCA concerns. The RNS function of decay heat removal is not a principal means of satisfying the safety function. Non-pressure retaining portions of the RNS, supporting the decay heat removal function, are treated as Class 2 SSCs.

Table 15A-1. AP1000 UK Categorisation and Classification of Mechanical SSCs (cont.)

Tag Number	Description	AP1000 Class	Seismic Category	Principal Design Code	UK Safety Category	Safety Function(s) Provided by the SSC	UK Safety Class	Justification of the Safety Class
Normal Residual Heat Removal System (RNS) Location: Containment and Auxiliary Building (cont.)								
RNS-PL-V024A/B	RNS Discharge to IRWST Isolation	C	I	ASME III-3	A	Preventing the release of radioactive material through the boundary of the RCS. Removing decay heat from the reactor coolant during normal operation and accident conditions (including providing a heat sink for those systems involved in the removal of heat from the reactor coolant during normal operation and accident conditions).	1	RNS pressure boundary is considered Class 1 in order to address inter-system LOCA concerns. The RNS function of decay heat removal is not a principal means of satisfying the safety function. Non-pressure retaining portions of the RNS, supporting the decay heat removal function, are treated as Class 2 SSCs.
RNS-PL-V025	V023 Bonnet Overpressure Protection Valve	C	I	ASME III-3	A	Preventing the release of radioactive material through the boundary of the RCS.	1	Provides the principal means of fulfilling the safety function.
RNS-PL-V026	V023 Test Connection Isolation Valve	C	I	ASME III-3				
RNS-PL-V029	RNS Discharge to CVS	C	I	ASME III-3	A	Maintaining the reactor coolant pressure boundary.	1	RNS pressure boundary is considered Class 1 in order to address inter-system LOCA concerns.
RNS-PL-V030A	RNS HX A Shell Drain	D	NNS	ANSI B16.34	C	Provide support for maintenance of Category A function.	3	Flow path provided to support system maintenance. Valves must remain closed to maintain CCS inventory.
RNS-PL-V030B	RNS HX B Shell Drain	D	NNS	ANSI B16.34				
–	Instrument Isolation Valves	C	I	ASME III-3	A	Preventing the release of radioactive material through the boundary of the RCS.	1	RNS pressure boundary is considered Class 1 in order to address inter-system LOCA concerns. The RNS function of decay heat removal is not a principal means of satisfying the safety function. Non-pressure retaining portions of the RNS, supporting the decay heat removal function, are treated as Class 2 SSCs.
RNS-PL-V035A	RNS HX A Shell Vent	D	NNS	ANSI 16.34	C	Provide support for maintenance of Category A function.	3	Flow path provided to support system maintenance. Valves must remain closed to maintain CCS inventory.
RNS-PL-V035B	RNS HX B Shell Vent	D	NNS	ANSI 16.34				
RNS-PL-V036A	RNS Pump A Suction Piping Drain Isolation	C	I	ASME III-3	A	Preventing the release of radioactive material through the boundary of the RCS.	1	RNS pressure boundary is considered Class 1 in order to address inter-system LOCA concerns.
RNS-PL-V036B	RNS Pump B Suction Piping Drain Isolation	C	I	ASME III-3				
RNS-PL-V045	RNS Pump Discharge Relief	C	I	ASME III-3	A	Preventing the release of radioactive material through the boundary of the RCS. Protecting against internal/external hazards that would directly and inevitably result in loss of one of the other Category A safety functions.	1	RNS pressure boundary is considered Class 1 in order to address inter-system LOCA concerns. The RNS function of decay heat removal is not a principal means of satisfying the safety function. Non-pressure retaining portions of the RNS, supporting the decay heat removal function, are treated as Class 2 SSCs.
–	Pump Seal Cooler Vent and Drain Valve	C	I	ASME III-3	A	Preventing the release of radioactive material through the boundary of the RCS	1	RNS pressure boundary is considered Class 1 in order to address inter-system LOCA concerns.
RNS-PL-V050	RNS Pump A Casing Drain Isolation	C	I	ASME III-3				
RNS-PL-V051	RNS Pump B Casing Drain Isolation	C	I	ASME III-3				

Table 15A-1. AP1000 UK Categorisation and Classification of Mechanical SSCs (cont.)

Tag Number	Description	AP1000 Class	Seismic Category	Principal Design Code	UK Safety Category	Safety Function(s) Provided by the SSC	UK Safety Class	Justification of the Safety Class
Normal Residual Heat Removal System (RNS) Location: Containment and Auxiliary Building (cont.)								
RNS-PL-V052	RNS Pump Suction From Spent Fuel Pool Isolation	C	I	ASME III-3	A	Preventing the release of radioactive material through the boundary of the RCS. Maintaining spent fuel integrity such that significant radioactive releases do not occur (as a result of impacts or overheating).	1	RNS pressure boundary is considered Class 1 in order to address inter-system LOCA concerns. The RNS is not a principal means of satisfying the spent fuel pool cooling safety function. Non-pressure retaining portions of the RNS, supporting the spent fuel pool cooling function, are treated as Class 2 SSCs.
RNS-PL-V053	RNS Pump Discharge to Spent Fuel Pool Isolation	C	I	ASME III-3				
RNS-PL-V055	RNS Pump Suction to Cask Loading Pit Isolation	C	I	ASME III-3	A	Removal of decay heat from the reactor coolant during normal operation and accident conditions (including providing a heat sink for those systems involved in the removal of heat from the reactor coolant during normal operation and accident conditions).	1	RNS pressure boundary is considered Class 1 in order to address inter-system LOCA concerns. The RNS function of decay heat removal is not a principal means of satisfying the safety function. Non-pressure retaining portions of the RNS, supporting the decay heat removal function, are treated as Class 2 SSCs.
RNS-PL-V056	RNS Pump Suction to Cask Loading Pit Isolation	C	I	ASME III-3				
RNS-PL-V057A	RNS Pump A Miniflow Isolation	C	I	ASME III-3	A	Removal of decay heat from the reactor coolant during normal operation and accident conditions (including providing a heat sink for those systems involved in the removal of heat from the reactor coolant during normal operation and accident conditions).	1	Pump minimum flow protection required to ensure RNS pumps remain functional when operating at low system flows.
RNS-PL-V057B	RNS Pump B Miniflow Isolation	C	I	ASME III-3				
RNS-PL-V059	RNS Pump Suction Containment Isolation Test Connection	C	I	ASME III-3	A	Provide long-term support of Category A or B functions.	1	Flow path provided to support system maintenance. Valve closed position required to ensure system Cat. A or B flow path is preserved.
–	HX Channel Head Drain Isolation Valves	C	I	ASME III-3	A	Preventing the release of radioactive material through the boundary of the RCS.	1	Provides the principal means of fulfilling the safety function.

Table 15A-1. AP1000 UK Categorisation and Classification of Mechanical SSCs (cont.)

Tag Number	Description	AP1000 Class	Seismic Category	Principal Design Code	UK Safety Category	Safety Function(s) Provided by the SSC	UK Safety Class	Justification of the Safety Class
Normal Residual Heat Removal System (RNS) Location: Containment and Auxiliary Building (cont.)								
RNS-PL-V061A/B	RNS Return from CVS – Containment Isolation	B	I	ASME III-2	A	Prevention of the release of radioactive material from the containment.	1	Provides the principal means of fulfilling the safety function.
RNS-PL-V065	RNS Discharge Isolation Valve	C	I	ASME III-3				
RNS-PL-V066A	DVI A Drain Isolation Valve	C	I	ASME III-3				
RNS-Pl-V066B	DVI B Drain Isolation Valve	C	I	ASME III-3				
RNS-PL-V067A	DVI A Drain Isolation Valve	B	I	ASME III-2				
RNS-PL-V067B	DVI B Drain Isolation Valve	B	I	ASME III-2				
RNS-PL-V068	IRWST Line Drain Isolation Valve	C	I	ASME III-3				
RNS-PL-V069A	RNS Pump A Miniflow Vent	C	I	ASME III-3				
RNS-PL-V069B	RNS Pump B Mininflow Vent	C	I	ASME III-3				
RNS-PL-V080	IRWST Suction Line to RNS Pump Vent	B	I	ASME III-2				
RNS-PL-V081	RNS Cask Loading Pit Suction Line Vent	C	I	ASME III-3				
RNS-PL-V082	RNS Discharge Drain	C	I	ASME III-3				
RNS-PY-C01	Normal Residual Heat Removal Suction Line Penetration	B	I	ASME III, MC				
RNS-PY-C02	Normal Residual Heat Removal Discharge Line Penetration	B	I	ASME III, MC				
RNS-PY-R01A	Residual Heat Removal Discharge to DVI Line Orifice A	C	I	ASME III-3				
RNS-PY-R01B	Residual Heat Removal Discharge to DVI Line Orifice A	C	I	ASME III-3				
RNS-PY-R02A	Residual Heat Removal Pump Miniflow Orifice A	C	I	ASME III-3				
RNS-PY-R02B	Residual Heat Removal Pump Miniflow Orifice B	C	I	ASME III-3				
RNS-PY-R03	Residual Heat Removal to IRWST Line Orifice	C	I	ASME III-3				
RNS-PY-R04	Residual Heat Removal to Spent Fuel Pool Line Orifice	C	I	ASME III-3				
Balance of system components are Class E					GNS	No nuclear safety implications.	GNS	SSCs are not designed or considered in the application of a safety function.
Raw Water System (RWS) Location: Yard, Turbine Building								
System components are Class E					GNS	No nuclear safety implications.	GNS	SSCs are not designed or considered in the application of a safety function.

Table 15A-1. AP1000 UK Categorisation and Classification of Mechanical SSCs (cont.)

Tag Number	Description	AP1000 Class	Seismic Category	Principal Design Code	UK Safety Category	Safety Function(s) Provided by the SSC	UK Safety Class	Justification of the Safety Class
Reactor System (RXS) Location: Containment								
–	Fuel Assemblies	C	I	M/f Std	A	Removal of decay heat from the reactor coolant during normal operation and accident conditions (including providing a heat sink for those systems involved in the removal of heat from the reactor coolant during normal operation and accident conditions). Maintaining spent fuel integrity such that significant radioactive releases do not occur (as a result of impacts or overheating). Protecting against internal/external hazards that would directly and inevitably result in loss of one of the other Category A safety functions.	1	Provides the principal means of fulfilling the safety function.
–	Control Rod Clusters	B	I	M/f Std	A	Control of core reactivity during normal operation and accident conditions.	1	Provides the principal means of fulfilling the safety function.
RXS-MI-01	Reactor Upper Internals	C	I	ASME III, NG	A	Protecting against internal hazards that, as part of a sequence of failures, could result in loss of a Category A or B safety function. Removing the nuclear core decay heat from the reactor core during normal and accident conditions.	1	The upper internals restrain the top of the fuel assemblies from vertical and horizontal movement. The upper internals provide a protective path for the fixed in-core flux detectors and core exit thermocouples. The upper internals provide the flow path for flow exiting the core to establish the required circulation for decay heat removal.
RXS-MI-02	Reactor Lower Internals	C	I	ASME III, NG	A	Protecting against internal hazards that could directly and inevitably result in loss of one of the other Category A safety functions. Removing the nuclear core decay heat from the reactor core during normal and accident conditions.	1	Provides protection, alignment, and support for the core.
RXS-MI-10	Fasteners	D	NNS	-	B	Protecting against internal hazards that, as part of a sequence of failures, could result in loss of a safety function.	3	Includes fasteners and pins that do not provide direct load carrying capabilities of core support structures.
RXS -MI-11	Threaded Structural Fasteners	C	I	ASME III, NG	A	Protecting against internal hazards that could directly and inevitably result in loss of one of the other Category A safety functions.	1	Provide direct load carrying capabilities of core support structures.
RXS-MI-20	Lower Core Support Plate	C	I	ASME III, NG	A	Protecting against internal hazards that could directly and inevitably result in loss of one of the other Category A safety functions. Removing the nuclear core decay heat from the reactor core during normal and accident conditions.	1	The lower core support assembly supports the core and the attached internal structures. Provides directional and metered control of reactor coolant flow through the core. Provides restraint and alignment of the core.
RXS-MI-21	Secondary Core Support	D	NNS	-	B	Functions that provide a backup to a Category A safety function.	3	In the event of an abnormal downward vertical displacement of the internals following a hypothetical failure, the secondary core support limits the dynamic force imposed on the reactor vessel.
RXS-MI-22	Vortex Suppression Plate	D	II	-	C	Removing nuclear heat from the reactor coolant during normal operation.	3	The lower plenum vortex-suppressor plate is positioned in the vessel's lower plenum to suppress flow vortices formed by reactor coolant flow reverser in this region.

Table 15A-1. AP1000 UK Categorisation and Classification of Mechanical SSCs (cont.)

Tag Number	Description	AP1000 Class	Seismic Category	Principal Design Code	UK Safety Category	Safety Function(s) Provided by the SSC	UK Safety Class	Justification of the Safety Class
Reactor System (RXS) Location: Containment (cont.)								
RXS-MI-23	Core Shroud Assembly	D	II	-	B	Functions that provide a backup to a Category A safety function.	3	The core shroud allows cooling water (i.e., bypass) to flow through the cavity between the core barrel and core shroud lateral panels while providing distance between the core and the RV. This distance protects the RV from detrimental radiation effects by limiting total exposure.
RXS-MI-24	Radial Supports (4)	C	I	ASME III, CS	A	Protecting against internal/external hazards that could directly and inevitably result in loss of one of the other Category A safety functions.	1	Restricts the lower end of the core barrel from rotational or translations movement and provides a load path for the lower core support plate horizontal loadings, while allowing for radial and axial displacements of the core barrel and lower core support plate.
RXS-MI-25	Core Barrel	C	I	ASME III, NG	A	Removing the nuclear core decay heat from the reactor core during normal and accident conditions.	1	Directs flow from the RV inlet nozzles through the downcomer annulus, through the flow skirt, and into the lower plenum.
RXS-MI-26	Core Barrel Nozzle	C	I	ASME III, NG	A	Removing the nuclear core decay heat from the reactor core during normal and accident conditions.	1	Provides the passageway for the reactor coolant from the core to the RV outlet nozzle projection.
RXS-MI-27	Head and Vessel Pins	D	II	-	B	Functions that provide a backup to a Category A safety function.	3	Pins provide an alignment guide and assist in the proper orientation and assembly of the lower internals, upper internals, and reactor vessel closure head.
RXS-MI-28	Lower Support Plate Fuel Alignment Pins	C	I	ASME III, NG	A	Protecting against internal hazards that could directly and inevitably result in loss of one of the other Category A safety functions.	1	Locates the bottom of the fuel assembly nozzle.
RXS-MI-29	Core Barrel Hold Down Spring	C	I	-	A	Protecting against internal hazards that could directly and inevitably result in loss of one of the other Category A safety functions.	1	Provides a preload to limit axial movement of the upper and lower core support assemblies during operation.
RXS-MI-50	Upper Support	C	I	ASME III, NG	A	Protecting against internal hazards that could directly and inevitably result in loss of one of the other Category A safety functions.	1	Provides the vertical restraint, lateral restraint, and lateral alignment to the top of the core through its main components.
RXS-MI-51	Upper Core Plate	C	I	ASME III, NG	A	Protecting against internal hazards that could directly and inevitably result in loss of one of the other Category A safety functions.	1	Transfers core loads to the upper support columns and compresses the fuel assembly springs creating a preload.
RXS-MI-52	Support Columns (42)	C	I	ASME III, NG	A	Protecting against internal hazards that could directly and inevitably result in loss of one of the other Category A safety functions.	1	Transfers vertical and lateral reaction loads to the upper support subassembly.
RXS-MI-53	Guide Tube Assemblies (69)	C	I	ANSI B31.1	A	Controlling subcritical reactivity of the fuel in the reactor core during normal operations and accident conditions.	1	The guide tube assemblies sheath and guide the control rod drive shafts and control rods.
RXS-MI-54	Upper Support Plate Fuel Alignment Pins	C	I	ASME III, NG	A	Protecting against internal hazards that could directly and inevitably result in loss of one of the other Category A safety functions.	1	Engage the top of the fuel assemblies.
RXS-MI-55	Upper Core Plate Inserts	C	I	ASME III, NG	A	Protecting against internal hazards that could directly and inevitably result in loss of one of the other Category A safety functions.	1	Provides the alignment plate engagement gaps.

Table 15A-1. AP1000 UK Categorisation and Classification of Mechanical SSCs (cont.)

Tag Number	Description	AP1000 Class	Seismic Category	Principal Design Code	UK Safety Category	Safety Function(s) Provided by the SSC	UK Safety Class	Justification of the Safety Class
Reactor System (RXS) Location: Containment (cont.)								
RXS-MI-56	Safety Injection Deflector	D	II	ANSI B31.1	A	Removal of decay heat from the reactor coolant during normal operation and accident conditions.	2	Prevents cold water from the DVI nozzle from impinging directly on the core barrel and directs the water downward.
RXS-MI-58	Head Cooling Nozzles	D	II	ANSI B31.1	B	Plant process control function that maintains variables with the limits assumed in the safety analysis.	3	The AP1000 RV is designed for maximum operating temperatures in accordance with applicable design codes. A contributing function to reduce susceptibility to fatigue of dissimilar metal welds and nozzle penetrations is the use of a reduced temperature closure head design (relative to the core exit temperature). The head cooling nozzles control RV inlet bypass flow to the closure head for this purpose.
RXS-MI-80	Reactor Vessel Flow Skirt	D	II	ASME III NG	A	Removing the nuclear decay heat from the reactor during normal operations and accident conditions.	2	The flow skirt provides a uniform core inlet flow distribution.
RXS-MN-01	Reactor Vessel Cavity Reflective Insulation	D	II	-	A	Functions provided to minimise the consequences of severe accidents in accordance with the plant design basis.	2	During severe accidents involving reactor cavity flooding, the RVLIS shall remain intact and provide a specified annulus with the outer surface of the reactor vessel and allow water in the reactor cavity to enter the bottom of the annulus for cooling of the reactor vessel. The RVLIS shall also allow the free discharge of steam from the top of the annulus.
–	Integrated Head Package CRDM Forced Air Cooling System	E	II	-	GNS	No nuclear safety implication.	GNS	The CRDM coiling system maintains the temperature of the coins contained within the coil stack below the specified design limit during normal operations and hot standby.
–	Integrated Head Package Radial Arm Hoist	E	II	AISC N690	C	Provides long-term support of a Category A or B safety function.	3	The radial arm hoist is provided for stud tensioning activities.
–	Integrated Head Package CRDM Seismic Support	C	I	ASME III NF	A	Protecting against an internal hazard that could directly or inevitably result in the loss of a principal means of fulfilling a Category A safety function.	1	Provides the principal means of seismically supporting the CRDM.
–	Integrated Head Package Lifting Rig	C	I	AISC N690	A	Protecting against an internal hazard that could directly or inevitably result in the loss of a principal means of fulfilling a Category A safety function.	1	The lifting rig removes the IHP during refuelling.
–	Integrated Head Package Integral Cable Support System (1E Cables)	C	I	IEEE 344	A	Protecting against an internal hazard that could directly or inevitably result in the loss of a principal means of fulfilling a Category A safety function.	1	The cable support system provides support to Class 1 cables.
RXS-MY-Y01	Integrated Head Package Shroud	C	I	ASME III NF	A	Permanently installed structure to provide shielding per the plant design basis.	1	The shroud provides shielding that reduces dose rates in the areas of the head assembly.
–	Integrated Head Package Service Structure	E	II	AISC N690	C	Provides long-term support of a Category A or B safety function.	3	The service structures include all handrails, ladders, platforms, and bridges that allow access for maintenance and inspection.
–	CRDM Pressure Housing (Latch Housing and Rod Travel Housing)	A	I	ASME III-NB	A	Prevention of the release of radioactive material through the boundary of the RCS.	1	Components are part of the primary coolant pressure boundary.

Table 15A-1. AP1000 UK Categorisation and Classification of Mechanical SSCs (cont.)

Tag Number	Description	AP1000 Class	Seismic Category	Principal Design Code	UK Safety Category	Safety Function(s) Provided by the SSC	UK Safety Class	Justification of the Safety Class
Reactor System (RXS) Location: Containment (cont.)								
–	CRDM Latch Assembly	C	I	M/f Std	A	Control of core reactivity during normal operation and accident conditions.	1	The control of core reactivity is performed by the RCCA neutron absorber material; the CRDMs are used in a support function for the positioning of the RCCAs to support power operation. The only safety related function of the latch assembly is that it be capable of releasing the drive rod when electrical power is cut to the coil stack assembly before and after an SSE event. The latch assembly is classified as Non-Code because it does not have a nuclear safety-related pressure retaining function.
–	CRDM Drive Rod Assembly	D	NNS	M/f Std	B	Plant process control function that maintains variables with the limits assumed in the safety analysis.	3	The control of core reactivity is performed by the RCCA neutron absorber material; the CRDMs are used in a support function for the positioning of the RCCAs to support power operation.
–	CRDM Coil Stack Assembly	D	NNS	M/f Std	B	Plant process control function that maintains variables with the limits assumed in the safety analysis.	3	The control of core reactivity is performed by the RCCA neutron absorber material; the CRDMs are used in a support function for the positioning of the RCCAs to support power operation.
–	CRDM Flux Rings	D	NNS	M/f Std	B	Plant process control function that maintains variables with the limits assumed in the safety analysis.	3	The flux rings direct the magnetic energy from the coil stack assemblies to actuate the latch assembly latches to hold or move the drive rod assembly and RCCA/GRCA.
–	CRDM Flux Ring Locking Straps	E	NNS	M/f Std	GNS	No nuclear safety implications.	GNS	SSCs are not designed or considered in the application of a safety function.
–	CRDM Rod Travel Housing Eyebolt	D	NNS	M/f Std	B	Protecting against internal hazards that could, as part of a sequence of failures, result in the loss of a safety function.	3	The eyebolt is used to lift and handle the rod travel housing during installation onto the reactor vessel head prior to plant operation.
–	CRDM Guide Sleeve	D	NNS	M/f Std	B	Plant process control function that maintains variables with the limits assumed in the safety analysis.	3	The guide sleeves guide the drive rod into the latch assembly following an outage. The failure during movement could affect the operation and integrity of the CRDM assembly.
RXS-MY-Y01	Irradiation Tube Plug Seat Jack	E	GNS	M/f Std	C	Providing support of a Category A or B function.	3	Specimen tubes are required to maintain integrity to prevent debris intrusion into the core and interfere with Category A functions.
-	Incore Instrumentation QuickLoc Assembly 1	A	I	M/f Std.	A	Maintaining the integrity of the reactor coolant pressure boundary.	1	Principal means of fulfilling the safety function.
Balance of system components are Class E					GNS	No nuclear safety implications.	GNS	SSCs are not designed or considered in the application of a safety function.
Sanitary Drainage System (SDS) Location: Various								
–	Main Control Room Isolation Valves	C	I	ASME III-3	A	Maintaining habitability of the main control room.	1	The isolation valves are the principal means of isolating the main control room envelope during VES operation.
Balance of system components are Class P					GNS	No nuclear safety implications.	GNS	SSCs are not designed or considered in the application of a safety function.

Table 15A-1. AP1000 UK Categorisation and Classification of Mechanical SSCs (cont.)

Tag Number	Description	AP1000 Class	Seismic Category	Principal Design Code	UK Safety Category	Safety Function(s) Provided by the SSC	UK Safety Class	Justification of the Safety Class
Spent Fuel Pool Cooling System (SFS) Location: Auxiliary Building, Containment								
SFS-MV-01A/B	Demineralisers	D	NNS	ASME VIII	C	Control of the level of radioactivity within the spent fuel pool and the IRWST.	3	The SFS provides for the control of radioactivity in the spent fuel coolant, as well as the IRWST which connects to the RCS during refuelling operations.
SFS-MV-02A/B	Filters	D	NNS	ASME VIII				
–	Demineraliser Resin Charge/Discharge Isolation Valves	D	NNS	ANSI B16.34				
–	Differential Pressure Isolation Valves	D	NNS	ANSI B16.34				
–	Demineraliser Flush Isolation Valves	D	NNS	ANSI B16.34				
–	Filter Vent/Drain Isolation Valves	D	NNS	ANSI B16.34				
–	Demineraliser Isolation Valves	D	NNS	ANSI B16.34				
SFS-ME-01A	Spent Fuel Pool Heat Exchanger A	D	NNS	ASME VIII	B	The SFS heat exchanger provides a backup or alternate method to the Category A function to remove heat from the spent fuel pool.	2	SFS provides a supplemental function of spent fuel pool heat removal.
SFS-ME-01B	Spent Fuel Pool Heat Exchanger B	D	NNS	ASME VIII				
SFS-MP-01A	Spent Fuel Cooling Pump A	D	NNS	Hydraulic Institute Standards	B	The SFS cooling pump provides a backup or alternate method to the Category A function to remove heat from the spent fuel pool.	2	SFS provides a supplemental function of spent fuel pool heat removal.
SFS-MP-01B	Spent Fuel Cooling Pump B	D	NNS	Hydraulic Institute Standards				
–	Valves Providing SFS AP1000 Equipment Class D Function	D	NNS	ANSI 16.34	A	Maintaining spent fuel integrity such that significant radioactive releases do not occur (as a result of impacts or overheating).	2	SFS provides a supplemental function of spent fuel pool heat removal. This function is considered important to safety.
SFS-PL-V024A	Spent Fuel Pool Level Instrument Isolation	C	I	ASME III-3	A	Functions required to provide information and control capabilities that allow specified manual actions necessary to reach the nonhazardous stable state.	1	Provides the principal means of fulfilling the safety function.
SFS-PL-V024B	Spent Fuel Pool Level Instrument Isolation	C	I	ASME III-3				
SFS-PL-V024C	Spent Fuel Pool Level Instrument Isolation	C	I	ASME III-3				
SFS-PL-V028	Cask Washdown Pit Level Instrument Isolation Valve	C	I	ASME III-3	A	Maintaining spent fuel integrity such that significant radioactive releases do not occur (as a result of impacts or overheating).	1	Provides the principal means of fulfilling the safety function.
SFS-PL-V031	SFS Refuelling Cavity Drain to SGS Compartment Isolation	C	I	ASME III-3	A	Maintaining reactor coolant inventory Removing decay heat from the reactor coolant during normal operation and accident conditions (including providing a heat sink for those systems involved in the removal of heat from the reactor coolant during normal operation and accident conditions).	1	Drain pathway provides a principal flow path for natural circulation cooling during an accident. Drain is closed during refuelling to preserve reactor canal inventory.

Table 15A-1. AP1000 UK Categorisation and Classification of Mechanical SSCs (cont.)

Tag Number	Description	AP1000 Class	Seismic Category	Principal Design Code	UK Safety Category	Safety Function(s) Provided by the SSC	UK Safety Class	Justification of the Safety Class
Spent Fuel Pool Cooling System (SFS) Location: Auxiliary Building, Containment (cont.)								
SFS-PL-V032	SFS Refuelling Cavity Suction Isolation	C	I	ASME III-3	A	Maintaining reactor coolant inventory. Removing decay heat from the reactor coolant during normal operation and accident conditions (including providing a heat sink for those systems involved in the removal of heat from the reactor coolant during normal operation and accident conditions).	1	Provides the principal means of fulfilling the safety function.
SFS-PL-V058	SFS Containment Isolation Valve V034 Test	C	I	ASME III-3				
SFS-PL-V033	SFS Refuelling Cavity Drain to Containment Sump Isolation	C	I	ASME III-3	A	Maintaining reactor coolant inventory.	1	Provides the principal means of fulfilling the safety function.
SFS-PL-V034	SFS Suction Line Containment Isolation Valve	B	I	ASME III-2	A	Maintaining the integrity of the containment; thereby minimising the release of radioactive material from the containment. Preserve IRWST inventory.	1	Provides the principal means of fulfilling the safety function.
SFS-PL-V035	SFS Suction Line Containment Isolation Valve	B	I	ASME III-2				
SFS-PL-V038	SFS Discharge Line Containment Isolation Valve	B	I	ASME III-2				
SFS-PL-V037	SFS Discharge Line Containment Isolation Valve	B	I	ASME III-2	A	Maintaining the integrity of the containment; thereby minimising the release of radioactive material from the containment.	1	Provides the principal means of fulfilling the safety function.
SFS-PL-V048	SFS Containment Penetration Test Connection Valve	B	I	ASME III-2				
SFS-PL-V056	SFS Containment Penetration Test Connection Isolation Valve	B	I	ASME III-2				
SFS-PL-V067	SFS Containment Isolation Relief Valve	B	I	ASME III-2				
SFS-PL-V039	SFS Suction Line from IRWST Isolation	C	I	ASME III-3	A	Removing the nuclear core decay (or residual) heat from the reactor coolant during normal operations and accident conditions (includes those SSCs that provide the heat sink removal of decay heat from the reactor coolant).	1	The IRWST provides the heat sink for the PRHR HX, which removes the nuclear core decay heat from the reactor coolant during accident conditions. The PXS is the principal means to fulfil this decay heat removal Category A function. This valve provides support for refuelling operations to fill, drain, cool and purify the refuelling cavity and IRWST
SFS-PL-V040	SFS Fuel Transfer Canal Drain Isolation	C	I	ASME III-3	A	Maintaining spent fuel integrity such that significant radioactive releases do not occur (as a result of impacts or overheating).	1	Provides the principal means of fulfilling the safety function.
SFS-PL-V041	SFS Cask Loading Pit Drain Isolation	C	I	ASME III-3				
SFS-PL-V042	Cask Loading Pit to Pump Suction Isolation	C	I	ASME III-3				
SFS-PL-V043	SFS Cask Loading Pit Level Instrument Root	C	I	ASME III-3				
SFS-PL-V045	SFS Discharge to Cask Loading Pit Isolation	C	I	ASME III-3				
SFS-PL-V049	SFS Cask Loading Pit Drain to WLS Isolation	C	I	ASME III-3				
SFS-PL-V066	Spent Fuel Pool to Cask Washdown Pit Isolation	C	I	ASME III-3				
SFS-PL-V068	Cask Washdown Pit Drain Isolation Valve	C	I	ASME III-3				

Table 15A-1. AP1000 UK Categorisation and Classification of Mechanical SSCs (cont.)

Tag Number	Description	AP1000 Class	Seismic Category	Principal Design Code	UK Safety Category	Safety Function(s) Provided by the SSC	UK Safety Class	Justification of the Safety Class
Spent Fuel Pool Cooling System (SFS) Location: Auxiliary Building, Containment (cont.)								
SFS-PL-V044	SFS Suction Line from IRWST Isol. ORC Valve	D	NNS	ANSI B16.34	C	Controlling the level of radioactivity within the reactor coolant.	3	Provides the principal means of fulfilling the safety function.
SFS-PL-V047	SFS Demineralised Water Makeup to SFP Reverse Flow Prevent	D	NNS	ANSI B16.34	C	Providing long-term support of Category A or B functions.	3	Provides the principal means of fulfilling the safety function.
SFS-PL-V071	Refuelling Cavity Overflow to SG Compartment	C	I	ASME III-3	A	Maintaining reactor coolant inventory Removal of decay heat from the reactor coolant during normal operation and accident conditions (including providing a heat sink for those systems involved in the removal of heat from the reactor coolant during normal operation and accident conditions).	1	Drain pathway provides a principal flow path for natural circulation cooling during an accident. Drain is closed during refuelling to preserve reactor canal inventory.
SFS-PL-V072	Refuelling Cavity Overflow to SG Compartment	C	I	ASME III-3				
SFS-PL-V029	FTC & CWP Cross Connect from SFS Pump Discharge Valve	D	NNS	ANSI B16.34	C	Providing long-term support of Category A or B functions.	3	Provides the principal means of fulfilling the safety function.
SFS-PL-V050	SFS Demin Water Makeup to SFP Isolation Valve	E	NNS	M/f Std				
SFS-PL-V055	SFS Ctmt Isolation Valve V038 Test	D	NNS	ANSI B16.34				
SFS-PL-V057	SFS Test Connection Isolation Valve	D	NNS	ANSI B16.34				
SFS-PL-V059	SFS Ctmt Isolation Valve V035 Test	D	NNS	ANSI B16.34				
SFS-PL-V030	SFS Refuelling Cavity Discharge Isolation Valve	D	NNS	ANSI B16.34	C	Controlling the level of radioactivity within the reactor coolant.	3	Provides the principal means of fulfilling the safety function.
SFS-PL-V036	SFS Discharge Line To IRWST Isolation Valve	D	NNS	ANSI B16.34				
SFS-PL-V060	SFS Drain Line to Aux. Bldg Sump Isolation Valve	D	NNS	ANSI B16.34				
SFS-PL-V061	SFS Demin Flush Water Inlet Isolation Valve	D	NNS	ANSI B16.34				
SFS-PL-V064	SFS Pumps Discharge to Refuelling Cavity Isol Valve IRC	D	NNS	ANSI B16.34				
SFS-PL-V065	SFS Pumps Discharge to Refuelling Cavity Isol Valve ORC	D	NNS	ANSI B16.34				
SFS-PL-V075	Refuelling Cavity Post-Accident Containment Floodup Valve	C	I	ASME III-3	A	Maintaining reactor coolant inventory.	1	Provides the principal means of fulfilling the safety function.
SFS-PL-V105	PCS Water to SPF Spray Drain Valve	D	NNS	ANSI B16.34	B	Functions provided to reach and maintain safe state for beyond design accidents as specified in station operating procedures.	2	Provides the principal means of fulfilling the safety function.
SFS-PL-V110A	PCS Water Line to SFP Spray FT023 Isolation Valve	D	NNS	ANSI B16.34				
SFS-PL-V110B	PCS Water Line to SFP Spray FT023 Isolation Valve	D	NNS	ANSI B16.34				

Table 15A-1. AP1000 UK Categorisation and Classification of Mechanical SSCs (cont.)

Tag Number	Description	AP1000 Class	Seismic Category	Principal Design Code	UK Safety Category	Safety Function(s) Provided by the SSC	UK Safety Class	Justification of the Safety Class
Spent Fuel Pool Cooling System (SFS) Location: Auxiliary Building, Containment (cont.)								
SFS-PL-V070	FPS Hose Station Line to Spent Fuel Pool Spray Isol Valve	G	NNS	MSS-SP-67	B	Functions provided to reach and maintain safe state for beyond design accidents as specified in station operating procedures.	3	Does not provide the principal means of fulfilling the safety function.
SFS-PL-V106	FPS Water to SPF Spray Drain Valve	G	NNS	ANSI B16.34				
SFS-PL-V111A	FPS Water Line to SFP Spray FT024 Isolation Valve	D	NNS	ANSI B16.34				
SFS-PL-V111B	FPS Water Line to SFP Spray FT024 Isolation Valve	D	NNS	ANSI B16.34				
SFS-PL-V117	SFS Refuelling Cavity Drain Line Test Connection	C	I	ASME III-3	A	Maintaining inventory of the refuelling cavity.	1	Provides the principal means of fulfilling the safety function.
SFS-PY-C01	Spent Fuel Cooling Pump Discharge to IRWST	B	I	ASME III, MC	A	Prevention of the release of radioactive material from the containment.	1	Each containment penetration provides a principal means of maintaining containment integrity.
SFS-PY-C02	Spent Fuel Cooling Pump Suction from IRWST	B	I	ASME III, MC				
SFS-PY-R04	SFS Cask loading and Washdown Orifice	C	I	ASME III-3	A	Maintaining spent fuel integrity such that significant radioactive releases do not occur (as a result of impacts or overheating).	2	Flow limiting orifice in SFS pump discharge line; adequate NPSH is available without this orifice installed.
SFS-PY-S03A/B SFS-PY-S04A/B	SFP and Refuelling Cavity Skimmers	D	NNS	M/f Std	C	Control of the level of radioactivity within the spent fuel pool, refuelling cavity, and the IRWST.	3	Skimmers remove particulate contamination from the SFP water.
Balance of system components are Class D					A	Maintaining spent fuel integrity such that significant radioactive releases do not occur (as a result of impacts or overheating).	2	SFS provides a supplemental function of spent fuel pool heat removal. This function is considered important to safety.
Steam Generator System (SGS) Location: Containment and Auxiliary Building								
SGS-MY-Y01A	Steam Generator A PORV Silencer	D	NNS	M/f Std	A	Removing the nuclear core decay heat from the reactor coolant during normal operation and accident conditions (including providing a heat sink for those systems involved in the removal of heat from the reactor coolant during normal operation and accident conditions).	2	PORV silencers are specified for ambient noise abatement and are not required to facilitate decay heat removal. This class assumes no credible failure mode can result in exhaust path restrictions that effect PORV operation.
SGS-MY-Y01B	Steam Generator B PORV Silencer	D	NNS	M/f Std				
–	SGS Class B Root Isolation Valves	B	I	ASME III-2	A	Prevention of the release of radioactive material from the containment.	1	The instrument isolation valves are the principal means of fulfilling the safety function.
–	SGS Class C Root Isolation Valves	C	I	ASME III-3	A	Prevention of the release of radioactive material from the containment.	1	The instrument isolation valves are the principal means of fulfilling the safety function.
SGS-PL-V014A	PORV Discharge Condensate Drain Isolation	D	NNS	ANSI B16.34	A	Removing the nuclear core decay heat from the reactor coolant during normal operation and accident conditions (including providing a heat sink for those systems involved in the removal of heat from the reactor coolant during normal operation and accident conditions).	2	The PORV drains serve as a removal point for condensation. However, experience has shown that this condition does not preclude proper PORV operation.
SGS-PL-V014B	PORV Discharge Condensate Drain Isolation	D	NNS	ANSI B16.34				
SGS-PL-V019A	Main Steam Line Vent Isolation	B	I	ASME III-2	A	Prevention of the release of radioactive material from the containment.	1	The isolation valves are the principal means of fulfilling the safety function.
SGS-PL-V019B	Main Steam Line Vent Isolation	B	I	ASME III-2				

Table 15A-1. AP1000 UK Categorisation and Classification of Mechanical SSCs (cont.)

Tag Number	Description	AP1000 Class	Seismic Category	Principal Design Code	UK Safety Category	Safety Function(s) Provided by the SSC	UK Safety Class	Justification of the Safety Class
Steam Generator System (SGS) Location: Containment and Auxiliary Building (cont.)								
SGS-PL-V027A	PORV Block Valve SG 01	B	I	ASME III-2	A	Prevention of the release of radioactive material from the containment. Removing the nuclear core decay heat from the reactor coolant during normal operation and accident conditions (including providing a heat sink for those systems involved in the removal of heat from the reactor coolant during normal operation and accident conditions).	1	These manual, self-actuated, and power operated valves are the principal means of fulfilling the safety function of containment integrity/isolation. The safety valves are the principal means of fulfilling the safety function of nuclear core decay heat removal and overpressure protection.
SGS-PL-V027B	PORV Block Valve SG 02	B	I	ASME III-2				
SGS-PL-V030A	Main Steam Safety Valve SG 01	B	I	ASME III-2				
SGS-PL-V030B	Main Steam Safety Valve SG 02	B	I	ASME III-2				
SGS-PL-V031A	Main Steam Safety Valve SG 01	B	I	ASME III-2				
SGS-PL-V031B	Main Steam Safety Valve SG 02	B	I	ASME III-2				
SGS-PL-V032A	Main Steam Safety Valve SG 01	B	I	ASME III-2				
SGS-PL-V032B	Main Steam Safety Valve SG 02	B	I	ASME III-2				
SGS-PL-V033A	Main Steam Safety Valve SG 01	B	I	ASME III-2				
SGS-PL-V033B	Main Steam Safety Valve SG 02	B	I	ASME III-2				
SGS-PL-V034A	Main Steam Safety Valve SG 01	B	I	ASME III-2				
SGS-PL-V034B	Main Steam Safety Valve SG 02	B	I	ASME III-2				
SGS-PL-V035A	Main Steam Safety Valve SG 01	B	I	ASME III-2				
SGS-PL-V035B	Main Steam Safety Valve SG 02	B	I	ASME III-2				
SGS-PL-V036A	Steam Line Condensate Drain Isolation	B	I	ASME III-2				
SGS-PL-V036B	Steam Line Condensate Drain Isolation	B	I	ASME III-2				
SGS-PL-V038A	Steam Line #1 Nitrogen Supply Isolation	B	I	ASME III-2				
SGS-PL-V038B	Steam Line #2 Nitrogen Supply Isolation	B	I	ASME III-2				
SGS-PL-V040A	Main Steam Line Isolation	B	I	ASME III-2				
SGS-PL-V040B	Main Steam Line Isolation	B	I	ASME III-2				
SGS-PL-V042A	MSIV Bypass Control Isolation	B	I	ASME III-2				
SGS-PL-V042B	MSIV Bypass Control Isolation	B	I	ASME III-2				
SGS-PL-V043A	MSIV Bypass Control Isolation	C	I	ASME III-3				
SGS-PL-V045A	SG 1 Condensate Pipe Drain Valve	B	I	ASME III-2				
SGS-PL-V045B	SG 2 Condensate Pipe Drain Valve	B	I	ASME III-2				
SGS-PL-V057A	Main Feedwater Isolation	B	I	ASME III-2	A	Prevention of the release of radioactive material from the containment.	1	The isolation valves are the principal means of fulfilling the safety function.
SGS-PL-V057B	Main Feedwater Isolation	B	I	ASME III-2				
SGS-PL-V058A	Main Feedwater Check	B	I	ASME III-2				
SGS-PL-V058B	Main Feedwater Check	B	I	ASME III-2				

Table 15A-1. AP1000 UK Categorisation and Classification of Mechanical SSCs (cont.)

Tag Number	Description	AP1000 Class	Seismic Category	Principal Design Code	UK Safety Category	Safety Function(s) Provided by the SSC	UK Safety Class	Justification of the Safety Class
Steam Generator System (SGS) Location: Containment and Auxiliary Building (cont.)								
SGS-PL-V067A	Startup Feedwater Isolation	B	I	ASME III-2	A	Prevention of the release of radioactive material from the containment.	1	The isolation valves are the principal means of fulfilling the safety function.
SGS-PL-V067B	Startup Feedwater Isolation	B	I	ASME III-2				
SGS-PL-V074A	SG Blowdown Isolation	B	I	ASME III-2				
SGS-PL-V074B	SG Blowdown Isolation	B	I	ASME III-2				
SGS-PL-V075A	SG Series Blowdown Isolation	C	I	ASME III-3				
SGS-PL-V075B	SG Series Blowdown Isolation	C	I	ASME III-3				
SGS-PL-V076A	SG1 Blowdown Vent Line Isolation	C	I	ASME III-3				
SGS-PL-V076B	SG2 Blowdown Vent Line Isolation	C	I	ASME III-3				
SGS-PL-V084A	SG 1 Nitrogen Sparging Isolation	B	I	ASME III-2				
SGS-PL-V084B	SG 2 Nitrogen Sparging Isolation	B	I	ASME III-2				
SGS-PL-V086A	Steam Line Condensate Drain Control	C	I	ASME III-3				
SGS-PL-V086B	Steam Line Condensate Drain Control	C	I	ASME III-3				
SGS-PL-V093A	Orifice Isolation Valve	C	I	ASME III-3	A	Prevention of the release of radioactive material from the containment.	1	The instrument isolation valves are the principal means of fulfilling the safety function.
SGS-PL-V093B	Orifice Isolation Valve	C	I	ASME III-3				
SGS-PL-V094A	Orifice Cleanout Line Isolation Valve	C	I	ASME III-3				
SGS-PL-V094B	Orifice Cleanout Line Isolation Valve	C	I	ASME III-3				
SGS-PL-V095A	Orifice Isolation Valve	C	I	ASME III-3				
SGS-PL-V095B	Orifice Isolation Valve	C	I	ASME III-3				
SGS-PL-V096A	Steamline Condensate Drain Level Isolation Valve	B	I	ASME III-2				
SGS-PL-V096B	Steamline Condensate Drain Level Isolation Valve	B	I	ASME III-2				
SGS-PL-V097A	Steamline Condensate Drain Level Isolation Valve	B	I	ASME III-2				
SGS-PL-V097B	Steamline Condensate Drain Level Isolation Valve	B	I	ASME III-2				

Table 15A-1. AP1000 UK Categorisation and Classification of Mechanical SSCs (cont.)

Tag Number	Description	AP1000 Class	Seismic Category	Principal Design Code	UK Safety Category	Safety Function(s) Provided by the SSC	UK Safety Class	Justification of the Safety Class
Steam Generator System (SGS) Location: Containment and Auxiliary Building (cont.)								
SGS-PL-V100A	SG 1 SFW Line Drain	C	I	ASME III-3	A	Prevention of the release of radioactive material from the containment.	1	The principal means of fulfilling the safety function.
SGS-PL-V100B	SG 2 SFW Line Drain	C	I	ASME III-3				
SGS-PL-V101A	SG 1 MFW Line Drain	B	I	ASME III-2				
SGS-PL-V101B	SG 2 MFW Line Drain	B	I	ASME III-2				
SGS-PL-V102A	SG 1 SFW Line Vent	C	I	ASME III-3				
SGS-PL-V102B	SG 2 SFW Line Vent	C	I	ASME III-3				
SGS-PL-V103A	SG 1 MFW Line Vent	B	I	ASME III-2				
SGS-PL-V103B	SG 2 MFW Line Vent	B	I	ASME III-2				
SGS-PL-V104A	SG 1 MFW Line Drain	C	I	ASME III-3				
SGS-PL-V104B	SG 2 MFW Line Drain	C	I	ASME III-3				
SGS-PL-V233A	Power Operated Relief Valve	C	I	ASME III-3	A	Prevention of the release of radioactive material from the containment.	1	The isolation valves are the principal means of fulfilling the safety function.
SGS-PL-V233B	Power Operated Relief Valve	C	I	ASME III-3				
SGS-PL-V240A	MSIV Bypass Isolation	B	I	ASME III-2				
SGS-PL-V240B	MSIV Bypass Isolation	B	I	ASME III-2				
SGS-PL-V250A	Main Feedwater Control	C	I	ASME III-3				
SGS-PL-V250B	Main Feedwater Control	C	I	ASME III-3				
SGS-PL-V255A	Startup Feedwater Control	C	I	ASME III-3	A	Prevention of the release of radioactive material from the containment.	1	The isolation valves are the principal means of fulfilling the safety function.
SGS-PL-V255B	Startup Feedwater Control	C	I	ASME III-3				
SGS-PL-V256A	Startup Feedwater Check Valve	C	I	ASME III-3				
SGS-PL-V256B	Startup Feedwater Check Valve	C	I	ASME III-3				
SGS-PY-C01A	Main Steam Line A Penetration	B	I	ASME III, MC	A	Prevention of the release of radioactive material from the containment.	1	Each containment penetration provides a principal means of maintaining containment integrity.
SGS-PY-C01B	Main Steam Line B Penetration	B	I	ASME III, MC				
SGS-PY-C02A	Main Feedwater Line A Penetration	B	I	ASME III, MC				
SGS-PY-C02B	Main Feedwater Line B Penetration	B	I	ASME III, MC	A	Prevention of the release of radioactive material from the containment.	1	Each containment penetration provides a principal means of maintaining containment integrity.
SGS-PY-C03A	Steam Generator A Blow down Line Penetration	B	I	ASME III, MC				
SGS-PY-C03B	Steam Generator B Blow down Line Penetration	B	I	ASME III, MC				
SGS-PY-C05A	Startup Feedwater Line A Penetration	B	I	ASME III, MC				
SGS-PY-C05B	Startup Feedwater Line B Penetration	B	I	ASME III, MC				
-	Flexible Hose for instrument level, pressure, and flow taps	B	I	ASME III-2	A	Prevention of the release of radioactive material from the containment.	1	The principal means of fulfilling the safety function.
Balance of System Components are Class E					GNS			

Table 15A-1. AP1000 UK Categorisation and Classification of Mechanical SSCs (cont.)

Tag Number	Description	AP1000 Class	Seismic Category	Principal Design Code	UK Safety Category	Safety Function(s) Provided by the SSC	UK Safety Class	Justification of the Safety Class
Secondary Sampling System (SSS) Location: Turbine Building								
System components are Class E					GNS	No nuclear safety implications.	GNS	SSCs are not designed or considered in the application of a safety function.
Service Water System (SWS) Location: Turbine Building and Yard								
–	Service Water Cooling Tower Fans	D	NNS	M/f Std	A	Removing the nuclear core decay (or residual) heat from the reactor coolant during normal operations and accident conditions (includes those SSCs that provide the heat sink removal of decay heat from the reactor coolant). Maintaining spent fuel integrity such that significant radioactive release does not occur as a result of overheating.	2	SWS supports the CCS defence in depth functions of decay heat removal and spent fuel cooling.
–	Service Water Cooling Tower	D	NNS	M/f Std				
SWS-MP-01A/B	Service Water Pumps	D	NNS	Hydraulic Institute Std				
–	Valves Providing SWS AP1000 Equipment Class D Function	D	NNS	ANSI B16.34				
Balance of system components are Class E					GNS	No nuclear safety implications.	GNS	SSCs are not designed or considered in the application of a safety function.
Turbine Building Closed Cooling Water System (TCS) Location: Turbine Building								
System components are Class E					GNS	No nuclear safety implications.	GNS	SSCs are not designed or considered in the application of a safety function.
Turbine Island Vents, Drains and Relief System (TDS) Location: Turbine Building								
–	Piping and components that provide the path from the GSS and CMS to atmosphere and rad monitor	D	NNS	ANSI B3 1.1	C	Monitoring of radioactivity released to the environment.	3	The CMS and the GSS discharge into the TDS. The exhaust from the TDS into the turbine island vent is continuously monitored for radiation.
Balance of system components are Class E					GNS	No nuclear safety implications.	GNS	SSCs are not designed or considered in the application of a safety function.
Radiologically Controlled Area Ventilation System (VAS) Location: Auxiliary Building and Annex Building								
–	CVS and RNS Pump Room Coolers	L/R (D)	NNS	M/f Std	C	Providing long-term support of Category A or B functions.	3	These components support normal operation of the RNS pumps and CVS make-up pumps by maintaining the pump rooms within their design temperature range. Unavailability of coolers would not lead to immediate loss of supported SSCs; time is available for remedial action to be taken.
VAS-MD-D700 VAS-MD-D705	Dampers for the HEPA filter pathway	C	I	ASME AG-1	A	Controlling the levels of radioactivity released to the environment.	1	Filtered exhaust for the VAS may be provided by the VFS during abnormal conditions.
–	Fire Dampers	D	NNS	UL-555	B	Protecting against internal/external hazards that could, as part of a sequence of failures, result in loss of one of the safety functions, for example preventing fire spread.	3	Fire dampers are provided to prevent fire spread outside of the designated fire areas.
VAS-MS-101	HEPA Filters	D	I	ANSI N509	A	Controlling the level of radioactivity released to the environment.	2	HEPA filtration is located on the VAS subsystem serving the fuel handling area to capture potential airborne particulates containing radioactivity.
–	Shutoff, Isolation, and Balancing Dampers	L	NNS	ANSI / AMCA500	B	Control of levels of radioactivity released to the environment.	3	The VAS provides HVAC to radiologically controlled areas and provides for the means of filtering and monitoring of environmental releases.
–	Air Handling Units	L	NNS	M/f Std				
–	Filters	L	NNS	UL 900				
–	Fans, Ductwork	L	NNS	SMACNA				
Balance of system components are Class L								

Table 15A-1. AP1000 UK Categorisation and Classification of Mechanical SSCs (cont.)

Tag Number	Description	AP1000 Class	Seismic Category	Principal Design Code	UK Safety Category	Safety Function(s) Provided by the SSC	UK Safety Class	Justification of the Safety Class
Nuclear Island Non-radioactive Ventilation System (VBS) Location: Auxiliary Building and Annex Building								
–	Battery Rooms Exhaust Fans	D	NNS	AMCA	B	Plant process control functions that maintain the main process variables within the limits assumed in the safety analysis.	2	Maintains the temperature in the electrical rooms and the main control room during normal operation. Maintains proper airflow in the battery rooms to prevent hydrogen building during battery charging.
–	PCS Room Heaters	D	NNS	M/f Std	C	Provide long-term support of Category A or B functions.	3	The PCS room heaters maintain proper conditions to facilitate the proper operation of the PCS makeup function after 72 hours.
–	Combination Fire/Smoke Dampers	D	NNS	UL-555	A	Protecting SSCs from internal/external hazards that could result in the loss of a principal means of fulfilling a Category A safety function.	2	Fire/smoke dampers are provided to prevent fire or smoke spread between areas of the plant that could impact a safety function.
–	Fire Dampers	E	NNS	UL-555	B	Protecting against internal/external hazards that could, as part of a sequence of failures, result in loss of one of the safety functions.	3	Fire dampers are provided to prevent fire spread outside of the designated fire areas.
–	Dampers Providing AP1000 Equipment Class D Function	D	NNS	ANSI / AMCA500	A	Maintaining habitability of the main control room and maintains design temperatures in the equipment rooms.	2	VBS provides a supplementary ventilation function to preserve habitability and SSC function. This has been determined to be important to safety.
–	Dampers in Lines Isolating Radioactive Contamination	R	NNS	ASME-509	C	Control of levels of radioactivity entering the plant from the environment.	3	Dampers are used to control the intake of radioactivity.
–	Shutoff, Isolation, and Balancing Dampers	L	NNS	ANSI / AMCA500	GNS	No nuclear safety implications.	GNS	SSCs are not designed or considered in the application of a safety function.
–	VBS Radiation Monitoring Package	C	I	M/f Std	A	Maintaining habitability of the main control room.	1	VBS contains two skid mounted MCR radiation monitoring packages consisting of radiation detectors, local radiation processors, and sampling components to continuously measure and record the radioactive materials in the MCR main supply air duct and actuate VBS supplemental air filtration and VES operation.
–	MCR/CSA Supplemental Air Filtration Units	D	NNS	ASME AG-1	A	Maintaining habitability of the main control room.	2	VBS provides a supplementary ventilation function to preserve habitability and SSC function of the CSA in support of the MCR.
–	MCR Isolation Valve	C	I	ASME III-3	A	Maintaining habitability of the main control room.	1	The isolation valves are the principal means of fulfilling the safety function.
–	Valves Providing VBS AP1000 Equipment Class D Function	D	NNS	ANSI 16.34	A	Maintaining habitability of the main control room and maintains design temperatures in the equipment rooms.	2	VBS provides a supplementary ventilation function to preserve habitability and SSC function. This has been determined to be important to safety.
–	Other Air Handling Units	D	NNS	M/f Std	A	Maintains design temperatures in the equipment rooms containing Class 1 electrical and C&I equipment.	2	VBS provides a ventilation function to support operation of Class 1 SSCs
–	Filters	D	NNS	UL 900				
–	Fans, Ductwork	D, L or R	NNS	SMACNA				
–	Ancillary Fan	D	Note 2	ANSI/ AMCA 210, 211, 300	B	Reduce the probability of requiring the use of offsite SSCs to maintain Category A safety functions after 72 hours following an accident.	2	MCR ancillary fans allow for post-72 hour ventilation of the MCR. This function has been determined to be important to safety. This component reduces the probability that offsite SSCs would be needed to support post 72 hour actions.
Balance of system components are Class L					GNS	No nuclear safety implications.	GNS	SSCs are not designed or considered in the application of a safety function.

Table 15A-1. AP1000 UK Categorisation and Classification of Mechanical SSCs (cont.)

Tag Number	Description	AP1000 Class	Seismic Category	Principal Design Code	UK Safety Category	Safety Function(s) Provided by the SSC	UK Safety Class	Justification of the Safety Class
Containment Recirculation Cooling System (VCS) Location: Containment								
VCS-MS-01A/B	Fan Coil Units	L	II	M/f Std	B	Function that provides a backup to a Category A safety function.	3	The fain coil units provide an alternative means to remove heat lost to containment from the primary systems.
–	Dampers	L	NNS	ANSI / AMCA500	GNS	No nuclear safety implications.	GNS	SSCs are not designed or considered in the application of a safety function.
–	Fans, Ductwork	L	NNS	SMACNA				
Balance of system components are Class L								
Main Control Room Emergency Habitability System (VES) Location: Auxiliary Building								
VES-MD-D001A	Relief Damper	Note 1	I	ASME 509/ 510	A	Maintaining habitability of the MCR.	1	Provides the primary means of maintaining positive pressure in the MCR during VES operation.
VES-MD-D001B	Relief Damper							
VES-MD-D002	Balancing Damper	NOTE 1	I	ASME N509/N510	A	Maintaining habitability of the MCR.	1	Provides the primary means of fulfilling the safety function.
VES-MD-D003	Balancing Damper	NOTE 1	I	ASME N509/N510	A	Maintaining habitability of the MCR.	1	Provides the primary means of fulfilling the safety function.
–	Emergency Air Storage Tanks 01-32	C	I	ASME VIII, Appendix 22	A	Maintaining habitability of the MCR.	1	Provides the primary means of supplying fresh breathable air to the control room during VES operation.
VES-MY-G001	Ducting Grill/ Supply/Exhaust Air Ducting Register	NOTE 1	I	ASME N509	A	Maintaining habitability of the MCR.	1	Provides the primary means of fulfilling the safety function.
VES-MY-R001 through -003	Ducting Register	NOTE 1	I	ASME N509	A	Maintaining habitability of the MCR.	1	Provides the primary means of fulfilling the safety function.
VES-MY-Y01	Air Amplifier Intake Line Silencer	NOTE 1	I	ASME AG-1 Section SA	A	Maintaining habitability of the MCR.	1	Provides the primary means of fulfilling the safety function.
VES-MY-Y02	Air Amplifier Discharge Line Silencer	NOTE 1	I	ASME AG-1 Section SA	A	Maintaining habitability of the MCR.	1	Provides the primary means of fulfilling the safety function.
VES-PL-V001	MCR Supply Line B Manual Isolation Valve	C	I	ASME III-3	A	Maintaining habitability of the MCR.	1	Provides the primary means of fulfilling the safety function.
VES-PL-V002A	Pressure Regulating Valve A	C	I	ASME III-3	A	Maintaining habitability of the MCR.	1	Provides the primary means of fulfilling the safety function.
VES-PL-V002B	Pressure Regulating Valve B	C	I	ASME III-3	A	Maintaining habitability of the MCR.	1	Provides the primary means of fulfilling the safety function.
VES-PL-V005A	Air Delivery Main Isolation Valve A	C	I	ASME III-3	A	Maintaining habitability of the MCR.	1	Provides the primary means of fulfilling the safety function.
VES-PL-V005B	Air Delivery Main Isolation Valve B	C	I	ASME III-3	A	Maintaining habitability of the MCR.	1	Provides the primary means of fulfilling the safety function.
VES-PL-V006A	Air Delivery Line Pressure Instrument Isolation Valve A	C	I	ASME III-3	A	Maintaining habitability of the MCR.	1	Provides the primary means of fulfilling the safety function.
VES-PL-V006B	Air Delivery Line Pressure Instrument Isolation Valve B	C	I	ASME III-3	A	Maintaining habitability of the MCR.	1	Provides the primary means of fulfilling the safety function.

Table 15A-1. AP1000 UK Categorisation and Classification of Mechanical SSCs (cont.)

Tag Number	Description	AP1000 Class	Seismic Category	Principal Design Code	UK Safety Category	Safety Function(s) Provided by the SSC	UK Safety Class	Justification of the Safety Class
Main Control Room Emergency Habitability System (VES) Location: Auxiliary Building (cont.)								
–	Air Delivery Line Maintenance Isolation Valves	C	I	ASME III-3	A	Maintaining habitability of the MCR.	1	Provides the primary means of fulfilling the safety function.
–	Temporary Instrument Isolation Valves	C	I	ASME III-3	A	Maintaining habitability of the MCR.	1	Provides the primary means of fulfilling the safety function.
VES-PL-V022A	Pressure Relief Isolation Valve A	C	I	ASME III-3	A	Maintaining habitability of the MCR.	1	Provides the primary means of fulfilling the safety function.
VES-PL-V022B	Pressure Relief Isolation Valve B	C	I	ASME III-3	A	Maintaining habitability of the MCR.	1	Provides the primary means of fulfilling the safety function.
–	Air Bank Isolation, Fill, & Vent Valves	C	I	ASME III-3	A	Maintaining habitability of the MCR.	1	These valves provide the principal means on isolating and refilling individual banks of the VES air storage tanks.
VES-PL-V040A VES-PL-V040B VES-PL-V040C VES-PL-V040D	Air Tank Safety Relief Valves	C	I	ASME III-3	A	Maintaining habitability of the MCR.	1	Provides the primary means of fulfilling the safety function.
VES-PL-V043A/B	Differential Pressure Instrument Line Isolation Valves	C	I	ASME III-3	A	Maintaining habitability of the MCR	1	Provides the primary means of fulfilling the safety function.
VES-PL-V044	MCR Supply Line A Manual Isolation Valve	C	I	ASME III-3	A	Maintaining habitability of the MCR	1	Provides the primary means of fulfilling the safety function.
VES-PL-V045	Eductor Main Air Flow path Isolation Valve	C	I	ASME III-3	A	Maintaining habitability of the MCR.	1	Provides the primary means of fulfilling the safety function.
VES-PL-V046	Eductor Bypass Flow Path Isolation Valve	C	I	ASME III-3	A	Maintaining habitability of the MCR.	1	Provides the primary means of fulfilling the safety function.
VES-MY-F01	MCR Air Filtration Line Charcoal Filter	Note 1	I	ASME AG-1	A	Maintaining habitability of the MCR.	1	Provides the primary means of fulfilling the safety function.
VES-MY-F02	MCR Air Filtration Line HEPA Filter	Note 1	I	ASME AG-1	A	Maintaining habitability of the MCR.	1	Provides the primary means of fulfilling the safety function.
VES-MY-F03	MCR Air Filtration Line High Efficiency Filter	Note 1	I	UL 900	A	Maintaining habitability of the MCR.	1	Provides the primary means of fulfilling the safety function.
VES-PY-N01	MCR Eductor/Air Amplifier	Note 1	I	ASME III-3	A	Maintaining habitability of the MCR.	1	Provides the primary means of fulfilling the safety function.
VES-PY-N02	Eductor Bypass Isolation Discharge Silencer	C	I	ASME III-3	A	Maintaining habitability of the MCR.	1	Provides the primary means of fulfilling the safety function.
VES-PY-R02	Eductor Bypass Flow Orifice	C	I	ASME III-3	A	Maintaining habitability of the MCR.	1	Provides the primary means of fulfilling the safety function.
Balance of Components are Class E					GNS	No nuclear safety implications.	GNS	SSCs are not designed or considered in the application of a safety function.

Table 15A-1. AP1000 UK Categorisation and Classification of Mechanical SSCs (cont.)

Tag Number	Description	AP1000 Class	Seismic Category	Principal Design Code	UK Safety Category	Safety Function(s) Provided by the SSC	UK Safety Class	Justification of the Safety Class
Containment Air Filtration System (VFS) Location: Auxiliary Building and Annex Building								
VFS-PY-C01	Containment Supply Duct Penetration	B	I	ASME III, MC	A	Prevention of the release of radioactive material from the containment.	1	Each containment penetration provides a principal means of maintaining containment integrity.
VFS-PY-C02	Containment Exhaust Duct Penetration	B	I	ASME III, MC				
VFS-MY-Y01	Containment Air Supply Debris Screen	C	I	ASME III-3	A	Prevention of the release of radioactive material from the containment. Control of levels of radioactivity released to the environment.	1	The debris screens are structurally designed to withstand the maximum pressure differential assuming that they are blocked with debris generated by a LOCA. This is the Class 1 function of the screens. The debris screens support a Class 2 function of controlling radioactive release.
VFS-MY-Y02	Containment Air Exhaust Debris Screen	C	I	ASME III-3				
VFS-PL-V003	Containment Purge Supply Containment Isolation Valve	B	I	ASME III-2	A	Prevention of the release of radioactive material from the containment.	1	The isolation valves are the principal means of fulfilling the safety function.
VFS-PL-V004	Containment Purge Supply Containment Isolation Valve	B	I	ASME III-2				
VFS-PL-V007	RCS Ejector Discharge Isolation	C	I	ASME III-3				
VFS-PL-V008	ILRT Vent Discharge Isolation	B	I	ASME III-2				
VFS-PL-V009	Containment Purge Discharge Containment Isolation Valve	B	I	ASME III-2				
VFS-PL-V010	Containment Purge Discharge Containment Isolation Valve	B	I	ASME III-2				
VFS-PL-V006 VFS-PL-V012 VFS-PL-V015	Containment Penetration Test Valves	C	I	ASME III-3				
VFS-PL-V101	Containment Air Supply Line Test Connection	C	I	ASME III-3	A	Prevention of the release of radioactive material from the containment.	1	The isolation valves are the principal means of fulfilling the safety function.
VFS-PL-V202	Containment Atmosphere to Filtration Units Isolation	C	I	ASME III-3	A	Prevention of the release of radioactive material from the containment.	1	The isolation valves are the principal means of fulfilling the safety function.
VFS-PL-V587	Filtration Units to Containment Atmosphere Manual Isolation	C	I	ASME III-3	A	Prevention of the release of radioactive material from the containment.	1	The isolation valves are the principal means of fulfilling the safety function.
VFS-PL-V800 A/B	Vacuum Relief Containment Isolation	B	I	ASME III-2	A	Prevention of the release of radioactive material from the containment. Provides containment vacuum relief.	1	The isolation valves are the principal means of fulfilling the safety function.
VFS-PLV803 A/B	Vacuum Relief Containment Isolation Check Valve	B	I	ASME III-2	A	Prevention of the release of radioactive material from the containment.	1	The isolation valves are the principal means of fulfilling the safety function.
–	Valves Providing VFS AP1000 Equipment Class D Function	D	NNS	ANSI 16.34	C	Control of levels of radioactivity released to the environment. Monitoring of radioactivity released to the environment.	3	VFS provides the means to release and monitor gaseous effluent.
–	Dampers in Lines Isolating Radioactive Contamination	R	NNS	ASME-509	C	Control of levels of radioactivity released to the environment.	3	Dampers are used to control the release of radioactivity.
–	Shutoff, Isolation, and Balancing Dampers	L	NNS	ANSI / AMCA500	GNS	No nuclear safety implications.	GNS	SSCs are not designed or considered in the application of a safety function.

Table 15A-1. AP1000 UK Categorisation and Classification of Mechanical SSCs (cont.)

Tag Number	Description	AP1000 Class	Seismic Category	Principal Design Code	UK Safety Category	Safety Function(s) Provided by the SSC	UK Safety Class	Justification of the Safety Class
Containment Air Filtration System (VFS) Location: Auxiliary Building and Annex Building (cont.)								
–	Fire Dampers	E	NNS	UL-555	B	Protecting against internal/external hazards that could, as part of a sequence of failures, result in loss of one of the safety functions, for example preventing fire spread.	3	Fire dampers are provided to prevent fire spread outside of the designated fire areas.
–	Supply Air Handling Units	L	NNS	M/f Std	GNS	No nuclear safety implications.	GNS	SSCs are not designed or considered in the application of a safety function.
	HEPA Filters	R	NNS	ASME AG-1	B	Controlling the level of radioactivity released to the environment.	3	HEPA filtration captures potential airborne particulate containing radioactivity.
–	Air Exhaust Filtration Units (other than HEPA filters)	R	NNS	ASME AG-1	C	Control of levels of radioactivity released to the environment. Monitoring of radioactivity released to the environment	3	VFS provides the means to release and monitor gaseous effluent.
–	Fans, Ductwork	L or R	NNS	SMACNA or ASME AG-1	GNS	No nuclear safety implications.	GNS	SSCs are not designed or considered in the application of a safety function.
Balance of system components are Class L and Class R								
Health Physics and Hot Machine Shop HVAC System (VHS) Location: Annex Building								
–	Annex Bldg Exhaust Radiation Package	E	NNS	M/f Std	C	Monitoring the level of radioactivity released into the environment.	3	The system exhaust is provided with a radiation monitor to record and alarm release of radioactive effluent.
–	Shutoff, Isolation, and Balancing Dampers	L	NNS	ANSI / AMCA500	GNS	No nuclear safety implications.	GNS	SSCs are not designed or considered in the application of a safety function.
–	Fire Dampers	E	NNS	UL-555	B	Protecting against internal/external hazards that could, as part of a sequence of failures, result in loss of one of the safety functions, for example preventing fire spread.	3	Fire dampers are provided to prevent fire spread outside of the designated fire areas in the annex building.
–	HEPA Filters	R	NNS	ANSI N509	B	Controlling the level of radioactivity released to the environment.	3	HEPA filtration is provided in or at the individual machine tools.
–	Air Handling Units w/ Filters	L	NNS	M/f Std	GNS	No nuclear safety implications.	GNS	SSCs are not designed or considered in the application of a safety function.
–	Fans, Ductwork	L	NNS	SMACNA				
Balance of system components are Class E or Class L								
Containment Hydrogen Control System (VLS) Location: Containment								
–	Hydrogen Igniters	D	NNS	M/f Std	B	Functions provided to reach and maintain safe state for beyond DBAs as specified in the station operating procedures.	2	Hydrogen igniters are identified as important to safety per the ANSI process and are the principal means of beyond design basis hydrogen mitigation.
VLS-MY-E01A	Catalytic Hydrogen Recombiner A	D	NNS	M/f Std	B	Plant process control function that maintains process variables within safety analysis limits.	3	Hydrogen recombiners are provided for hydrogen mitigation during DBAs. The principal means of hydrogen mitigation is the design of the containment and the amount of free volume. The recombiners are provided for additional level of defence against hydrogen accumulation.
VLS-MY-E01B	Catalytic Hydrogen Recombiner B	D	NNS	M/f Std				
Balance of system components are Class E or Class L					GNS	No nuclear safety implications.	GNS	SSCs are not designed or considered in the application of a safety function.

Table 15A-1. AP1000 UK Categorisation and Classification of Mechanical SSCs (cont.)

Tag Number	Description	AP1000 Class	Seismic Category	Principal Design Code	UK Safety Category	Safety Function(s) Provided by the SSC	UK Safety Class	Justification of the Safety Class
Radwaste Building HVAC System (VRS) Location: Radwaste Building								
–	HEPA Filters	R	NNS	ANSI N509	B	Controlling the level of radioactivity released to the environment.	3	HEPA filtration is located on the VRS discharge line to capture potential airborne particulate containing radioactivity.
–	Radwaste Bldg Exhaust Radiation Package	E	NNS	M/f Std	C	Monitoring the level of radioactivity released into the environment.	3	The system exhaust is provided with a radiation monitor to record and alarm release of radioactive effluent.
–	Shutoff, Isolation, and Balancing Dampers	L	NNS	ANSI / AMCA500	GNS	No nuclear safety implications.	GNS	SSCs are not designed or considered in the application of a safety function.
–	Fire Damper	E	NNS	UL-555	B	Protecting against internal/external hazards that could, as part of a sequence of failures, result in loss of one of the safety functions, for example preventing fire spread.	3	Fire dampers are provided to prevent fire spread outside of the designated fire areas in the radwaste building.
–	Air Handling Units	L	NNS	M/f Std	GNS	No nuclear safety implications.	GNS	SSCs are not designed or considered in the application of a safety function.
–	Filters	L	NNS	UL 900				
–	Fans, Ductwork	L	NNS	SMACNA				
Balance of system components are Class E or Class L								
Turbine Building Ventilation System (VTS) Location: Turbine Building								
–	Shutoff, Isolation, and Balancing Dampers	L	NNS	ANSI / AMCA500	GNS	No nuclear safety implications.	GNS	SSCs are not designed or considered in the application of a safety function.
–	Fire Dampers	D	NNS	UL-555	B	Protecting against internal/external hazards that could, as part of a sequence of failures, result in loss of one of the safety functions, for example preventing fire spread.	3	Fire dampers are provided to prevent fire spread outside of the designated fire areas in the turbine building.
–	Air Handling Units w/ Filters	L	NNS	M/f Std, UL-900	GNS	No nuclear safety implications.	GNS	SSCs are not designed or considered in the application of a safety function.
–	Fans, Ductwork	L	NNS	SMACNA				
Balance of system components are Class L					GNS	No nuclear safety implications.	GNS	SSCs are not designed or considered in the application of a safety function.
Containment Leak Rate Test System (VUS) Location: Auxiliary Building								
VUS-PL-V015	Main Equipment Hatch Test Connection	B	I	ASME III-2	A	Prevention of the release of radioactive material from the containment.	1	The identified valves and hatches form part of the primary containment boundary.
VUS-PL-V016	Maintenance Equipment Hatch Test Connection	B	I	ASME III-2				
–	Personnel Hatch Test Connections	B	I	ASME III-2				
VUS-PL-V023	Fuel Transfer Tube Test Connection	B	I	ASME III-2				
–	Electrical Penetration Test Isolation Valves	B	I	ASME III-2				
–	Spare Penetration Test Connection	B	I	ASME III-2				
Balance of system components are Class E					GNS	No nuclear safety implications.	GNS	SSCs are not designed or considered in the application of a safety function.

Table 15A-1. AP1000 UK Categorisation and Classification of Mechanical SSCs (cont.)

Tag Number	Description	AP1000 Class	Seismic Category	Principal Design Code	UK Safety Category	Safety Function(s) Provided by the SSC	UK Safety Class	Justification of the Safety Class
Central Chilled Water System (VWS) Location: Various								
VWS-MS02 and -MS03	Air Cooled Chiller MS02 and MS03	D	NNS	M/f Std	C	Provide long-term support of a Category A or B function.	3	The VWS provides a source of chilled water to the VBS supply air handling units that are used to maintain the MCR and Class 1 electrical room passive heat sink temperatures within their normal design temperature range. The VWS provides chilled water to the VAS pump room unit coolers which support operation of the RNS and CVS pumps.
VWS-MP02 and –MP03	Pumps	D	NNS	M/f Std				
VWS-MT-04	Tanks	D	NNS	ASME VIII				
VWS-MT-05	Air Cooled Chiller Chemical Add Tank	D	NNS	ASME VIII				
–	Valves Providing VWS AP1000 Equipment Class D Function	D	NNS	ANSI 16.34				
VWS-PY-C01	Containment Chilled Water Supply Penetration	B	I	ASME III, MC	A	Prevention of the release of radioactive material from the containment.	1	Each containment penetration provides a principal means of maintaining containment integrity.
VWS-PY-C02	Containment Chilled Water Return Penetration	B	I	ASME III, MC				
VWS-PL-V053	Containment Penetration Thermal Relief Valve	C	I	ASME III-3	A	Prevention of the release of radioactive material from the containment.	1	The isolation valves are the principal means of fulfilling the safety function.
VWS-PL-V057	Containment Penetration Thermal Relief Valve	C	I	ASME III-3				
VWS-PL-V058	Fan Coolers Supply Containment Isolation	B	I	ASME III-2				
VWS-PL-V062	Fan Coolers Supply Containment Isolation	B	I	ASME III-2				
VWS-PL-V080	VWS Containment Isolation Relief Valve	B	I	ASME III-2				
VWS-PL-V082	Fan Coolers Return Containment Isolation	B	I	ASME III-2				
VWS-PL-V086	Fan Coolers Return Containment Isolation	B	I	ASME III-2				
VWS-PL-V424	Containment Penetration Test Connection	B	I	ASME III-2				
VWS-PL-V425	Containment Penetration Test Connection	B	I	ASME III-2				
Balance of system components are Class E					GNS	No nuclear safety implications.	GNS	SSCs are not designed or considered in the application of a safety function.

Table 15A-1. AP1000 UK Categorisation and Classification of Mechanical SSCs (cont.)

Tag Number	Description	AP1000 Class	Seismic Category	Principal Design Code	UK Safety Category	Safety Function(s) Provided by the SSC	UK Safety Class	Justification of the Safety Class
Annex/Auxiliary Building Nonradioactive Ventilation System (VXS) Location: Auxiliary Building and Annex Building								
–	Air Handling Unit Fans Providing AP1000 Equipment Class D Function	D	NNS	AMCA	C	Provide long-term support of Category A or B functions.	3	These components support operation of ZOS by maintaining the diesel bus switchgear rooms and battery charger rooms (containing dc switchgear) within their design temperature range.
–	Dampers Providing VXS AP1000 Equipment Class D Function	D	NNS	ANSI / AMCA500				
–	Exhaust Fan Providing Ancillary Diesel Room Ventilation	D	NNS	AMCA	C	Provide long-term support of Category A or B functions.	3	These components support operation of ZOS by maintaining the diesel bus switchgear rooms and battery charger rooms (containing dc switchgear) within their design temperature range.
–	Fire Dampers	D	NNS	UL-555 or UL-555S	B	Protecting against internal/external hazards that could, as part of a sequence of failures, result in loss of one of the safety functions, for example preventing fire spread.	3	Fire dampers are provided to prevent fire spread outside of the designated fire areas in the diesel generator building, which contains equipment supporting Class 2 safety functions.
–	Air Handling Units	L	NNS	M/f Std	GNS	No nuclear safety implications.	GNS	SSCs are not designed or considered in the application of a safety function.
–	Filters	L	NNS	UL 900				
–	Fans, Ductwork	L	NNS	SMACNA				
Balance of system components are Class E or Class L								
Hot Water Heating System (VYS) Location: Various								
System components are Class E					GNS	No nuclear safety implications.	GNS	SSCs are not designed or considered in the application of a safety function.
Diesel Generator Building Heating and Ventilation System (VZS) Location: Diesel Generator Building								
–	Unit Heaters Providing AP1000 Equipment Class D Function	D	NNS	UL-1025; NFPA 70	C	Provide long-term support of Category A or B functions.	3	The equipment maintains ambient temperature within the diesel generator rooms and the electrical equipment service modules to ensure equipment operation and reliability during periods of diesel generator operation.
–	Fans Providing AP 1000 Equipment Class D Function	D	NNS	AMCA				
–	Dampers Providing VZS AP1000 Equipment Class D Function	D	NNS	AMCA				
–	Fire Dampers	D	NNS	UL-555	B	Protecting against internal/external hazards that could, as part of a sequence of failures, result in loss of one of the safety functions, for example preventing fire spread.	3	Fire dampers are provided to prevent fire spread outside of the designated fire areas in the diesel generator building, which contains equipment supporting Class 2 safety functions.
–	Air Handling Units	L	NNS	M/f Std	GNS	No nuclear safety implications.	GNS	SSCs are not designed or considered in the application of a safety function.
–	Filters	L	NNS	UL 900				
–	Fans, Ductwork	L	NNS	SMACNA				
Balance of system components are Class E								

Table 15A-1. AP1000 UK Categorisation and Classification of Mechanical SSCs (cont.)

Tag Number	Description	AP1000 Class	Seismic Category	Principal Design Code	UK Safety Category	Safety Function(s) Provided by the SSC	UK Safety Class	Justification of the Safety Class
Gaseous Radwaste System (WGS) Location: Auxiliary Building								
–	Gas Cooler	D	NNS	ASME VIII/ TEMA	B	Prevention of the release of radioactive waste material from onsite storage facilities.	2	This is a radioactive waste processing system which is considered a plant storage/treatment facility. This system is designed to prevent the release of radiation.
–	Sample Pumps	D	NNS	M/f Std				
–	Guard and Delay Beds	D	NNS	ASME VIII				
–	Moisture Separator	D	NNS	ASME VIII				
–	Valves Providing WGS AP1000 Equipment Class D Function	D	NNS	ANSI 16.34				
Liquid Radwaste System (WLS) Location: Containment, Auxiliary, and Radwaste Buildings								
–	Heat Exchangers, WLS and CCS Side	D	NNS	ASME VIII/ TEMA	B	Prevention of the release of radioactive waste material from onsite storage facilities.	2	This is a radioactive waste processing system which is considered a plant storage/treatment facility. This system is designed to prevent the release of radiation.
–	Pumps	D	NNS	M/f Std				
–	Tanks	D	NNS	ASME III without Code Stamp				
–	Degasifier	D	NNS	ASME VIII				
–	Ion Exchangers	D	NNS	ASME VIII				
–	Filters	D	NNS	ASME VIII				
–	Pulse Dampers	D	NNS	M/f Std				
–	Leak Chase Collection Pots	D	NNS	ASME VIII				
–	Vapour Condenser	D	NNS	ASME VIII TEMA-C	B	Prevention of the release of radioactive waste material from onsite storage facilities.	2	This is a radioactive waste processing system which is considered a plant storage/treatment facility. This system is designed to prevent the release of radiation.
–	Valves Providing WLS AP1000 Equipment Class D Function (local drain valves in Radwaste Building)	D	NNS	ANSI 16.34				
WLS-PL-V055	Sump Discharge Containment Isolation IRC	B	I	ASME III-2	A	Prevention of the release of radioactive material from the containment.	1	The isolation valves are the principal means of fulfilling the safety function.
WLS-PL-V057	Sump Discharge Containment Isolation ORC	B	I	ASME III-2				
WLS-PL-V058	WLS Containment Isolation Relief Valve	B	I	ASME III-2				
WLS-PL-V067	RCDT Gas Outlet Containment Isolation IRC	B	I	ASME III-2				
WLS-PL-V068	RCDT Gas Outlet Containment Isolation ORC	B	I	ASME III-2				

Table 15A-1. AP1000 UK Categorisation and Classification of Mechanical SSCs (cont.)

Tag Number	Description	AP1000 Class	Seismic Category	Principal Design Code	UK Safety Category	Safety Function(s) Provided by the SSC	UK Safety Class	Justification of the Safety Class
Liquid Radwaste System (WLS) Location: Containment, Auxiliary, and Radwaste Buildings (cont.)								
WLS-PL-V071A	CVS Compartment to Sump	C	I	ASME III-3	A	Protecting SSCs from internal/external hazards that would directly and inevitably result in the loss of a principal means of fulfilling a Category A safety function.	1	During a DBA, it is necessary to prevent premature flooding of the PXS compartment and the CVS compartment. The drain line from each of these compartments to the sump has two check valves in series. These check valves prevent reverse flow through the drain lines which could cause premature cross flooding.
WLS-PL-V071B	PXS A Compartment to Sump	C	I	ASME III-3				
WLS-PL-V071C	PXS B Compartment to Sump	C	I	ASME III-3				
WLS-PL-V072A	CVS Compartment to Sump	C	I	ASME III-3				
WLS-PL-V072B	PXS A Compartment to Sump	C	I	ASME III-3				
WLS-PL-V072C	PXS B Compartment to Sump	C	I	ASME III-3				
–	PXS & CVS Compartment Drains	C	I	M/f Std				
WLS-MY-Y34	Containment Sump Stilling Well	D	I	M/f Std	B	Functions that continuously monitor the availability of Category A safety functions for proper operation or to alert control room staff of their failures.	2	Supports monitoring a Category A safety function; the sump instruments are the primary means for monitoring the Category A safety function. Although they are classified as Safety Class 2 based on their function, these components are designed Seismic Category I because they ensure sump level sensors (which detect leakage) remain functional when subjected to safe shutdown earthquake.
WLS-MY-Y35	Containment Sump Stilling Well	D	I	M/f Std				
WLS-MY-Y36	Containment Sump Stilling Well	D	I	M/f Std				
WLS-PY-C02	Reactor Coolant Drain Tank WLS Connection Penetration	B	I	ASME III, MC	A	Prevention of the release of radioactive material from the containment.	1	Each containment penetration provides a principal means of maintaining containment integrity.
WLS-PY-C03	Containment Sump Pumps Combined Discharge Penetration	B	I	ASME III, MC				
Balance of system components are Class E					GNS	No nuclear safety implications.	GNS	SSCs are not designed or considered in the application of a safety function.
Radioactive Waste Drain System (WRS) Location: Auxiliary Building								
–	Pumps	D	NNS	M/f Std	B	Prevention of the release of radioactive waste material from onsite storage facilities.	2	This is a radioactive waste processing system which is considered a plant storage/treatment facility. This system is designed to prevent the release of radiation.
–	Drains	D	NNS	M/f Std				
–	Leak Chase Collection Pots	D	NNS	ASME VIII				
–	Pulse Dampers	D	NNS	M/f Std				
–	Valves Providing WRS AP1000 Equipment Class D Function	D	NNS	ANSI 16.34				
Balance of system components are Class E					GNS	No nuclear safety implications.	GNS	SSCs are not designed or considered in the application of a safety function.
Solid Radwaste System (WSS) Location: Auxiliary Building								
–	Pumps	D	NNS	M/f Std	B	Prevention of the release of radioactive waste material from onsite storage facilities.	2	This is a radioactive waste processing system which is considered a plant storage/treatment facility. This system is designed to prevent the release of radiation.
–	Tanks	D	NNS	ASME VIII				
WSS-MV-03	Resin Fines Filter	D	NNS	ASME VIII				
–	Valves Providing WSS AP1000 Equipment Class D Function	D	NNS	ANSI B16.34				
Balance of system components are Class E					GNS	No nuclear safety implications.	GNS	SSCs are not designed or considered in the application of a safety function.

Table 15A-1. AP1000 UK Categorisation and Classification of Mechanical SSCs (cont.)

Tag Number	Description	AP1000 Class	Seismic Category	Principal Design Code	UK Safety Category	Safety Function(s) Provided by the SSC	UK Safety Class	Justification of the Safety Class
Waste Water System (WWS) Location: Various								
WWS-PL-V506	MCR WWS Isolation Valve	C	I	ASME III-3	A	Maintaining habitability of the MCR.	1	The isolation valves are the principal means of isolating the MCR envelope during VES operation.
System components are Class E					GNS	No nuclear safety implications.	GNS	SSCs are not designed or considered in the application of a safety function.
Onsite Standby Power System (ZOS) Location: Diesel Generator Building								
ZOS-MS-05A/B	Diesel Generator Engines	D	NNS	M/f Std	A	Removal of decay heat from the reactor coolant during normal operation and accident conditions (including providing a heat sink for those systems involved in the removal of heat from the reactor coolant during normal operation and accident conditions).	2	The onsite diesel generators have been identified as important to safety. These SSCs provide standby power for supplementary decay heat removal functions. This does not represent the principal means of decay heat removal.
–	Diesel Generator Starting Units	D	NNS	M/f Std				
–	Diesel Generator Radiators	D	NNS	CAGI				
–	Diesel Generator Silencers	D	NNS	API 661	GNS	No nuclear safety implications.	GNS	The silencers do not support the Class 2 function of the standby diesels as they are designed for occupational noise abatement. This class assumes no credible failure mode can result in exhaust path restrictions that affect diesel operation.
–	Valves Providing ZOS Diesel Generator Engines AP 1000 Equipment Class D Function	D	NNS	ANSI 16.34	A	Removal of decay heat from the reactor coolant during normal operation and accident conditions (including providing a heat sink for those systems involved in the removal of heat from the reactor coolant during normal operation and accident conditions).	2	The onsite diesel generators have been identified as important to safety. These SSCs provide standby power for supplementary decay heat removal functions. This does not represent the principal means of decay heat removal.
Balance of system components are Class E					GNS	No nuclear safety implications.	GNS	SSCs are not designed or considered in the application of a safety function.

Notes:

1. Component performs a safety-related function equivalent to **AP1000** equipment Class C. The component is constructed using the standards for Class R and a quality assurance program in conformance with 10 CFR Part 50 Appendix B.
2. The equipment is generally of rugged construction and the seismic design requirements are limited to the anchorage of the equipment and layout review to preclude failure due to seismic interactions.

Table 15A-2. AP1000 UK Categorisation and Classification of Electrical SSCs

Tag Number	Description	AP1000 Class	Seismic Category	Principal Design Code	UK Safety Category of the Function Provided by the SSC	Safety Function(s) Provided by the SSC	UK Safety Class of the SSC	Justification of the Safety Class
Main AC Power System (ECS) Location: Various								
–	RCS switchgear	C	I	ANSI/NEMA/UL/ NEC IEEE 323, 344, 382 10 CFR 21	A	Prevention of the release of radioactive material through the boundary of the RCS. Control of core reactivity during normal operation and accident conditions.	1	Principal means of reactor shutdown and core reactivity control.
–	Bus ES-1 and ES-2	D	II	ANSI/NEMA/UL/ NEC IEEE242, 317,336	A	Removal of decay heat from the reactor coolant during normal operation and accident conditions (including providing a heat sink for those systems involved in the removal of heat from the reactor coolant during normal operation and accident conditions).	2	Buses support power delivery associated with the ZOS. This is considered a function important to safety.
–	Ancillary Diesel Generators	D	Note 2		B	Reduce the probability of requiring the use of offsite SSCs to maintain Category A safety functions after 72 hours following an accident. Prevention of the release of radioactive material from the containment.	2	Ancillary diesels provide for alternate power generation for post-72 hour operation and supplement the function of containment heat removal. This component reduces the probability that offsite SSCs would be needed to support post 72 hour actions.
–	Equipment associated with connection to ZBS	E	NNS		C	Power for normal operations to support removing nuclear heat from the reactor is provided via the ECS.	3	ECS is the principal means of providing plant power during normal operations.
Balance of system components are Class E					GNS	No nuclear safety implications.	GNS	SSCs are not designed or considered in the application of a safety function.
Class 2 DC and Uninterruptible Power Supply System (EDS) Location: Various								
–	EDS Equipment supporting AP1000 Class D Function	D	NNS	ANSI/NEMA/UL/ NEC IEEE141, 242, 336,450, 484, 485, 944, 946	B	Removal of decay heat from the reactor coolant during normal operation and accident conditions (including providing a heat sink for those systems involved in the removal of heat from the reactor coolant during normal operation and accident conditions).	2	Supports control power and monitoring instrumentation, as well as hydrogen igniters which are only required in a beyond DBA, providing diverse means of hydrogen dispersion to catalytic converters.
-	EDS Battery Monitors	E	NNS	IEEE 1491	C	Functions to monitor the availability of the batteries.	3	Principal means to fulfil the safety function.
Communication Systems (EFS) Location: Various								
System components are Class E					GNS	No nuclear safety implications.	GNS	SSCs are not designed or considered in the application of a safety function.
Grounding and Lightning Protection System (EGS) Location: Various								
System components are Class E					C	EGS provides hazard protection of plant SSCs required for removal of nuclear heat during operations.	3	EGS is the principal means of providing earthing and lightning protection.
Special Process Heat Tracing System (EHS) Location: Various								
System components are Class E					GNS	No nuclear safety implications.	GNS	SSCs are not designed or considered in the application of a safety function.

Table 15A-2. AP1000 UK Categorisation and Classification of Electrical SSCs (cont.)

Tag Number	Description	AP1000 Class	Seismic Category	Principal Design Code	UK Safety Category of the Function Provided by the SSC	Safety Function(s) Provided by the SSC	UK Safety Class of the SSC	Justification of the Safety Class
Plant Lighting System (ELS) Location: Various								
–	Emergency Lighting, MCR and Remote Shutdown Workstation	D	II	Industry Standard	A	Maintaining habitability of the MCR.	2	Provides control room lighting in the event of loss of normal power.
-	Fuel Handling Area Emergency Lighting	D	II	Industry Standard	A	Allow placement of fuel in a safe location	2	Enables recovery actions.
Balance of system components are Class E					GNS	No nuclear safety implications.	GNS	SSCs are not designed or considered in the application of a safety function.
Cathodic Protection System (EQS) Location: Various								
System components are Class E					GNS	No nuclear safety implications.	GNS	SSCs are not designed or considered in the application of a safety function.
Class 1E DC and UPS System (IDS) Location: Various								
–	Batteries, Chargers, UPS	C	I	IEEE 323, 344, 382	A	Removal of decay heat from the reactor coolant during normal operation and accident conditions (including providing a heat sink for those systems involved in the removal of heat from the reactor coolant during normal operation and accident conditions). Prevention of the release of radioactive material from the containment. Prevention of the release of radioactive material through the boundary of the RCS. Control of core reactivity during normal operation and accident conditions. Maintaining habitability of the MCR. C&I systems required to automatically actuate or provide manual actuation (where this is the only means of actuation) for SSCs delivering other Category A functions.	1	Provides the principal means of fulfilling the safety function. Segregation of four systems. Redundant bank of batteries and associated monitoring.
–	Battery Monitoring System	E	II	ANSI/NEMA/UL/ NEC	C	Functions to monitor the availability of the Class 1 batteries.	3	Provides the principal means of fulfilling this safety function.
Balance of system components are Class E					GNS	No nuclear safety implications.	GNS	SSCs are not designed or considered in the application of a safety function.
Plant Security System (SES) Location: Various								
–	Access control system	E	NNS	Industry Standard	C	Functions that provide access control to the nuclear power plant.	3	Provides the principal means of fulfilling the safety function.
System components are Class E					GNS	No nuclear safety implications.	GNS	SSCs are not designed or considered in the application of a safety function.

Table 15A-2. AP1000 UK Categorisation and Classification of Electrical SSCs (cont.)

Tag Number	Description	AP1000 Class	Seismic Category	Principal Design Code	UK Safety Category of the Function Provided by the SSC	Safety Function(s) Provided by the SSC	UK Safety Class of the SSC	Justification of the Safety Class
Closed Circuit TV System (Nuclear Operations) (TVS) Location: Various								
System components are Class E					GNS	No nuclear safety implications.	GNS	SSCs are not designed or considered in the application of a safety function.
Main Generation System (ZAS) Location: Turbine Building								
System components are Class E					GNS	No nuclear safety implications.	GNS	SSCs are not designed or considered in the application of a safety function.
Transmission Switchyard and Offsite Power System (ZBS) Location: Yard								
System components are Class E					GNS	No nuclear safety implications.	GNS	SSCs are not designed or considered in the application of a safety function.
Onsite Standby Power System (ZOS) Location: Yard								
–	Class D Function of the ZOS	D	NS	ANSI/NEMA/UL/ NEC IEEE242, 317,336	A	Removal of decay heat from the reactor coolant during normal operation and accident conditions (including providing a heat sink for those systems involved in the removal of heat from the reactor coolant during normal operation and accident conditions).	2	Diesels only required in the event of loss of grid connections, and only in the event of an accident requiring use of the containment cooling system. 72 hour grace time, following loss of AC supplies, before diesels are required. This gives time to restore grid connection or connect portable, engine-driven generators to the safety-related connection.
Excitation and Voltage Regulation System (ZVS) Location: Turbine Building								
System components are Class E					GNS	No nuclear safety implications.	GNS	SSCs are not designed or considered in the application of a safety function.

Notes:

1. The principal design codes and standard provided in this table are associated with the AP1000 standard plant design. As deemed appropriate, corresponding IEC standards will be supplemented in place of the listed design standard.

2. The equipment is generally of rugged construction and the seismic design requirements are limited to the anchorage of the equipment and layout review to preclude failure due to seismic interactions.

Table 15A-3. AP1000 UK Categorisation and Classification of C&I SSCs

System Function or Equipment	Applicable IEC Standards	UK Safety Category of the Function Provided by the SSC	Safety Function(s) Provided by the SSC	UK Safety Class of the SSC	Justification of the Safety Class
Protection and Safety Monitoring System (PMS)					
Reactor Trip Functions	60880 61513 61226 60987	A	PMS initiates functions required to reach the nonhazardous stable state, to prevent a DBA from leading to unacceptable consequences or to mitigate its consequences. Initiates reactor trip when plant conditions reach specified limits.	1	PMS is the primary C&I system to initiate a reactor trip.
Engineered Safety Features	60880 61513 61226 60987	A	PMS initiates functions required to reach the nonhazardous stable state, to prevent a DBA from leading to unacceptable consequences or to mitigate its consequences. Actuates engineered safety features to limit the consequences of DBAs.	1	PMS is the primary C&I system to initiate engineered safety functions such as containment isolation, decay heat removal, and safety injection.
Diverse Actuation System (DAS)					
Reactor Trip Functions	61513 61508 61226	A	DAS initiates functions required to reach the nonhazardous stable state, to prevent a DBA from leading to unacceptable consequences or to mitigate its consequences. Initiates reactor trip when plant conditions reach specified limits.	2	DAS is the diverse C&I system to initiate a reactor trip.
Engineered Safety Features	61513 61508 61226	A	DAS initiates functions required to reach the nonhazardous stable state, to prevent a DBA from leading to unacceptable consequences or to mitigate its consequences. Actuates engineered safety features to limit the consequences of DBAs.	2	DAS is the diverse C&I system to initiate engineered safety functions such as containment isolation, decay heat removal, and safety injection.
Plant Control System (PLS)					
Reactor Power Control	61513 62138 61226 60987	B	Plant process control functions that maintain the main process variables within the limits assumed in the safety analysis. Failure of this function could lead directly to the actuation or operation of a Category A safety function. Functions that considerably reduce the frequency of an initiating event as identified by the DBA analysis.	2	PLS monitors the neutron flux and reactor core outlet temperatures and automatically controls the reactivity to maintain a proper magnitude and distribution of fission energy production during startup and power production.

Table 15A-3. AP1000 UK Categorisation and Classification of C&I SSCs (cont.)

System Function or Equipment	Applicable IEC Standards	UK Safety Category of the Function Provided by the SSC	Safety Function(s) Provided by the SSC	UK Safety Class of the SSC	Justification of the Safety Class
Plant Control System (PLS) (cont.)					
Rod Control	61513 62138 61226 60987	B	Plant process control functions that maintain the main process variables within the limits assumed in the safety analysis. Failure of this function could lead directly to the actuation or operation of a Category A safety function. Functions that considerably reduce the frequency of an initiating event as identified by the DBA analysis.	2	The PLS controls movement of the control rods during plant startup and power production.
Pressuriser Pressure and Level Control	61513 62138 61226 60987	B	Plant process control functions that maintain the main process variables within the limits assumed in the safety analysis. Failure of this function could lead directly to the actuation or operation of a Category A safety function. Functions that considerably reduce the frequency of an initiating event as identified by the DBA analysis.	2	PLS monitors and controls RCS pressure to maintain the pressure within the design limits and provides for the proper system pressure during power production. PLS maintains pressuriser level during heatup and cooldown and in the event of a minor RCS leakage to maintain reactor coolant inventory.
Steam Generator Water Level Control	61513 62138 61226 60987	B	Plant process control functions that maintain the main process variables within the limits assumed in the safety analysis. Failure of this function could lead directly to the actuation or operation of a Category A safety function. Functions that considerably reduce the frequency of an initiating event as identified by the DBA analysis.	2	PLS monitors and controls the steam generation process to maintain an adequate water level inside the steam generators during power production. PLS controls steam generator level to maintain heat removal from the RCS.
Steam Dump Control	61513 62138 61226 60987	B	Plant process control functions that maintain the main process variables within the limits assumed in the safety analysis. Failure of this function could lead directly to the actuation or operation of a Category A safety function. Functions that considerably reduce the frequency of an initiating event as identified by the DBA analysis.	2	PLS controls the steam dump valves to provide a rapid steam generator load demand upon loss of electrical load transients to match reactor power with steam demand during power production. PLS controls the steam dump valves to dissipate residual heat and core decay heat during reactor shutdown.
Rapid Power Reduction	61513 62138 61226 60987	B	Plant process control functions that maintain the main process variables within the limits assumed in the safety analysis. Failure of this function could lead directly to the actuation or operation of a Category A safety function. Functions that considerably reduce the frequency of an initiating event as identified by the DBA analysis.	2	PLS initiates a rapid insertion of negative reactivity upon loss of electrical load transient to match reactor power with steam demand during power production.

Table 15A-3. AP1000 UK Categorisation and Classification of C&I SSCs (cont.)

System Function or Equipment	Applicable IEC Standards	UK Safety Category of the Function Provided by the SSC	Safety Function(s) Provided by the SSC	UK Safety Class of the SSC	Justification of the Safety Class
Plant Control System (PLS) (cont.)					
Rod Position Indication	61513 62138 61226 60987	C	Function that provide continuous monitoring of Category B function (Rod Control) to indicate the continued availability for operation and alert control room staff.	3	PLS monitors rod position to provide interlocking and operator alert functions during startup and power production.
Balance of Plant Controls	61513 62138 61226 60987	C	The balance of the PLS provides monitoring and control functions that are important to plant startup, power production, and shutdown.	3	The balance of the PLS provides monitoring and control functions that are important to plant startup, power production, and shutdown.
Operation and Control Centre System (OCS)					
Hardware required for Manual Reactor Trip and Manual Engineered Safety Features for PMS Reactor Trip and ESF Displays for PMS	60880 61513 61226 60987	A	Required to provide information and control capabilities that allow specified manual actions necessary to reach the nonhazardous stable state.	1	The OCS provides the primary hardware used to manually initiate and monitor Class 1 SSCs.
Hardware required for Manual Reactor Trip and Manual Engineered Safety Features for DAS Reactor Trip and ESF Displays for DAS	61513 62138 61226 60987	A	Required to provide information and control capabilities that allow specified manual actions necessary to reach the nonhazardous stable state.	2	The OCS provides the human interface design as well as the location and mounting arrangement for the operator interface equipment necessary to support defence in depth safety functions.
Hardware required for Post-accident Monitoring System Functions from PMS and RMS	60880 61513 61226 60987	B	Required to provide information that allows specified manual actions necessary after the nonhazardous stable state has been reached to prevent a DBA from leading to unacceptable consequences, or mitigate the consequences.	2*	*The Qualified Data Processing System provides displays of Category 1 post-accident monitoring system variables. This hardware will be implemented as Class 1.
Software required for Post-accident Monitoring System Functions from PMS and RMS	61513 62138 61226 60987	B	Required to provide information that allows specified manual actions necessary after the nonhazardous stable state has been reached to prevent a DBA from leading to unacceptable consequences, or mitigate the consequences.	2	The software that supports the Qualified Data Processing System, the principal means of providing the operator post-accident monitoring information.
Balance of Operator Displays and Controls	61513 62138 61226 60987	C	Provide continuous or intermittent monitoring and control capabilities for normal operation.	3	The OCS provides the human interface design as well as the location and mounting arrangement for the operator interface equipment necessary to support normal plant operations.

Table 15A-3. AP1000 UK Categorisation and Classification of C&I SSCs (cont.)

System Function or Equipment	Applicable IEC Standards	UK Safety Category of the Function Provided by the SSC	Safety Function(s) Provided by the SSC	UK Safety Class of the SSC	Justification of the Safety Class
Main Turbine Control and Diagnostics System (TOS)					
Turbine Control	61513 62138 61226 60987	C	The TOS supports removing nuclear heat from the reactor during normal operation. Failure of this system can result in a power manoeuvre thus affecting nuclear safety.	3*	*The TOS provides the primary means of controlling the turbine generator. It supports such functions as turbine trip and overspeed protection. Due to its importance to power production and equipment protection this system will be implemented as a Class 2 system.
In-core Instrumentation System (IIS)					
Core Exit Temperature Measurements used by PMS for Post-Accident Monitoring	60880 61513 61226 60987	B	Required to provide information that allows specified manual actions necessary after the nonhazardous stable state has been reached to prevent a DBA from leading to unacceptable consequences, or mitigate the consequences.	2*	*Core exit temperature measurements are not used for reactor trip or engineered safety feature functions. Some of the measurements are inputs to the PMS system for post-accident monitoring. These sensors are implemented as Class 1 as identified in the applicable IEC standards column.
Balance of Core Exit Temperature Measurements	61513 62138 61226 60987	B	Required to provide information that allows specified manual actions necessary after the nonhazardous stable state has been reached to prevent a DBA from leading to unacceptable consequences, or mitigate the consequences.	2	The core exit temperature measurements are provided to DAS for display and monitoring of post-accident core cooling. The purpose of providing core exit temperature measurements to DAS is to provide information to the reactor operator to monitor core cooling as a basis for manual actuation of the ADS during post-accident conditions.
Core Flux Measurements	61513 62138 61226 60987	C	Provides continuous monitoring of Category B function (reactor power control) to indicate the continued availability for operation and alert control room staff.	3	The IIS provides online neutron flux data. This data is used to generate a 3-D indication of the core power distribution.
Special Monitoring System (SMS)					
Digital Metal Monitoring	61513 62138 61226 60987	C	Monitor for the occurrence of and alert personnel to take mitigating actions for abnormal events.	3	The SMS provides plant personnel with information pertaining to the presence and general location of loose parts or abnormal structural conditions in the RCS.
Reactor Coolant Pump Vibration Monitoring	61513 62138 61226 60987	C	Monitor for the occurrence of and alert personnel to take mitigating actions for abnormal events.	3	The primary purpose of the reactor coolant pump vibration monitoring system is to provide early detection of abnormal vibration levels of the reactor coolant pumps to avoid or mitigate damage.

Table 15A-3. AP1000 UK Categorisation and Classification of C&I SSCs (cont.)

System Function or Equipment	Applicable IEC Standards	UK Safety Category of the Function Provided by the SSC	Safety Function(s) Provided by the SSC	UK Safety Class of the SSC	Justification of the Safety Class
Radiation Monitoring System (RMS)					
Containment High Range	60880 61513 61226 60987	A	Maintaining the integrity of the containment; thereby minimising the release of radioactive material from the containment.	1	There are four trains for the containment high range radiation detectors which measure the containment area radiation. Inputs from the RMS provide radiation signals to PMS for processing. When a predetermined setpoint is exceeded on the high range detectors, PMS will isolate containment.
MCR HVAC	61513 62138 61226 60987	A	Maintaining habitability of the MCR.	1	The MCR supply duct is monitored for particulates, iodines, and noble gas. Inputs from the RMS provide radiation signals to PMS. When a predetermined setpoint is exceeded on the noble gas channel, PMS will initiate the supplemental air filtration system. When a predetermined setpoint is exceeded on the particulate or iodine channel, PMS will isolate the MCR and initiate VES.
Balance of System Functions	61513 62138 61226 60987	C	Monitoring radioactivity released into the environment.	3	Radiation detection signals from the RMS to PLS are used to process various plant control functions such as valve control, pump operation, as well as pressure and flow control functions.

Table 15A-4. AP1000 UK Categorisation and Classification of Structures

Description	Seismic Category	UK Safety Category of the Function Provided by the SSC	Safety Function(s) Provided by the SSC	UK Safety Class of the SSC	Justification of the Safety Class
Containment Vessel	I	A	Removal of decay heat from the reactor coolant during accident conditions. Prevention of the release of radioactive material from the containment. Protecting against internal/external hazards that would directly and inevitably result in loss of one of the other Category A safety functions.	1	The AP1000 containment vessel supports the function of various Class 1 SSCs by providing the principal means of decay heat removal to the atmosphere, of containment integrity, and structural integrity.
Shield Building	I	A	Providing a heat sink for those systems involved in the removal of heat from the reactor coolant during accident conditions. Protecting against external hazards that would directly and inevitably result in loss of one of the other Category A safety functions.	1	The AP1000 shield building provides for the proper airflow path to support the principal means of decay heat removal and also protects the containment vessel from hazards.

Table 15A-4. AP1000 UK Categorisation and Classification of Structures (cont.)

Description	Seismic Category	UK Safety Category of the Function Provided by the SSC	Safety Function(s) Provided by the SSC	UK Safety Class of the SSC	Justification of the Safety Class
Auxiliary Building	I	A	Protecting against internal/external hazards that would directly and inevitably result in loss of one of the other Category A safety functions.	1	The auxiliary building contains various Class 1 SSCs and the MCR. This structure serves to protect Class 1 SSCs from hazards.
Annex Building Area Outlined by Columns A-D and 8-13	NNS	GNS	No nuclear safety implications.	GNS	SSCs are not designed or considered in the application of a safety function.
Annex Building Area Outlined by Columns A-G and 13-16	NNS	GNS	No nuclear safety implications.	GNS	SSCs are not designed or considered in the application of a safety function.

Table 15A-4. AP1000 UK Categorisation and Classification of Structures (cont.)

Description	Seismic Category	UK Safety Category of the Function Provided by the SSC	Safety Function(s) Provided by the SSC	UK Safety Class of the SSC	Justification of the Safety Class
Annex Building Area Outlined by Columns E-I.1 and 2-13	II	A	Protecting against internal/external hazards that would directly and inevitably result in loss of one of the other Category A safety functions.	2	The annex building houses electrical equipment that supports a Category A function that is important to safety. The portion of the annex building next to the auxiliary building is designed to prevent adverse interaction with the auxiliary building during seismic events. The annex building houses equipment that reduces the probability of requiring the use of offsite SSCs to support post 72 hour actions following a DBA.
Radwaste Building	NNS	B	The radwaste building helps control the level of radioactivity released to the environment.	3	The radwaste building houses radioactive waste systems that are treated as onsite storage/treatment facilities.
Diesel-Generator Building	NNS	A	Protecting against internal/external hazards that would directly and inevitably result in loss of one of the other Category A safety functions.	2	The diesel generator building houses mechanical and electrical equipment that supports a Category A function that is important to safety.

Table 15A-4. AP1000 UK Categorisation and Classification of Structures (cont.)

Description	Seismic Category	UK Safety Category of the Function Provided by the SSC	Safety Function(s) Provided by the SSC	UK Safety Class of the SSC	Justification of the Safety Class
Circulating Water Pump House and Towers	NNS	GNS	No nuclear safety implications.	GNS	SSCs are not designed or considered in the application of a safety function.
Turbine Building (First Bay)	II	A	Protecting against internal/external hazards that would directly and inevitably result in loss of one of the other Category A safety functions.	2	The first bay of the turbine building houses various types of equipment that supports a Category A functions. The first bay of the turbine building is designed to prevent adverse interaction with the auxiliary building during seismic events.
Turbine Building (Balance of Bays)	NNS	C	The turbine building supports reliable power production. Failure of portions of the turbine building would likely result in power manoeuvres thus affecting nuclear a safety.	3	SSCs are not designed or considered in the application of a safety function.

TABLE OF CONTENTS

TABLE OF CONTENTS (cont.)

TABLE OF CONTENTS (cont.)

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS AND ACRONYMS

ACI	American Concrete Institute
ADS	automatic depressurisation system
AISC	American Institute of Steel Construction
AISI	American Iron and Steel Institute
ALARP	as low as reasonably practicable
ASME	American Society of Mechanical Engineers
ASCE	American Society of Civil Engineers
ASTM	American Society for Testing and Materials
BDB	beyond design basis
BRL	Ballistic Research Laboratory
C-I	Seismic Category I
C-II	Seismic Category II
C-III	Seismic Category III
CA module	SC module – not forming part of the shield building cylindrical wall
CCS	component cooling water system
C&I	control and instrumentation
CSDRS	certified seismic design response spectra
CVS	chemical and volume control system
DBA	design basis accident
DBE	design basis event
GDA	generic design assessment
GNS	general non-safety
HCLPF	high confidence of low probability of failure
HR	hard rock
HVAC	heating, ventilation, and air conditioning
IRWST	in-containment refuelling water storage tank
LOCA	loss-of-coolant accident
MCR	main control room
MSIV	main steam isolation valve
NDE	non-destructive examination
NDRC	Modified National Defence Research Committee
NNS	non-nuclear seismic
PCCWST	passive containment cooling water storage tank
PCS	passive containment cooling system
PCSR	Pre-Construction Safety ReportPPF pressure part failure
RNS	normal residual heat removal system
SAP	safety assessment principle
SC	steel-concrete composite
SCC	self-consolidating concrete
SFP	spent fuel pool
SG	steam generator
SM	soft-to-medium soil
SQEP	suitably qualified and experienced person
SRV	safety relief valve
SSC	system, structure, or component
SSE	safe shutdown earthquake
SSI	soil structure interaction

LIST OF ABBREVIATIONS AND ACRONYMS (cont.)

SWS	service water system
UBC	Uniform Building Code
UBSM	upper-bound soft-to-medium soil
UK	United Kingdom
US	United States
WLS	liquid radwaste system
WRS	radioactive waste drain system
ZPA	zero period acceleration

16 CIVIL ENGINEERING

16.1 INTRODUCTION

The AP1000 nuclear power plant, including its civil engineering aspects, has been designed with the intent that it can be constructed and operated at a wide range of potential sites throughout the world. In particular, the design has specifically addressed construction at any potential location within the eastern and central United States (US), demonstrating a capability for withstanding a wide range of different environments and site conditions more onerous than would be present at potential AP1000 plant sites in the United Kingdom (UK).

The AP1000 design is founded on international nuclear safety practices and needs to be demonstrated as safe in the UK, taking into account UK-established nuclear safety practices consistent with the safety assessment principles (SAPs) (Reference 16.1) considered by the UK Nuclear Regulator when making licensing decisions. The international civil engineering case is, on many occasions, more demanding than needed to satisfy UK requirements. This is because of the more benign environments at potential sites in the UK compared with those at the potential locations considered in the design (see Chapter 12, External Hazards). However, the absence of a prescriptive regulatory regime in the UK means that it is necessary to present the evidence that underpins the AP1000 design within a new logical framework that is consistent with the UK regulatory approach.

This chapter describes the civil engineering design of the AP1000 plant structures for a set of environmental conditions established by site interface parameters shown in Table 16-3. It justifies the AP1000 design assuming a site defined by the site interface parameters. Chapter 12 demonstrates that the UK sites are expected to be bounded by these interface parameters.

Once a specific site is decided upon for an AP1000, a site characterisation evaluation against the current plant design will set the design limits for that project.

This chapter addresses the expectations of the UK Regulator for the justification of the civil engineering structures. It makes extensive reference to relevant Westinghouse design documentation.

The civil engineering structures have been designed for rapid construction by making maximum use of offsite fabricated steel modules, which are subsequently filled with concrete when located onsite, rather than conventional, cast-in-place, reinforced concrete. Instead of fixing reinforcement bars and pouring concrete between shuttering, concrete is placed between two steel plates to form a module wall; these plates provide the reinforcement and act as shuttering. This form of construction, called steel-concrete composite (SC) construction, is unconventional in the UK for nuclear power station construction. Therefore, the justification for SC structures has been considered in particular detail. The design reports for the enhanced shield building and the response to RI-AP1000-02 provide justification of the design approach (References 16.3, 16.4, 16.39, 16.40, and 16.41). The civil engineering design and safety justification has proceeded in accordance with criteria developed for the AP1000 design that are recorded in a number of documents.

16.1.1 Purpose

The civil engineering structures are required to provide structural support to the structures, systems, or components (SSCs), including supporting systems, that enable safe nuclear power generation. Loads from normal operations, fault conditions, maintenance activities,

construction, and decommissioning must be safely transferred from each SSC attached to the civil engineering structure to a foundation of suitable strength and rigidity.

In addition to providing structural support, the civil engineering structures need to act as suitable barriers. Examples of barrier functions are the retention of liquids, protection from the weather, radiation shielding, prevention of the spread of fire and the control of accidentally generated missiles so that they do not cause significant harm. This chapter addresses all these barrier functions with the exceptions of the radiation shielding, which is addressed in Chapter 24; and fire resistance, which is addressed in Chapter 11.

An earthquake causes vibrations that will pass through the civil engineering structures and cause the SSCs that make up the nuclear power plant to experience dynamic loads. In addition to demonstrating seismic integrity, the civil engineering structures need to be suitably analysed for the seismic motions at SSC support points to be defined. The SSCs can then be analysed to determine seismic responses.

Nuclear safety functions placed on the civil engineering structures are addressed by demonstrating that the civil structures will withstand the loads arising from normal operations, internal hazards, external hazards, and internal plant faults. The structures need to be appropriately constructed and shown not to suffer any significant deterioration through life. The evidence needed to support a nuclear safety function depends on the significance of the safety function with regards to nuclear safety.

Safety functions are categorised according to safety importance of the contribution made by an SSC in meeting the function classified. The categorisation and classification process is explained in Chapter 5. The approach to the justification of the civil engineering structures takes into account the category and class assigned to a structure. The nuclear island houses the SSCs of greatest safety significance, and therefore the nuclear island civil engineering structures are assigned Category A safety functions and are Class 1. They are justified to withstand the most severe hazards using the most reliable methods adopted for the plant civil engineering structures.

The objective of this chapter is to provide evidence that the designs of the civil engineering structures deliver the necessary nuclear safety functions in an appropriate manner, depending on the safety function category and the civil engineering class. The level of information provided is commensurate with the safety significance of the structure. The nuclear island structures, which house the Class 1 safety systems, are reported in most detail.

16.1.2 Scope

This chapter is limited to addressing the following civil engineering structures that have been assigned nuclear safety functions.

- Containment internal structures
- Shield building
- Auxiliary building
- Nuclear island foundation
- Annex building
- Diesel generator building
- Radwaste building
- Turbine building
- SWS (service water system) cooling towers

This chapter addresses the effects of normal operations, internal plant faults, internal hazards, external hazards, and life cycle engineering for the above structures. Safety functions are categorised and the role of an SSC in meeting this function is classified as explained in Section 16.3. Structures are assigned a seismic category depending on the performance required following an earthquake. Sections 16.4 and 16.5 include explanations to justify that the hazards, codes, and standards considered in the design are appropriate for each civil engineering structure, depending on the safety function, class, and seismic category.

The containment vessel itself is outside the scope of this chapter, as this is considered to be a vessel justified in Appendix 20K. Equipment design is outside the scope of this chapter. The interface between civil engineering structures and internal equipment occurs at the support point. Items encasted in concrete are considered to be part of the civil engineering structure whereas any protrusions for the purpose of supporting equipment are justified as part of the equipment justification.

16.1.3 Format

The evidence needed to support construction in the UK exists and has been documented as part of the generic AP1000 design and licensing process. As noted previously, this chapter presents this information within a framework compatible with the UK regulatory regime. This chapter utilises the information in the AP1000 criteria documents and summaries of the global analyses. Other equally important references referred to are the design report for the AP1000 enhanced shield building (Reference 16.3) and the response to RI-AP1000-02 (Reference 16.4, 16.39, 16.40, and 16.41). Detailed technical information, tabulations, and figures in these documents are referenced within this chapter without being reproduced.

16.1.4 Structural Descriptions and Layouts

General descriptions of the structures identified in Section 16.1.2 are presented in Section 6.11. More detailed civil/structural information is provided in this chapter.

Figures 16-1 and 16-2 show the general arrangements of an AP1000 plant and the locations of systems within the civil engineering structures. For the generic design, it is assumed that the north/south axis runs parallel with the longitudinal axis of the turbine building. The radwaste building is located to the south of the auxiliary building and the turbine building is located to the north.

The details of the major structures are given in References 16.48 through 16.86. The plant was originally designed to US customary units with grade level defined as 100'-0". This PCSR uses metric units and the grade level is taken as +100.000 m.

16.1.5 Interfaces

The internal and external hazards assessments (Chapters 11 and 12) define events that lead to loads being placed on the civil structures. Normal operations and fault conditions also place loads on the civil engineering structures.

16.1.5.1 Normal Operations and Internal Plant Faults

The civil engineering structures are required to support the vessels, pipework, cable trays, mechanical plant, and electrical equipment during normal operations. If internal faults occur in the plant, additional demands can be placed upon the civil engineering structures. Loads relating to normal operations and internal plant faults have been considered as explained in Section 16.7.

16.1.5.2 Internal Hazards

The requirements have been identified for the walls and floors forming the rooms contained within the nuclear island to act as barriers against relevant internal hazards. This information has been presented in the form of a barrier matrix (Reference 16.9). PCSR Chapter 11 identifies claims with respect to the civil engineering structures. The civil engineering design criteria address loads arising from the following internally generated hazards:

- Flooding
- Fire
- Pressure part failure (PPF)

The layout and the structural design for the loads specified in Reference 16.6, including requirements for radiation shielding and for the external hazards, provide inherent protection for other internal hazards. The justification of adequately designed barriers against internal hazards is provided in Chapter 11. The provision of barriers for radiation shielding is considered in Chapter 24.

16.1.5.3 External Hazards

Chapter 12 derives magnitudes of external hazard events appropriate to the AP1000 plant UK generic safety case. The events considered are typical upper-bound events, which will need to be confirmed in UK site-specific studies. Chapter 12 compares these events with the external hazards addressed by the design. The responses of the civil engineering structures to external hazards are considered in Section 16.4.

16.2 SITE CHARACTERISTICS

The site-related parameters for which the plant has been designed are given in Chapter 4; those affecting the civil engineering structures are shown in greater detail in Table 16-3. These parameters reflect potential bounding site characteristics for possible worldwide AP1000 plant sites. In the UK context, these site parameters and conditions represent the envelope beyond which additional validation would be required.

In general, the sources of the site parameters and conditions presented in Chapter 4 are irrelevant to the UK justification. What is required is a demonstration that the parameters and conditions associated with any particular UK site at which a plant is to be built will not fall outside this envelope. If parameters and conditions fall outside this envelope, then further justification will be required to demonstrate that the design is acceptable. The demonstration that site-specific data falls within the acceptable envelope will be addressed during site licensing.

Although UK site-specific data is not available for GDA submissions, it is often possible, using general data for potential plant locations in the UK, to show the margins that exist

between potential natural hazards in the UK and those for which the plant has been designed. Chapter 12 (External Hazards) presents such comparisons.

16.3 UK CATEGORISATION AND CLASSIFICATION APPLIED TO THE CIVIL ENGINEERING STRUCTURES

A method for the categorisation of safety functions and classification of SSCs has been developed and is presented in Chapter 5. Structures are also assigned a seismic category depending on their required performance during and following a seismic event. The seismic categories are discussed in the following sections.

16.3.1 Seismic Category I

Seismic category I (C-I) structures have both functional and integrity requirements placed upon them. The main seismic functional requirement is to respond to an earthquake in a manner that can be defined so that an SSC that relies on the structure for support can be seismically justified. Other functional requirements may also need to be justified, such as providing a substantially watertight barrier during and following a seismic event.

16.3.2 Seismic Category II

If failure of a structure (not classed as C-I) can result in an unacceptable interaction with a Class 1, C-I SSC, or another seismic category II (C-II) SSC, or cause an incapacitating injury to occupants of the control room, then the structure is designated as C-II. C-II structures are justified as having appropriate integrity but provision of functionality is not required.

16.3.3 Seismic Category Non-Nuclear Seismic

All UK Class 2 and 3 structures for which failure can be accepted, allowing for all reasonably possible modes of failure, are designated as seismic category non-nuclear seismic (NNS). Even though a structure has been assigned as NNS, a seismic justification is undertaken. This is because a plant could be located in a seismic zone where normal industrial practice would be to provide some form of seismic protection to all new structures. For the standard plant these structures are designated as seismic category III (C-III).

16.3.4 AP1000 Structures

The functional and integrity requirements for C-I structures are met by ensuring full compliance with the codes and standards referred to in Section 16.5.1. C-II structures are designed to the same codes and standards as C-I to conservatively ensure no unacceptable adverse interaction with a Category A safety function.

In the UK, civil engineering structures have been categorised according to their safety function and have been classified according to their significance in delivering this function. The seismic categories assigned to the AP1000 structures are shown in Table 16-1.

The nuclear island structures house SSCs that provide the principal means of delivering the Category A safety functions. These functions must be delivered to achieve and maintain a safe, stable state for 72 hours from the initiating event for design basis accidents (DBAs). The primary civil engineering structures that make up the nuclear island are designated as A1 and C-I (A1 refers to a Category A safety function and Class 1 contribution to this safety function in accordance with Chapter 5).

The first bay of the turbine building, the diesel generator building, and the SWS cooling towers contain active systems that deliver Category A functions. The systems in these structures provide an alternative means of delivering the functions provided by the Class 1 components. These Class 2 components make a significant contribution to delivering Category A safety functions but are not the principal means of achievement. Therefore these structures are designated as A2. The first bay of the turbine building is C-II to prevent adverse interaction with the nuclear island. The remaining structures housing Class 2 components are assigned to the NNS category. The turbine building north of the first bay closest to the nuclear island is C3 and NNS.

Immediately adjacent to the nuclear island, the annex building is of multi-storey construction, with the potential for undesirable interactions with the nuclear island; therefore, this multi-storey area of the annex building is C-II. The remaining single-storey area of the annex building, of lightweight construction, is Class general non-safety (GNS) and seismic category NNS.

Areas of the annex building contain SSCs that need to support Category A safety functions after 72 hours following an accident. Hazard protection in excess of that afforded by designing to normal industrial standards is deemed necessary to ensure equipment availability post-72 hours.

The radwaste building is Category B3 because the function of the equipment in the building is not nuclear safety-significant. It is seismic category NNS because seismic failure of the building would not be of any consequence for the functioning of the systems within the nuclear island.

16.4 DESIGN BASIS EXTERNAL HAZARDS

The magnitudes of external hazards in the UK are generally enveloped by those specified for the design (see Chapter 12). This section considers whether the designs of the civil engineering structures are conservative with regard to their responses to naturally occurring hazards defined by the site interface parameters. Only natural hazards are discussed in this chapter because manmade external hazards, originating from outside the nuclear site boundary (excluding malicious aircraft impact), are a site-specific issue to be addressed during site-specific licensing. Detailed information on the loads arising from external hazards is provided in Sections 16.7 and 16.8.

16.4.1 A1 Civil Engineering Structures – Nuclear Island

The external hazards that the nuclear island structures have been designed to withstand are shown in Table 16-3. In the UK, natural hazards are included in the design basis unless conservatively they have a predicted frequency of less than 1 in 10,000 year (Reference 16.1). The AP1000 design considers both severe operating events with a frequency of about 1 in 50 year as well as extreme environmental events with a frequency of about 1 in 10,000 year. In some cases, such as snow, design is based only on the severe condition since the load factors or allowable stresses and the load combinations used in the design are sufficient that these loads are more limiting than the extreme condition with unit load factor or allowable stresses up to yield.

This report uses the terminology from ACI 349 (Reference 16-15) and AISC N690 (Reference 16-24) to differentiate between the recurrence frequency of the hazards.

- Severe environmental loads are those that could infrequently be encountered during the plant life. These include the severe design wind and snow. The magnitudes correspond to the values that would be applicable to a commercial building at the same location.

- Extreme environmental loads are those which are credible but are highly improbable. These include the tornado and the SSE.

Chapter 12 compares the natural hazards for which the nuclear island structures have been designed with the natural hazards applicable in the UK using generic UK data. The natural hazards most likely to challenge the civil engineering structures are wind, extreme snow, tornadoes, and earthquakes.

16.4.1.1 Design Wind

The AP1000 plant is designed for the design wind (Reference 16.6) in accordance with ASCE 7 (Reference 16.20). The design wind is specified as a basic wind speed of 64.8 m/s (145 mph) with an annual probability of occurrence of 0.02 based on the most severe location in the United States identified in Reference 16.20 (wind speeds in the UK are generally lower as discussed in Chapter 12). This wind speed is the 3 second gust speed at 10.06 m (33 feet) above the ground in open terrain (Reference 16.20, exposure C). Higher winds with a probability of occurrence of 0.01 are used in the design of the nuclear island by using an importance factor of 1.15.

Velocity pressure exposure coefficients and gust response factors are calculated according to Reference 16.20 for exposure C, which is applicable to shorelines in hurricane prone areas. The topographic factor is taken as unity.

The design wind loads calculated as described above are considered as a severe environmental condition with appropriate load factors for concrete design and allowable stresses for steel design. Loads and load combinations are shown in Tables 3 and 4 of Reference 16.6.

16.4.1.2 Tornado

The nuclear island is designed for the design basis tornado (Reference 16.6) specified as follows:

- Maximum wind speed – 134.1 m/s (300 mph)
- Maximum rotational speed –107.3 m/s (240 mph)
- Maximum translational speed – 26.8 m/s (60 mph)
- Radius of maximum rotational wind from centre of tornado – 45.8 m (150 ft)
- Atmospheric pressure drop – 13.8 kPa (2.0 psi)
- Rate of pressure change – 6.9 kPa/s (1.2 psi/sec)

It is estimated that the probability of wind speeds greater than the design basis tornado is between 10^{-6} and 10^{-7} per year for an AP1000 plant at a "worst location" anywhere within the contiguous United States.

The exterior walls and roof of the nuclear island are designed to protect the nuclear island

against damage from the tornado missiles shown in Table 16-3.

Chapter 12 identifies that the tornadoes considered in the design are far more onerous than what could occur in the UK. The concrete is designed to ACI-349-01, which is acceptable UK practice (see Section 16.5.1.5); therefore, it can be concluded that the international design follows a very conservative approach with respect to tornadoes in the UK.

16.4.1.3 Snow

The AP1000 plant is designed for deep snow loads associated with a 1 in 50 year event (Reference 16.6) in accordance with ASCE 7 (Reference 16.20). The nuclear island roof is constructed from reinforced concrete at least 200 mm thick and is designed to resist a ground snow load of 3.6 kN/m^2 (75 lb/sq. ft) (Reference 16.6, Section 5.2.2B) using ultimate load factors of 1.4 and 1.7 for dead and live loads, respectively (Reference 16.6, Table 3). Snow is considered to be a live load as explained in Section 16.7.4.2; therefore, the auxiliary building roof provides a rugged barrier.

A study of the effects of automobiles acting as missiles during a tornado has been made (Reference 16.13). This study considered an 1814-kg (4000-lb) vehicle impacting the roof with a vertical velocity of 33 m/s (74 mph) with the vehicle assumed to be a soft missile impacting a rigid target. Noting this, if snow or icicles were to slide off the sloping roof of the shield building and impact the roof of the auxiliary building, it is to be expected that the effects on the roof would be bounded by the postulated vehicle impact.

16.4.1.4 Earthquake

The AP1000 standard plant is designed for a safe shutdown earthquake (SSE) defined by the US Certified Seismic Design Response Spectra (CSDRS) scaled to 0.3g zero period acceleration (ZPA). The response spectra are based on USNRC Regulatory Guide 1.60 (Reference 16.31) with additional amplification at 25 Hz. The horizontal and vertical spectra are shown in Figures 1 and 2 of Reference 16.7 for various damping values (the horizontal spectrum is shown in Figure 12C-1 for 5% damping). The horizontal and vertical components of the ZPA have been taken to be the same with both scaled to 0.3g for the SSE.

The AP1000 plant will be demonstrated to satisfy all seismic design acceptance criteria using the site-specific input. This demonstration may include a combination of comparisons of ground motion and soil conditions, and site specific analyses. The nuclear island has been designed to the CSDRS for a wide variety of soil conditions. It is therefore expected that the site specific demand will be lower than the standard plant design basis.

It is not expected that there will be significant changes for the AP1000 plant in the UK. The basic design will retain the existing design and hence retain the margins inherent in the enveloping parameters of the standard plant seismic design. Where design changes are required for other reasons, the revised design will be demonstrated to satisfy site-specific requirements.

16.4.2 A2 Civil Engineering Structures

The nuclear island houses the Class 1 passive safety components that have a low frequency of failure per demand. When designed to resist the same hazard, a single passive safety system will be more reliable than a single active safety system because the passive safety systems are of a simple design based on the application of the fundamental laws of physics. To benefit from this, it is deemed reasonable for the backup systems to be less reliable than those with

Class 1 components; therefore, the backup systems do not need to be designed to withstand hazard loadings as onerous as those specified for the design of the Class 1 components.

A2 civil engineering structures have been designed to withstand the same onerous extreme events as A1 only if their failure when subjected to such an event could cause an adverse interaction with an A1 system. When such a failure would not cause an adverse interaction, justification of A2 SSCs against natural hazards is only considered necessary from the point-of-view of investment protection and as low as reasonably practicable (ALARP), because the Class 1 components housed in the A1 nuclear island structure are capable of mitigating DBAs.

A2 structures may be C-II or seismic category NNS. Table 16-2 explains the logic behind the external hazard events addressed by the design and gives the underlying reasoning.

For A2 structures designated as C-II, the seismic motion used for the integrity justification is the same as the one used for C-I structures to provide the necessary consistency.

For A2 structures designated as seismic category NNS, the design is based on less onerous external hazard events than the 1 in 10,000 year events normally expected to be considered in the UK (Reference 16.1). The approach for each A2 structure is explained below with respect to the more significant natural hazards for the civil engineering design.

16.4.2.1 Turbine Building (A2 and C3)

The first bay of the turbine building on the side of the building closest to the nuclear island, south of grid line 11.2, is A2 and C-II. This houses Class 2 equipment associated with the component cooling and service water systems (CCS and SWS, respectively). The turbine building, apart from the first bay, is a C3 structure and is seismic category NNS. A seismic gap separates the A2 first bay from the C3 area.

The first bay of the turbine building has a 610-mm-thick (24 inches) reinforced concrete wall around its perimeter with reinforced floors and roof (References 16.67 through 16.74)It is, therefore, a relatively rigid and strong structure resistant to external hazards.

The C3 area comprises the main turbine hall with three floor levels and a basement below. The C3 area contains no equipment assigned a safety function. The roof to this area is generally at a level of 144.2 m (473.1 feet), whereas the roof of the first bay is considerably lower, at the same level as the turbine building operating deck at 118.59 m (380.1 feet).

The NNS area of the turbine building is more flexible and less hazard-resistant than the first bay. It is a steel-framed structure. A seismic gap is provided between the first bay and the rest of the turbine building. The robust nature of the first bay means that if some interaction were to occur, the first bay would act as a partial barrier to prevent damage to the Class 1 components in the nuclear island. The Turbine Building NNS area is on a stable foundation media so that the basemat beneath the Turbine Building does not endanger the first bay.

The approaches to tornado, extreme wind, extreme snow, and earthquake are explained in the sections that follow.

16.4.2.1.1 Tornado

Tornadoes must not lead to collapse of the turbine building onto the nuclear island; however, it is unnecessary for the Class 2 equipment housed in the first bay to be protected from tornadoes. The design approach to tornadoes is as follows:

- The reinforced concrete walls of the first bay of the turbine building are designed to withstand the same tornado wind loading as the nuclear island following the American Concrete Institute (ACI) design criteria presented in ACI 349-01 (Reference 16.15), which is appropriate to the UK. This ensures that tornado loading could not cause the first bay to collapse onto the nuclear island. The first bay is not designed to withstand tornado missile loads as they would lead to local effects that could not credibly lead to gross failure of the first bay. Local damage could cause some elements of the structure to be blown against the nuclear island; however, the resulting missiles would be enveloped by those considered for the tornado design of the nuclear island, presented in Table 16-3.

- The C3 area of the turbine building is designed to withstand the same tornado wind loading as the first bay, but different criteria are applied. First, it is acceptable for the cladding to be blown off. The objective of the design is to demonstrate that the heavy elements of the C3 area of the turbine building (floors and structural steel-frame components) will not collapse or become tornado borne missiles (see Reference 16.6, Sections 6.2.1 and 6.3.2 for the assumptions to be made about the building area and its contents being considered as projected into the wind). Second, the C3 area of the turbine building is designed to the industrial codes and standards identified in Section 16.5.2.

Chapter 12 identifies that the tornadoes considered in the design are far more onerous than what could occur in the UK. The concrete is designed to ACI-349-01, which is acceptable UK practice (see Section 16.5.1.5); therefore, it can be concluded that the international design follows a very conservative approach with respect to tornadoes in the UK.

16.4.2.1.2 Extreme Wind

The turbine building is designed for the 1 in 50 year design wind in accordance with ASCE 7 (Reference 16.20). No damage is permitted under this condition. The building is not evaluated for the 1 in 10,000 year event since this wind is enveloped by the tornado. Extreme wind must lead to neither collapse of the turbine building onto the nuclear island nor damage to the first bay sufficient to affect Class 1 components.

How the design addresses the 1 in 50 year design wind is explained in Reference 16.6, Section 5. The main part of the turbine building structure, which envelopes the C3 area, is designed to withstand the same wind loading as applied to the nuclear island except that the importance factor is reduced from 1.15 to 1.0 (an importance factor is US terminology and is a factor applied to the wind loading to take into account the importance of a building). The American Institute of Steel Construction (AISC) allowable steel stresses presented in AISC S335 (Reference 16.16) are increased by 33 percent (Reference 16.6, Table 8) for the natural hazards considered in the design of Category NNS structures. The magnitude of the wind considered is similar to the UK 1 in 10,000 year wind as shown in Chapter 12. The design criteria with respect to wind loads is similar to the criteria followed in the UK in the past when using a permissible stress code (i.e., stresses up to yield are acceptable for tension members). Considering that it is not necessary for the Class 2 equipment to be justified to withstand 1 in 10,000 year events, the case against extreme wind for the turbine building is adequate for the UK. The protection provided by the first bay provides additional assurance. Note that the main part of the turbine building is being redesigned for the 50 Hz turbine in the

UK; the structural design will use UK design codes to provide margin similar to that provided by the US codes.

The design against tornado, which is far more onerous than an extreme wind, demonstrates that an extreme wind could not cause an adverse reaction between the first bay of the turbine building and the nuclear island.

16.4.2.1.3 Snow

Design snow loads are explained in Reference 16.6, Section 5.2.2. The roof over the entire area of the turbine building is designed to withstand the same snow loading as applied to the nuclear island (see Section 16.4.1.1) except that the importance factor is reduced from 1.2 to 1.0. For uniform snow conditions, this is conservative for the UK as discussed in Chapter 12.

Chapter 12 identifies snow drifting or snow sliding off the shield building roof as potential hazards, which are relevant to the A2 first bay of the turbine building. This will be constructed of at least 200-mm-thick (7.87 inches) reinforced concrete slab, which should be more than capable of resisting such events. If the roof slab were to fail, only the Class 2 components would be affected and there would be no potential for damage to the Class 1 components.

16.4.2.1.4 Earthquake

The A2 first bay of the turbine building is designed to withstand the same earthquake as the A1 nuclear island. A seismic gap between the turbine building first bay and the nuclear island and between the turbine building first bay and the C3 portion of the turbine building is provided above grade.

The C3 portion of the turbine building is qualified against the seismic ground motion specified in the 1997 Uniform Building Code (UBC) (Reference 16.17). The UBC seismic motion is for US Zone 3 with an importance factor of 1.0. This input is higher than that used on other NNS buildings in order to reduce the risk of the upper part of the turbine building collapsing onto the first bay and the nuclear island. Note that the main part of the turbine building is being redesigned for the 50 Hz turbine in the UK; the structural design will use seismic input and design codes to provide margin similar to that provided by the UBC design.

16.4.2.2 Diesel Generator Building and SWS Cooling Towers

The diesel generator building and SWS cooling towers are located so that there is no potential for their collapse to lead to any adverse reaction with the Class 1 components located in the nuclear island. These buildings contain Class 2 equipment. The buildings are seismic category NNS.

16.4.2.3 Annex Building (A2/GNS)

The annex building comprises a multi-storey part east of the auxiliary building (between gridlines E-I1 and 2-13); and a single-storey lightweight part, mainly housing offices, north and east of this (between gridlines A-D and 8-13, and between gridlines A-G and 13-16). The building arrangement is shown in References 16.62 through 16.64 and 16.87 through 16.96. The multi-storey part of the annex building is adjacent to the nuclear island; it is of relatively heavy construction with a potential interaction hazard with the nuclear island; therefore, the multi-storey part is C-II. The single-storey part is classified as GNS. The multi-storey part of the annex building is designed to suffer no adverse reaction from collapse of the GNS part, so the GNS part is not discussed further in this chapter.

The multi-storey part of the annex building contains SSCs that need to maintain Category A safety functions 72 hours after a DBA. The SSCs required to support Category A safety functions after 72 hours are protected from hurricanes. The boundary of the room in the multi-storey part of the annex building housing the ancillary diesels and their supporting equipment provides hurricane protection.

The design approach to external hazards acting on the annex building is conservative in the UK context as identified in the sections that follow.

16.4.2.3.1 Earthquake

The A2 annex building is designed to withstand the same earthquake as the A1 nuclear island. A seismic gap between the annex building and the nuclear island and between the annex building A2 and the C3 portion is provided above grade.

16.4.2.3.2 Wind

The annex building is designed for the 1 in 50 year design wind in accordance with ASCE 7 (Reference 16.20). No damage is permitted under this condition. The building is not evaluated for the 1 in 10,000 year event since this wind is enveloped by the tornado.

The annex building has been designed for the same 1 in 50 year wind loading as the nuclear island structures except that the importance factor has been reduced from 1.15 to 1.0, based on Reference 16.6, Section 5.2. Chapter 12 points out that the 1 in 50 year design wind load would be similar to a UK 1 in 10,000 year wind loading. Wind loads are combined with other loads conservatively in the AP1000 design as identified in Reference 16.6, Tables 5 and 6 (i.e., a load factor of 1.7 has been used for concrete structures and permissible stress criteria have been used for steel structures that include inherent margins). In the UK, common nuclear practice is to allow structures to be stressed close to their ultimate limit states under extreme external hazards (i.e., a load factor of 1.0 or 1.05 is used for concrete structures and permissible stresses for steel structures are enhanced so that tensile stresses are allowed to approach yield). The 1 in 50 year severe wind used in the AP1000 design is similar to the UK 1 in 10,000 year extreme wind, so the overall approach to extreme wind is conservative.

16.4.2.3.3 Tornadoes and Hurricanes

The A2 portion of the annex building adjacent to the nuclear island is designed to withstand the same tornado loading as the nuclear island, but the cladding, but not the concrete walls, is permitted to be blown from the building by a tornado. The walls and ceiling of the annex building room housing the ancillary diesel generators are designed to remain in place under hurricane wind loading and to protect the equipment from hurricane missiles. The wall to the nuclear island, at the interface with the annex building, is designed to withstand the full effects of a tornado.

Chapter 12 reports that the tornadoes considered as part of the international design are very conservative compared with potential UK tornadoes. The precise performance of a particular structure under the design tornado loading is not of concern in the UK because such a large tornado is not predicted.

16.4.2.3.4 Snow

The annex building has been designed for the same snow loading as the nuclear island structures (see Section 16.4.1.1) except that the importance factor has been reduced from 1.2 to 1.0 (Reference 16.6, Section 5.2). For uniform snow loading, this reduction does not affect the conclusion in Chapter 12 that the uniform snow loading addressed by the AP1000 design is conservative when compared with possible snow accumulation at potential UK sites. The AP1000 plant is designed for deep snow associated with a 1 in 50 year event. The roof is designed to resist a ground snow load of 3.6 kN/m^2 (75 lb/sq. ft.) (Reference 16.6, Section 5.2.2B) using ultimate load factors of 1.4 and 1.7 for dead and live loads, respectively (Reference 16.6, Table 3). Snow is considered to be a live load as explained in Section 16.7.4.2. Also see Section 12B.2.

16.4.3 B3 Civil Engineering Structure – Radwaste Building

Compared with the nuclear island structures, the radwaste building is a small, lightweight structure. Three methods are used to demonstrate that a potential radwaste building impact on the nuclear island during a seismic event will not impair its structural integrity (Reference 16.45):

- The maximum kinetic energy of the impact during a seismic event considers the maximum radwaste building and nuclear island velocities. The total kinetic energy is considered to be absorbed by the nuclear island and converted to strain energy. The deflection of the nuclear island is less than 0.51 cm (0.2″). The shear forces in the nuclear island walls are less than the ultimate shear strength based on a minus one standard deviation of test data.

- Stress wave evaluation shows that the stress wave resulting from the impact of the radwaste building on the nuclear island has a maximum compressive stress less than the concrete compressive strength.

- An energy comparison shows that the kinetic energy of the radwaste building is less than the kinetic energy of tornado missiles for which the exterior walls of the nuclear island are designed.

The equipment located in the radwaste building is not required to function following any credible hazard. The building is designed for the same snow and design wind loads discussed in Section 16.4.2.1 above in relation to the C3 area of the turbine building. The radwaste

building is designed to the UBC seismic requirements, Zone 2A with an importance factor of 1.25 (Reference 16.6, Section 5.2.4). Note that the building is being redesigned and the structural design will use UK design codes to provide margin similar to that provided by the US codes.

Return periods of natural hazards needing to be considered in the design of the B3 civil engineering structures are not well defined in the UK. The expectation is that the approach will reflect the importance of the structure to nuclear safety. A reasonable baseline is the natural hazards and their frequencies of occurrence that would be considered for the design of conventional UK industrial structures. The radwaste building exceeds this baseline by a good margin as it has been designed to withstand more onerous international environments. Conventional UK industrial structures are not normally designed to withstand earthquakes unless the consequences of their failure are particularly significant.

16.5 APPLICABLE CODES, STANDARDS AND METHODOLOGIES

16.5.1 A1 Civil Engineering Structures

For A1 structures, the adopted codes and standards should lead to a clearly conservative design under all DBEs (design basis events), with no sudden change in response to BDB (beyond design basis) events of either increasing magnitude or lower frequency. The preference is for nuclear-specific codes and standards to be adopted when appropriate codes and standards are available. For innovative design features not covered by established codes, appropriate design methodologies, specifications, or testing are used.

16.5.1.1 Seismic Analysis Codes

The American Society of Civil Engineers (ASCE) standard ASCE 4-98 (Reference 16.18) was specified for the seismic analyses of the nuclear island (Reference 16.6, Table 2), which are presented in detail in Reference 16.32. ASCE 4-98 is a well-established nuclear-specific standard regularly referred to in the UK for determining appropriate assumptions and methodologies when undertaking seismic analyses of major new nuclear facilities. This is noted in Reference 16.19. Information specific to seismic analysis of AP1000 plant structures is presented in Reference 16.7.

16.5.1.2 Wind and Tornado Loading

ASCE 7-98 (Reference 16.20) was used when determining wind and tornado loads under the defined wind and tornado hazards as explained in Reference 16.6, Section 5.2.3 and Reference 16.12. Reference 16.19 provides some comparisons between ASCE 7-98 and the later versions of the code, concluding that the use of ASCE 7-98 should be appropriate.

The 1 in 50 year wind loads addressed by the AP1000 design are similar to the 1-in-10,000 wind loads for a UK environment. The application of the design codes incorporates margins in excess of those normally considered necessary in the UK. For instance, Table 3 in Reference 16.6 shows that an ultimate load factor of 1.7 has been applied to the wind loading, when in the UK an ultimate load factor of 1.0 or 1.05 would normally be used when considering 1 in 10,000 year wind loads. The margin of 1.7 is conservative and allows for any differences in the US and European wind codes when determining wind loads from wind speeds; hence, the choice of wind code is not critical to the justification of the nuclear island for a UK site.

16.5.1.3 Methodology for Justifying Missile Barriers and Protective Structures

The empirical relationships used for design of missile barriers and protective structures are the modified National Defence Research Committee (NDRC) Formula for concrete, and either the Ballistic Research Laboratory (BRL) or Stanford relationship for steel. Full details are provided in Reference 16.6, Section 4.3.

In the UK, current practice would be to use the R3 Impact Assessment Procedure (Reference 16.21) to evaluate the effects of missiles on structures. This procedure includes the BRL relationship for steel so the AP1000 design use of this relationship is aligned with UK nuclear practice.

16.5.1.4 Methodology for Evaluating Effects Associated with Postulated Rupture of Piping

For the AP1000 design, barriers and shields constructed of either steel or reinforced concrete are provided to protect essential equipment, including instrumentation, from the effects of jet impingement resulting from postulated pipe breaks (Reference 16.6, Section 4.2). Barriers differ from shields in that they may also resist the impact of the whipping pipes. Barriers and shields include walls, floors, and structures specifically designed to provide protection from postulated pipe breaks. Dynamic effects are evaluated using the elastic or elastic-plastic methods presented in "Introduction to Structural Dynamics" by Biggs (Reference 16.22), a standard dynamic analysis text often referred to in the UK.

16.5.1.5 Reinforced Concrete Design Code

ACI 349-01 (Reference 16.15) has been used for the design of the reinforced concrete, taking into account the supplementary requirements in Reference 16.6, Section 6.2.1.

ACI 349-01 is a nuclear-specific code that is fully applicable for determining reinforcement and concrete requirements for A1 structures when demonstrating load-resistance capabilities. The design of anchorages (Reference 16.15, Appendix B) and the provision of reinforcement to provide ductility (Reference 16.15, Chapters 12 and 21) ensure a safe design with no unacceptable step changes in response.

Reference 16.19 compares ACI 349-01 with ACI 349-06 and concludes that the AP1000 applied design provides a basis for the structural safety of the plant.

16.5.1.6 Specification of Materials and Detailing of Reinforcement for Reinforced Concrete

The concrete and reinforcement specified for construction of the AP1000 plant are addressed in Reference 16.6, Sections 7.1 and 7.2. Self-consolidating concrete (SCC) is specified to ACI 237R-07 (Reference 16.23). Design to ACI 349-01 is based on the presumption that materials and workmanship will be specified in accordance with US standards, appropriate for nuclear application, as indicated in Reference 16.6, Section 7. Such standards would not naturally be followed in the UK, where reference to the Europe-wide harmonised technical specifications for materials, workmanship, and testing would be expected. Using a consistent set of US nuclear standards has the advantage of addressing the full intent of ACI 349-01. Reference 16.42 provides the metrication plan for the AP1000 plant; including definition of the extent to which metrication shall apply and to what level of detail metrication shall reach into the design, procurement, licensing, construction, testing, information & configuration management, operation and maintenance of AP1000 plants deployed in the UK. For this document, metrication is defined as the act of adopting metric (SI) units in the design, procurement, construction, operation, and decommissioning phases of an AP1000 plant.

16.5.1.7 Structural Steelwork Design Code

The AISC design criteria for nuclear structures, presented in ANSI/AISC-N690-1994 (Reference 16.24), have been followed for the design of the structural steelwork. The supplementary requirements in Reference 16.6, Section 6.2.2 have been taken into account. This is a nuclear-specific code applicable to the design of steelwork for A1 structures for resisting loads.

ANSI/AISC-N690-1994 (Reference 16.24) has been used for the design. Reference 16.19 compares ANSI/AISC-N690-1994 with ANSI/AISC-N690-2006 and concludes that the AP1000 applied design criteria provide a basis for the structural safety of the plant. In addition, the seismic detailing in the older version of the code is not consistent with the latest recommendations in AISC 341 (Reference 16.25). The shortfall against modern standards is not considered to be of such significance to the A1 structures that the established AP1000 design process should be changed.

The analysis and design of cold-formed steel structures conform to the American Iron and Steel Institute (AISI) code.

16.5.1.8 Specification of Materials and Detailing of Structural Steelwork

Structural steel and associated materials are used as identified in Reference 16.6, Sections 7.3 to 7.9. Basic materials used in the structural and miscellaneous steel construction in the AP1000 design conform to the ASTM standards listed in Reference 16.6. Construction assurance is discussed in more detail in Section 16.19.

16.5.1.9 Steel-Concrete Composite Modular Construction

Steel-Concrete Composite Modules are constructed from concrete and structural steelwork. Justification of the design methodology for SC modular construction is presented in References 16.3 and 16.4. ACI 349 is used as guidance in the design of SC structures. For example, ACI 349 is used to guide member dimensions, plate thicknesses, and strength calculations. To validate this approach, first principle engineering mechanics justifications have been developed and detailed analysis and confirmatory testing has been completed as described in References 16.3 and 16.4.

16.5.2 A2 Civil Engineering Structures

The Class 1 equipment located within the nuclear island structures is the principal means for ensuring nuclear safety. These components are highly reliable. It is appropriate to take credit for this by not making the reliabilities of the Class 2 components be as high as would be required if they had to reduce risks to meet the UK probabilistic criteria. Thus, the structures containing the Class 2 components do not need to be designed to the nuclear-specific codes and standards that are used for the design of the nuclear island.

In accordance with the AP1000 Safety Categorisation and Classification methodology presented in Chapter 5, nuclear codes and standards are applied to Class 1 SSCs, and Class 2 nuclear codes and standards are applied to Class 2 SSCs where appropriate Class 2 nuclear codes and standards exist. Within the context of civil engineering, Class 2 nuclear codes and standards do not exist either in Europe or the US. In the US, codes and standards are either nuclear-specific or normal industrial standard. To design A2 structures to the US nuclear-specific codes and standards would be to ignore the safety advantage of having very reliable Class 1 components; therefore, it is acceptable to design the A2 structures to

robust industrial standards with identified supplemental requirements. Designing Class 2 structures to robust industry codes and standards with the appropriate supplemental requirements supports the overall design reliability requirements. The approach to codes and standards for Class 2 structures, together with the underlying reasoning, is included in the summary information in Table 16-2. This is discussed further in the sections that follow for each A2 building.

16.5.2.1 Turbine Building – First Bay

The first bay of the turbine building is C-II and is designed to ACI 349-01 (Reference 16.15) and ANSI/AISC-N690-1994 (Reference 16.24) as used for the A1 structures described above.

16.5.2.2 Diesel Generator Building and SWS Cooling Towers

The Class 2 diesel generator building and SWS cooling towers are seismic category NNS and are designed to industrial standards. Reinforced concrete elements are designed to ACI 318-99 (Reference 16.26) and structural steel to AISC S335 (Reference 16.16), as used for the C3 area of the turbine building. Seismic analysis and design are based on Reference 16.17. Note that these structures are being redesigned and the structural design will use UK design codes to provide margin similar to that provided by the US codes.

16.5.2.3 Annex Building

The A2 areas of the annex building are designed to the same codes and standards as the A1 nuclear island structures as explained in of Reference 16.6, Section 6.2.1. The remaining GNS area is designed to normal industrial standards.

16.5.3 B3 and C3 Civil Engineering Structures

B3 and C3 structures are designed to normal industrial standards. By definition, failure of a B3 or C3 structure will not have any safety implications with respect to either Class 1 or Class 2 SSCs. Use of normal industrial standards for structures where failure has no nuclear safety implications is acceptable practice in the UK.

16.5.3.1 Turbine Building

The C3 area of the turbine building is designed to ACI 318-99 (Reference 16.26) for concrete structures and AISC S335 (Reference 16.16) for steel structures. These are normal industrial standards as is appropriate for a C3 structure (Reference 16.1, guidance to Principle ECS.3).

Under tornado loading, the acceptance criteria are based on ACI 318 for concrete structures using a load factor of 1.0 and AISC S335 for steel structures with stresses enhanced by 70 percent (Reference 16.6, Tables 5 and 6). It is acceptable for some cladding to be blown from the building and for cladding rails to fail, provided that they do not become detached from the main structural frame (Reference 16.6, Section 6.2.1). The adopted load factor and stress enhancement are chosen so as to remove any margin on the tornado load that allows for loading uncertainties. This is consistent with the normal practice of removing loading margins when considering the effects of extreme loads on normal industrial structures. It is considered acceptable under such extreme conditions for the structure to be damaged and close to collapse, but collapse must not occur.

Seismic analysis and design is to UBC 1997 (Reference 16.17). This is a normal industrial standard for structures sited in seismic regions of the world. Further detail is provided in Reference 16.7.

Note that the C3 area of the turbine building is being redesigned and the structural design will use UK design codes to provide margin similar to that provided by the US codes.

16.6 DESIGN ASSURANCE

Design quality processes that provide an equally high level of assurance for the design justifications for all the civil engineering structures, regardless of the safety class, are followed. The general approach to quality assurance and independent reviews is presented in Chapter 3. When issues arise that might need special consideration, for instance, the design approach falls outside the scope of the adopted codes and standards, expert independent external advice is sought. An example is the expert panel set up to advise on the design of SC construction. The independent experts, suitably qualified and experienced persons (SQEPs), were drawn from a variety of organisations to determine a best-engineering practice approach as described in Reference 16.3.

16.7 ANALYSIS (EXCLUDING SEISMIC), LOADS, AND LOAD COMBINATIONS

16.7.1 Load Identification and Reconciliation Process

Plant structures have been designed and analysed for normal operational loads and design basis loads arising from internal hazards, external hazards, and internal plant faults.

Initially, system and equipment loads are postulated for the civil and structural design. At a later stage, as the design of the systems and equipment progresses, the loads acting on the civil structures may be revised. The structural designer is responsible for ensuring that any revised loading is appropriately allowed for in the design. For example, preliminary interface loads were defined for the reactor coolant loop supports. When the interface loads were finalised, the structural designer reconciled them with the initial postulated loads.

Loads from small items of equipment are frequently included as uniformly distributed loads derived by making conservative assumptions. When the actual arrangements are decided, a reconciliation exercise is undertaken to confirm that the uniform loads assumed in the design bound the loads from the equipment present.

Loads from major items of equipment not included as uniformly distributed loads are recorded in vessel and equipment specifications, such as the Reactor System Interface Control Document (Reference 16.27).

16.7.2 Analysis Approach

Analyses are undertaken using general-purpose structural analysis codes, as described in the civil/structural design criteria (Reference 16.6). The structural systems analysed are described in Section 8 of the same document.

The dynamic effects from the impulsive and impact loads as a result of pipe rupture, tornado-induced missiles, and other such accidents are addressed using one of the following methods:

- Applying an appropriate dynamic load factor to the peak value of the transient load

- Using impulse, momentum, and energy balance techniques
- Performing a time-history dynamic analysis

Elastoplastic behaviour is assumed by applying appropriate ductility ratios unless excessive deflections could cause an adverse interaction with a Class 1 system. Dynamic increase factors, appropriate for the strain rates involved, are applied to the static material strengths of steel and concrete when determining section strength.

Material properties assumed for the design justification are presented in Reference 16.6, Section 7 and Table 9. The concrete compressive strength, as defined in ACI 349-01 (Reference 16.15) and ACI 318-99 (Reference 16.26), is taken as 27.6 N/mm^2 (4000 psi) generally, and 41.4 N/mm^2 (6000 psi) for portions of the shield building.

16.7.3 Load Combinations

For concrete structures, individual loads are combined by multiplying the loads by a factor and combining them with other factored loads. The factors are in accordance with ACI 349-01 (Reference 16.15) with supplemental requirements as cited in Reference 16.6, Section 6.2.1 and take into account uncertainties, the frequency of the loading, and acceptable structural responses. The resulting member forces are checked against the ultimate limit state criteria presented in ACI 349-01.

Steel structures are designed to the permissible stress code in ANSI/AISC-N690-1994 (Reference 16.24) with supplemental requirements as cited in Reference 16.6, Section 6.2.2. All load factors are set to unity and permissible code stresses are applied for all normal operation conditions. For less frequent events, the permissible stresses are enhanced by a stress limit coefficient, with the value depending on the frequency of the loading and acceptable structural responses.

The load combinations considered are presented in the civil/structural design criteria report (Reference 16.6) as follows:

- C-I concrete structures – Table 3
- C-I steel structures – Table 4
- C-II concrete structures – Table 5
- C-II steel structures – Table 6
- Seismic category NNS concrete structures – Table 7 (identified as seismic Category III (C-III) structures)
- Seismic category NNS steel structures – Table 8 (identified as C-III structures)

In these tables, each load case is designated by a letter; for ease of reference, the designated letters are included in the following section titles relating to load cases.

16.7.4 Normal Design Loads

Normal operational loads conservatively reflect the maximum loads expected during the design life. The civil engineering structures are not vulnerable to damage as a result of

repeated application of normal operating loads. The case for "through-life" safety of the civil engineering structures is presented in Section 16.18.

Normal practice in the UK would be to justify structures against external hazards with return periods of slightly greater duration than the design life of the facility. Such external hazards reflect operational basis events and are considered to occur several times and in combination with other operational loads. The margins required are more onerous than those applicable to the less frequent DBEs; however, the AP1000 design does not include such a justification. Instead, a conservative approach is followed with respect to the justification against the less frequent DBEs such that the design justification criteria for DBEs bounds that for operational basis events.

16.7.4.1 Dead Loads (D) and Liquid Loads (F)

Dead loads arising from small items of equipment are addressed by uniformly distributed loads derived using conservative assumptions. Specific large-item loads are included when appropriate; e.g., the dead load from the vertical support to the steam generator (SG). These loads are recorded in the appropriate design specifications as explained in Section 16.7.1 above.

The Civil/Structural Design Criteria report (Reference 16.6) provides information on the dead loads and liquid loads (combined and factored as if they were dead loads). Dead loads include all permanent piping and equipment loads. The following loads are summarised in Reference 16.6:

- Section 5.2.1 presents the dead loads considered generally for the design of the civil engineering structures. The weight of normal concrete is taken as 23.6 kN/m^3 (150 lb/ft3).

- Appendix A identifies the additional uniform loads included to cater for the dead loads from permanently attached small items of equipment appropriate for the design of the turbine building.

- Appendix B identifies the hydrostatic loads to be considered in the design of the in-containment structures that account for the water inventory and its location during various plant operations.

- Appendix C identifies the hydrostatic loads to be considered for the structural design of the fuel handling area.

- Section 5.2 indicates that differential settlement is included as a dead load for the design of C-I steel structures.

16.7.4.2 Live Loads (L)

Live loads include snow loading, movable equipment loads, and other loads that vary in intensity and occurrence. Live loads arising from small items of equipment are frequently addressed by uniformly distributed loads derived using conservative assumptions. Specific large-item live loads are included; e.g., the live loads associated with operation of refuelling equipment. These loads are recorded in specifications as explained in Section 16.7.1.

The following loads are summarised in Reference 16.6:

- Section 5.2 identifies the live loads considered generally in the civil engineering design. Tables 16-4 to 16-7 of this chapter present these in metric units.

- Appendix A identifies the live loads specific to the turbine building.

- Appendix B identifies the live loads specific to the in-containment structures.

- Section B.4 of Appendix B identifies that loads due to operation of the spargers are addressed as live loads (the operation of the spargers and the resulting automatic depressurisation system (ADS) load cases, ADS1 and ADS2, are also explained in this section, together with an explanation of how these loads are combined with seismic loads).

- Section 5.2.2 (E) identifies that loads occurring during construction are temporary live loads. Section 5.2.8 of Reference 16.6 identifies that stresses are increased by a third for such temporary live loads.

16.7.4.2.1 Concrete Placement Loads

Information on wet concrete placement loads acting on the steel faceplates to the walls of the structural modules is provided below (Reference 16.46). An explanation is provided as to why the resulting stresses are not combined with the stresses associated with post construction load combinations.

The steel faceplates of the structural wall modules, designed for the hydrostatic pressure of the concrete, act as concrete forms. The concrete placement loads are 1050 pounds per square foot determined in accordance with ACI-347. The bending stress in the faceplate due to this hydrostatic pressure of the concrete is approximately 89.63 MPa (13 ksi), based on the assumption of a continuous faceplate, or 137.89 MPa (20 ksi) based on the assumption of simple spans. The minimum yield strength of material for the faceplates is 344.74 MPa (50 ksi). The stress is well below the allowable, since the plate is designed to limit the out-of-plane deflection. After the concrete has gained strength, these stresses remain in the steel; however, since the average residual stress is zero and since the concrete no longer requires hydrostatic support, the ultimate strength of the composite section is not affected, and the full steel plate is available to carry other loads as described below.

The steel plates and the concrete act as a composite section after the concrete has reached sufficient strength. The composite section resists bending moment by one face resisting tension and the other face resisting compression. The steel plate resists the tension and behaves as reinforcing steel in reinforced concrete. The composite section is underreinforced so that the steel would yield before the concrete reaches its strain limit of 0.003 in/in. As the steel faceplates are strained beyond yield to allow the composite section to attain its ultimate capacity, the modest residual bending stress from concrete placement is relieved, since the stress across the entire faceplate in tension is at yield. The small residual strain induced by the concrete placement loads is secondary and has negligible effect on the ultimate bending capacity of the composite section. The stresses in the faceplates resulting from concrete placement are therefore not combined with the stresses in the post-construction load combinations.

16.7.4.3 Static Earth Pressures (H)

Static earth pressures are evaluated using standard geotechnical relationships; soil profiles consistent with those assumed in the seismic design are used. Static earth pressures are

combined and factored in the same way as live loads. When considering sliding stability, resistance is considered to be provided by sliding resistance at the bottom of the basemat with no account taken of passive soil resistance.

16.7.4.4 Normal Operating Loads (To) and Equipment Reactions (Ro)

Normal operating live loads comprise thermal loads (To) and their effects, plus piping and equipment reactions (Ro). These are assigned the maximum values associated with normal operations or shutdown conditions, based on the most critical transient or steady-state condition. Operating loads of a minor nature are addressed within the uniformly distributed loads, derived using conservative assumptions. Specific operating loads are included when appropriate and for all large items of equipment such as the frictional loads, associated with thermal expansion, at the supports to the major vessels. These loads are recorded in specifications as explained in Section 16.7.1.

The approach for determining the operating thermal loads is presented in Reference 16.6, Section 5. Reference 16.6, Section 10.3 indicates that thermal analyses are performed to evaluate the effects of thermal gradients. Reference 16.6, Section B.4 identifies the normal thermal loads addressed within the design of the in-containment structures. Reference 16.6, Sections C.3 and C.4 identify the normal thermal conditions addressed by the design for the fuel handling area structures. ADS1 leads to hydrodynamic loads on the boundaries to the in-containment refuelling water storage tank (IRWST). Section 16.7.4.2 above identifies that these loads, arising as a result of operation of the spargers, are considered to be live loads (L). Reference 16.6, Appendix B indicates that ADS2 leads to temperature transients that affect the boundaries to the IRWST. These temperature transients are considered as a normal thermal load (To).

16.7.5 Loads Arising from Internal Plant Faults and Internal Hazards

Chapter 11 reviews all internal hazards, and from the findings presented in Chapter 11, it is concluded that flooding (including temperature effects), internal missiles, dropped loads, explosions, fire and postulated PPF are considered in the civil engineering design, either in applicable load combinations or on a case-by-case basis

Building collapses are also a potential internal hazard catered to by designing the buildings so that their responses to hazards will not lead to any adverse response to the Class 1 equipment located in the nuclear island.

It is possible for an item of equipment to experience loads in excess of normal loads as a result of an internal plant fault. Such accidents are considered in load combinations where margins are substantially reduced because of the low frequency of such postulated events. For instance, when designing concrete, all load factors may be reduced to unity with the exception of accident pressure (Pa) (Reference 16.6, Table 3).

16.7.5.1 Temperature Effects (T_a)

The barrier matrix (Reference 16.9) identifies the temperature ranges for compartments within the nuclear island that are addressed in the design of the walls and slabs forming the compartment. Reference 16.6, Section 10.3, identifies the thermal analyses to be undertaken to evaluate the effects of thermal gradients. Reference 16.6, Section B.4, identifies the accidental thermal transients addressed by the design of the in-containment structures. Reference 16.6, Appendix C.5, identifies the accident thermal conditions addressed by the design for the fuel handling area structures.

16.7.5.2 Flooding (D and L)

Table 11-1 identifies the compartments within the nuclear island for which flooding is a potential internal hazard. For each compartment, the potential maximum depth of stagnant water as a result of an abnormal operational occurrence is given. Reference 16.6, Section 5.2, identifies that liquid loads are treated as dead loads (D), except for external pressures from groundwater, which are treated as live loads (L).

Site flooding could also affect equipment if it is located below the site flood level. The design of the basement walls to withstand extreme flood loads and the provision of a watertight barrier up to plant grade level, which is above the maximum design site flood level, ensure that flooding of the nuclear island from external sources does not occur.

16.7.5.3 Postulated Pressure Part Failure and Other Accidents (P_a, T_a, R_a, Y_r, Y_j, and Y_m)

Pressure part failures for which it is considered reasonable to postulate failure are all associated with the rupture of piping. Other accidents that can cause accidental loads to be applied to the civil engineering structures arise from loss of cooling accidents (LOCA) and safety relief valve (SRV) operation. These postulated accidents lead to the types of load described in the following sections.

Accident Pressure Load (P_a)

A postulated pipe break can lead to a differential pressure across a subcompartment, compartment, or building wall or slab. Determination of the pressure loads (including dynamic effects) is discussed in Reference 16.10. [

]

Accident Thermal Load (T_a)

The civil engineering design considers thermal loads as a result of temperature gradients caused by postulated pipe breaks. Determination of subcompartment temperatures is discussed in Reference 16.10. Accidental thermal transients addressed by the design of the in-containment structures are presented in Reference 16.6, Section B4. Accidental thermal conditions addressed by the design of the fuel handling area structures are presented in Reference 16.6, Section C5.

Accident Pipe Reaction (R_a)

Piping and equipment reactions generated by the postulated break including Ro (see Section 16.7.4.4) are considered under thermal conditions. The determination of pipe reactions generated by postulated breaks is discussed in Reference 16.10.

Reaction from Pipe Rupture (Y_r)

Loads on structures generated by the reactions from the broken high-energy pipe during a postulated break are addressed by the civil engineering design. Determination of the loads is discussed in Reference 16.10 which indicates that pipe whip restraints are provided when appropriate to transfer the restraint load to the main civil engineering structure.

Jet Impingement (Y_j)

Jet impingement loads on the structure generated by a postulated break are addressed by the civil engineering design. Determination of the loads is discussed in Reference 16.10 which indicates that barriers and shields are provided to protect against the effects of jet impingement resulting from postulated pipe breaks.

Missile Impact Load (Y_m)

Missiles can be generated as a result of a postulated break, which is addressed in a way similar to impact from pipe whipping. Determination of the loads is discussed in Reference 16.10.

16.7.6 Loads from External Hazards

Table 16-3 presents the parameters associated with external hazards and ground conditions applied to the design of the plant. UK site-specific studies should demonstrate that these parameters envelope conditions at UK sites.

16.7.6.1 Wind and Hurricanes (W)

The approach followed for determining the wind and hurricane forces on structures is explained in Reference 16.6, Section 5.2.3 and in Reference 16.12. Table 16-3 presents the loads addressed by the design.

16.7.6.2 Tornadoes (W_t)

The approach followed for determining the tornado effects on C-I structures is explained in Reference 16.6, Section 5.2.33 and in Reference 16.12. Table 16-3 presents the loads addressed by the design.

For C-II structures, the approach is modified as indicated in Reference 16.6, Section 6.2.1. The approach for the seismic category NNS turbine building structures (identified as C-III structures in Reference 16.6) is presented in Reference 16.6, Section 6.3.2. It is acceptable for external cladding, when provided, to be blown off a building; however, other structural elements forming the building envelope, such as reinforced concrete walls and roofs, are designed to withstand tornado loading as explained in Reference 16.6, Section 6.2.1.

16.7.6.3 Missiles

The approach to missile protection against externally and internally generated missiles is presented in Reference 16.6, Section 4.3. Table 16-3 presents the loads addressed by the design. Tornado missile loads (W_m) are combined with tornado wind loads (W_w) and pressure differential loads (W_p) as shown in Reference 16.12.

16.7.6.4 Water Level (Flood) Design

The plant is to be sited at a level so that flooding resulting from an event external to the plant site is no more severe than an onsite flooding event as discussed in Section 16.7.5.2. The determination of this level is a site-specific issue. It is also for the site-specific safety case to present the arguments that adequate margins exist with respect to flooding from sources external to the site (i.e., there are no step changes in consequences as a result of slightly lower frequency events than the DBEs).

16.7.6.5 Temperatures

The external building temperatures addressed when considering internal plant faults and internal hazards take into account the extreme temperatures presented in Table 16-3. It is for the site-specific cases to demonstrate that the temperatures considered envelope the extreme temperatures at the site, taking into account such factors as global warming, elevation, solar gain, and location in the UK.

16.8 SEISMIC ANALYSIS

16.8.1 Input Motions for Seismic Analysis of Category I and II Structures (E_s)

The seismic input motion used for the standard plant seismic design and analyses for C-I and C-II structures is explained in Chapter 12. The SSE is the CSDRS with peak vertical and horizontal ground accelerations set at 0.3g. References 16.7 and 16.32 describe the derivation of the CSDRS together with the justification of the design time histories produced to represent the CSDRS. The CSDRS is a free field ground response spectra applied at finished grade level (Reference 16.6, Section 2.2).

As the specific UK sites where plants might be located have not been determined, C-I and C-II structures have been analysed for the SSE for six possible soil profiles. The intention is that licence applicants will demonstrate that the ground conditions at a particular site are bounded by the soil profiles assumed in the analysis or alternatively that the design analyses utilising seismic demands developed for the UK site-specific conditions meet applicable codes and standards.

16.8.2 Analysis of Seismic Category I and II Structures

The structures that make up the nuclear island are all C-I. Reference 16.32 summarises the types of models and analysis methods used in the seismic analyses of the nuclear island, as well as the type of results obtained and where they are used in the design. This is discussed further in Section 16.8.3 below.

The first bay of the turbine building and the multi-storey portion of the annex building adjacent to the nuclear island are C-II structures. Reference 16.7 presents details of how these were modelled and analysed. Enveloped foundation response spectra were developed using results from the Soil Structure Interaction (SSI) studies summarised in Reference 16.32.

Seismic analyses are undertaken using appropriate analysis methods. Reference 16.32 describes the role of each of the analysis methods and the important assumptions. The analyses determine the seismic force distribution for use in the design of the nuclear island structures and in-structure seismic responses (accelerations, displacements, and floor response spectra). In-structure seismic responses are used for the analysis and design of seismic subsystems, when more detailed local evaluations of seismic responses are undertaken. Details of the computer modelling and methods followed are provided in Reference 16.32. Fluid and structure interaction effects are allowed for in the design. The criteria for determining the live loads to be taken as present in the seismic analysis are presented in Reference 16.6, Section 5.2.4.1.

When undertaking SSI, as described in Reference 16.32, it is impractical to include detailed representation of all of the nuclear island structural elements. Some floor slabs, walls, miscellaneous steel platforms, and framings are analysed as subsystems. Reference 16.7

describes the procedures and methods used when seismically analysing such civil engineering subsystems.

Exterior walls, below grade, are designed for two cases: first for dynamic earth pressures calculated in accordance with ASCE 4-98 (Reference 16.18), and second to resist full passive earth pressure.

Seismic loads are combined with other loads as shown in Reference 16.6, Tables 3 to 6.

16.8.3 Nuclear Island Seismic Analysis Models

An overview of some of the important features of the seismic analysis and reference to additional reports that present more detailed information is provided in Reference 16.32. The important models, which vary in complexity, are summarised below:

- **NI10 Dynamic Model** – This model was used for an ANSYS fixed-base finite element time history analysis undertaken to determine time histories at important locations in the structure. Substructuring was used to reduce the computer analysis time. The mesh finite element size used was typically about 3 m (10 feet).

- **Nuclear Island Stick Model** – Stick models were used for SSI sensitivity studies using the SASSI software. Six different ground conditions were analysed: a hard rock site and five sites with different ground stiffnesses as identified in Reference 16.32. The presence of adjacent buildings was investigated and it was concluded that the effects of these on the nuclear island seismic response was small; therefore, subsequent 3-D SASSI computer analyses of the nuclear island were performed with adjacent buildings excluded. A stick model was also used to investigate the effects of foundation liftoff from the underlying subgrade. This was found to increase the subgrade pressure by a maximum of 4 to 6 percent close to the west edge of the basemat, with insignificant effects beneath the rest of the basemat.

- **NI20 Dynamic Model** – This model has fewer nodes and elements than the NI10 model, with a typical finite element mesh size of about 6.1 m. Based on this model, 3-D SSI analyses were undertaken using the SASSI software, again for five different soil profiles. Acceleration time histories and floor response spectra were obtained. In addition, this model was used to determine the maximum bearing pressure, which occurred for the hard rock condition.

- **NI05 Static Model** – This model has more nodes and elements than the NI10 model with a typical finite element mesh size of about 1.4 m (5 feet). This model was used to calculate design member forces and moments using response spectra analysis.

Justification of structural elements proceeds at the following three levels:

- Level 1 determines the enveloping seismic response for the nuclear island structures taking into account SSI.

- Level 2 uses the more detailed NI05 model to evaluate element/member forces and deformations using the Level 1 response spectra.

- Level 3 applies appropriate design code clauses to the Level 2 force actions (i.e., axial tension/compression, in-plane and out-of-plane shears, torsions, and out-of-plane moments – including interactions of these effects) to evaluate capacity margins.

The standard plant dynamic analyses generate one set of in-structure responses for each soil profile. These in-structure responses are enveloped to obtain the seismic design envelope (design member forces, nodal accelerations, nodal displacements, and floor response spectra), which are used in the standard plant design and analysis of C-I structures, components, and seismic subsystems to ensure high confidence that a safe plant may be constructed at a specific site. Seismic in-structure spectra are given in Reference 16.32 for the following six key locations:

- Containment internal structures at the reactor vessel supports, elevation of 100 m (100'-0").
- Containment internal structures at the operating deck level, elevation of 110.44 m (134.25').
- Auxiliary shield building northeast corner at the control room floor level, elevation of 105.03 m (116.5').
- Auxiliary shield building at the corner of fuel building roof, elevation of 124.14 m (179.19').
- Auxiliary shield building roof area, elevation of 169.31 m (327.41').
- Steel containment vessel adjacent to the polar crane, elevation of 137.80 m (224').

16.8.4 Seismic Input Motions and Seismic Analysis of Category NNS Structures (Eq)

Seismic category NNS structures are analysed using the seismic methods in UBC 1997 (Reference 16.17). Further supplementary requirements are presented in Reference 16.6, Section 6.3.1. Section 16.4.2 of this chapter identifies the seismic input motions against which seismic category NNS structures have been justified. Seismic loads are combined with other loads as shown in Reference 16.6. Reference 16.6 (Section 5.2.4.1, Tables 7 and 8) identifies that seismic category NNS structures do not need to be designed for an earthquake vertical component.

Note that the NNS structures are being redesigned and the seismic analyses will use UK methodology to provide margin similar to that provided by the US codes.

16.9 DESIGN REQUIREMENTS OTHER THAN STRENGTH

16.9.1 Water Retaining Barriers

Reinforced concrete walls and slabs designed to ACI 349-01 (Reference 16.15) may not provide a watertight boundary as there is potential for water to flow through small cracks and joints formed during construction. To ensure a watertight boundary when one is required, an additional waterproof layer is provided. The passive containment cooling water storage tank (PCCWST) is provided with a leaktight stainless-steel barrier. A waterproof membrane is provided around the basemat to the nuclear island; this will be a site specific design. Walls and floors of the in-containment structures and auxiliary building internal structures exposed to water are constructed using stainless-steel plate. Leak chases are provided for pools inside containment and in the auxiliary building that are filled with borated water. The leak chases are provided to prevent borated water from getting behind the various pool liner plates and potentially corroding the structural elements behind the pool liners. The leak chases for the pools inside containment are part of the liquid radwaste system (WLS). The leak chases for

the pools outside of containment are part of the radioactive waste drain system (WRS). Reference 16.14 describes a leakage assessment and potential corrosion impact of leakage from the pools within the fuel handling area on the associated structure. This document also presents evidence that the current design of the AP1000 plant fuel handling provides capabilities of detecting a long term leak from the pools, pits and canals within the fuel handling area.

Some floor slabs in the nuclear island might become flooded as a result of an accident. The use of structural floor modules and metal decking to support the weight of wet concrete during construction provides confidence that any leakage through these slabs would be insignificant and would not be detrimental to Class 1 equipment.

16.9.2 Deflection Limits

Reference 16.6, Section 11.3, presents the deflection limits applied to different structural elements as part of the design.

16.9.3 Separation between Buildings

Reference 16.6, Section 12, presents the criteria followed for determining the gaps between building superstructures.

16.9.4 Doors within Walls Required To Act as a Barrier

The approach to doors within walls, excluding those in the containment vessel wall, required to act as a barrier is explained below:

- Doors are not generally designed to retain water, because under accident conditions it is assumed that water will flow under the door.

- Doors are not generally designed to resist pressures from accidental pressure releases. Such pressures will quickly diminish with distance. On a case-by-case basis, it is considered whether a door could act as a missile and whether a target exists with a safety function, or if a door can be challenged by a DB externally generated pressure pulse. If necessary, protection is provided.

- Exterior doors to the annex building and first bay of the turbine building are designed to withstand either wind loading or hurricane loading appropriate to the building barrier through which they pass.

- There are no exterior doors to the shield building or the auxiliary building. Access to the nuclear island is only via the buildings that surround the nuclear island. The doors leading into the nuclear island are typically heavy-duty security doors. On a case-by-case basis, it is considered whether one of these doors could act as a missile and whether a target exists with a safety function. If necessary, missile protection is provided.

16.9.5 Fire Resistance

Chapter 11 describes the internal fire hazards analysis. The AP1000 design civil engineering structures have been justified as either meeting or exceeding the fire resistance requirements for internal fires.

16.10 SHIELD BUILDING

The shield building, including its significant features, is described in Reference 16.3. The shield building, shown in Figure 16-4 of this chapter, is a C-I structure that provides shielding, protects the containment from external DBEs, and has functions associated with the design of the passive containment cooling system (PCS). The cylindrical shield building surrounds the containment vessel and shares a common basemat with it and the auxiliary building. A light coloured coating is provided on the exterior portions of the SC structure of the shield building. The cylindrical section of the shield building structurally supports the roof and the PCCWST. From a structural perspective, the shield building includes a number of key structural features as shown in Figure 16-3. The shield building design is extensively described and justified in Reference 16.3.

16.10.1 Shield Building Key Structural Features

16.10.1.1 Shield Building Cylindrical Wall

The cylindrical wall has a nominal outside radius of 22.1 m (72 feet) and thickness of 0.91 m (3 feet). This wall is generally constructed using SC construction. SC construction comprises two external 19-mm (0.75 inches) steel plates forming permanent shutters that act compositely with the concrete poured between them. The cylindrical wall section below the auxiliary building roof line on the west side of the plant is constructed using conventional reinforced concrete.

The concrete used for the SC-constructed walls is either standard concrete or self-consolidating concrete based on the region of the building and constructability assessments. The faceplates are made of American Society of Testing Materials (ASTM) A572 Grade-50 steel, which acts as concrete reinforcement. The thickness of the steel faceplate precludes failure modes such as thermal, creep, and fatigue. The material specification was chosen to improve the overall strength and ductility of the SC portion of the structure so that the design capacity has significant margin when compared with demand during DBEs. The SC is made fully composite by the provision of 152-mm-long (6 inches), 19-mm-diameter (0.75 inches) [ ] shear studs welded to the inner surfaces of the faceplates and 19-mm-diameter (0.75 inches) [ ] reinforcement tie bars that are welded at both ends to the faceplates and pass through the concrete core. The SC construction form is shown in Reference 16.3, Figures 3.1-1 and 3.1-2. In locations along the edges of the panels (Reference 16.3, Figure 3.1-2), tie bars may be mechanically connected, or replaced with pairs of deformed hooked bars or T-headed bars connected to opposing sides of the panels. The use of hooked bars, T-headed bars or mechanically connected tie rods facilitates alignment of panels for welding. These alternate connections provide shear capacity between the face plates and concrete at least equal to the shear capacity of the tie bars.

16.10.1.2 Steel-Concrete Composite/Reinforced Concrete Connections

Where the shield building connects to the auxiliary building, specially designed connections are provided. To ensure continuity between reinforced concrete and SC construction, the steel plate modules are anchored to the reinforced concrete basemat and walls by mechanical connections. The connectors provide for the direct transfer of forces from the reinforcement in conventional reinforced concrete to the SC faceplates.

At the horizontal connection that occurs on the bottom of the lowest SC section, each vertical reinforcing bar in the reinforced concrete basemat or wall is connected to a mechanical coupler. A similar vertical connection occurs on the vertical edges of panels that interface with the reinforced concrete portion of the shield building wall. In the vertical connection, forces are transferred directly from the hoop bars to the SC faceplate via mechanical couplers. At the junction between the roof and the tension ring of the shield building, a specially designed cap connection is provided. It transfers forces from the reinforcement in the reinforced concrete section into reinforcement couplers and thence into a steel-plated composite section contiguous with the tension ring beam.

The mechanical connections are designed for tension loads of 125 percent of the yield strength of the reinforcing bars in accordance with ACI 349-01. The design of each SC to reinforced concrete connection is presented in Reference 16.3, Section 4.2. Using mechanical connectors ensures the integrity of the reinforced concrete/SC connections under cyclic loading and improves the overall ductility of the connection zone so that the structure behaves in a ductile manner under seismic events.

Benchmarked nonlinear analyses were performed on the shield building anchorages and roof anchorage connections. This is presented in Reference 16.3, Section 10. The benchmarked nonlinear analyses demonstrate significant margin over and above that demonstrated in the linear elastic analyses. Benchmarked Level 2 and 3 analyses were performed to demonstrate the system strength and ductility, both at the global level (Level 2) and at the component level (Level 3). In all cases, the analyses demonstrate large margins and sufficient ductility.

16.10.1.3 Air Inlet Structure and Tension Ring

The air inlet structure is located at the top of the cylindrical wall portion of the shield building. The air inlets serve as the intake for air used as the means for transferring heat as part of the PCS. The air inlet structure is similar in form to the cylindrical wall SC construction, but the overall wall thickness is increased to 1.372 m (4.5 feet)and steel faceplate thicknesses are increased to 25.4 mm (1 inch).

Composite action is provided solely by closely spaced 19-mm-diameter (0.75 inches) tie bars between the faceplates. [ ] shear studs are not used in this instance. The air vents cast-in to the concrete core are formed using 457-mm-diameter (18 inches) carbon steel pipes with [ ] shear connectors on the outer pipe surface. Above the air inlet structure is the region designated as the tension ring that supports the conical roof. The tension ring comprises a SC box girder with 38-mm-thick (1.5 inches) webs and flanges stiffened with internal diaphragms. Composite action between the internal concrete and external steel plating is provided by 19-mm-diameter (0.75 inches) [ ] shear connectors. The contribution of the concrete has been conservatively ignored in deriving the strength of the box girder to ANSI/AISC-N690-1994 (Reference 16.24) code provisions. The tension ring also contains 32 radial beam connections where the radial beams that support the conical roof are connected. These details can be seen in Reference 16.3, Figures 5.1-1 to 5.1-7.

The air inlet structure is sized as a reinforced concrete member equivalent to a cylindrical shell with openings in accordance with ACI 349-01 guidelines assuming conservative section properties for the walls. The air inlet pipes are not credited in the air inlet structure design analyses. Shear studs are welded to the outside surface of the air inlet pipes so that they contribute to composite action and provide additional margin for out-of-plane shear resistance. The design adequacy of the tension ring girder steel plates and the air inlet plates is verified by calculating stresses using detailed finite element models of these components (Reference 16.3, Section 10) at critical sections for the load combinations from the Level 2

analyses member forces and comparing them with ANSI/AISC-N690-1994 (Reference 16.24) allowable stresses. The comparison is presented in Reference 16.3, Sections 5.2.4 and 5.2.5, and shows that significant margins are provided for each component.

16.10.1.4 Shield Building Roof including Compression Ring and Knuckle Region

The roof is a conical shell supporting the PCCWST and air diffuser. Reference 16.3, Section 6.2 presents the detailed methodology for the analysis and design of the shield building roof structure, and the structural steelwork and reinforced concrete details in Figures 6.1.4 to 6.1.6.

16.10.1.5 Passive Containment Cooling System Water Tank

The PCCWST, located above the roof of the shield building, has a stainless-steel liner that provides a leak tight barrier on the inside surfaces of the tank. Its wall liner consists of a plate with stiffeners on the concrete side of the plate. The floor liner is welded to steel plates embedded in the concrete with leak chase channels provided over the liner welds. The liner for the PCCWST is analysed by hand-calculation. The design considers construction loads during concrete placement, loads due to handling and shipping, normal loads including thermal, and the SSE. Buckling of the liner is prevented by anchoring it using the embedded stiffeners and welded studs. The liner is designed as a C-I steel structure.

16.10.2 Analysis and Design Justification for the Reinforced Concrete Construction of the Shield Building

The nuclear island must be analysed as a whole to capture the complex load distributions through the basemat, walls, and slabs of the shield building and auxiliary building. The seismic analyses of nuclear island computer models are discussed in Section 16.8.3. Reference 16.3, Section 6.2, provides information on the design and analysis procedures followed for the RC portions of the cylindrical wall and for the shield building roof.

16.10.3 Analysis and Design Justification of Steel-Concrete Composite Construction for the Shield Building

Reference 16.3 reports that the SC construction justification has been established through extensive testing and international experience. The detailed information in Reference 16.3 demonstrates that SC construction for the shield building can be substantiated conservatively using reinforced concrete code provisions with longitudinal shear transfer between the steel faceplates and concrete core designed in accordance with provisions of ANSI/AISC-N690-1994 (Reference 16.24).

The shield building was analysed using detailed finite element models. Both linear elastic analyses and nonlinear analyses were performed to confirm that the load distribution does not lead to significant cracking and to confirm that the shield building behaves as a monolithic structure. The analyses demonstrated that a margin exists when the shield building is subjected to BDB earthquake loadings. Reference 16.3, Section 3.3 presents nonlinear analyses for the SC modules, which demonstrate that buckling, creep, and shrinkage are not significant effects with regard to the design. Thermal analysis was also performed to quantify the effect of daily and seasonal thermal cycles on the cylindrical wall and the effect of cracking due to thermal gradients.

To provide further assurance about the AP1000 structures, a combination of testing and analysis was performed to confirm the structural adequacy of the design. The confirmatory

research programme comprised seven different types of tests to demonstrate the adequacy of the design approach and to address regulatory concerns on shear strength and ductility provision. The scope of the tests was formulated to confirm the assumed behaviour of the shield building SC construction used in analysis and design as follows:

- Out-of-plane shear without tension to demonstrate that the provisions given in ACI 349-01 for the shear strength of reinforced concrete beams are conservative.
- Out-of-plane shear with tension to demonstrate that axial tension will not significantly affect the ACI strength prediction.
- Cyclic out-of-plane shear to demonstrate ductility.
- Push-out samples on panels to demonstrate the effectiveness of the composite behaviours of the SC structures for both shear connectors and tie bars.
- Weld fatigue tests on tie bars to the steel faceplates to confirm that the fatigue life can meet the anticipated number of stress cycles.
- Cyclic in-plane shear to demonstrate that shear strength of SC can be conservatively estimated using ACI code provisions for reinforced concrete walls as well as ductility requirements.
- Anchorage in the concrete to demonstrate the strength of the reinforced concrete/ SC connection in tension.

The programme was carried out at Purdue University and the tests were fully instrumented to record their behaviour through the loading sequence to destruction so that this could be captured in the nonlinear analyses. The results effectively demonstrate that the ACI 349-01 code provisions for reinforced concrete nuclear structures are conservatively applicable to the SC design of the shield building. The tests results presented in Reference 16.3, Section 7 demonstrate the robust behaviour of the SC structural components in the AP1000 design.

The nuclear island is substantiated using three levels of analysis as identified in Section 16.8. For the shield building SC construction, each level of analyses is verified using two separate approaches (standard and confirmatory). The standard approach uses simpler analytical techniques and design code provision; the confirmatory approach uses benchmarked nonlinear material properties to examine the effects of cracking and local yielding in critically loaded elements to ensure robustness in the design and to confirm that a significant design margin is achieved.

The confirmatory tests at Purdue University are used in the benchmarking of the nonlinear analyses presented in Reference 16.3, Section 8. Examination of the conservatisms associated with the analyses and design assumptions of the shield building (Reference 16.3, Sections 11.1 and 11.2) shows that the design has reserve strength that provides seismic margin above the review-level earthquake. The analyses presented in Reference 16.3, Section 11.3 show that the seismic high confidence of low probability of failure (HCLPF) value is above the review-level earthquake value of 0.5g. The standard seismic margin calculations are based on conservative design loads.

16.10.4 Containment Air Baffle

The containment air baffle is located within the upper annulus of the shield building, providing an airflow path for the PCS as shown in Figure 6-5. The functional requirements are specified in Reference 16.47. The air baffle separates the downward airflow entering at the air inlets from the upward airflow that cools the containment vessel and flows out of the discharge stack. The air baffle is a seismic C-I structure and includes the following sections:

- A wall supported off the shield building roof
- A series of panels attached to the containment vessel cylindrical wall and the knuckle region of the dome
- A flexible seal closing the gap between the wall and the panels fixed to the containment vessel, designed to accommodate the differential movements between the containment vessel and shield building
- Flow guides attached at the bottom of the air baffle to minimize pressure drop

The air baffle is designed to meet the following functional requirements:

- The baffle and its supports are configured to minimize pressure losses as air flows through the system
- The baffle and its supports have a design objective of 60 years
- The baffle and its supports are configured to permit visual inspection and maintenance of the air baffle as well as the containment vessel. Periodic visual inspections are primarily to inspect the condition of the coatings
- The baffle is designed to maintain its function during postulated design basis accidents
- The baffle is designed to maintain its function under specified external events including earthquakes, hurricanes, and tornadoes

The integrity of the steel structure has been demonstrated by applying the criteria presented in ANSI/AISC-N690-1994 (Reference 16.24).

16.11 AUXILIARY BUILDING

The auxiliary building is a C-I structure, forming part of the nuclear island, which houses the Class 1 equipment that is outside the shield building.

The layout of the auxiliary building and its interface with the other buildings of the nuclear island is shown in figures in Reference 16.2. The following are the principal systems and components of the auxiliary building:

- Main control room (MCR)
- Remote shutdown room
- Class 1 dc switchgear
- Class 1 batteries
- Reactor trip switchgear
- Reactor coolant pump trip switchgear

- Main steam and feedwater piping
- MCR heating, ventilating, and air conditioning (HVAC)
- Class 1 switchgear rooms' HVAC
- Spent fuel pool (SFP)
- Fuel transfer canal
- Cask loading and washdown pits
- New fuel storage area
- Cask handling crane
- Fuel handling machine
- CVS makeup pumps
- Normal residual heat removal system (RNS) pumps and heat exchangers
- Liquid radwaste tanks and components
- Spent fuel pool cooling system
- Gaseous radwaste processing system
- Mechanical and electrical containment penetrations

16.11.1 Structural Description

The auxiliary building is a reinforced concrete and structural steel structure. Three floors are above grade and two are located below grade. It is one of three buildings that make up the nuclear island and shares a common basemat with the containment vessel and the shield building.

The auxiliary building is a C-shaped section of the nuclear island that wraps around approximately 50 percent of the circumference of the shield building. As noted in the description of the shield building above, the floor slabs and the structural walls of the auxiliary building are structurally connected to the cylindrical section of the shield building.

Structural modules are used for part of the south side of the auxiliary building using SC construction similar to that used in the construction of the shield building cylindrical wall. Reference 16.38, Figure 4 shows the location of the structural modules. The thickness of the structural wall modules ranges from 762 to 1524 mm (30 to 60 inches) for the key structural walls. The auxiliary building modules also include smaller structural walls that act as labyrinth walls or barrier access walls with thicknesses less than 762mm (30 inches). Local variation in the design of the trusses and spacing of the trusses and shear studs may be required to address internal obstructions and accessibility for fabrication and inspection. The minimum thickness of the faceplates is 12.7 mm (0.5 inch). Portions of the faceplates are thicker than the nominal design thickness to provide strength for localized loads due to attachments and connections. The auxiliary building modules are placed on the nuclear island basemat. A typical connection is shown in Reference 16.4, Figure 3-6. The SC structural modules used in the construction of the auxiliary building and the in-containment structures are termed CA modules. The largest CA module is CA20, which is approximately four storeys high and weighs about 1000 tonnes (2,200,000 pounds) when it is lifted into position before concrete is placed between the steel faceplates.

CA20 is a large portion of the fuel handling area in the radiological controlled portion of the auxiliary building. The fuel handling area provides for transferring new fuel assemblies from the auxiliary building rail car bay to and from the new fuel storage area to the containment building, and for transferring spent fuel assemblies from the containment building to the spent fuel storage pit within the auxiliary building. The spent fuel storage facility is designed to the guidelines of ANS 57.2 (Reference 16.43). The spent fuel storage facility is located

within the seismic C-I auxiliary building fuel handling area. The walls of the SFP are an integral part of the auxiliary building structure.

The SFP provides storage space for the spent fuel. The spent fuel storage racks are designed as seismic C-I equipment. Additionally, the racks are evaluated for uplift loads, fuel assembly drop accidents, and live loads due to lifting.

The fuel handling area provides the means for removing the spent fuel assemblies from the spent fuel storage pit and loading the assemblies into a shipping cask for transfer from the facility.

The fuel handling area is protected from external events such as tornadoes and tornado-produced missiles. Protection is provided for the spent fuel assemblies, the new fuel assemblies, and the associated radioactive systems from external events.

The new fuel storage area is a separate reinforced-concrete pit providing temporary dry storage for the new fuel assemblies.

A cask handling crane travels in the east-west direction. The location and travel of this crane prevents it from carrying loads over the SFP, thus preventing crane loads from falling into the SFP.

The non radiological portion of the auxiliary building contains the MCR, remote shutdown room, and Class 1 electrical and control and instrumentation (C&I) equipment rooms. The ceilings of the MCR and the C&I rooms are designed as finned floor modules. A finned floor consists of a 609.6-mm-thick (24 inches) concrete slab poured over a stiffened steel plate ceiling. The fins are rectangular plates welded perpendicular to the underside of the plate. Shear studs are welded on the upper side of the steel plate so that the steel and concrete act as a composite section. The fins are exposed to the environment of the room and enhance the heat-absorbing capacity of the ceiling. Several shop-fabricated steel panels, placed side by side, are used to construct the stiffened plate ceiling in a modular manner. The stiffened plate is designed to withstand construction loads from wet concrete.

16.11.2 Analysis and Design Justification of Auxiliary Building

The nuclear island must be analysed as a whole to capture the complex load distributions acting on the basemat, walls, and slabs of the shield building and auxiliary building. The seismic analyses of nuclear island computer models are discussed in Section 16.8.3 above. Reinforced concrete and structural steel are justified in design calculations for each structural element to the codes and standards identified in Section 16.5.1 to sustain the loads and effects specified in Sections 16.7 and 16.8. The general approach is described below for each type of structural element.

16.11.2.1 Shear Walls

Shear walls in the auxiliary building vary in size, configuration, aspect ratio, and the amount of reinforcement they contain. The stress levels in the shear walls depend on these parameters and the seismic acceleration level. Exterior shear walls are several stories high and do not have many large openings. Interior shear walls, however, are discontinuous in both vertical and horizontal directions. The in-plane behaviour of these shear walls, including the large openings, is adequately represented in the analytical models for the global seismic response. Where the refinement of these finite element models is insufficient for design of the reinforcement, for example, in walls with a large number of openings, detailed finite element models are used. The shear walls are used as the primary system for resisting lateral loads

such as earthquakes. The auxiliary building shear walls are also evaluated for flexure and shear due to the out-of-plane loads.

The auxiliary building shear walls are designed to withstand the loads discussed in Sections 16.7 and 16.8. Besides dead, live, and other normal operating condition loads, the following loads are considered in the shear wall design:

- Seismic loads
  - The SSE loads for the wall are obtained from the seismic analyses of the auxiliary building and shield building described in Section 16.8.3.
  - Calculations are performed by considering shear wall segments. Segments are rectangles bounded by the floors above and below each segment and perpendicular walls that define the sides of the segment. Appropriate boundary conditions are assumed for the four edges of the segment. The natural frequencies of wall segments are determined using finite element models or text book formulas for the frequency of plate structures. The corresponding spectral acceleration is determined from the applicable response spectrum.
  - Exterior walls, below grade level, are also evaluated for dynamic earth pressure exerted during an SSE for two cases: dynamic earth pressure calculated in accordance with ASCE 4-98 (Reference 16.18) and passive earth pressure.
- Accident pressure load
  - Shear walls of the MSIV rooms are designed for 41 kN/m^2 (6 psi) differential pressure acting in conjunction with the seismic loads. Member forces due to accident pressure and SSE are combined by absolute sum.
  - The MCR wall of the east MSIV compartment is evaluated for the pressure and the jet load due to a postulated main steam line break.
- Tornado load
  - Tornado loads are considered for exterior walls above grade level.

Reference 16.6 includes the design temperatures for thermal gradient and contains the load combinations for which the shear walls are designed, as applicable. The wall sections are designed in accordance with the requirements of ACI 349-01 (Reference 16.15).

16.11.2.2 Composite Structures (Floors and Roof)

The floors consist of a concrete slab on a metal deck, which rests on structural steel floor beams. Several floors in the auxiliary building are designed as one-way reinforced concrete slabs supported continuously on steel beams. Typically, the beams span between two reinforced concrete walls. The beams are designed as composite with formed metal deck spanning perpendicular to the members. Unshored construction is used. For the floors, beams are predominately spaced at about 1.5 to 1.83-m (4.92 to 6 feet) intervals and spans are between 4.6 and 7.6 m (15 and 25 feet). Based on local geometry considerations, the intervals and spans are outside these ranges in a limited number of locations. The spacing between the beams or between beams and walls is as small as 0.91m (3 feet) and as large as 2.44m (8 feet). The span of the beams is as small as 7.6m (25 feet) and as large as 11.7m (38.39 feet). The designs of the beams satisfy the requirements in AISC N690 for composite structures.

The metal deck rests on the top flanges of the structural steel floor beams with the longitudinal axes of the metal deck ribs and floor beams perpendicular to each other. The reinforcement size and spacing are based on loads and spans for this type of floor and are determined at each location based on the requirements in ACI 349-01 and ACI 318-11, Section 12.6. The development of the floor reinforcement in the walls can be either headed reinforcement or standard hooks. The beam size and spacing and beam support designs are based on loads and spans for this type of floor. The beam support designs include beam seats or shear plates connected to the web of the beam. The detail design of the support for the beam, including the portion embedded in the concrete wall, is based on the load and structural system configuration. The designs of these floors are in conformance with AISC N690 and ACI 349. The concrete slab is tied to a structural steel floor beam by shear connectors welded to the top flange of a floor beam. The concrete slab and the floor beams form a composite floor system. For the design loads after hardening of concrete, the transformed section is used to evaluate stresses.

The construction sequence is as follows:

- A section of structural steel floor (comprising a floor beam, metal deck, and shear connectors) is fabricated in the shop, brought to the floor location, and placed in position. In some cases, all the beams and deck are preassembled and placed as a module.

- The metal deck is used as the formwork, and concrete is poured on the metal deck. Until the concrete hardens, the load is carried by the metal deck and the supporting steel floor beams.

- During concreting, no shoring is provided.

The floor design considers the dead, live, construction, extreme environmental, and other applicable loads as identified in the civil structural design criteria (Reference 16.6). The design floor loading includes the equipment attached to the floor. The end conditions for the steel beams are simply supported or continuous as appropriate. The seismic load is obtained using the applicable floor acceleration response spectrum (7-percent damping for the SSE loads).

The load combinations applicable to the design of these floors are shown in Reference 16.6 for steel and reinforced concrete C-I structures. The design of the floor system is performed in two parts:

- Design of steel beams

  – The structural steel floor beams are evaluated to withstand the weight of wet concrete during the placement of concrete. The composite section is designed for the design loads during normal and extreme environmental conditions. Shear connectors are also designed.

- Design of concrete slab

  – The concrete slab and the steel reinforcement of the composite section are evaluated for normal and extreme environmental conditions. The slab concrete and the reinforcement are designed to ACI 349-01 (Reference 16.15).

  – The slab design considers the in-plane and out-of-plane seismic forces. The global in-plane and out-of-plane forces are obtained from the response spectrum analysis of the 3-D finite element model of the auxiliary and shield buildings. The out-of-plane

seismic forces due to the floor local responses are determined by hand calculations using the applicable vertical seismic response spectrum and slab frequency.

16.11.2.3 Reinforced Concrete Slabs

Reinforced concrete floors in the auxiliary building are either 610 or 915 mm (24 or 36 inches) thick. These floors are constructed with reinforced concrete placed on top of 203 to 305-mm-thick (8 to 12 inches) precast concrete panels. The precast concrete panels are installed at the bottom to serve as the formwork and withstand the weight of the wet concrete. The main reinforcement is provided in the cast-in-place concrete. Reinforcement is placed in both the top and bottom layers of the cast-in-place concrete in both directions. For the design of the reinforcement in the cast-in-place floors, post-construction loads are conservatively assumed to be resisted only by the cast-in-place concrete and the reinforcement placed within it. The reinforcement in the cast-in-place portion is fully developed into supporting adjacent walls such that the connection is assumed to be a fixed connection. The development of the floor reinforcement in the walls is achieved using either headed reinforcement or standard hooks.

The precast panels, which are connected to the concrete above by shear reinforcement, satisfy the requirements of ACI 349 Chapter 17. The precast panels and the cast-in-place concrete are made to act together as a composite reinforced concrete slab by roughening the top surface of the precast panel and providing shear ties between the two elements. The detail designs of the supports for the precast panels are based on the loading and design requirements.

The finite element analysis model used for the auxiliary building seismic response assumes a homogenous thickness of concrete for the floor system, and includes floor-to-wall connections that are fixed over the full thickness of the reinforced concrete floor. The detailed design of the floor system includes a gap between the precast panel and the wall and between adjacent precast panels. Although the gap between the precast panels and the wall reduces the thickness of the floor in direct contact with the wall, the design of the floor system satisfies the requirements of ACI 349, including fully developing the floor reinforcement in the wall. The design of the floor system and the connection with the wall provide a fixed connection that transfers forces and moments from the floor to the wall.

Detailed analysis of the floor system connection design details, including the gap between the precast panel and wall, is performed for the floor constructed with precast panels and is consistent with the nuclear island seismic model. The effects of stiffness, reinforcement anchorage, and concrete cracking are considered in the detailed analyses. The detailed analyses demonstrate that these floors have vertical response above 33 Hz and are rigid, which is consistent with the nuclear island seismic model.

16.11.2.4 Concrete Finned Floors

The ceilings of the MCR and C&I room in the auxiliary building are designed as finned-floor modules. A typical floor design is shown in Reference 16.38, Figure 3b. A finned floor consists of a 610–mm-thick (24 inches) concrete slab poured over a stiffened steel plate ceiling. The fins, welded to stiffen the steel plate, are rectangular sections perpendicular to the plate. Shear studs are welded on the other side of the steel plate to allow composite action of the steel and concrete. The fins are exposed to the environment of the room and enhance the heat-absorbing capacity of the ceiling. Several shop-fabricated steel panels, cut to room width and placed side by side perpendicular to the room length, are used to construct the

stiffened-plate ceiling in a modularised fashion. The stiffened plate with fins is designed to withstand construction loads prior to concrete hardening.

The MCR ceiling, comprising a finned floor, is designed for dead, live, and seismic loads.

The finned floor structure is evaluated for the load combinations referred to in Section 16.7.3.

The finned floors are designed as reinforced concrete slabs in accordance with ACI 349-01 (Reference 16.15). The finned floors resist vertical and in-plane forces for both normal and extreme loading conditions. For positive bending, the concrete above the neutral axis carries compressive stresses and the stiffened steel plate resists tension. The steel plate with fin stiffeners serves the function of bottom reinforcement. Negative bending compression is resisted by the stiffened plate and tension in the top reinforcement. For negative bending, the potential for the steel fins to buckle because of compression is checked using ANSI/AISC-N690-1994 (Reference 16.24). In addition, the concrete restrains twisting and therefore lateral buckling of the stiffener. The neutral axis for negative bending is located in the stiffened-plate section and the concrete in tension is assumed to be inactive. Horizontal in-plane forces are resisted by the stiffened plate and the longitudinal reinforcement.

Minimum top reinforcement is provided in the slab in each direction for shrinkage and temperature crack control. In addition, top reinforcement located parallel to the fin stiffeners is used as tension reinforcement in negative bending. The stiffened plate provides crack control capability for the bottom of the slab in the transverse direction.

Composite section properties, based on an all steel-transformed section, as detailed in ANSI/AISC-N690-1994 (Reference 16.24, Section Q1.11), are used to design the following:

- Weld strength between stiffener and steel plate
- Spacing of shear studs for composite action

The stiffened plate alone is designed to resist all construction loads prior to the concrete hardening. The plate is designed against the criteria for bending and shear, specified in ANSI/AISC0-N690-1994 (Reference 16.24, Sections Q1.5.1.4 and Q1.5.1.2). In addition, the weld between the stiffener and the steel plate is designed to satisfy the code requirements. Finned panels have an approximate short span of 4.9 m (16 feet), except for the main control room ceiling finned panel, which has a short span of 11.23 m (37 feet) and requires temporary supports at mid span during construction.

16.11.2.5 Structural Modules

Structural modules are used for some of the structural elements on the south side of the auxiliary building. These structural modules are structural elements built up with welded steel structural shapes and plates. The modules consist of steel faceplates connected by steel vierendeel frames as shown in Reference 16.38. The thicknesses of the steel faceplates are generally 12.7 mm (0.5 inch). In certain locations, the face plates are thickened.

The primary purpose of the frames is to stiffen and hold together the faceplates during handling, erection, and concrete placement. The nominal spacing of the frames is 762 mm (30 inches). Shear studs are welded to the inside faces of the steel faceplates. Faceplates are welded to adjacent faceplates on the same face with full-penetration welds so that the weld is at least as strong as the plate. The structural wall modules are anchored to the concrete base by a mechanical connection that uses reinforcing bars and mechanical connectors. After erection, concrete is placed between the faceplates.

These modules include the SFP, fuel transfer canal, cask loading pit, and cask washdown pit. The structural modules in the auxiliary building are similar to the structural modules for the in-containment structures. Reference 16.38 shows the location of the structural modules in the auxiliary building. The loads and load combinations applicable to the structural modules in the auxiliary building are the same as for the containment internal structures, except that there are no ADS or pressure loads due to pipe breaks.

The design methodology of these modules in the auxiliary building is similar to the design of the in-containment modules presented in Section 16.13.

The design of SC CA modules was a cause of concern for the UK Regulator (see Section 16.20) as the form of construction was not the same as that used for the shield building cylindrical wall. To address this issue, a separate justification was prepared for the SC-constructed CA modules (Reference 16.4).

The concrete floors on steel plates in the CA20 module are designed as reinforced concrete slabs in accordance with ACI 349-01. The steel panels are designed and constructed in accordance with AISC N690. For positive bending, the steel plate is in tension and the steel plate and stiffeners serve as the bottom reinforcement. For negative bending, compression is resisted by the concrete and the stiffened plate and tension by top reinforcement in the concrete. This methodology is described in Reference 16.38, Section 7.2.

16.12 IN-CONTAINMENT CIVIL ENGINEERING STRUCTURES

The design justification of the in-containment structural modules is provided in Reference 16 -4 and is supported by the additional information provided in Reference 16.41. The in-containment structures are part of the nuclear island and are A1 C-I structures. The containment internal structures are those concrete and steel structures inside (not part of) the containment pressure boundary that structurally support the Class 1 components. The containment internal structures include the primary shield wall, reactor cavity, secondary shield walls, IRWST, refuelling cavity walls, operating floor, intermediate floors, various platforms, and the internal structures' basemat. The polar crane girder is considered part of the containment vessel and is addressed in Chapter 20.

Component supports are those steel members designed to transmit loads from the vessels, systems, and components back to the load-carrying elements of the in-containment structures. Component supports are addressed in the ASME jurisdictional boundary and are not considered to be civil engineering structures; therefore, component supports are outside the scope of this chapter. Component failures are addressed through the Structural Integrity program.

16.12.1 Structural Descriptions

The containment internal structures are designed using reinforced concrete and structural steelwork. At the lower elevations, conventional reinforced concrete is used for construction of the basemat, which includes a number of rooms. Permanent steel forms are frequently used in lieu of removable forms based on constructability considerations. These steel form modules (liners) consist of plate reinforced with angle stiffeners and tee sections. The angles and the tee sections are on the concrete side of the plate. Welded studs, or similar embedded steel elements, are attached on the concrete face of the permanent steel form where surface attachments transfer loads into the concrete. Where these surface attachments are C-I, the portion of the steel form module transferring the load into the concrete is classified as C-I.

Walls and floors are generally concrete-filled steel plate structural modules. The walls are supported on the mass concrete containment internal structures basemat with the steel faceplate extending down to the concrete floor on each side of the wall. The steel faceplates of the structural modules provide reinforcement to the concrete. The structural modules are anchored to the base concrete using mechanical connections. Reference 16.38 shows the locations of typical structural modules (Figure 1), the typical structural configuration of the wall modules (Figure 2-5), and a representative floor module (Figure 3a). These structural modules are structural elements built up with welded steel structural shapes and plates. Concrete is used where required for shielding, but reinforcing steel is not normally used.

Walls and floors exposed to water during normal operation or refuelling are constructed using stainless-steel plates.

16.12.1.1 Containment Internal Structures Basemat

The containment internal structures basemat is the reinforced concrete structure filling the bottom head of the containment vessel. It extends from the bottom of the containment vessel head up to the bottom of the structural modules that start between elevations 91.3 m (71'-6") and 100.9 m (103'-0"). The basemat includes rooms as shown in Reference 16.49. The primary shield wall and reactor cavity extend from elevation 91.3 m (71'-6") to 102.2 m (107'-3"). They provide support for the reactor vessel and portions of the secondary shield walls and refuelling cavity walls. The general arrangement drawings in References 16.48 through 16.60, show the location and configuration of the primary shield wall and reactor cavity. The walls of the primary shield, the SG compartments, and the CVS room are structural modules as shown in Reference 16.38, Figure 1. The rest of the basemat is reinforced concrete.

16.12.1.2 Structural Wall Modules

Structural wall modules are used for the primary shield wall around the reactor vessel, the wall between the vertical access and the CVS room, secondary shield walls around the SGs, and pressuriser, for the east side of the IRWST and for the refuelling cavity.

The general arrangement drawings of the nuclear island are shown in References 16.48 through 16.60. Reference 16.38 shows the locations of the structural modules in detail in Figure 1; it provides an isometric view showing some typical arrangements of the structural modules where the steel faceplates provide wall reinforcement in Figures 2 and 6. The structural wall modules are as follows:

- The secondary shield walls are a series of walls that, together with the refuelling cavity wall, enclose the SGs and pressurizer. Each of the two secondary shield wall compartments provides support and houses a SG and reactor coolant loop piping.

- The IRWST extends from approximately elevation 100.9 m (103'-0") to directly below the operating deck. On the west side, along the containment vessel wall, the tank wall consists of a stainless-steel plate stiffened with structural steel sections in the vertical direction and angles in the horizontal direction. Structural steel modules, filled with concrete and forming, in part, the refuelling cavity, SG compartment, and pressuriser compartment walls, compose the east wall.

- The refuelling cavity has two floor elevations: the area around the reactor vessel flange is at elevation 102.2 m (107'-2"), and the lower level is at elevation 99.4 m (98'-1"). The

upper and lower reactor internals storage is at the lower elevation, as is the fuel transfer tube.

- Structural wall modules consist of steel faceplates connected by vierendeel frames. The primary purpose of these frames is to stiffen and hold together the faceplates during handling, erection, and concrete placement. At corner locations, the trusses are replaced with diaphragms. These diaphragms have similar purpose as the trusses and are used to fabricate the modules in the corners. Shear studs are welded to the inside faces of the steel faceplates. Faceplates are welded to adjacent plates with full penetration welds so that the weld is at least as strong as the plate.

The design methodology of the structural wall modules is provided in Reference 16.38, and justification for the design of the structural wall modules is provided in Reference 16.4.

16.12.1.3 Structural Floor Modules

Structural floor modules are used for the operating deck at elevation 110.7 m (135'-3") over the IRWST and for the 102.2 m (107'-2") Maintenance Floor over the rooms in the containment internal structures' basemat. The floors are shown on the general arrangement drawings in References 16.48 through 16.60. The floors consist of steel tee- and wide-flange sections, welded to horizontal steel bottom plates stiffened by transverse stiffeners. After erection, concrete is placed on top of the horizontal plate and around the structural steel section. A portion of the operating floor consists of a concrete slab placed on metal decking supported by structural steel beams. The operating deck is supported by the IRWST walls, refuelling cavity walls, secondary shield walls, and steel columns. Structural details for a representative example of the containment operating deck floor structural module are shown in Reference 16.38, Figure 3a.

16.12.1.4 Internal Steel Framing

The region of the operating floor away from the IRWST consists of a concrete slab placed on metal decking supported by structural steel beams. The maintenance floor mezzanine at elevation 105.6 m (118'-6") consists of steel grating supported by structural steel framing. In addition, a number of steel platforms are located above and below the operating floor. These platforms support either grating floors or equipment such as piping and valves.

16.12.2 Analysis and Design Justification of In-Containment Structures

The loads and load combinations plus the methods of analysis methods generally followed are as presented in Sections 16.7 and 16.8; however, wind loads (W) and tornado loads (Wt) are not applicable to the design of the in-containment internal structures because these structures are protected by both the shield building and the steel containment.

The nuclear island must be seismically analysed as a whole to capture the complex load distributions through the basemat, walls and slabs of the shield building and auxiliary building. The seismic analyses using the nuclear island computer models are discussed in Section 16.8.3. The NI10 model is used to calculate the seismic forces and moments for the in-containment structures.

Section 16.5.1 identifies the codes, standards, and methodologies followed when preparing the design justification for the structures making up the nuclear island, including the in-containment structures. More specific information on how this has been applied is provided in Reference 16.4.

16.13 NUCLEAR ISLAND FOUNDATIONS

16.13.1 Description and Load Paths

The nuclear island structures, consisting of the containment vessel and in-containment structures, shield building, and auxiliary building are founded on a common, cast-in-place, reinforced concrete basemat foundation. The concrete basemat is a C-I structure. The top of the foundation is at elevation 89.8 m (66'-6"). The cellular construction of the auxiliary building serves an important function in stiffening the basemat and distributing the load from the shield building and containment vessel. The cellular construction comprises vertical shear/bearing walls and horizontal floor slabs. The walls carry the vertical loads from the structure to the basemat. Lateral loads are transferred to the walls by the roof and floor slabs. The walls then transmit the loads to the basemat. Reference 16.75 shows a plan of the basemat; References 16.82 through 16.86 show sections through the nuclear island showing the basemat.

Adjoining buildings, such as the radwaste building, turbine building, and annex building are structurally separated from the nuclear island structures by a minimum 50-mm (2 inches) gap at and below the grade. A 101-mm (4 inches) minimum gap is provided above grade. This provides space to prevent interaction between the nuclear island structures and the adjacent structures during a seismic event. Reference 16.97 shows the foundation plan for the nuclear island and the adjoining structures.

For ease of construction, the foundation is built on a mud mat. The mud mat (termed blinding concrete in the UK) is lean, non-structural concrete and rests upon the load-bearing soil. Waterproofing is provided using an appropriate technique as explained in Section 16.9.1.

The ground conditions at a particular site will need to be demonstrated as no more onerous than those considered in the design. The potential exists for ground engineering techniques to be used when undertaking construction specific to a particular site. These are matters to be addressed during site licensing. The Civil/Structural Design Criteria (Reference 16.6) provides information on the criteria used in design of the AP1000 foundation. As required by Chapter 12, site-specific justification will be developed for the AP1000 nuclear island foundation design.

16.13.2 Codes and Standards

The reinforced concrete foundation is designed to ACI 349-01 (Reference 16.15) as is all reinforced concrete in the nuclear island.

16.13.3 Loads and Load Combinations for Integrity and Stability Evaluations

Loads and load combinations are as described in Sections 16.7 and 16.8. The basemat is designed for the upward hydrostatic pressure due to groundwater reduced by the downward deadweight of the basemat.

The containment vessel is a vertical steel cylinder, closed at the top and bottom by hemispherical-shaped steel plates as shown in Figure 16-4. The lower hemisphere is capable of resisting the containment internal pressure without benefit of the nuclear island basemat; however, containment pressure loads affect the nuclear island basemat since the concrete is stiffer than the steel plate forming the lower hemisphere. The containment design pressure is included in the design of the nuclear island basemat as an accident pressure load (Pa), see Section 16.7.5.3.

In addition to evaluating the integrity of the nuclear island foundation to ACI 349-01 requirements (Reference 16.15), the nuclear island is evaluated for stability against sliding and overturning. The loads considered arise from the SSE, winds, and tornadoes. Absence of flotation of the nuclear island basement under floods and high groundwater levels is also verified. The load combinations and minimum required factors of safety against overturning, sliding, and flotation are presented in Section 6.4 of Reference 16.6.

16.13.4 Design and Analysis (Excluding Construction)

The design of the basemat consists primarily of applying the design loads to the structures, calculating shears and moments in the basemat, and determining the required reinforcement. For a site with hard rock below the underside of the basemat, vertical loads are transmitted directly through the basemat into the rock. Horizontal loads arising during an earthquake are distributed to the underside of the basemat, resulting primarily in small membrane forces in the basemat slab.

The analyses of the basemat make use of the NI05 model of the auxiliary building and containment internal structures, which is summarised in Section 16.8.3 above. Interaction of the basemat with the overlying structures and the soil is addressed. Provisions are made in the model for two possible uplifts: the uplift of the containment internal structures from the lower basemat, and the uplift of the basemat from the soil. The 3-D finite element model of the basemat includes the structures above the basemat and their effect on the distribution of loads on the basemat.

The subgrade is modelled with one vertical spring and two horizontal springs at each node of the basemat. The vertical springs act in compression only for the nonlinear analyses. The horizontal springs are active when the vertical spring is closed and inactive when the vertical spring lifts off. The analyses of the basemat account for the range of soil sites specified in Table 16-3. Horizontal bearing reactions on the exterior walls below grade are conservatively neglected.

The nuclear island basemat below the containment vessel, and the containment internal structures basemat above the bottom of the containment vessel, are simulated with solid tetrahedral elements. Nodes on the two basemats are connected with spring elements normal to the theoretical surface of the containment vessel.

Dead loads are applied as inertia loads. Live loads and the SSE loads are applied as concentrated loads at the nodes of the computer model. The SSE loads are applied as equivalent static loads using the assumption that while the maximum response from one direction occurs, the responses from the other two directions are 40 percent of the maximum. Combinations of the three directions of the SSE are evaluated.

Initially, linear analyses are performed for all specified load combinations, assuming that the soil springs can resist tension. Critical load cases are then selected for subsequent nonlinear analyses with basemat liftoff based on the results of the linear cases. The results from the analysis include the forces, shears, and moments in the basemat; the bearing pressures under the basemat; and the area of the basemat that is uplifted. Reinforcing-steel areas are calculated from the member forces for each load combination case.

The required reinforcing steel for the portion of the basemat under the auxiliary building and the shield building is determined by considering the reinforcement envelope for the full nonlinear response of the nuclear island, during the period of seismic shaking, for the most critical load combination cases. Additional reinforcement is provided in the design of the basemat for soil sites so that the basemat can resist loads that are [ ] greater than

the demand calculated by the equivalent static acceleration analyses on uniform soil springs. This increase accommodates potential site-specific lateral variability of the soil, investigated separately in a series of parametric studies.

16.13.5 Analyses of Settlement during Construction

Construction loads have the potential to be significant to the design of the nuclear island basemat, depending on the soil conditions present at a particular site. Settlement evaluations are based on the most onerous soil conditions considered to fall within the scope of the foundation design. Site-specific settlement analyses will be performed at soil sites to provide justification for the nuclear island foundation.

It is anticipated that the basement concrete would be cast as a single placement. The placement would include the first 1.83 m (6 feet) of the thicker basemat below the containment vessel and shield building, but would exclude the central zone directly below the bottom of the containment vessel. Construction would continue with a portion of the shield building foundation and containment internal structure and the walls of the auxiliary building. The critical location for shear and moment in the basemat is around the perimeter of the shield building. Once the shield building and auxiliary building walls are completed to elevation 94.7 m (82'-6"), the load path changes and loads are resisted by the basemat stiffened by the shear walls.

The analyses account for the construction sequence, the associated time-varying load and stiffness of the nuclear island structures, and the resulting settlement time history. To maximise the potential settlement, the analyses consider a 109.7-m-deep (360 feet) soft-soil site. The following two soil profiles are analysed to represent limiting foundation conditions, and address both cohesive and cohesionless soils and combinations thereof:

- A soft-soil site with alternating layers of sand and clay. The assumptions in this profile maximise both the settlement in the early stages of construction and the impact of dewatering.

- A soft-soil site with clay. This assumption maximises the settlement during the later stages of construction and during plant operation.

The analyses focus on the response of the basemat in the early stages of construction when it could be susceptible to differential loading and deformations. As subsequent construction incorporates concrete shear walls associated with the auxiliary building and the shield building, the structural system strengthens significantly, minimising the impact of differential settlement. The displacements, moments, and shear forces induced in the basemat are calculated at various stages in the construction sequence. These member forces are evaluated in accordance with ACI 349-01 (Reference 6.15) using the load factors given in Reference 16.6. Three construction sequences are examined to demonstrate construction flexibility within broad limits:

- A base construction sequence that assumes no unscheduled delays. The site is dewatered and excavated. Concrete for the basemat is placed in a single pour. Concrete for the exterior walls below grade is placed after the basemat is in place. Exterior and interior walls of the auxiliary building are placed in 4.9- to 5.5-m (16 to 18 feet) lifts.

- A delayed shield building case that assumes a delay in the placement of concrete in the shield building while construction continues for the auxiliary building. This bounding case maximises tension stresses on the top of the basemat. The delayed shield building

case assumes that no additional concrete is placed in the shield building after the pedestal for the containment vessel head is constructed. The analysis incorporates construction in the auxiliary building to elevation 105.3 m (117'-6") and filling the CA20 module with concrete to elevation 110.74 m (135'-3"), and thereafter assumes that construction is suspended.

- A delayed auxiliary building case that assumes a delay in the construction of the auxiliary building while concrete placement for the shield building continues. This bounding case maximises tension stresses in the bottom of the basemat. The delayed auxiliary building case assumes that no concrete is placed in the auxiliary building after the basemat is constructed. The analysis incorporates construction in the shield building to elevation 95.123 m (84'-0") and thereafter assumes that construction is suspended.

For the base construction sequence, the largest basemat moments and shears occur at the interface with the shield building before the connections between the auxiliary building and the shield building are credited. Once the shield building and auxiliary building walls are completed to elevation 94.7 m (82'-6"), the load path for successive loads changes and the loads are resisted by the basemat stiffened by the shear walls. Dewatering is discontinued once construction reaches grade, resulting in the rebound of the subsurface.

Of the three construction scenarios analysed, the delayed auxiliary building case results in the largest demand for the bottom reinforcement in the basemat. The delayed shield building results in the largest demand for the top reinforcement in the basemat. The analyses of the three construction sequences demonstrate the following:

- The design of the basemat and superstructure accommodates the construction-induced stresses considering the construction sequence and the effects of the settlement time history.

- The design of the basemat can accommodate delays in the shield building so long as the auxiliary building construction is suspended at elevation 105.2 m (117'-6"). Construction of the auxiliary building can resume once the shield building is advanced to elevation 100 m (100'-0").

- The design of the basemat can accommodate delays in the auxiliary building so long as the shield building construction is suspended at elevation 95.1 m (84'-0"). Construction of the shield building can resume once the auxiliary building is advanced to elevation 100 m (100'-0").

- After the structure is in place and cured to elevation 100 m (100'-0"), the basemat and structure act as an integral 12.0 m (39.5 feet) deep structure; the loading due to construction above this elevation is not expected to cause significant additional flexural demand with respect to the basemat and the shield building concrete below the containment vessel. Accordingly, there is no need for placing constraints on the construction sequence above elevation 100 m (100'-0").

The site conditions considered in the evaluation provide reasonable bounds on construction-induced stresses in the basemat. Accordingly, the basemat design is adequate for practically all soil sites and can tolerate major variations in the construction sequence without causing excessive deformations, moments, and shears due to settlement during the construction period and over the plant life.

The analyses of alternate construction scenarios show that member forces in the basemat are acceptable subject to the limits shown below, imposed for soft-soil sites on the relative level of construction of the buildings. Construction of the plant, when located at a soil site, will satisfy the limits shown below or a site-specific analysis of settlement and member forces will be completed. These limits do not apply to units with a soil profile that satisfies the requirements for soft rock, firm rock, or hard rock.

Prior to completion of both the shield building and auxiliary building at elevation 94.7 m (82'-6"), concrete may not be placed as follows:

- Above elevation 95.1 m (84'-0") for the shield building or containment internal structure.
- Above elevation 105.3 m (117'-6") in the auxiliary building, except in the CA20 structural module, where it may be placed at elevation 110.74 m (135'-3").

Member forces in the basemat considering settlement during construction differ from those obtained from the analyses on uniform elastic soil springs described in Section 16.14.4 above. Although the bearing pressures at the end of construction are similar in the two analyses, the resulting member forces differ because of the progressive changes in structural configuration during construction. Using the results of the analyses described in Section 16.14.4, the design provides sufficient structural strength to resist the specified loads, including bearing reactions on the underside of the basemat. The member forces in these analyses are those due to primary externally applied loads and do not consider secondary stresses and strains locked in during early stages of construction. A confirmatory evaluation was performed to demonstrate that the member forces due to design basis loads, including locked-in forces due to construction settlement, remain within the capacity of the section. The evaluation was performed for critical locations that were selected as locations where the effect of locked-in member forces were judged to be most significant.

The governing scenario is the case with a delay in the auxiliary building construction for the soft-soil site with alternating layers of sand and clay. The delay is postulated to occur just prior to the stage where the auxiliary building walls are constructed. Member forces at the end of construction are calculated considering the effects of settlement during construction. The differences in these member forces from those calculated for dead load in the analyses on soil springs are added as additional dead loads in the critical SSE load combination.

For the five critical sections with the most heavily stressed members, the member forces for the load combination of dead load plus SSE (including the member forces locked-in during various stages of plant construction) lead to stresses that are acceptable with respect to the ACI 349-01 design criteria (Reference 16.15); thus, the strength capacities of the structural members are not exceeded.

16.13.6 Stability Evaluations

16.13.6.1 Bearing Pressure

Bearing pressure demand was calculated using both 2-D and 3-D analyses. Both linear and nonlinear finite element analyses were performed using the 2-D nuclear island model. The maximum bearing pressures calculated include the effects of dead, live, and seismic loads.

The effects of basemat uplift were evaluated using an east-west lumped-mass ANSYS stick model of the nuclear island structures supported on a rigid basemat with nonlinear springs. Since the largest bearing pressure will result from the east-west seismic excitation because of

the smaller width of the basemat in this direction, liftoff was evaluated using an east-west stick model of the nuclear island structures supported on a rigid basemat with nonlinear springs. Finite element time history analyses were performed. Liftoff increases the bearing pressure close to the west edge by 4 to 6 percent, with insignificant effect beneath most of the basemat.

The SASSI soil-structure interaction analyses were performed based on the nuclear island 3-D SASSI model for the HR (hard rock) and the five soil conditions established from the AP1000 2-D SASSI analyses (Reference 16.32, Section 4.4.1.2). The SASSI model of the nuclear island is based on the NI20 finite element model. The bearing pressures from the 3-D SASSI analyses have been obtained by combining the time history results from the north-south, east-west, and vertical earthquakes. The limit on bearing pressure is presented as a site interface parameter in Table 16-3.

16.13.6.2 Sliding, Overturning, and Floatation

The minimum required factors of safety against sliding, overturning, and flotation for the nuclear island structures are given in Section 6.4 of Reference 16.6. The factors of safety for sliding and overturning for the SSE are calculated for each soil case for the base reactions in terms of shear and bending moments about the edges of the auxiliary building and the west side of the shield building at each time step of the seismic time history at a hard rock site. The reactions from the 2-D SASSI model (see Section 16.8.3) are used to obtain seismic response factors between the HR case to the UBSM (upper-bound soft-to-medium soil) case and the SM case (Reference 16.32). These factors are used to adjust the HR time history to reflect the seismic response for the other two potential governing soil cases, UBSM and SM (soft-to-medium soil). The firm rock, soft rock, and soft soil cases have higher factors of safety against sliding and, therefore, are not considered.

Using the 2-D ANSYS model, a nonlinear finite element analysis with sliding friction elements was performed. Sliding was only modelled in the east-west direction. There is no need to consider the north-south direction since the nuclear island deflections, calculated to maintain a factor of safety of 1.1, are largest in the east-west direction. This model was modified by introducing friction elements between the bottom of the basemat and soil media interface. Time history analysis was performed with vertical uplift and sliding allowed. The three cases that have the lowest factor of safety related to sliding were evaluated: HR, UBSM, and SM. The magnitude of the seismic input was increased by 10 percent to maintain the factor of safety against sliding of 1.1. No passive soil resistance is considered. Sliding during the seismic event is therefore negligible and no passive soil resistance is necessary from the backfill (side soil). Hence, it can be concluded that the nuclear island is stable against sliding, and there is no requirement for the backfill material adjacent to the nuclear island basement walls to maintain stability against sliding.

16.13.6.3 Effect of Nuclear Island Basemat Uplift on Seismic Response

The effects of basemat uplift were evaluated using an east-west lumped-mass stick model (see Section 16.13.6.1). Floor response spectra from the SSE time history analyses, which included basemat uplift, were compared with those from analyses that did not include uplift. The comparisons showed that the effect of basemat uplift on the floor response spectra is not significant.

16.14 DESIGN OF STRUCTURES EXTERNAL TO THE NUCLEAR ISLAND

The loads, analysis methods, and design criteria applied for the design of the structures external to the nuclear island are presented in previous sections of this chapter. The design of the structures will meet all the criteria. In particular, the design ensures that no C-II structures will collapse against the nuclear island with consequences that affect nuclear safety. As the safety of the plant is predominantly dictated by the robustness of the nuclear island, it is not necessary for detailed information to be provided on the design of the structures external to the nuclear island.

16.15 MARGINS BEYOND THE DESIGN BASIS

For SSCs required for safe shutdown, the HCLPF magnitudes are equal to or greater than the review-level earthquake, set at 0.5g; thus, it can be concluded that an adequate seismic margin is present for the nuclear island and the Class 1 equipment within it.

Section 16.4 considers extreme wind, extreme snow, hurricanes, and tornadoes to determine whether the design is conservative with regards to potential environments at UK sites.

The shield building is a very robust barrier against winds, tornadoes, and missiles, thus preventing damage to the containment vessel and the in-containment Class 1 safety systems. The external envelope to the auxiliary building, although not as robust as the shield building, is nevertheless more than adequately robust as it has been designed to resist tornado loading. The intensity of tornadoes considered is very conservative in the UK context, indicating large margins with no potential for a step change in response beyond any possible UK tornado. A significant tornado missile considered for the design of the whole of the exterior envelope to the nuclear island is a 1814 kg (4000 lb) car with an impact velocity of 47 m/sec (105 mph) horizontally or 33 m/sec (74 mph) vertically. Thus it can be concluded that significant margins exist with respect to the ability of the nuclear island to withstand extreme wind, extreme snow, tornadoes, and missiles.

Noting that the nuclear island contains the highly reliable Class 1 equipment, the protection of the Class 2 equipment does not need to be so robust for the following reason:

- The hazard-withstand requirements applicable to the remaining Class 2 structures are predominantly driven by the need to ensure that risks are ALARP. Based on the robustness of the nuclear island, it is considered that the approach to the design of the civil engineering structures against extreme wind, extreme snow, tornadoes, and missiles, when considered in its entirety, ensures an adequate margin with respect to nuclear safety.

The absence of site flooding sufficient to lead to an event with nuclear consequences depends on the plant being located at an appropriate elevation, which is a site-specific issue. It is for site-specific safety cases to present the arguments that adequate margins exist with respect to flooding from sources external to the site (i.e., there are no step changes in consequence as a result of slightly lower-frequency events than DBEs).

Should temperatures exceed the design basis limits, there would be some forewarning of such an event and mitigating action would be taken by the operator. The response of the buildings would not change significantly as a result of temperatures moving outside the DBE limits and any building effects would not be significant for the SSCs within the plant.

16.16 RECORDING AND RESPONDING TO EARTHQUAKES

16.16.1 Seismic Instrumentation

The plant seismic instrumentation has no safety function, and therefore, is assigned neither a safety class nor a seismic classification. The instrumentation and associated equipment are used to measure plant response to earthquake motion. Four triaxial acceleration sensor units are connected to a time-history analyser. The time-history analyser recording and playback system is located in a panel in the nuclear island in a room near the main control room. Seismic event data from these sensors are recorded on a solid-state digital recording system at 200 samples per second per data channel.

16.16.2 Post-Earthquake Procedures

Site-specific procedures will be prepared for activities following an earthquake. These procedures will be used to accurately determine both the response spectrum and the cumulative absolute velocity of the recorded earthquake ground motion from the seismic instrumentation system. The procedures and the data from the seismic instrumentation system will provide sufficient information to guide the operator on a timely basis to determine if the level of earthquake ground motion requiring shutdown has been exceeded.

16.17 LIFE CYCLE ENGINEERING SUBSTANTIATION

The plant has a planned 60 years operating life. The capability of the nuclear island civil engineering structures to support and protect the Class 1 SSCs is essential for safety. The engineering and safety arrangements throughout the life cycle of the AP1000 plant are presented in Chapter 7, “Life Cycle Engineering and Safety.” It focuses on specific aspects of the management arrangements associated with the achievement of nuclear safety throughout the design life cycle of the plant considering the design, change control, construction, commissioning, maintenance, ageing, degradation and decommissioning.

Beyond 60 years, it is likely that the nuclear island structures will still need to provide such safety functions until such time as decommissioning has removed all the significant nuclear materials. Replacing the nuclear island civil engineering structures is generally not an option, which can be a possibility when considering internal plant; therefore, the nuclear island structures will need to have a working life well in excess of 60 years, with the exception of some of the water storage structures that may no longer be needed following cessation of power operation.

The nuclear island is constructed from a combination of reinforced concrete, structural steelwork, and SC-constructed elements. A working life of 120 years is achievable in line with normal civil engineering criteria (Reference 16.30, Table NA.2.1). The factors that determine the life of a civil engineering structure and which should be considered to achieve a working life of 120 years are as follows:

- Use of the structure
- Design criteria
- Environmental conditions
- Composition, properties, and performance of the materials and products
- Properties of the soil
- Choice of the structural system
- Shape of members and the structural detailing
- Quality of workmanship and the level of control

- Particular protective measures
- Intended maintenance during the design working life

The nuclear island civil structures are designed and constructed to nuclear-specific codes and standards and will be maintained to a high standard. It is to be expected, therefore, that the life expectancy of the structures will be equivalent to the best that has been achieved for normal construction. Site-specific studies will be undertaken to evaluate whether there are any corrosive effects local to a site and, if found, appropriate protection will be provided. In addition, through-life inspection and testing will be undertaken to ensure that no site-specific or other effects, local to a structure, could cause accelerated ageing.

The nuclear island structures are generally of massive proportions and are not vulnerable to local defects since forces within the structure would redistribute. Where the potential for redistribution may be limited, inspections will be undertaken on a more regular basis.

The tolerability of a reinforced concrete structure to ageing effects depends on the concrete cover, the concrete mix design, and the quality of workmanship. The concrete for construction is specified as having a minimum concrete strength of 27.6 N/mm^2 (4 ksi) (Reference 16.6, Section 7.1) and cover as follows (Reference 16.6, Section 11.2):

Structure	Thickness of Reinforcement Cover
Auxiliary building exterior walls	50 mm (2.0 inch)
Auxiliary building interior walls	38 mm (1.50 inch)
Shield building	50 mm (2.0 inch)
Slabs	25 mm (1.0 inch)

Assuming a 10-mm (0.5 inch) construction tolerance allowance, there will be a minimum reinforcement cover of 38 mm (1.50 inch), which normally provides sufficient protection for an environment containing airborne salts representative of a coastal site. The adequacy of 40-mm protection will depend on the details of the concrete mix design, specified to ACI 349-01 (Reference 16.15), for which more information will be provided during site licensing.

Reference 16.6, Section 7.2 identifies that epoxy-coated reinforcement bars are used when environments are identified as corrosive.

The shield building cylindrical wall is constructed in part using SC construction. The external steel plates will be provided with an external corrosion-resistant coating. This will be inspected, and repaired or renewed as required. The effects of ageing on the SC-constructed structures have been considered in Reference 16.3.

16.18 CONSTRUCTION ASSURANCE

The earlier sections of this chapter explain the justification of the design of the civil engineering structures. The designs must be transformed into real structures that comply with the design intent and are compatible with all the design assumptions. The civil engineering output from the design is typically certified for construction drawings that show the arrangements and sizes of the structures, their components, and the elements forming the components, together with reference to the relevant specifications.

As necessary, this information is translated to construction and fabrication details. Configuration control and quality assurance processes are in place to ensure that the licensed

design configuration is maintained. Specific quality processes track potential changes and deviations during construction. These types of processes provide confidence that the construction-related work is suitable and sufficient, so that the requirements of the safety case for safe operation of the plant are fully achieved relative to the plant structures.

The processes to be followed to provide construction assurance are in part generic to the AP1000 design and depend in part on the country, site, and organisations with responsibility for construction.

16.18.1 Generic Approach to Providing Construction Assurance

The design specifies the requirements that the construction contractor needs to achieve according to US nuclear construction practices:

- The materials, components, and construction methods of the C-I civil engineering structures are specified in accordance with accepted practices and adhere to nuclear-specific codes and standards as appropriate based on the structures safety classification.

- Modular construction is used extensively throughout the plant. Modular construction allows for civil fabrication work to be completed offsite in controlled environments. Construction, examination, and inspection details are specified in accordance with accepted practices and are consistent with nuclear-specific codes and standards as appropriate based on the structures safety classification. The structures supporting the PCCWST within the shield building roof are to be examined before and after first filling of the tank.

- C-II and NNS concrete structures are constructed to the accepted industrial standard embodied in ACI 318-99 (Reference 16.26). C-II and NNS steel structures are constructed to AISC S335 (Reference 16.16). The civil/structural design criteria document (Reference 16.6, Section 7 and Table 9) provides more information on the materials suitable for construction.

The constructability of the AP1000 plant structures using a quality-assured approach is established as part of the design. Westinghouse works closely with its construction partners. Construction, planning, and constructability reviews are performed concurrently with the civil engineering design. Lessons learned from earlier and ongoing construction projects are filtered back into the design, and the construction process will be improved as a result of AP1000 plant construction experience.

SC construction is an example of how the need to provide construction assurance is considered as an integral part of the design process. Construction inspection is conducted to verify the concrete wall thicknesses and the faceplate thicknesses. The location for measurement of the structural wall modules is at the locations of the trusses used to provide the structural framework for the modules. Thicknesses will be measured at appropriate sections including openings and penetrations. Inspections will confirm that each section provides the minimum-required steel and concrete thicknesses. The minimum-required steel and concrete thicknesses represent the minimum values needed to meet the design basis loads. Steel plate thickness provided may exceed the minimum required value for the following reasons:

- Structural margin
- Ease of construction

- Construction loads
- Use of standard thicknesses

The construction and inspection requirements were identified and reviewed early in the design process to ensure that the design was capable of being constructed using a validated approach. Potentially more difficult areas for construction have been identified and mock-ups are built to demonstrate that these areas were capable of being soundly constructed. Following concrete setting, the mock-ups are disassembled for examination for defects by the construction technicians, quality control inspectors, and construction supervisors. This process helps ensure the required construction quality is achieved.

Existing and potential new methods of non-destructive examination (NDE) have been evaluated for their ability to confirm that concrete placed between the permanent steel forms contained neither excessive voids nor other defects that could affect strength. More information is presented in Reference 16.3, Section 9.

16.19 CONCLUSIONS

This chapter summarises the generic design information used to justify that the civil engineering structures will withstand the loads arising from normal operations, internal hazards, external hazards, and internal plant faults. There is clearly a dependency on site-specific information (more so than for equipment housed within the civil engineering structures); however, the approach followed allows for a range of site conditions, providing confidence that the design is suitable and sufficient for a variety of UK sites. The design is based on external hazard data representative of an onerous worldwide site. This leads to structures having robust load-resisting systems well able to withstand the generally more benign UK environments.

The approach to construction is presented in Section 16.18. Demonstrating the achievement of the design intent has some dependency on the site and the organisations with responsibilities for construction. It would be inappropriate for the construction processes to be fully defined during the generic phase because input from all the responsible organisations is needed to deliver a safe and economically constructed AP1000 plant that fully meets the design intent. There are construction processes still to be defined relating to transfer of the design to the UK. Whilst still complying with the codes and standards identified in Section 16.5, choices remain relating to the specification and methods of construction. The construction of AP1000 plants in China clearly demonstrates that the appropriate organisational responsibilities can be defined and delivered so that the design intent is fully achieved.

The design has taken into account the 60 years design life. There will be no erosion of the capability of the civil engineering structures to withstand the loads required by the nuclear safety case. This is subject to appropriate maintenance being undertaken (including examination, inspections, and testing) to confirm that the design assumptions relating to the design life of the plant civil engineering structures remain valid. The details have some dependency on the licensee procedures.

The format of this chapter has been chosen to be consistent with the safety case logic presented in the SAPs (Reference 16.1), specifically addressing those principles applicable to the justification of the plant civil engineering structures. In particular, the process has done the following:

- Explained the categorisation and classification process followed

- Justified the codes, standards, and methods used
- Presented the process for determination of loads and load combinations
- Summarised the justification of the nuclear island structures in some detail because this is where the Class 1 equipment is located, and provided an appropriate level of scrutiny of the remaining structures of less nuclear significance

It is concluded that the design demonstrates that the deterministic justifications of the civil engineering structures are appropriate to their safety function and class; and that the necessary normal and hazard loads will be withstood as required, subject to appropriate investigations and confirmations being provided and relevant to a particular site.

16.20 REFERENCES

16.1 "Safety Assessment Principles for Nuclear Facilities," Rev. 0, Office for Nuclear Regulations, 2014.

16.2 Not used

16.3 Westinghouse Report APP-1200-S3R-003, Rev. 4, "Design Report for the AP1000 Enhanced Shield Building," June 2011.

16.4 Westinghouse Report UKP-GW-GLR-018, Rev. 0, "Westinghouse Response to RI-AP1000-02 and RO-AP1000-079," October 2010.

16.5 Not used

16.6 Westinghouse Report APP-GW-C1-001, Rev. 3, "AP1000 Civil/Structural Design Criteria," February 2015.

16.7 Westinghouse Report APP-GW-G1-003, Rev. 6, "AP1000 Seismic Design Criteria," August 2011.

16.8 Not used

16.9 Westinghouse Report UKP-1000-GEC-004, Rev. 1, "UK AP1000 Barrier Matrix," January 2017.

16.10 Westinghouse Report APP-GW-N1-001, Rev. 5, "Pipe Rupture Protection Design Criteria for AP1000 Plant," April 2015.

16.11 Not used

16.12 Westinghouse Report APP-GW-S1-004, Rev. 0, "AP1000 Design Guide for Wind and Tornado," August 2010.

16.13 Westinghouse Report APP-GW-GLR-133, Rev. 1, "Summary of Automobile Tornado Missile 30' Above Grade," May 2010.

16.14 Westinghouse Report UKP-GW-GL-799, Rev. 2, "AP1000 Plant ALARP Assessment of Structural Impact from Fuel Handling Area Pools Leakage," August 2016.

16.15 ACI 349-01, "Code Requirements for Nuclear Safety Related Concrete Structures and Commentary," American Concrete Institute, February 2001.

16.16 AISC S335, "Specification for Structural Steel Buildings," American Institute of Steel Construction, June 1989.

16.17 Uniform Building Code, International Council of Building Officials, 1997.

16.18 ASCE 4-98 "Seismic Analysis of Safety-Related Nuclear Structures," American Society of Civil Engineers, January 2000.

16.19 Westinghouse Report UKP-GW-GL-045, Rev. 2, "AP1000 Equivalence/ Maturity Study of the U.S. Codes and Standards," September 2011.

16.20 ASCE 7-98 "Minimum Design Loads for Buildings and Other Structures," American Society of Civil Engineers, March 2000.

16.21 BNFL Report "R3 Impact Assessment Procedure, Missiles, Blast, Jets, Pipewhip and Impact," Rev. 4, British Nuclear Fuels Limited, October 2005.

16.22 J. M. Biggs, *Introduction to Structural Dynamics,* McGraw-Hill Book Company, (New York, June 1964).

16.23 ACI 237R-07, "Self-Consolidating Concrete," American Concrete Institute, April 2007.

16.24 ANSI/AISC-N690-1994, "Specification for the Design, Fabrication, and Erection of Steel Safety-Related Structures for Nuclear Facilities," American National Standards Institute/American Institute of Steel Construction, 1994.

16.25 AISC 341, "Seismic Provisions for Structural Steel Buildings," April 1997, including Supplement 2, American Institute of Steel Construction, November 2000.

16.26 ACI 318-99, "Building Code Requirements for Structural Concrete and Commentary," American Concrete Institute, March 1999.

16.27 Westinghouse Report APP-RXS-M8-001, Rev. 6, "Reactor System (RXS) Interface Control Document (ICD)," March 2016.

16.28 Not used

16.29 Not used

16.30 NA to BS EN 1990: 2002+A1:2005, "UK National Annex for Eurocode. Basis of Structural Design," British Standards Institution, December 2004.

16.31 USNRC Regulatory Guide 1.60, Design Response Spectra for Seismic Design of Nuclear Power Plants, Rev. 1, December 1973

16.32 Westinghouse Report APP-GW-S2R-010, Rev. 5, "Extension of Nuclear Island Seismic Analyses to Soil Sites," March 2011.

16.33 Not Used.

16.34 Not Used.

16.35 Not Used.

16.36 "Manual for Railway Engineering," American Railway Engineering and Maintenance-of-Way Association, 1990.

16.37 "AASHTO Specification for Highway Bridges," American Association of State Highway and Transportation Officials, 1989.

16.38 Westinghouse Report APP-GW-SUP-001, Rev. 4, "Design Methodology for Structural Modules," May 2014.

16.39 Westinghouse Letter DCP_JNE_000484, "Response to Action Items from November 30-December 2 GDA Civil Engineering Meeting," December 2010.

16.40 Westinghouse Letter DCP_JNE_000493, "Response to Action Items from GDA Civil Engineering Meeting," December 2010.

16.41 Westinghouse Letter DCP_JNE_000496, "Response to Action Items from GDA Civil Engineering Meeting," January 2011.

16.42 Westinghouse Report APP-GW-G1-011, Rev. 7, "AP1000 Plant Metrication Strategy and ALARP Assessment for the United Kingdom," November 2016.

16.43 ANS 57.2-1983, "Design Requirements for Light Water Reactors Spent Fuel Storage Facilities at Nuclear Power Plants," 1983.

16.44 ACI 318-11, "Building Code Requirements for Structural Concrete," 2011.

16.45 Westinghouse Report APP-5000-S2C-001, Rev 0, "AP1000 Radwaste Building Seismic Interaction," November 2009.

16.46 Westinghouse Report APP-1100-SUC-005, Rev 0, "Structural Modules - Containment – Effects of Concrete Placement Stresses," December 2005.

16.47 Westinghouse Report APP-SB01-Z0-001, Rev 1, "AP1000 Containment Vessel Air Baffle Functional Specification," July 2011.

16.48 Westinghouse Drawing APP-1010-ARK-021 Rev 1, "Nuclear Island General Arrangement Plan at Elevation 66'-6" (89.789 m)," October 2008.

16.49 Westinghouse Drawing APP-1020-ARK-021 Rev 1, "Nuclear Island General Arrangement Plan at Elevation 82'-6" (94.666 m)," October 2008.

16.50 Westinghouse Drawing APP-1020-ARK-022 Rev 2, "Nuclear Island General Arrangement Plan at Elevation 96'-6" (98.932 m)," October 2008.

16.51 Westinghouse Drawing APP-1030-ARK-021 Rev 3, "Nuclear Island General Arrangement Plan at Elevation 107'-2" (102.184 m) & 111'-0" (103.353 m)," October 2008.

16.52 Westinghouse Drawing APP-1040-ARK-021 Rev 4, "Nuclear Island General Arrangement Plan at Elevation 117'-6" (105.334 m) & 130'-0" (109.144 m)," October 2008.

16.53 Westinghouse Drawing APP-1040-P2K-001 Rev 7, "Nuclear Island General Arrangement Plan at Elevation 117'-6" (105.334 m) with Equipment," November 2015.

16.54 Westinghouse Drawing APP-1050-ARK-021 Rev 4, "Nuclear Island General Arrangement Plan at El. 135'-3" (110.740 m)," October 2008.

16.55 Westinghouse Drawing APP-1060-ARK-021 Rev 4, "Nuclear Island General Arrangement Plan at Elevation 153'-0" (116.154 m) & 160'-6" (118.440 m)," October 2008.

16.56 Westinghouse Drawing APP-1070-ARK-021 Rev 2, "Nuclear Island General Arrangement Plan at Elevation 160'-6" (118.440 m)& 180'-0" (124.384 m)," October 2008.

16.57 Westinghouse Drawing APP-1000-ARK-921 Rev 5, "Nuclear Island General Arrangement Section A-A," October 2008.

16.58 Westinghouse Drawing APP-1000-P2K-901 Rev 5, "Nuclear Island General Arrangement Section A-A with Equipment," October 2008.

16.59 Westinghouse Drawing APP-1000-ARK-922 Rev 3, "Nuclear Island General Arrangement Section B-B," October 2008.

16.60 Westinghouse Drawing APP-1000-P2K-902 Rev 6, "Nuclear Island General Arrangement Section B-B with Equipment," October 2008.

16.61 Westinghouse Drawing APP-4000-AR-901 Rev.1, "Annex Building General Arrangement Section A-A," August 2007.

16.62 Westinghouse Drawing APP-4030-ARK-001 Rev 2, "Annex Building General Arrangement Plan at Elevation 100'-0" (100.00 m)," February 2011.

16.63 Westinghouse Drawing APP-4040-ARK-001 Rev 1, "Annex Building General Arrangement Plan at Elevation 117'-6" (105.334 m) & 126'-3" (108.00 m)," February 2011.

16.64 Westinghouse Drawing APP-4050-ARK-001 Rev 1, "Annex Building General Arrangement Plan at Elevation 135'-3" (110.74 m), 156'-0" (117.009 m) & 158'-0" (117.678 m)," February 2011.

16.65 Westinghouse Drawing APP-6030-ARK-001 Rev 1, "Diesel Generator Building General Arrangement Plan at Elevation 100'-0" (100.00 m) & Section A-A," August 2007.

16.66 Westinghouse Drawing APP-5000-ARK-001 Rev 0, "Radwaste Building General Arrangement Plan at Elevation 100'-0" (100.00 m)," August 2007.

16.67 Westinghouse Drawing APP-2030-ARK-001 Rev 1, "Turbine Building General Arrangement Plan at Elevation 100'-0" (100.00 m)," May 2009.

16.68 Westinghouse Drawing APP-2040-ARK-001 Rev 1, "Turbine Building General Arrangement Plan at Elevation 117'-6" (105.334 m)," June 2009.

16.69 Westinghouse Drawing APP-2050-ARK-001 Rev 2, "Turbine Building General Arrangement Plan at Elevation 135'-3" (110.74 m)," June 2009.

16.70 Westinghouse Drawing APP-2060-ARK-001 Rev 0, "Turbine Building General Arrangement Plan at Elevation 161′-0″," August 2007.

16.71 Westinghouse Drawing APP-2060-P2K-001 Rev 1, "Turbine Building General Arrangement Plan at Elevation 161′-0″ with Equipment," June 2009.

16.72 Westinghouse Drawing APP-2070-ARK-001 Rev 1, "Turbine Building General Arrangement Plan at Elevation 245′-0″ & 226′-0″," June 2009.

16.73 Westinghouse Drawing APP-2000-ARK-901 Rev 1, "Turbine Building General Arrangement Section A-A," May 2009.

16.74 Westinghouse Drawing APP-2000-ARK-902 Rev 1, "Turbine Building General Arrangement Section B-B," May 2009.

16.75 Westinghouse Drawing APP-1010-C2K-001 Rev 1, "Nuclear Island Key Structural Dimensions Plan at El. 66'-6" (89.789 m)," October 2008.

16.76 Westinghouse Drawing APP-1020-C2K-001 Rev 1, "Nuclear Island Key Structural Dimensions Plan at El. 82'-6" (94.666 m)," October 2008.

16.77 Westinghouse Drawing APP-1030-C2K-001 Rev 1, "Nuclear Island Key Structural Dimensions Plan at El. 100'-0" (100.00 m)," October 2008.

16.78 Westinghouse Drawing APP-1040-C2K-001 Rev 1, "Nuclear Island Key Structural Dimensions Plan at El. 117'-6" (105.334 m)," October 2008.

16.79 Westinghouse Drawing APP-1050-C2K-001 Rev 2, "Nuclear Island Key Structural Dimensions Plan at El. 135'-3" (110.740 m)," October 2008.

16.80 Westinghouse Drawing APP-1060-C2K-001 Rev 2, "Nuclear Island Key Structural Dimensions Plan at El. 153'-0" (116.154 m)," October 2008.

16.81 Westinghouse Drawing APP-1070-C2K-001 Rev 1, "Nuclear Island Key Structural Dimensions Plan at El. 160'-6" (118.440 m)," October 2008.

16.82 Westinghouse Drawing APP-1000-C2K-901 Rev 2, "Nuclear Island Key Structural Dimensions Section A – A," October 2008.

16.83 Westinghouse Drawing APP-1000-C2K-902 Rev 2, "Nuclear Island Key Structural Dimensions Section B – B," October 2008.

16.84 Westinghouse Drawing APP-1000-C2K-903 Rev 1, "Nuclear Island Key Structural Dimensions Sections C - C and H – H," October 2008.

16.85 Westinghouse Drawing APP-1000-C2K-904 Rev 1, "Nuclear Island Key Structural Dimensions Section G – G," October 2008.

16.86 Westinghouse Drawing APP-1000-C2K-905 Rev 1, "Nuclear Island Key Structural Dimensions Section J – J," October 2008.

16.87 Westinghouse Drawing APP-4030-C2K-001 Rev 1, "Annex Building Key Structural Dimensions Plan at Elevation 100'-0" (100.000 m)," February 2009.

16.88 Westinghouse Drawing APP-4040-C2K-001 Rev 1, "Annex Building Key Structural Dimensions Plan at Elevation 107'-2" (102.184 m) and 117'-6" (105.334 m)," February 2009.

16.89 Westinghouse Drawing APP-4050-C2K-001 Rev 1, "Annex Building Key Structural Dimensions Plan at Elevation 135'-3" (110.74 m)," February 2009.

16.90 Westinghouse Drawing APP-4060-C2K-001 Rev 1, "Annex Building Key Structural Dimensions Plan at Elevation 158'-0" (117.678 m) and 146'-3" (114.097 m)," February 2009.

16.91 Westinghouse Drawing APP-4070-C2K-001 Rev 0, "Annex Building Key Structural Dimensions Roof Plan at Elevation 154'-0" (116.46 m) and 181'-11 ¾" (124.99 m)," August 2007.

16.92 Westinghouse Drawing APP-4000-C2K-901 Rev 1, "Annex Building Key Structural Dimensions Section A – A," February 2009.

16.93 Westinghouse Drawing APP-4000-C2K-902 Rev 0, "Annex Building Key Structural Dimensions Section B – B," August 2007.

16.94 Westinghouse Drawing APP-4000-C2K-903 Rev 0, "Annex Building Key Structural Dimensions Section C – C," August 2007.

16.95 Westinghouse Drawing APP-4000-C2K-904 Rev 1, "Annex Building Key Structural Dimensions Sections D - D, E - E, & F – F," February 2009.

16.96 Westinghouse Drawing APP-4000-C2K-905 Rev 1, "Annex Building Key Structural Dimensions Sections G - G, H - H, & J – J," February 2009.

16.97 Westinghouse Drawing APP-0000-X2K-011 Rev 0, "Foundation Plan," August 2007.

Table 16-1. UK Categorisation and Classification of Civil Engineering Structures

Structure	UK Cat/Class[1]	Seismic Category[2]
• Nuclear Island:		
– Basemat	A1	I
– Containment internal structures	A1	I
– Structural CA wall modules	A1	I
– Structural floor modules	A1	I
– Shield building	A1	I
– Auxiliary building	A1	I
– Foundations	A1	I
• Other structures:		
– Turbine building first bay	A2	II
– Turbine building excluding first bay	C3	NNS
– Diesel generator building	A2	NNS
– Annex building	A2/GNS	II/NNS
– SWS Cooling towers	A2	NNS
– Radwaste building	B3	NNS

Notes:

1. UK categorisation and classification are explained in Chapter 5.
2. Seismic categories are explained in Section 16.3.

Table 16-2. Natural External Hazards – Justification Logic for A2 Structures

Activity	Seismic Category	Requirement for A2 Civil Structures	Reasoning
Loading specification	II	Hazard loading considered to be the same as for C-I structures, i.e., SSE, tornado, extreme wind.	C-II structures are positioned where they could strike and impair the function of a Class 1 SSC. This must not occur for any event under which the Class 1 SSC has been designed to function; therefore, C-II structures must be designed to withstand the same hazard loads as C-I structures.
	NNS	Hazard loading considered in the design as normal practice for industrial structures situated in onerous regions of the world, including seismic regions.	Seismic category NNS structures are located so that their failure could not cause any adverse interaction with a Class 1 system. UK environments are generally more benign than those considered in the design for onerous regions of the world, (see Chapter 12); therefore, hazard loading exceeds UK practice for normal industrial structures. Seismic category NNS structures have hazard-withstand capabilities in between those of C-I structures and normal UK industrial structures.
Structural analysis	II	Use of ASCE 4-98 (Reference 16.18) for seismic analysis, as noted in the civil structural design criteria (Reference 16.6, Table 2), supplemented by information presented in the AP1000 seismic design criteria (Reference 16.7, Section 6). Otherwise, use of normal structural analysis tools is as explained in Reference 16.6, Sections 9 and 10.	Seismic analysis approach is consistent with that adopted for C-I structures. Normal structural analysis tools will provide results of sufficient reliability, provided that appropriate verification and validation procedures are in place.
	NNS	Seismic methods presented in UBC 1997 (Reference 16.17) and use of normal structural analysis tools as explained in Reference 16.6, Sections 9 and 10. See note 1.	Use of simplified methods of seismic analysis, as presented in UBC 1997, is justified for the same reasons noted above against “Loading Specification” for seismic category NNS structures.

Table 16-2. Natural External Hazards – Justification Logic for A2 Structures (cont.)

Activity	Seismic Category	Requirement for A2 Civil Structures	Reasoning
Design/ acceptance criteria	II	Strength of sections determined using ACI 349-01 (Reference 16.15) for reinforced concrete and ANSI/AISC- N690-1994 (Reference 16.24) for structural steelwork (Reference 16.6, Tables 5 and 6).	C-II structures are positioned where they could strike and impair the function of a Class 1 SSC. This must not occur for any event under which the Class 1 SSC has been designed to function. Therefore C-II structures are designed to the same standards as C-I structures.
	NNS	Load cases analysed as presented in Reference 16.6, Tables 7 and 8. Class 2 structures, designated NNS, are designed to ACI 318-99 (Reference 16.26) and AISC S335 (Reference 16.16). These structures will comply with the requirements of UBC 1997 (Reference 16.17). See note 1.	Using non-nuclear specific methods of design is justified for the same reasons noted above against "Loading Specification" for seismic category NNS structures.
Construction	II	The requirements for construction quality assurance during construction are in accordance with ACI 318-99 and AISC S335 (References 16.26 and 16.16).	Provision for using non-nuclear specific controls during construction for C-II structures is justified for the same reasons noted above against "Structural Detailing" applied to C-II structures.
	NNS	As above for C-II.	Provision for using non-nuclear specific controls during construction for NNS structures is justified for the same reasons noted above against "Structural Detailing" applied to C-II structures.

Note: 1) The NNS structures are being redesigned to UK codes; the structural design will use seismic input and design codes to provide margin similar to that provided by the US codes.

Table 16-3. Site Interface Parameters for Civil Design (Excluding Turbine Building) (Reference 16.6, Section 5.2.3 and Table 1)

Parameter	Value	
External building temperatures (excluding nuclear island)	Maximum: Minimum:	38.33°C -23.33°C
Temperatures external to the nuclear island	Maximum: Minimum:	46.11°C dry bulb 30.06°C wet bulb -40 °C
Design Wind speed (1 in 50 year) (3-second gust)		64.82 m/sec
Tornado wind (1 in 1,000,000 year):		
– Design velocity		134.11 m/sec
– Radius of maximum rotational wind from tornado centre		45.7 m
– Atmospheric pressure change		13.8 kN/m^2
– Rate of pressure change		8.3 kN/m^2/sec
• Tornado missiles:		
– 1814-kg automobile (deformable) able to impact the nuclear island at all elevations above grade (Reference 16.13) and other structures at elevations up to 9.1 m above grade.	Horizontal velocity: or Vertical velocity:	47 m/sec 33 m/sec
– A rigid 124.7-kg missile, assumed to be a 203.2-mm diameter armour piercing artillery shell striking the face of a structure at normal incidence.	Horizontal velocity: or Vertical velocity:	47 m/sec 33 m/sec
– A solid steel sphere 25 mm in diameter able to pass through any openings in the protective barriers and assumed to be travelling in the most damaging direction.	Velocity:	47 m/sec 89.41 m/sec
Hurricane wind speed 1 in 10,000 year (3-second gust)		
• Hurricane missiles (injected into the wind at a height of 10 m, unless stated otherwise):		
– 100 mm x 300 mm x 3.65 m long wood plank weighing 90 kg	Velocity:	41.1 m/sec
– 3 m long 75 mm diameter steel pipe weighing 35 kg	Velocity:	21.9 m/sec
– 0.9 m long 25 mm steel rod weighing 3.7 kg	Velocity:	21.9 m/sec
– 3 m long 150 mm diameter steel pipe weighing 130 kg	Velocity:	14.3 m/sec
– 4.5 m long 300 mm steel pipe weighing 337 kg	Velocity:	11.2 m/sec
– 10.7 m long 340 mm diameter telegraph pole weighing 675 kg, injected into the wind at a height of 6 m	Velocity:	11 m/sec
– 2 m x 1.3 m x 5 m car weighing 1814 kg, injected into the wind at a height of 3 m	Velocity:	7.1 m/sec
Standard plant SSE peak ground acceleration		0.3g

Table 16-3. Site Interface Parameters for Civil Design (Excluding Turbine Building) (Reference 16.6, Section 5.2.3 and Table 1) (cont.)

Parameter	Value
Soil parameters:	
– Average allowable static soil-bearing capacity	The allowable bearing capacity, including a factor of safety appropriate for the design load combination, shall be greater than or equal to 426.1 kN/m2 over the footprint of the nuclear island at its excavation depth.
– Maximum allowable dynamic bearing capacity for normal loads plus the SSE	The allowable bearing capacity, including a factor of safety appropriate for the design load combination, shall be greater than or equal to the maximum bearing demand of 1675.8 kN/m2 at the edge of the nuclear island at its excavation depth, or site-specific analyses demonstrate a factor of safety appropriate for normal and SSE loads.
– Minimum soil angle of internal friction	Greater than or equal to 35 degrees below footprint of nuclear island at its excavation depth.
– Shear wave velocity	Greater than or equal to 305 m/sec at the bottom of the foundation, and greater than or equal to 152.5 m/sec at the free surface.
– Liquefaction potential	Negligible
– Lateral variability	Soils supporting the nuclear island should not have extreme variability in subgrade stiffness. (To be demonstrated as shown in Table 4-9 .)
Flood level	Less than plant elevation +100 m
Ground water level	Less than plant elevation +99.39 m
Precipitation:	525.8 mm/hr
– Rain (Probable Maximum Precipitation)	160.0 mm/5 min
– Roof snow/ice 1 in 50 year	3.0 kN/m^2
– Ground snow/ice 1 in 50 year	3.6 kN/m^2

Table 16-4. Building Floor Live Loads
(Reference 16.6, Section 5.2.2)

Building Floor Area(1)	Floor Loading
Containment operating deck	38.3 kN/m^2 (during maintenance and refuelling outages). 9.6 kN/m^2 (during normal operation).
Offices	2.4 kN/m^2
Assembly and locker rooms	4.8 kN/m^2
Laboratories and laundry rooms	4.8 kN/m^2
Stairs and walkways	4.8 kN/m^2 (or a moving concentrated Load of 4.44 kN).
Structural platforms and gratings	4.8 kN/m^2 (However, the grating areas of concrete floors shall be designed for the same live load as the adjacent concrete floor.)
Maintenance & service platforms	(Load shall be calculated for individual locations based on the functional requirements and service equipment).
All other floors (ground floor and elevated floors)	9.6 kN/m^2 (For non-seismic load combinations and for global seismic analysis, this load shall be reduced if the equivalent dead load on the floor is more than 2.4 kN/m^2. The sum of the live load and the equivalent dead load shall be 12 kN/m^2).
In design reconciliation analysis, if actual loads are established to be lower than the above loads, the actual loads may be used for reconciliation. Floor live loads for the design of the operational areas will not be reduced below 4.8 kN/m^2.	
Railroad support structures Truck support structures	Based on American Railway Engineering and Maintenance-of-Way Association manual (Reference 16.36). HS20 loading per American Association of State Highway and Transportation Officials standards (Reference 16.37).

Table 16-5. Roof Loads
(Reference 16.6, Section 5.2.2)

Roof Area	Roof Loading
General	1.43 kN/m^2 or a uniform snow load, whichever is greater.

Table 16-6. Concentrated Loads for the Design of Local Members
(Reference 16.6, Section 5.2.2)

Local Member Type[(1)]	Concentrated Load
Concentrated load on beams and girders, in load combinations that exclude seismic.	22.2 kN to be applied to maximise the induced moment or shear. This load is not carried to the columns. It is not applied in office or access controlled areas (areas where no heavy equipment will be located or transported).
Concentrated load on slabs, to be considered with dead load only.	22.2 kN to be applied to maximise the induced moment or shear. This load is not cumulative and is not carried to the columns. It is not applied in office or access controlled areas (areas where no heavy equipment will be located or transported).

Note:
1. In design reconciliation analysis, if actual loads are established to be lower than the above loads, the actual loads may be used for reconciliation.

Table 16-7. Construction Loads and Temporary Exterior Wall Surcharge
(Reference 16.6, Section 5.2.2)

Local Member Type	Concentrated Load
Applicable exterior subsurface wall	The more critical of either a minimum surcharge outside and adjacent to the subsurface wall of 12 kN/m^2 or a railroad surcharge (the 12 kN/m^2 is a wheel load converted to a lateral equivalent).
Construction live load	Loads produced by cranes, trucks or any type of vehicle when fully loaded, as required for construction.
Steel beams supporting concrete floors	Weight of concrete plus 4.8 kN/m^2 uniform load or 22.2 kN concentrated load, distributed near points of maximum shear and moment. Allowable stresses are permitted to be increased by a third.
Metal decking and precast concrete panels used as formwork concrete floors	Weight of wet concrete plus a uniform live load of 0.96 kN/m^2 or a concentrated load of 0.67 kN.

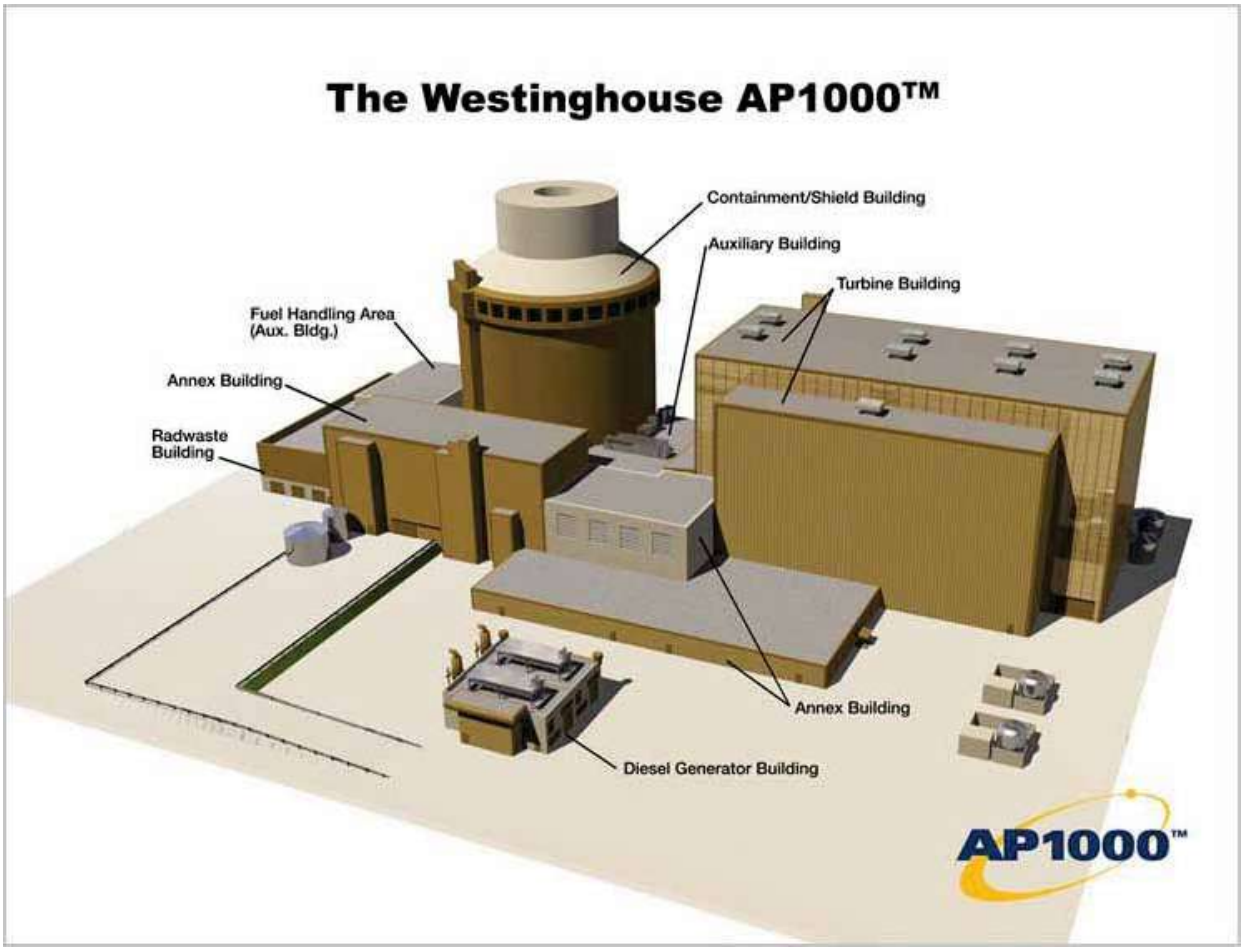


Figure 16-1. General Arrangement of the AP1000 Plant

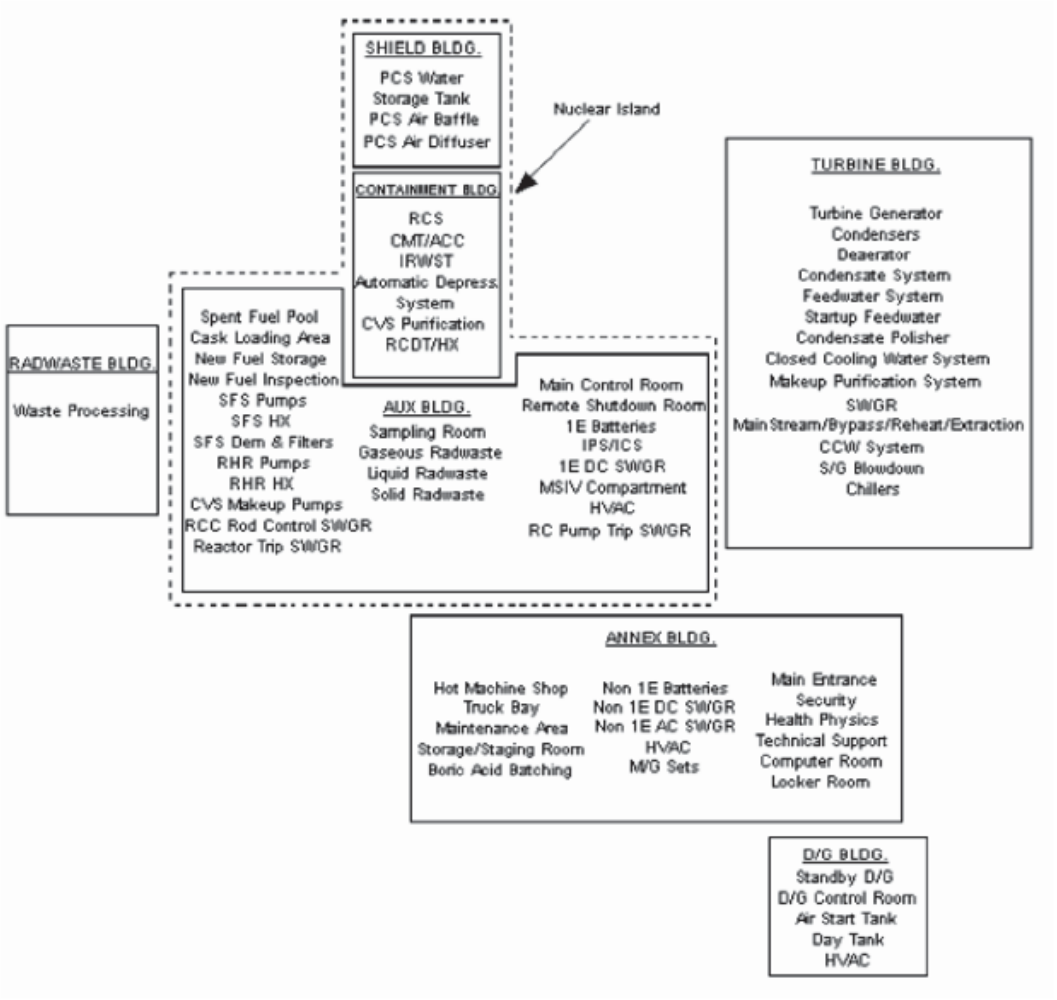


Figure 16-2. Location of Systems within the AP1000 Civil Engineering Structures

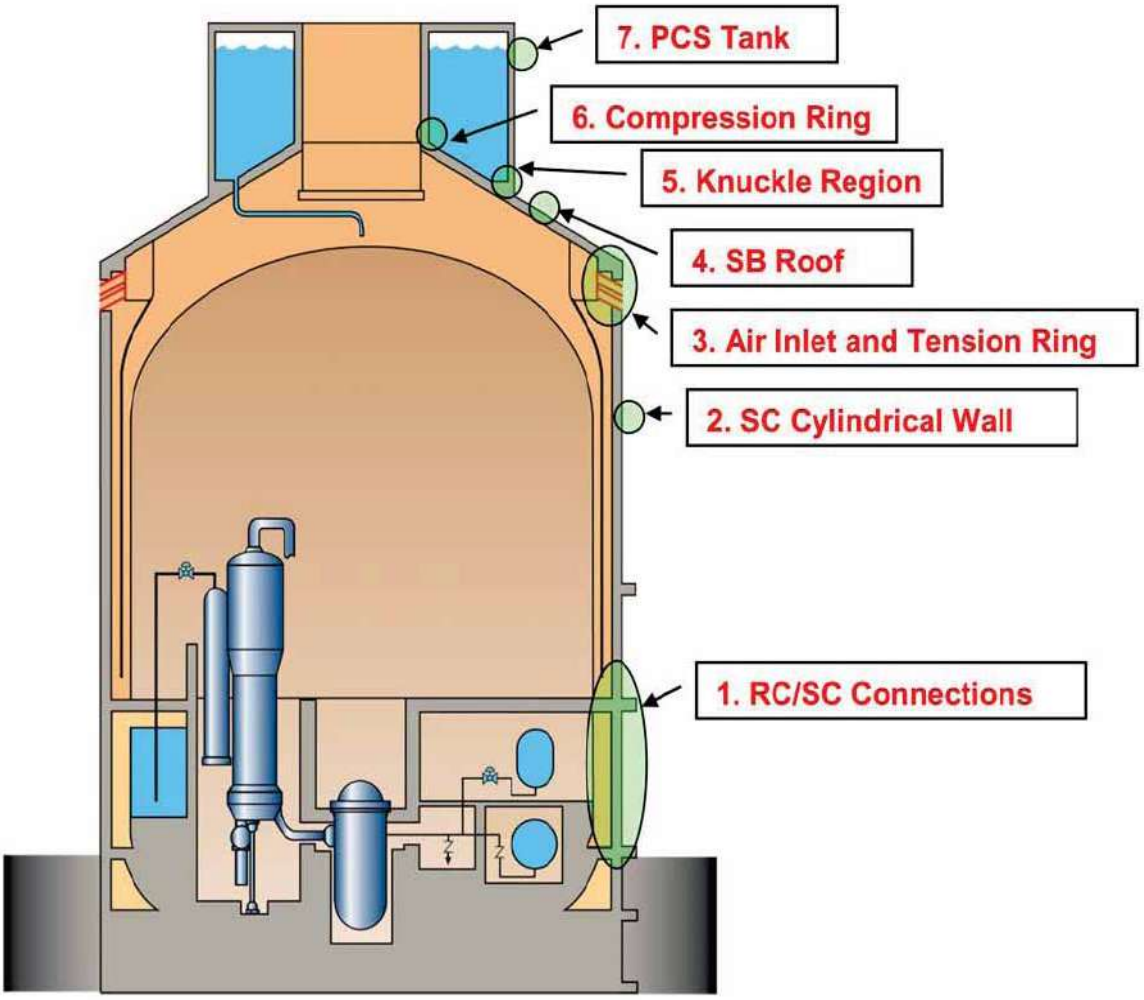


Figure 16-3. Section through Shield Building Showing Key Structural Features

TABLE OF CONTENTS

LIST OF TABLES

None

LIST OF FIGURES

None

LIST OF ABBREVIATIONS, ACRONYMS, AND TRADEMARKS

ac	alternating current
ACI	American Concrete Institute
ADS	automatic depressurisation system
ALARP	as low as reasonably practicable
ALWR	advanced light water reactor
ANS	American Nuclear Society
ASME	American Society of Mechanical Engineers
ATWT	anticipated transient without trip
BDS	steam generator blowdown system
C-I	Category I
C-II	Category II
CCS	component cooling water system
CIV	containment isolation valve
CMT	core makeup tank
CRDM	control rod drive mechanism
CST	condensate storage tank
CVS	chemical and volume control system
DAS	diverse actuation system
dc	direct current
DNB	departure from nucleate boiling
DOS	standby diesel and auxiliary boiler fuel oil system
D-RAP	Design Reliability Assurance Programme
ECS	main ac power system
EMIT	examination, maintenance, inspection, and testing
FHS	fuel handling and refuelling system
FPS	fire protection system
FWS	feedwater system (main and startup feedwater system)
HVAC	heating, ventilation, and air conditioning
HX	heat exchanger
ILRT	integrated leak rate test
INPO	Institute of Nuclear Power Operations
IRWST	in-containment refuelling water storage tank
ISLOCA	interfacing system loss-of-coolant accident
IST	in-service testing
LOCA	loss-of-coolant accident
LLRT	local leak rate test
LTOP	low temperature overpressure protection
MCR	main control room
MFCV	main feedwater control valve
MFIV	main feedwater isolation valve
MSIV	main steam isolation valve
MSR	moisture separator reheater
MSS	main steam system
MTS	main turbine system
NI	nuclear island
PCCWST	passive containment cooling water storage tank
PCCAWST	passive containment cooling ancillary water storage tank
PCS	passive containment cooling system
PCSR	Pre-Construction Safety Report
PLS	plant control system
PMS	protection and safety monitoring system

LIST OF ABBREVIATIONS, ACRONYMS, AND TRADEMARKS (cont.)

PORV	power-operated relief valve
PRHR	passive residual heat removal
PSA	probabilistic safety assessment
PWR	pressurised water reactor
PXS	passive core cooling system
RCCA	rod control cluster assembly
RCP	reactor coolant pump
RCS	reactor coolant system
RNS	normal residual heat removal system
RXS	reactor system
SFCV	startup feedwater control valve
SFIV	startup feedwater isolation valve
SFP	spent fuel pool
SFS	spent fuel pool cooling system
SFW	startup feedwater
SG	steam generator
SGS	steam generator system
SGTR	steam generator tube rupture
SSC	systems, structures, or components
SSD	system specification document
SWS	service water system
Tech Spec	technical specification
URD	Utility Requirements Document
VTS	turbine building ventilation system
VWS	central chilled water system
VXS	annex/auxiliary building non-radioactive HVAC system
ZOS	onsite standby power system

TRADEMARKS

Inconel is a registered trademark of Special Metals Corporation.

17 MECHANICAL ENGINEERING

17.1 Introduction

This chapter provides the evidence that the mechanical engineering design of the systems in the AP1000 plant is adequate to meet the safety claims placed upon these systems in other parts of the safety case, both for normal operations and under fault conditions. System Specification Documents (SSDs) are referenced for each relevant mechanical system. The SSD provides additional details and evidence for the safety claims placed upon SSCs. Each SSD identifies the specific design requirements for the system and documents the system design that satisfies the requirements. SSDs do the following:

- Summarises the functions, design criteria, and design data of system
- Describes system layout, instrumentation and control, interfacing systems, and environmental requirements.
- Describes system operations and identifies examination, maintenance, inspection, and testing (EMIT) guidelines.
- Listing of the pertinent Piping and Instrumentation Diagrams for the system.
- Lists supporting references

The mechanical systems largely provide safety functions to prevent fuel damage and the consequent release of radioactivity. Analysis of these systems has therefore been carried out to review their requirements against three primary safety functions: reactivity control, heat transfer/residual heat removal, and containment. The intention of the justification against these safety functions is to demonstrate how the risks have been reduced to a level that can be considered as low as reasonably practicable (ALARP).

The mechanical systems, subsystems, and components and their operation are described in Chapter 6. Consequently, Chapters 6 and 17 are interrelated and complement each other. In addition, Appendix 15A contains the various component safety categorisation and classification.

Generic component failure data parameters for the SSCs discussed in Chapter 17 are shown in Table 10-34 and Table 10-35. The component failure data is used as an input to the AP1000 plant Probabilistic Safety Assessment (PSA) discussed in Chapter 10.

Justification against the reactivity control primary safety function considers the way in that the mechanical design of plant systems can influence control of the nuclear fission chain reaction in the reactor core.

Justification against the heat transfer/residual heat removal primary safety function considers the way in that the mechanical design of plant systems influences the management of heat from its production in the fuel assemblies to its dispersal in the ultimate heat sink.

Justification against the containment primary safety function examines how the mechanical design of plant systems ensures that the containment boundary provided by the fuel cladding is protected. It also examines how the containment provided by the reactor coolant system (RCS), and the associated systems linked to it, are protected. Finally, it reviews how the containment provided by the containment vessel is protected.

The report against each of the relevant mechanical systems is structured:

- Discussion of its role in normal and abnormal operation and identification of the primary safety functions to that the system contributes; and discussion of how the system contributes to the relevant primary safety functions.

- Description of the relevant system's structures and components that contribute to providing the system function.

- Classification and categorisation of these components and identification of what they must do to meet any safety requirements..

- Justification of requirements.

It is noted that for components that provide a Category A, Class 1 structural pressure boundary function and which do not have any other Class 1 or 2 safety function and no claim is made, a specific description has not been included in the discussion below. These components however are included in the safety categorisation and classification listing provided in Appendix 15A. Examples include components such as a closed vent or drain valve in the RCS pressure boundary, check valves that prevent backflow and which have no safety function to open, and the RCS pressuriser heaters.

Note the components within this chapter designed to the ASME Boiler and Pressure Code Section III are Division 1. The value following "Section III" (if specified) indicates the ASME BPVC Class.

17.2 Scope of Mechanical Systems

The scope of mechanical systems has been selected by examination of fault studies work and can be grouped as those that interface directly with reactor control or are directly connected to the RCS function as part of the engineered safety features

The mechanical equipment and systems are grouped by their functions:

- Function as part of the RCS and the reactor itself

- Are associated with the provision of feedwater to, and the acceptance of steam from, the steam generators (SGs)

- Collectively make up the passive core cooling system (PXS)

- Provide and help to maintain the integrity of the reactor containment

- Are associated with the movement of new and irradiated fuel

- Are associated with the handling of heavy loads over the reactor and RCS and also around the spent fuel pool (SFP)

- Are associated with the safe storage of irradiated fuel

- Are other mechanical systems that support other systems in the provision of their safety roles

17.3 REACTOR COOLANT AND ASSOCIATED SYSTEMS

17.3.1 Reactor Coolant Pumps (RCS-MP-01A/B, RCS-MP-02A/B)

17.3.1.1 Role

A detailed description of the reactor coolant pumps (RCPs) is given in Section 6.4. See Reference 17.1 for more detail on the Reactor Coolant System.

The pumps draw RCS primary coolant from the SG (RCS-MB-01/02) cold side channel head and pump it, via the RCS cold leg pipework, into the reactor vessel where the water is heated. The water then flows, via the RCS hot leg pipework, into the SGs where the water is cooled and returns to the RCP suction. The continued operation of the RCPs is required to permit removal of fission and decay heat from the reactor core when the plant is at power. If they fail during power operation, then the capacity for heat removal is reduced and there are consequent demands on the protection system to shut the reactor down. The pumps are not a part of a formal safety system, but their continued operation is required to permit removal of fission heat from the core when the reactor is at power. Whilst the normal operation of the pumps is not part of a safety function, there is a requirement for them to continue to provide circulation during coastdown following a loss of their ac electrical power supplies that is consistent with the time required for reactor trip. The RCPs also form a portion of the RCS natural circulation flow path if they lose power supplies. This feature contributes to the heat transfer/residual heat removal primary safety function.

The pumps are also structurally a part of the RCS and therefore, in terms of structural integrity, they have a role in providing RCS primary circuit integrity. This contributes to the containment primary safety function. Three concerns are associated with structural integrity:

- The RCS pressure boundary remains intact to ensure that RCS water inventory is maintained.

- The consequences of impact of any debris created through the failure of pump internals does not lead either to direct damage to fuel or to fuel damage due to overheating caused by impaired coolant flows.

- The disintegration of the pump flywheel does not cause consequential damage to the RCS pressure boundary or cause missiles which jeopardise the containment vessel boundary function.

There are four RCPs. Each one consists of a removable pump assembly that includes the rotating assembly, motor stator, and casing. Through the use of a sealless, wet-wound motor, there is no need for a seal assembly associated with the pump unit. It also means that the pump unit is lubricated by primary coolant, thus removing the requirement for a lubricating oil system. There is, however, a motor cooler that is required to operate whenever the RCP is running. This cooler enables the pump motor and bearings to operate at a temperature that is consistent with their design. The rotating assembly includes a flywheel to ensure that an appropriate pump coastdown characteristic is provided. A thermal barrier assembly is provided to remove heat generated by the flywheel and enable the flywheel to operate at a low and uniform temperature.

Cooling to the RCP motor coolers and the thermal barrier is provided by the component cooling water system (CCS) and this system therefore supports the RCPs in normal operation. It does not support structural integrity and the associated safety requirements.

The RCPs do not support other systems in their safety functions.

17.3.1.2 System Components and Equipment Contributing to Safety Function

The pump impeller, flywheel, motor electrical rotor, and shaft are linked together solidly and form an integral rotating assembly. The flywheel casing/thermal barrier and the motor casing are all bolted to the pump casing and form an integral RCS pressure boundary. The following components contribute to the RCPs performing their safety function:

- **Pump unit** – One pump unit is associated with each RCP. Each one is a single-stage centrifugal pump designed to produce an approximate head of 111 m (365 ft) at the the approximate design flow rate of 17,900 m^3/hr (78,750 gpm). The pump casing is manufactured from a ferritic forging with an austenitic cladding of the wetted surface and is designed for approximately 17.2 MPa (2,500 psia) and 343°C (650°F). The unit is mounted vertically onto the bottom of the SG channel head and all bearings are lubricated by the RCS primary coolant. There is no separate lubrication system. A requirement that the pumps can be shut down on demand is achieved through isolation of the electrical supply and is not therefore a feature of the pump itself.

- **Flywheel/thermal barrier assembly** – A single flywheel/thermal barrier assembly is associated with each RCP. The flywheel is formed from a single stainless-steel forging with axially aligned holes into that tungsten cylinders are fitted. The tungsten cylinders provide flywheel mass whilst the stainless-steel forging acts as the structural component. The thermal barrier is supplied with a cooling flow from the CCS and serves to cool the water that circulates from the pump casing into the motor assembly to ensure that the flywheel energy does not heat up the pump motor. The thermal barrier is an integral part of the forged martensitic stainless-steel pressure casing. The safety requirements are that the components forming part of the RCS pressure boundary will maintain their structural integrity, the flywheel assembly will also maintain its structural integrity, and the flywheel assembly will provide enough rotational inertia to provide the required coastdown characteristics for the entire pump, motor rotor, shaft, and flywheel assembly.

- **Motor unit** – A single motor is associated with each RCP. The motor is a squirrel-cage, induction-type fed from a variable-frequency drive to allow the pump speed to be changed as required during warm-up and cooldown of the RCS. When the RCS is at elevated temperature and during power operation, the RCP motors operate at 6900 V and 60 Hz. The motor has a “wet-wound” stator that contains the individually insulated windings so that the motor is cooled directly by RCS primary coolant flowing over the motor windings. The principal safety requirement, as with the pump unit, is the maintenance of the RCS pressure boundary. The requirement that the motor can be shut down on demand is achieved through isolation of the electrical supply and is not therefore a feature of the motor itself.

- **Motor Cooling System** - The flow of RCS primary coolant around the motor internals provides the cooling of the motor, and this circulation is achieved through the use of an auxiliary impeller on the shaft. This flow then passes through a separate heat exchanger (HX) that allows waste heat to be transferred to the CCS. The CCS also removes heat from the thermal barrier to cool the RCS water entering the pump flywheel assembly to maintain a low and uniform flywheel temperature and to minimise the temperature of the water entering the motor. These cooling functions are essential to support operation of the RCPs, but not in supporting RCP structural integrity or the coastdown capability. The flywheel and motor cooling system therefore supports a Category C safety function and is not considered further.

17.3.1.3 Claims on Components and Equipment

Pump Unit

The RCP pump unit is an integral part of the RCS pressure boundary. Maintaining the integrity of the RCS pressure boundary is a Category A safety function. RCP integrity is fundamental to preventing RCS leakage and hence the RCP structure must be considered Class 1 as discussed in Chapter 5.

Flywheel/Thermal Barrier Assembly

The thermal barrier assembly is an integral part of the RCS pressure boundary. Maintaining the integrity of the RCS pressure boundary is a Category A safety function. Thermal barrier integrity is fundamental to preventing RCS leakage and so the RCP structure must be considered Class 1. See Appendix 15A.

The role of maintaining sufficient RCS flow while the reactor trip function reduces core power following a loss of electrical power is also a Category A safety function. The RCP coastdown characteristics are essential to maintain sufficient departure from nucleate boiling (DNB) ratio to avoid fuel cladding damage and, as the flywheel is instrumental in providing this, it must also be considered Class 1 in this respect. See Appendix 15A.

The integrity of the flywheel assembly prevents the generation of hazards leading to the consequential damage to other plant components that could impact the heat transfer/residual heat removal primary safety function. This safety function is again Category A and the integrity justification is the primary means of demonstrating safety, so these components are also Class 1. See Appendix 15A.

The flywheel/thermal barrier assembly requirement is that they prevent the generation of hazards leading to the consequential damage to other plant components that could impact the heat transfer/residual heat removal primary safety function .

Motor Unit

The RCP motor unit includes a motor casing, which is an integral part of the RCS pressure boundary. Maintaining the integrity of the RCS pressure boundary is a Category A safety function. Motor casing integrity is fundamental to preventing RCS leakage and so the RCP structure must be considered Class 1. See Appendix 15A.

The integrity of the motor casing also prevents the generation of hazards leading to the consequential damage to other plant components that could impact heat transfer/residual heat removal primary safety function. This safety function is again Category A and the integrity justification is the primary means of demonstrating safety, so these components are also Class 1. See Appendix 15A.

The requirement of the RCP motor units is, therefore, that they will not fail in such a way that threatens RCS pressure boundary integrity or generates debris that might affect other RCS components or fuel assemblies.

17.3.1.4 Justification of Claims on Components and Equipment

Pump Unit

The pressure boundary of pump unit is described above. The selected material is considered stronger and more straightforward in terms of in-service inspection procedures than alternative cast austenitic materials. The pressure boundary integrity of the pump unit is justified in Appendix 20F.

The RCP pump unit incorporates a number of features to help guarantee highly reliable operation:

- Lubrication is by RCS fluid so there is no dependency on a separate lubricating oil system.
- There is no shaft seal because the rotating elements of the pump unit are entirely contained within the pressure boundary.
- The damped natural frequency of the rotating assembly exceeds 120 percent of normal operating speed or is sufficiently damped to prevent adverse effects on the rotating assembly, to ensure smooth operation and minimise induced vibration.
- Mounting the pump unit directly in the SG channel head eliminates the crossover loop piping eliminating the need for a pump support structure, eliminating stresses due to thermal growth, as well as reducing the number of welds in the RCS loop.

The pump units are continuously in service during periods of reactor operation. As such, they are continuously monitored, and thus indications of temperature, vibration, speed, RCS flow, etc., would indicate if degradation had occurred. In addition to this, there is an ongoing in-service inspection programme to meet the standards of American Socoety of Mechanical Engineers (ASME) Boiler and Pressure Vessel Code, Section XI.

Flywheel/Thermal Barrier Assembly

The thermal barrier and associated pressure casing are manufactured from forged martensitic stainless steel to ensure compatibility with the reactor coolant fluid that passes through them. The tungsten cylinders fitted in the flywheel have stainless-steel end caps welded in position to ensure that they are isolated from the reactor coolant. The pressure boundary integrity of the thermal barrier assembly is covered further in Appendix 20F.

Integrity of the flywheel itself is a particular safety concern and a number of design features are included to reduce risk as follows:

- The flywheel has no central bore and is equipped with a Hirth radial-face toothed-serration connection to couple it to both the pump impeller and the motor rotor. These arrangements eliminate any shrink-fit to attach the flywheel to the shaft, and hence any of the associated high stresses in the bore.
- The design enables the flywheel to have journal bearings on either side. This robust arrangement will aid the running stability of the motor.
- In the unlikely event of flywheel failure, the analysis of the thermal barrier indicates that the pressure boundary function would still be maintained.

- The flywheel is situated in the thermal barrier that ensures that the flywheel is kept at a relatively constant temperature. This helps to minimise any stresses in the flywheel that might otherwise develop as a result of temperature gradients in the material.

- The pump flywheel has a design speed of 125 percent of the motor operating speed. This provides a generous design margin, that, along with the extensive testing and inspection during fabrication, provides confidence that integrity will be maintained during operation.

Motor Unit

As a part of the reactor coolant pressure boundary, the motor unit shell is also designed to ASME Boiler and Pressure Vessel Code, Section III- Division 1 (Reference 17.4). The motor unit casing is manufactured from forged martensitic stainless steel to ensure compatibility with the reactor coolant fluid that passes through them. In the unlikely event that rotating electrical elements of the motor should fail, analysis shows that any fragments will be contained without loss of the pressure boundary function performed by the motor casing. See Appendix 20F for justification of the motor unit pressure boundary. The RCP motor unit incorporates a number of features to help guarantee highly reliable operation:

- The windings are insulated by a specially developed cross-linked polyethylene insulation system. The insulation has a high resistance against environmental strain cracking and is stable at elevated temperatures. This property provides a built-in safety factor in case of a temperature fluctuation occurring during a transient of the cooling system.

- The use of wet windings ensures that more even cooling of the motor is provided; this helps to avoid hot spots that can lead to more rapid degradation of the insulation.

- With vertical mounting and impeller on top, the motors are "self-venting" and automatically vent any entrained gas into the pump casing. This minimises the potential for the motor to be operated with inadequate cooling of the windings.

- Because the motors are driven through variable-frequency drives, the speed can be controlled to ensure that the current drawn by the motor remains within limits and that consequent heatup of the motor components can also be controlled.

The motor units are continuously in service during periods of reactor operation. As such, they are continuously monitored, and thus indications of temperature, vibration, and speed will indicate if degradation has occurred.

17.3.2 Reactor Coolant System Pressure Relief

17.3.2.1 Role

The RCS and associated pressure-relief capability is described in detail in Section 6.4. See Reference 17.1 for more detail on the Reactor Coolant System.

In normal operation and during all fault conditions, it is vital to maintain the integrity of the RCS. The RCS pressure relief components ensure this and therefore provide a major input to the core heat removal/heat transfer primary safety function, and the containment primary safety function. Under normal operating conditions, the pressuriser sprays, with flow controlled by the pressuriser spray control valves (RCS-PL-V110A/B), are used to control RCS over-pressure. If the spray valves should stick open, there is a risk that the consequent

depressurisation could be a threat to continued plant operation, so the pressuriser spray block valves (RCS-PL-V111A/B) are fitted to protect against this fault. Under extreme conditions, the pressuriser sprays may not be able to adequately control system over-pressure, and under these circumstances, the pressuriser safety relief valves (RCS-PL-V005A/B) are available to protect RCS integrity. A subsystem of the RCS is the automatic depressurization system (ADS). The ADS acts in conjunction with the PXS to mitigate the consequences of loss-of-coolant accidents (LOCAs). The safety-related ADS function is to automatically depressurize the RCS so that the PXS can adequately cool the core during small-break LOCAs. Even though the ADS are RCS components they are dicussed in the PXS section below.

The pressuriser spray valves are air operated and therefore supported by the instrument air system. The pressuriser spray block valves are motor-driven and therefore supported by the main ac power system. The pressuriser safety valves themselves do not require any separate motive force for operation and so are not supported by other systems.

The pressure relief components of the RCS do not support other systems.

17.3.2.2 System Components and Equipment Contributing to Safety Function

The reactor coolant pressure relief system is effectively a part of the RCS itself. The integrity of the pipework itself, along with the pressuriser vessel, is discussed in the section on structural integrity (Chapter 20). The following components contribute to the ability of the RCS pressure relief system to perform its safety function:

- **Pressuriser Safety Valves (RCS-PL-V005A/B)** – These are 150-mm DN (6-inch), spring-loaded, self-actuated safety relief valves with back-pressure compensation. Each one is set to open at 17.13 MPa and is sized to ensure that the full insurge to the pressuriser can be accommodated should there be a complete loss of steam flow to the turbine, with coincident loss of feedwater at 102 percent of reactor rated power. The valves do not require separate actuation, but opening at the setpoint pressure is a safety requirement.

- **Pressuriser Spray Valves (RCS-PL-V110A/B)** – These are 100-mm DN (4-inch), air-operated ball valves set up to fail closed on loss of air supply. The valves are controlled by the plant control system (PLS) and do not have a specific protection actuation signal.

- **Pressuriser Spray Block Valves (RCS-PL-V111A/B)** – These are 100-mm DN (4-inch), motor-operated gate valves and are manually actuated through the PLS if the operator deems that the pressuriser spray valves are not operating correctly on demand.

17.3.2.3 Claims on Components and Equipment

Pressuriser Safety Valves (RCS-PL-V005A/B)

The pressuriser safety valves provide the principal Class 1 protection against RCS overpressure which could result from the expansion of primary coolant that takes place due to the temperature rise following load rejection transients. Maintenance of the RCS pressure boundary is considered a Category A safety function. See Appendix 15A. Whilst the pressuriser pressure control system would provide the first response to high RCS pressure, the primary safety requirement rests with the pressuriser safety valves. This is a Category A safety fuction and designed to Class 1.

There are two pressuriser safety valves mounted in parallel. Both valves are required to function under the most limiting transient conditions. They are also required to close when the RCS pressure falls below their setpoint.

These valves are subject to two requirements. The first is that they will open on demand when RCS pressure exceeds a specific setpoint.. The second requirement is that having opened and relieved the overpressure transient, the valve reseats at the correct pressure. If this does not happen, then the initial overpressure transient becomes a RCS leak or LOCA depending on the leak rate.

Pressuriser Spray Valves (RCS-PL-110A/B)

The pressuriser spray valves control the flow of spray water to provide their role in the normal pressuriser pressure control function (the other part of the normal pressure control function is provided by the pressuriser heaters, that serve to maintain and increase RCS pressure). The spray valves offer the first response to, but not the primary Class 1 protection against, any overpressure transient. Control of RCS pressure and maintenance of the RCS pressure boundary is a Category A safety function, and as such their pressure boundary is Class 1. See Appendix 15A.

There are two spray valves, each one deriving flow from separate RCS cold legs. They perform the full-pressure control function and maintain pressure within normal operating limits except under the most limiting transient conditions.

The normal operation requirement for these valves is that they will modulate correctly in response to the control signals from the pressuriser pressure control system.

Pressuriser Spray Block Valves (RCS-PL-V111A/B)

The pressuriser spray block valves provide an extra level of protection against the depressurisation transient that would result from a stuck-open pressuriser spray valve. This could lead to a loss of primary coolant and RCS fluid subcooling and so be a potential challenge to core cooling. This is a Category A safety function. The pressuriser spray block valves are providing a defence in depth function and so they are Class 2. Additionally it serves as a RCS pressure boundary which is a Category A safety function and is a Class 1 component. See Appendix 15A.

The requirement for these valves is that they will close on demand to isolate the pressuriser sprays. This demand will only be provided by operator action: there is no automatic system demand.

17.3.2.4 Justification of Requirements on Components and Equipment

Pressuriser Safety Valves (RCS-PL-V005A/B)

The pressuriser safety valves are of the spring-loaded, self-actuated type and operation depends only upon the pressure difference across them and not on any method of powered actuation. This passive approach offers a high degree of inherent safety and reliability.

The total pressuriser safety valve capacity is required to be sufficient to limit the RCS pressure during the maximum surge rate into the pressuriser during an overpressure transient. The maximum surge rate into the pressuriser for this transient occurs before the valve setpoint is reached and the main steam safety valves are opened; therefore, the relief capacity

specified for the pressuriser safety valves is greater than that required to limit the peak RCS pressure to 110 percent of the design pressure for the transient being analysed. Additional conservatism is included in this sizing procedure by maintaining reactor power at its initial value during the entire transient as described in Reference 17.6, Section 3.

The valves are manufactured from stainless steel to provide compatibility with the RCS chemistry conditions and are designed to ASME Boiler and Pressure Vessel Code, Section III, Division 1. This code has been specifically developed to qualify pressure-retaining components in safety-significant applications on nuclear power stations. The Code, with its supporting testing and examination, provides the foundations for performance claims made on the pressuriser safety valves.

The valves are very similar to those already in service that are providing the same function on currently operating power stations. As a result, the information from testing these in-service valves offers a high degree of confidence about the reliability to be expected from these valves. Data collected from in-service plants (Reference 17.7, Table 5.1) indicate a low probability of failure to open. This is better than the value assumed in the PSA and indicates that the claims against these valves are conservative. In addition, both valves are equipped with positive position indication so that operations staff can determine their true position.

The failure mechanism of concern would involve the valve sticking or jamming. This could be a result of wear, corrosion, or maintenance-induced failure. In addition to being designed to ASME Boiler and Pressure Vessel Code, Section III, Division 1, the valves are designed and installed to seismic Category I (C-I) standards (Reference Table 15A-1). The combination of the ASME Boiler and Pressure Vessel Code, Section III and other design and manufacture codes with the test regime described below will minimise the probability of these failure mechanisms occurring.

The maintenance and testing arrangements for the pressuriser safety relief valves are based on the programmes associated with ASME Boiler and Pressure Vessel Code, Section III qualification. The testing requires every valve to be tested as installed, or bench-tested, every 5 years; and to have its position-indication equipment inspected every 2 years.

Pressuriser Spray Valves (RCS-PL-110A/B)

The pressuriser spray valves are air operated with the actuators designed to close the valve in the event of a loss of air supply (i.e., “fail closed”). This is an inherently safe mechanism, meaning that only in the event of a valve sticking will there be a failure to a condition other than safe.

The valves are designed to ASME Boiler and Pressure Vessel Code, Section III-1.

A failure mechanism of particular concern would involve the valves sticking or jamming. This could be a result of wear, corrosion, or maintenance-induced failure; however, the valves proposed are very similar in like service in many operating power stations, and this extensive operational experience provides confidence in their high reliability. In addition to being designed to ASME Boiler and Pressure Vessel Code, Section III-1, the valves are designed and installed to seismic Category I (C-I) standards and are qualified for operation in a harsh environment (Reference Table 15A-1). The ASME Boiler and Pressure Vessel Code and other codes for design and manufacture will minimise the probability of these failure mechanisms occurring. Two valves are provided in parallel. In the event of a failure of one of these valves to open, the other pressuriser spray valve is capable of providing spray flow sufficient to maintain pressure within normal operating limits except in the case of a large load rejection transient.

If the failure results in a spray valve being stuck open, the pressuriser spray block valves can be closed to mitigate the impact of this event.

The pressuriser spray valves, by the nature of their function, are always demonstrating correct operation when RCS pressure is maintained within normal control limits.

Pressuriser Spray Block Valves (RCS-PL-111A/B)

The two pressuriser spray block valves are both motor operated, which means they will inherently fail "as is" and this is not fail-safe with respect to the pressuriser spray isolation function. However, given that spurious actuation of this function when not required could give rise to safety concerns, because of the involvement of the system in RCS pressure control, this arrangement is judged appropriate.

The valves are manufactured from stainless steel to provide compatibility with the RCS fluid that passes through them. They are designed to ASME Boiler and Pressure Vessel Code, Section III-1. The failure mechanism of concern would involve the valves sticking or jamming. This could be a result of wear, corrosion, or maintenance-induced failure. However, these valves are very similar to those in like service in many operating power stations, and the extensive operational experience gives confidence of high reliability. In addition to being designed to ASME Boiler and Pressure Vessel Code, Section III, the valves are designed and installed to seismic C-I standards (Reference Table 15A-1). The combination of the ASME Boiler and Pressure Vessel Code, Section III and other codes for design and manufacture will minimise the probability of these failure mechanisms occurring.

17.3.3 Control Rod Drive Mechanism (RXS-MY-Y01)

17.3.3.1 Role

A full description of the control rod drive mechanisms (CRDMs) is given in Section 6.3. Further design details of this system and its constituent components are delineated in Reference 17.37

The CRDMs contribute to the reactivity control primary safety function. There are two groups of control rods:

- **Rod control cluster assemblies (RCCAs)** − Shutdown and power control assemblies that are effectively "black" to neutrons.
- **Gray rod cluster assemblies** − Assemblies used for load follow that are "gray" to neutrons.

In each case, the contribution to reactivity control is made through the movement of the absorber rods of an RCCA or gray rod cluster assembly into and out of the reactor core by its CRDM.

The CRDM housings are part of the primary reactor coolant pressure boundary. The pressure housing therefore also contributes to providing the containment primary safety function by maintaining the integrity of the RCS pressure boundary.

The integrity of the CRDM pressure housing also contributes to the reactivity control primary safety function in that failure of the pressure housing could lead to ejection of a control rod from the core, or could challenge alignment that could prevent a control rod from falling into the core on demand.

The overriding safety requirement of the CRDMs is to be able to release the control rod drive rods on demand and drop the RCCAs into the core within a required time.

The CRDMs, once de-energised, are not supported by other systems in achieving their safety function, nor do they support other systems in achieving their safety function.

17.3.3.2 System Components and Equipment Contributing to Safety Function

The following components contribute to the CRDM performing its safety function:

- **CRDM pressure housing** – There are 69 individual CRDMs, each with its own associated pressure housing. This component does have a significant safety requirement in contributing to maintenance of RCS integrity.

- **Latch assembly** – Each CRDM has a dedicated latch assembly inside its pressure housing. Each latch assembly has two different latches that work in sequence to move the RCCA or gray rod. The stationary latch is required to hold the CRDM shaft in position whilst its actuating magnet is energised and release the CRDM shaft to fall when de-energised. The stationary latch performs a grip or release role only. The moveable latch is engaged when the RCCA or gray rod assembly is stepped into or out of the reactor core. The engaged movable latch combined with its requirement to be magnetically raised or lowered, raises or lowers the RCCA or gray rod through individual steps.

  The safety function of the stationary latches is achieved by their relaxing automatically to the "release" position when power is cut from their associated control magnets. This happens on receipt of a reactor trip signal for all rods and on receipt of certain load rejection signals for selections of rods.

  The safety function of the movable latches is achieved by their relaxing automatically to the "release" position when power is removed from their associated control magnets. This is the case when the RCCA or gray rod cluster assembly is not being stepped; on receipt of a reactor trip signal for all rods; and for selections of rods on receipt of certain load rejection signals.

- **Magnets** – Whilst the CRDM magnets and associated flux rings have a key role in the operation of the CRDM, no movement is required and so, from a mechanical perspective, no further analysis is required. The magnets are de-energised to their safe (reactor trip) state by isolation of the electrical supply and therefore this is not a feature of the magnet itself.

- **CRDM drive shafts** – The CRDM drive shafts provide the link that ensures that the individual RCCAs move in the required way. They are, however, basically passive components with all active control of movement remaining with the latch mechanisms; no further analysis is required.

17.3.3.3 Claims on Components and Equipment

Pressure Housing

Maintenance of the RCS pressure boundary is a Category A safety function. The pressure housings are considered to be Class 1. See Appendix 15A.

The individual pressure housings are each mounted separately on the reactor vessel head, and each one effectively has a separate requirement with respect to structural integrity that it will not fail catastrophically.

Latch Assembly

The latch assembly controls the movement of the control rods either through the mechanism for individual "steps" or by releasing the control rod drive shaft so that the rods can fall into the reactor core by gravity. This movement of control rods is used to control reactivity, that is a Category A safety function. Given that control rod movement is the principal method of controlling reactivity and that the latch assembly is integral to control movement control, it is considered to be Class 1. See Appendix 15A.

Each set of latches is within its own CRDM pressure housing and can therefore be considered independent with respect to performance.

17.3.3.4 Justification of Claims on Components and Equipment

Pressure Housing

The design of the internally mounted, magnetically actuated latch assembly means that no components pass through the pressure housing and, therefore, that there are no seals, etc. Demonstration of the integrity of this arrangement is inherently more straightforward. It also justifies why integrity need only be a structural issue, there being no seals, etc.

Latch Assembly

The latch assembly, through detailed design and orientation of installation, will always sit in the released position when the magnets are not energised. Energising of the associated magnets is required to grip the CRDM drive rod, raise, lower, or hold it in place through individual steps. De-energisation of the magnets, associated with the action of gravity, will ensure that the latches release the CRDM drive rod. This arrangement ensures that the safety function, to release the rods so that they drop into the core, requires no motive power and is inherently safe.

The latch assembly is a proprietary design and so no specific design standards apply. The design is, however, very similar to that used on previous generations of Westinghouse pressurised water reactors (PWR) and so service experience from these can give an accurate picture of the expected reliability. Analysis of this service experience suggests a low probability of an RCCA failing to drop into the core on demand because of mechanical faults with the CRDM.

On this basis, even with a very conservative claim on individual rod reliability, the scenario with two or more RCCAs failing to insert for reasons of mechanical failure is not considered credible. This is reflected in the reactivity faults presented in Chapter 9.

The only credible failure would therefore be in the case of some form of common mode failure. Although examination of the latch mechanism has indicated that there is no credible inherent common mode failure mechanism that could simultaneously affect the operation of all RCCAs for anticipated transient without trip (ATWT) evaluations of frequent faults presented in Chapter 9, a common mode failure of all RCCAs to insert is conservatively assumed.

An extensive test programme has also been carried out to demonstrate the number of cycles that an individual CRDM unit can be expected to complete without failure. This is discussed further in Reference 17.37.

As the latches wear, there is increased incidence of "missed steps" when the CRDM is instructed to move the control rod by a step and either the rod withdrawal does not take place or the rod insertion is by more than one step. The resulting misalignment will be picked up as a part of the routine operational surveillance programmes. This is discussed further in Reference 17.37.

17.3.4 Chemical and Volume Control System

17.3.4.1 Role

A detailed description of the chemical and volume control system (CVS) is given in Section 6.4.

The CVS contributes to the provision of three primary safety functions: reactivity control, containment, and RCS water inventory required for removal of heat from the core. In normal operation, the CVS passes a portion of the reactor coolant through a filtration and purification process (Chapter 21). This is carried out at full RCS pressure by the chemical control subsystem with the RCP head providing the differential pressure to drive fluid through the system. This element of the system makes no specific operational contribution to safety; however, through the makeup subsystem, the CVS can provide a makeup and letdown function for inventory control. Also, there is the ability for this makeup to be of variable boron concentration.

Isolation of the makeup on high pressuriser level and of the letdown on low pressuriser level contributes to the maintenance of the integrity of the RCS and adequate coolant inventory respectively. Consequently, this contributes to the heat transfer/residual heat removal primary safety function.

The ability to provide makeup water of variable boron concentration is part of normal operations and would not normally be a contribution to the primary safety function of reactivity control. The prevention of inadvertent undetected RCS dilution, that could occur immediately after a reactor trip if a dilution was in progress at the time or at other times when the reactor is shutdown, is a contribution to this safety function by the makeup subsystem.

The makeup subsystem supplies makeup to the RCS through the containment boundary; the system isolation valves at this point support the integrity of containment and thus contribute to the containment primary safety function.

The operation of the CVS makeup pumps taking suction from the boric acid tank is clearly available to help mitigate the impact of a very small LOCA, since this would reduce the demands on the automated safety injection systems. There is no requirement specifically made for the CVS makeup pumps; however, they do provide a defence in depth function for maintaining RCS inventory and core reactivity control. The CVS is supported by the essential electrical supplies in the provision of its safety functions. Except for infrequent EMIT activities (e.g., providing borated makeup to PXS tanks), the CVS does not support other systems in provision of their safety functions.

Further design details of this system and its constituent components are delineated in Reference 17.3.

17.3.4.2 System Components and Equipment Contributing to Safety Function

The pipework systems associated with the CVS that are designed and constructed to ASME standards are: the sections directly connected to the RCS are ASME Boiler and Pressure Vessel Code, Section III-1; the sections associated with containment isolation are ASME Boiler and Pressure Vessel Code, Section III, and certain other in-containment pipework is ASME Boiler and Pressure Vessel Code, Section III. The remaining parts of the system are constructed either to ASME Boiler and Pressure Vessel Code, Section VIII (Reference 17.9) or the ANSI/ASME Section B31.1 Power Piping Code (Reference 17.10). The following components contribute to the CVS performing its safety functions:

- **Demineralised Water System Isolation valves (CVS-PL-V136A/B)** – These are 75-mm DN (3-inch), air-operated butterfly valves that fail closed on loss of air supply. They close on receipt of a boron dilution block signal from the protection and safety monitoring system (PMS), shutting off the supply of demineralised water and so terminating any dilution of the RCS that is in progress, as a backup to the closure of CVS-PL-V090 and CVS-PL-V091 as discussed below.

- **Makeup Pump Suction Header Three-way Blend Valve (CVS-PL-V115)** – This is a 100-mm DN (4-inch), three-way, air-operated plug valve. It is normally set so that it can modulate to control the blend of boric acid and demineralised water to the CVS makeup pump suction, but on loss of the air supply, it fails to the full borate position. On receipt of a boron dilution block signal, the valve is signalled by the PLS, but from a signal originating in the PMS, to move to the full borate position so that the blend supplied is to the full boric acid concentration. This is intended to ensure that if an RCS makeup operation is in progress, the makeup will switch from whatever boron concentration was originally desired to makeup at maximum boron concentration only. This is a defence in depth function to the demineralised water supply isolation valves. Therefore, there are no safety claims on this valve.

- **RCS Purification Stop Valves (CVS-PL-V001, -V002, and -V003)** – These are two 75–mm DN (3-inch), motor-operated gate valves and a 75-mm DN (3-inch), motor-operated globe valve respectively. All valves are required to close on demand from the PMS by a purification line isolation signal or manual initiation of the CVS isolation signal. This is intended to isolate a potential source of leaks and also isolate planned system letdown operations in the event of an apparent reduction in RCS inventory.

- **Makeup Line Containment Isolation Valves (CVS-PL-V090 and CVS-PL-V091)** – These are 75-mm DN (3-inch), motor-operated gate valves. They are required to close on demand from a CVS isolation signal generated in the PMS. This is a safety requirement. They are also containment isolation valves (CIVs) and are required to isolate the CVS makeup line through the containment boundary on receipt of a containment isolation signal.

- **Letdown Containment Isolation Valves (CVS-PL-V045 and V047)–** These are 75-mm DN (3-inch), air-operated globe valves. They are required to close on demand from a CVS isolation signal generated in the PMS; therefore this is a safety requirement. They are also containment isolation valves (CIVs) and are required to isolate the CVS letdown line through the containment boundary on receipt of a containment isolation signal.

- **Zinc Injection Containment Isolation Valve (CVS-PL-V092 and V094)** – This is a 25-mm DN (1-inch), air-operated globe valve. It is required to close on demand from a CVS isolation signal on an RCS pressuriser Low-1 level signal generated in the PMS. This actuation occurs only to prevent an accumulation of zinc acetate in the piping and therefore, this is not a safety requirement. It is also a CIV and is required to isolate the zinc injection line through the containment boundary on receipt of a containment isolation signal.

- **Hydrogen Injection Containment Isolation Valve (CVS-PL-219) –** This is a 12-mm (0.5-inch) nominal-bore, air-operated globe valve. It is required to close on demand from a CVS isolation signal on an RCS pressuriser Low-1 level signal generated in the PMS. This actuation occurs to prevent an accumulation of H_2 in the piping should this signal be generated prior to a containment isolation signal and therefore, this is a Class 1 safety requirement. It is also a CIV and is required to isolate the H_2 addition line through the containment boundary on receipt of a containment isolation signal.

17.3.4.3 Claims on Components and Equipment

Demineralised Water System Isolation Valves (CVS-PL-V136A/B)

The demineralised water supply makeup isolation valves prevent the inadvertent dilution of the RCS and thus protect against inadvertent criticality. Control of core reactivity is considered to be a Category A safety function. Given that the control rods are normally fully inserted when the reactor is shut down, prevention of inadvertent dilution becomes the primary method of maintaining the shutdown condition. As such, these valves are considered to be Class 1. See Appendix 15A.

The requirement against these valves is that they will close on demand. There are two valves in series, so either one closing successfully will achieve the safety function.

Makeup Pump Suction Header Three-way Blend Valve (CVS-PL-V115)

Failure of this valve will result in boration of the primary coolant and a reduction in plant power generation. This is not the primary means of boration of the RCS but spurious failure could interrupt power operations. The valve provides a Category C function and is Class 3. See Appendix 15A.

RCS Purification Stop Valves (CVS-PL-V001, -V002, and -V003)

These valves provide an element of control of RCS inventory in response to loss of inventory faults. Control of RCS inventory is instrumental in providing adequate heat removal and so this is a Category A function. These valves are a primary means of maintaining adequate inventory by isolating the CVS purification loop so they are Class 1. See Appendix 15A.

The requirement against these valves is that they will close on demand. There are two gate valves and one globe valve in series: any one of the three successfully closing will achieve the safety function.

Makeup Line Containment Isolation Valves (CVS-PL-V090 and CVS-PL-V091)

These valves protect RCS integrity and, under certain circumstances, SG integrity, by preventing overfilling. This is protecting against the release of radioactive material and so is a Category A safety function. In this role, they are Class 1. See Appendix 15A.

These valves also prevent the inadvertent dilution of the RCS and thus protect against inadvertent criticality. Control of core reactivity is considered to be a Category A safety function. Given that the control rods are normally fully inserted when the reactor is shut down, prevention of inadvertent dilution becomes the primary method of maintaining the shutdown condition.

These valves also provide containment isolation to protect the integrity of the containment pressure boundary and prevent the release radioactivity. This isolation also is credited as a means to terminate potential boron dilutions in Chapter 9. These are Category A safety functions. These valves are a primary means of performing these functions and are therefore Class 1. See Appendix 15A.

The requirement against these valves is that they will close on demand. There are two valves in series, so either one successfully closing will achieve the safety function.

See Table 10-34 for generic component failure data parameters.

Letdown Containment Isolation Valves (CVS-PL-V045 and V047)

These valves protect RCS integrity isolating the letdown of RCS fluid on pressuriser low level or following receipt of a safeguards actuation signal. This is a Category A function. These valves also provide containment isolation to protect the integrity of the containment pressure boundary and prevent the release of radioactivity, which are Category A safety functions. These valves are a primary means of performing these functions and are therefore Class 1. See Appendix 15A.

The requirement against these valves is that they will close on demand. There are two valves in series, so either one successfully closing will achieve the safety function.

Zinc Injection Containment Isolation Valves (CVS-PL-V092 and V094)

These valves protect RCS integrity isolating the zinc addition flow path to the RCS fluid on pressuriser low level or following receipt of a safeguards actuation signal. This is a Category A function. This valve also provides containment isolation to protect the integrity of the containment pressure boundary and prevent the release of radioactivity. These are also Category A safety functions. This valve is a primary means of performing these functions and is therefore Class 1. See Appendix 15A.

The requirement against these valves is that they will close on demand. There are two valves in series, so either one successfully closing will achieve the safety function.

See Table 10-34 for generic component failure data parameters.

Hydrogen Injection Containment Isolation Valve (CVS-PL-219)

This valve protects RCS integrity isolating the H_2 addition flow path to the RCS fluid on pressuriser low level or following receipt of a safeguards actuation signal. This is a Category A function. This valve also provides containment isolation to protect the integrity of the containment pressure boundary and prevent the release of radioactivity. These are also Category A safety functions. This valve is a primary means of performing these functions and is therefore Class 1. See Appendix 15A.

The requirement against this valve is that it will close on demand. There is another valve in series which is a check valve CIV (CVS-PL-V217) (see Section 17.6.2 below), so either one successfully closing will achieve the safety function.

17.3.4.4 Justification of Claims on Components and Equipment

Demineralised Water Supply Makeup Isolation Valves (CVS-PL-V136A/B)

The demineralised water supply makeup isolation valves are air operated with the actuators designed to fail closed in the event of a loss of air supply. This is an inherently safe mechanism meaning that only in the event of a valve sticking will there be a failure to a condition other than safe.

The valves are manufactured from stainless steel to ensure compatibility with the demineralised water that passes through them and to prevent potential for valve corrosion products from being injected into the RCS. They are designed to the ASME Boiler and Pressure Vessel Code, Section III-3 design code. This code has been specifically developed to qualify pressure-retaining components in safety-significant applications on nuclear power stations. The code, with its supporting testing and examination, provides the foundations for performance claims made on the demineralised water supply makeup isolation valves.

The failure mechanism of concern would involve the valve sticking or jamming. This could be a result of wear, corrosion, or maintenance-induced failure. In addition to being designed to ASME Boiler and Pressure Vessel Code, Section III, the valves are also designed and installed to seismic C-I standards (see Table 15A-1). The combination of ASME Boiler and Pressure Vessel Code, Section III and other codes for design and manufacture with the test regime described below will minimise the probability of these failure mechanisms occurring. The provision of two valves in series provides redundancy and hence further reduces the probability of failure.

The maintenance and testing arrangements for the demineralised water supply makeup isolation valves are based on the ASME Boiler and Pressure Vessel Code, Section III programmes appropriate for these types of valves as used in existing nuclear power stations. The testing is:

- A full stroke operability test is performed quarterly in accordance with the ASME Boiler and Pressure Vessel Code.

- Visual confirmation of valve operation during the stroke testing is performed every 2 years.

In addition to this, the valve will be seen to operate correctly every time the RCS makeup system is initiated, so this will provide numerous other opportunities to identify operational problems.

Makeup Pump Suction Header Three-way Blend Valve (CVS-PL-V115)

Failure of this valve will result in boration of the primary coolant and a reduction in plant power generation. This is not the primary means of boration of the RCS but spurious failure could interrupt power operations. This valves are designed in accordance with ASME B16.34.

Although there is no formal surveillance testing of the valve, routine maintenance and testing of the valve will be performed according to the manufacturer's recommendations and testing will be carried out to verify that performance has been maintained.

RCS Purification Stop Valves (CVS-PL-V001, -V002, and -V003)

The three purification stop valves are motor operated, which means they will fail "as is". Clearly, this is not fail-safe with respect to the letdown isolation function, but given that spurious actuation of this function when not required could give rise to safety concerns, and given the relationship between RCS pressure and letdown, it is judged as appropriate.

All three valves are manufactured from stainless steel to ensure compatibility with the reactor coolant water that passes through them. Two of the valves, are designed to ASME Boiler and Pressure Vessel Code, Section III-1; the third is designed to the ASME Boiler and Pressure Vessel Code, Section III-3 design code. The failure mechanism of concern would involve the valves sticking or jamming. This could be a result of wear, corrosion, or maintenance-induced failure. In addition to being designed to ASME Boiler and Pressure Vessel Code, Section III, the valves are also designed and installed to seismic C-I, and are qualified for operation in a harsh environment (see Table 15A-1). The provision of three valves in series further reduces the probability of failure. The fact that two of the valves are of different design (gate valves) from the third (globe valve) provides diversity and further confidence that common mode failure issues have been minimised.

The valves are very similar to those already in like service in many operating power stations. As a result, the information from testing these in-service valves offers a high degree of confidence about the reliability to be expected from these valves. Data collected from in-service plants (Reference 17.7, Table 5.1) indicate a low probability of failure to close indicating that the claim being made is conservative. The maintenance and testing arrangements for the purification stop valves are based on the ASME Boiler and Pressure Vessel Code, programmes that are appropriate for these types of valves as used in existing nuclear power stations. The testing is:

- A full stroke operability test is performed once during each refuelling outage.
- Visual confirmation of valve operation during the stroke testing is performed every 2 years.

Makeup Line Containment Isolation Valves (CVS-PL-V90 and CVS-PL-V091)

The two makeup discharge header CIVs are both motor operated, which means they will inherently fail "as is". Clearly, this is not fail-safe with respect to the containment isolation function itself, but given that spurious actuation of this function when not required could give rise to other safety concerns and because of the involvement of the system in RCS makeup, this arrangement is judged as appropriate. In addition, these motor operated valves are powered by 1E batteries which provides for a balance of high reliability to close in the vent of containment isolation with high reliability to be open when makeup is needed.

Both valves are manufactured from stainless steel to provide compatibility with the borated water that passes through them. They are designed to ASME Code, Section III-2. The code, with its supporting testing and examination provides the foundations for performance claims made on the makeup discharge header CIVs.

The valves are very similar to those already in service for the same function on many operating power stations. As a result, the information from testing these in-service valves offers a high degree of confidence about the reliability to be expected from these valves. Data collected from in-service plants (Reference 17.7, Table 5.1) indicate a low probability of failure to close indicating that the claim being made is conservative.

The failure mechanism of concern would involve the valve sticking or jamming. This could be a result of wear, corrosion, or maintenance-induced failure. In addition to being designed to ASME Boiler and Pressure Vessel Code, Section III, the valves are also designed and installed to seismic C-I standards, and the inside CIV is also qualified for operation in a harsh environment (see Table 15A-1). The combination of the ASME Boiler and Pressure Vessel Code, Section III and other codes for design and manufacture with the test regime described below will minimise the probability of these failure mechanisms occurring. The provision of two valves in series further reduces the probability of failure to achieve the safety function.

The maintenance and testing arrangements for the makeup discharge header CIVs are based on the ASME Boiler and Pressure Vessel Code programmes appropriate for these types of valves as used in existing nuclear power stations. The testing is:

- A full stroke operability test is performed quarterly in accordance with the ASME Boiler and Pressure Vessel Code.

- Visual confirmation of valve operation during the stroke testing is performed every 2 years.

- Given that they are CIVs, seat leakage limits will be tested to verify leak tightness. This test will be performed in line with the CIV leak test programme, the requirements for that are outlined in Reference 17.11.

Letdown Containment Isolation Valves (CVS-PL-V045 and V047)

The letdown line containment isolation valves are air operated with the actuators designed to fail closed in the event of a loss of air supply. This is an inherently safe mechanism meaning that only in the event of a valve sticking will there be a failure to a condition other than safe.

The valves are manufactured from stainless steel to ensure compatibility with the demineralised water that passes through them. They are designed to the ASME Boiler and Pressure Vessel Code, Section III-2 The code, with its supporting testing and examination provides the foundations for performance claims made on the demineralised water supply makeup isolation valves.

The failure mechanism of concern would involve the valve sticking or jamming. This could be a result of wear, corrosion, or maintenance-induced failure. In addition to being designed to ASME Boiler and Pressure Vessel Code, Section III, the valves are also designed and installed to seismic C-I standards (see Table 15A-1). The combination of ASME Boiler and Pressure Vessel Code, Section III, and other codes for design and manufacture with the test regime described below will minimise the probability of these failure mechanisms occurring. The provision of two valves in series provides redundancy and hence further reduces the probability of failure.

The maintenance and testing arrangements for the demineralised water supply makeup isolation valves are based on the ASME Boiler and Pressure Vessel Code programmes appropriate for these types of valves as used in existing nuclear power stations. The testing is:

- A full stroke operability test is performed quarterly in accordance with the ASME Boiler and Pressure Vessel Code.

- Visual confirmation of valve operation during the stroke testing is performed every 2 years.

In addition to this, the valve will be seen to operate correctly every time the RCS boration or dilution requires that letdown be initiated, so this will provide numerous other opportunities to identify operational problems.

Zinc Injection Containment Isolation Valve (CVS-PL-V092 and V094)

The zinc addition containment isolation valve is air operated with the actuators designed to fail closed in the event of a loss of air supply. This is an inherently safe mechanism meaning that only in the event of a valve sticking will there be a failure to a condition other than safe.

The valve is manufactured from stainless steel to ensure that no corrosion of the valve occurs since it contains zinc at elevated pressure. It is designed to the ASME Boiler and Pressure Vessel Code, Section III-2. The code, with its supporting testing and examination, provides the foundations for performance claims made on the zinc addition isolation valve.

The failure mechanism of concern would involve the valve sticking or jamming. This could be a result of wear, corrosion, or maintenance-induced failure. In addition to being designed to ASME Boiler and Pressure Vessel Code, Section III, the valve is also designed and installed to seismic C-I standards (see Table 15A-1). The combination of ASME Boiler and Pressure Vessel Code, Section III, and other codes for design and manufacture with the test regime described below will minimise the probability of these failure mechanisms occurring.

Hydrogen Injection Containment Isolation Valve (CVS-PL-V219)

The H_2 addition containment isolation valve is air operated with the actuators designed to fail closed in the event of a loss of air supply. This is an inherently safe mechanism meaning that only in the event of a valve sticking will there be a failure to a condition other than safe.

The valve is manufactured from stainless steel to ensure that no corrosion of the valve occurs since it contains H_2 at elevated pressure. It is designed to the ASME Boiler and Pressure Vessel Code, Section III-2. The code, with its supporting testing and examination, provides the foundations for performance claims made on the zinc addition isolation valve.

The failure mechanism of concern would involve the valve sticking or jamming. This could be a result of wear, corrosion, or maintenance-induced failure. In addition to being designed to ASME Boiler and Pressure Vessel Code, Section III, the valve is also designed and installed to seismic C-I standards (see Table 15A-1). The combination of ASME Boiler and Pressure Vessel Code, Section III, and other codes for design and manufacture with the test regime described below will minimise the probability of these failure mechanisms occurring. There is another valve in series which is a CIV check valve (see Section 17.6.2 below). The provision of two valves in series provides redundancy and hence further reduces the probability of failure.

The maintenance and testing arrangements for the H_2 addition isolation valve are based on the ASME Boiler and Pressure Vessel Code programmes appropriate for these types of valves as used in existing nuclear power stations. The testing is:

- A full stroke operability test is performed quarterly in accordance with the ASME Boiler and Pressure Vessel Code.

- Visual confirmation of valve operation during the stroke testing is performed every 2 years.

In addition to this, the valve will be seen to operate correctly every time the H_2 addition function is started or stopped, so this will provide numerous other opportunities to identify operational problems.

17.4 STEAM AND FEEDWATER SYSTEMS

17.4.1 Steam Generator and Main Steam Supply Systems

17.4.1.1 Role

A detailed description of the steam generator system (SGS) and main steam system (MSS) is given in Section 6.5.

The SGS consists of the feed water piping, steam generators, steam piping, valves, and related appurtenances that are located within the nuclear island (NI). The MSS exists to transfer the steam produced in the SGs from the NI boundary (Auxiliary Building wall into the First Bay) to the main turbine generator and thus the SGS and MSS have a power generation Category C function. This Category C function includes the functions to remove core decay heat during hot standby and during the initial phase of plant cooldown making use of the feedwater system (FWS) and the MSS steam bypass valves and the main condenser. The remaining discussions below apply to the SGS only.

The SGS supports the core reactivity control, core heat removal, and the containment primary safety functions. If there is a steam line break or other significant secondary-side depressurisation, the consequences are a rapid fall in temperature of the primary coolant with consequent impact on reactivity and potential impact on primary circuit integrity. In addition, significant overpressure of the SGs could result in a challenge to RCS integrity. The SGS also acts to remove core decay heat following design basis events making use of the SG secondary side water inventory and the SG safety valves. These are Category A functions and since the SGS provides a primary means of performing these functions, its systems, structures, or components (SSCs) are Class 1. Following a postulated break in a main steam line located within the containment, the SGS main steam isolation valves are automatically closed to prevent the blowdown of both SGs into the containment. For a steamline break outside containment, closure of both main steam isolation valves would isolate the break and limit the steam release to the turbine building. Following a SG tube rupture where contaminated primary coolant leaks to the secondary side, the SGS main steam isolation valves also contribute to the containment primary safety function by preventing the movement of contamination into the turbine building main steam pipework and potentially offsite.

The SGS isolation valves are adjacent to the containment boundary and are required to be CIVs and along with the SGS pressure boundary contribute to the containment safety function.

The SGS also provides protection against secondary-side overpressure and consequent support to RCS integrity that contributes to both the residual heat removal/heat transfer and the containment safety functions, through the provision of pressure relief valves.

The SGS is supported in providing its Category A safety functions by the essential electrical system. The main steam isolation valve (MSIV) actuators are qualified to operate throughout the normal and abnormal temperature range, including in case of loss of ac power and loss of heating, ventilation, and air conditioning (HVAC). The annex/auxiliary building non-radioactive HVAC system (VXS) does not support the SGS in the provision of its Category A safety functions and therefore carries the same classification as the MSS in the provision of its Category C safety function.

SGS also contributes to the reactivity control primary safety function and the containment primary safety function. This is achieved through the provision of main feedwater isolation valves (MFIVs) backed up by the main feedwater control valves (MFCVs), and in certain circumstances by the main feedwater check valves.

The reactivity control primary safety function is met by isolating the main feedwater line to prevent feedwater from being supplied to the SGs if they appear to be overfilling or if the heat removal is excessive. This prevents excessive temperature changes to the reactor coolant and consequent effects on reactivity.

The containment primary safety function is met by isolating the main feedwater line in the event of an SG tube leak to limit the amount of mass injected during an SG tube rupture (SGTR) to prevent SG overfill. The main feedwater line is also isolated to prevent the escape of high-energy fluid in the event of breaks in either feedwater or main steam lines not associated with SG tube leaks.

The MFIVs are also CIVs and contribute to the containment safety function.

The SGS is supported in providing its safety function by the essential electrical system, but it does not support other systems in their safety functions.

The SGS does not support other systems in their safety functions.

Further design details of this system and its constituent components are delineated in Reference 17.5 and Reference 17.8.

17.4.1.2 System Components and Equipment Contributing to Safety Function

The pipework systems associated with the SGS are designed and constructed to ASME Boiler and Pressure Vessel Code, Section III-2 (Reference 17.4). The pipework systems associated with the MSS are designed and constructed to ANSI/ASME B31.1 Power Piping Code standards (Reference 17.10).

The following components contribute to the main steam line performing its Class 1 safety functions:

- **Main Steam Line Isolation Valves (SGS-PL-V040A/B)** – These are 950-mm DN (38-inch), power-operated, quick-acting, bidirectional, wedge gate valves. The valve actuator consists of a piston and cylinder with a compressed nitrogen energy storage system. The valve is opened by driving hydraulic fluid into the cylinder so that the piston moves to compress the nitrogen “spring”. The hydraulic fluid is locked in the system at high pressure to keep the valve open. Two redundant pairs of solenoid valves

operate to control the flow of hydraulic fluid to move the valve. The valve has three modes of operation: slow close, fast close, and open. All solenoids remain de-energised for the "open" mode, with the hydraulic pump operating to pump fluid into the actuator cylinder to compress the nitrogen spring. For the "slow close" mode, both solenoids in either pair must energise. For the "fast close" mode, a specific solenoid valve in either pair must energise. The arrangement of the solenoids is designed to provide a fail "as is" capability on loss of all electrical supplies. The "fast close" mode is initiated on receipt of a main steam line isolation signal from the PMS to isolate their respective SGs from the effects of secondary-side depressurisation. This requirement to quickly isolate the main steam line is therefore a safety requirement. The MSIVs are also CIVs and are required to isolate on demand from a PMS containment isolation signal.

- **MSIV Bypass Isolation Valves (SGS-PL-V240A/B)** – These are 75-mm DN (3-inch), modulating air-operated globe valves. The valves fail closed on loss of air and redundant solenoid valves are actuated on receipt of a main steam line isolation signal from the PMS to dump air and close the valves. As with the MSIVs, this is to complete the isolation of the respective SG from the effects of secondary-side depressurisation, and is therefore a safety requirement. The MSIV bypass valves are also CIVs and are required to isolate on demand from a PMS containment isolation signal.

- **Main Steam Safety Valves (SGS-PL-V030A/B, -V031A/B, -V032A/B, -V033A/B, -V034A/B, and -V035A/B)** – These are 200-mm DN (8-inch), spring-loaded safety relief valves. Each valve must have a rated capacity of approximetly 623,240 kg/hr (1.374×10^6 lb/hr) at a pressure of approximetly 8.8 MPa (1274 psia). As spring-loaded safety valves, they do not require any external signals or motive power to initiate a lift, but they are required to lift at a set steam pressure and be capable of passing design flow at 110 percent of system design pressure to protect MSS integrity. This is therefore a safety requirement. Once excess steam pressure has been relieved, the valves are required to close because a stuck-open valve will have similar consequences to a steam system leak and will result in an RCS cool down. The re-isolation is therefore also a safety requirement.

- **PowerOperated Relief Valves (PORV) (SGS-PL-V233A/B)** – These are 300-mm DN (12-inch), air-actuated globe valves. The valve responds to signals from four separate pressure tappings on the associated steam line. The setpoint is variable and can be selected remotely from the main control room (MCR). In the event of a loss of air supply, the valves fail closed. In terms of system overpressure protection, the PORVs do not have a statutory role because full protection is provided by the main steam safety valves. The PORVs are used to provide a controlled steaming route to atmosphere and serve as the initial relief path to minimise the numbers of lifts of the main steam safety valves and consequent risk of failure to correctly reseat. As a result, the requirement to open is not a safety requirement; however, a stuck-open PORV will result in an RCS cool down, and the requirement to close in response to an SG relief isolation signal from the PMS is a Class 1 safety requirement.

- **PORV Block Valves (SGS-PL-V027A/B)** – These are 150-mm DN (6-inch), motor-operated gate valves. The valves serve to protect against the impact of a stuck-open PORV. Given that the PORV pressure relief capability is not classified as part of the formal pressure relief arrangements, it is acceptable to include additional isolation valves in the line. The valves are required to close on receipt of an SG relief isolation signal from the PMS and this is a Class 1 safety requirement.

- **SG Blowdown Isolation Valves (SGS-PL-V074A/B, -V075A/B) –** The blowdown isolation valves contribute to the SGS performing its safety function. They are 100-mm DN (4-inch), air-operated globe valves that fail closed on loss of air supply. They are required to close on receipt of an SG blowdown isolation signal from the PMS. This is intended to shut off the SG blowdown flow and stop further drain down of the associated SG. It will also terminate any associated contribution to an increased heat removal event and provide containment isolation.

- **Main Feed Water Isolation Valves (SGS-PL-V057A/B)** – These 500-mm (20-inch) nominal-bore, bidirectional, wedge-type gate valves are composed of a valve body welded into the system pipeline and provided with a hydraulic/pneumatic actuator. The valve actuator is supported by the yoke that is attached to the top of the body and consists of a piston and cylinder with a compressed nitrogen energy storage system. The valve is opened by driving hydraulic fluid into the cylinder so that the piston moves to compress the nitrogen that acts as a spring. The hydraulic fluid is maintained locked in the system at high pressure to maintain the valve open. Two redundant pairs of solenoid valves operate to control the flow of hydraulic fluid to move the valve. The valve has three modes of operation: slow close, fast close and open. All solenoids remain de-energised for open, with the hydraulic pump operating to pump fluid into the actuator cylinder to compress the nitrogen spring. For slow close, both solenoids in one of the two pair must energise. For fast close, the hydraulic dump solenoid valve in either pair must energise via signals from the PMS. The arrangement of the solenoids is designed to provide a fail "as is" capability on loss of all electrical supplies. The valves are required to fast close on receipt of a main feedwater line isolation signal, to isolate their respective SGs from the effects of overfeeding. They are also required to fast close to prevent the overfilling of an SG following a tube rupture to accomplish their containment isolation function. The ability to fast close is therefore a safety requirement.

- **Main Feedwater Control Valves (SGS-PL-V250A/B)** – These air-operated 500-mm (20-inch) nominal-bore globe valves are designed to fail closed on loss of air. The valve modulates to control feedwater flow to maintain a proper SG level. The air used for valve modulation passes through a solenoid-operated dump valve that is normally energised but is de-energised by the PMS main feedwater line isolation signal. This dumps the air pressure and causes the valve to run fully closed. The valve is a tight shutoff design that can provide isolation as well as modulating control. Whilst the primary role of the valve is to control feedwater flows during normal operation, it is required to provide a backup to the main feedwater line isolation valves, to terminate feedwater flow on demand, and to isolate the containment. This secondary role is a safety requirement.

- **Main Feedwater Check Valves (SGS-PL-V058A/B)** – These 500-mm (20-inch) nominal-bore, control closure, lift check valves are simple, passive devices that require no control action to operate. This valve provides some defence in depth for reverse flow feedwater isolation; no specific performance claims are made on its ability to isolate reverse flow in the safety case. There is a requirement; however, against its ability to close over a timescale slow enough to limit hydrodynamic shock loads on associated piping and nozzles.

- **Startup Feedwater Control Valves (SFCV) (SGS-PL-V255A/B)** – These 150-mm (6-inch) nominal-bore, air-operated, modulating control globe valves fail closed on loss of air supply. They are designed to ensure tight shutoff when closed to allow them to provide isolation as well as control startup feedwater over the required flow range. The SFCV actuator is equipped with an auxiliary air accumulator so that if normal

instrument air supply is lost, the valve can continue to modulate for a time. The control air is supplied through a solenoid-operated dump valve that has to be energised to provide the air supply. The Class 1 safety requirement of the valves is to contribute to the isolation of flow on receipt of a startup feedwater isolation signal from the PMS.

- **Statrtup Feedwater Isolation Valves (SFIV) (SGS-PL-V067A/B)** – These 150-mm (6-inch) nominal-bore, motor-operated, gate valves are designed to fail "as is". Their Class 1 safety requirement is to isolate startup feedwater flow on receipt of a startup feedwater isolation or containment isolation signal from the PMS.

- **Startup Feedwater Check Valve (SGS-PL-V256A/B)** – This 150-mm (6-inch) nominal-bore, nozzle-type check valve is located downstream of the SFIV. It is a simple passive device that is held open by flow and closed by differential pressure of the flowing medium: it requires no other power or actuation. The Class 1 safety role is to provide redundancy for Class 1 containment isolation.

17.4.1.3 Safety Requirements Identified against Components and Equipment

Main Steam Line Isolation Valves (SGS-PL-V040A/B)

The MSIVs protect against excessive containment pressurisation and RCS cooldown due to secondary-side steam leakage with the resulting challenges to containment integrity, and core reactivity and RCS integrity. In the event of an SGTR, these valves close to prevent the release of primary fluid and are also containment isolation valves. These are all Category A safety functions. The MSIVs are the principal means of providing this protection and, as such, are Class 1. See Appendix 15A.

There is a single MSIV on the steam line from each SG (two in total) and the requirement against each is that they will close on demand. In order to prevent the blowdown of both SGs following a postulated steam line break inside containment, either MSIV has to close to meet the safety function.

MSIV Bypass Isolation Valves (SGS-PL-V240A/B)

The MSIV bypass valves also provide protection against excessive RCS cooldown due to secondary-side steam leakage with the resulting challenges to core reactivity and RCS integrity. In the event of an SGTR, these valves close, if they are open, to prevent the release of primary fluid and are also containment isolation valves. They are therefore supporting a Category A safety function. These bypass valves are positioned in parallel with the MSIVs and they are normally closed during power operation. They are opened during plant heatup when the MSIVs are closed and they must close to achieve the safety function. This makes them Class 1. See Appendix 15A. In order to prevent the blowdown of both SGs following a postulated steam line break inside containment, either bypass valve has to close to meet the safety function.

Main Steam Safety Valves (SGS-PL-V030A/B, -V031A/B, -V032A/B, -V033A/B, -V034A/B, and -V035A/B)

The main steam safety valves protect against SG overpressure and consequent challenges to RCS integrity. This is a Category A safety function. Reseating following a lift to prevent uncontrolled cooldown is a requirement also associated with RCS integrity as well as core reactivity, and again makes the valves Category A. As the main steam safety valves are the primary method of providing this function, they are Class 1. See Appendix 15A.

Six safety valves are associated with the main steam line from each SG. They are set to a series of staggered lift points so that they open sequentially as steam pressure rises. The requirement against each valve, therefore, is that it will open at the correct set pressure and then reseat when the pressure falls appropriately. The capacity of the 12 main steam safety valves is claimed to provide sufficient capacity to prevent the SGS pressure from exceeding 110 percent of the design value.

Power Operated Relief Valves (PORV) (SGS-PL-V233A/B)

The main steam PORVs do not have a formal safety function for limiting main steam line pressure although they will still operate. They do have a safety function to close on demand to prevent cooldown due to secondary-side depressurisation. This is a Category A safety function. Although the primary requirement for isolation of the relief path is with the PORV block valve, closure of the PORV itself is required to ensure that the function remains available even in the event of a single failure. As a result, the PORVs are Class 1. See Appendix 15A.

One PORV is associated with each SG. It is arranged in series with its associated block valve so that either closing will achieve the safety function. The safety claim, therefore, is that the PORV will close on demand.

PORV Block Valves (SGS-PL-V027A/B)

The main steam system PORV block valves exist to protect against a stuck-open PORV. As this is protecting against the cooldown due to secondary-side depressurisation, these valves are again Category A. As they are the principal equipment to provide this on the PORV line, they are Class 1. See Appendix 15A.

One block valve is associated with each PORV, arranged in series as described above. The safety requirement is that the block valve will close on demand.

SG Blowdown Isolation Valves (SGS-PL-V074A/B, -V075A/B)

The blowdown isolation valves help to prevent uncontrolled cooldown and the consequent potential impact on reactivity. Control of reactivity is a Category A safety function. The normal protection for this function is provided by flow restrictions in the blowdown lines, and these restrictions are located downstream in the turbine building. Therefore, the blowdown isolation valves have a backup, or defence in depth, role in the event of a failure upstream of the flow restriction and downstream of the isolation valves. See Appendix 15A.

The blowdown isolation valves also close to preserve SG water inventory. This is to assist in maintaining a heat sink and is also considered a Category A safety function. Because the blowdown isolation valves are the only means of providing the maintenance of heat sink safety function, they are Class 1. See Appendix 15A.

The blowdown isolation valves also serve to preserve containment integrity. Containment integrity is a Category A safety function. Because the blowdown isolation valves are a primary means of providing the containment integrity safety function, they are Class 1. See Appendix 15A.

Thus the SG blowdown valves are Class 1. The requirement against these valves is that they will close on demand. There are two valves in series, so either one closing successfully will achieve the safety function for that SG. Clearly, to achieve the safety function in total, at least one valve in each SG blowdown line must close successfully.

Main Feed Water Isolation Valves (SGS-PL-V057A/B)

The MFIVs are designed to prevent inadvertent temperature changes of the reactor coolant and consequent reactivity concerns as a result of excess feedwater flow. Reactivity control is a Category A safety function. The MFIVs provide a primary means of supporting this safety function and are therefore deemed Class 1. See Appendix 15A.

The MFIVs are CIVs. Containment isolation is a Category A safety function and because the MFIVs are the primary isolation valves for the feedwater system penetrations, they are also Class 1 in this role. See Appendix 15A.

Two MFIVs are provided, one in the main feedwater line to SG A and one in the main feedwater line to SG B. The requirement against each is that they close on demand. Both valves have to close to ensure that the safety function is met in all circumstances. To limit the mass and energy addition to containment in the event of steam or feedwater line breaks inside containment, there is a requirement that the MFIV be capable of isolation in fast close mode within 5 seconds.

The design of the valve and its associated actuator is very similar to valves used for similar functions in existing in-service PWRs.

Main Feedwater Control Valves (SGS-PL-V250A/B)

The MFCVs, in addition to their normal role of controlling feedwater flow, are designed to provide defence in depth to the MFIVs in preventing inadvertent temperature changes of the reactor coolant and consequent reactivity concerns as a result of excess feedwater flow. Reactivity control is a Category A safety function. The MFCVs, in conjunction with the MFIVs, provide the primary means of supporting this safety function and are therefore deemed Class 1. See Appendix 15A.

Two MFCVs are provided: one each in the main feedwater lines to SGs A and B. The requirement against each is that they close on demand. Both valves have to close to ensure that the safety function is met in all circumstances.

The design of the valve and its associated actuator is very similar to valves used similar functions in existing in-service PWRs.

Main Feedwater Check Valves (SGS-PL-V058A/B)

As stated previously, there is no safety requirement against the ability of the main feedwater check valves to change state, but their ability to do so in a way that is not detrimental to the structural integrity of the feedwater system pipework is an implicit requirement. Longer-term protection of feedwater system pipework would be commensurate with protection against internal hazards from major pipework leaks and so can be considered a Category A safety function. The main feedwater check valve closure times are fundamental to preventing hydrodynamic shocks and so the valves are considered to be Class 1. See Appendix 15A. The bodies of the main feedwater check valves effectively form a part of the containment penetration. Providing containment integrity is a Category A safety function and, given that they form a part of the penetration, they are considered Class 1 in this respect.

Two main feedwater check valves are provided, one each in the main feedwater lines to SGs A and B. The requirement against each is that they close over such a timescale that the hydrodynamic shock generated will be within the design limits for the

main feedwater system. It is therefore required that the main feedwater check valves close in >1 but <2 seconds.

Startup Feedwater Flow Control Valve (SGS-PL-V255A/B)

The SFCVs, in addition to their normal role of controlling feedwater flow, are designed to support the SFIVs in providing containment isolation in addition to preventing inadvertent temperature changes of the reactor coolant and the consequent impact on reactivity as a result of excess feedwater flow. Reactivity control and containment isolation are Category A safety functions. The SFCVs, with the SFIVs, provide the principal means of supporting these safety functions and are therefore deemed Class 1. See Appendix 15A.

Two SFCVs are provided, one each in the startup feedwater lines to SG A and SG B. The requirement against each is that they will close on demand. Both valves have to close to ensure that the safety function is met in all circumstances.

Startup Feedwater Isolation Valve (SGS-PL-V067A/B)

The SFIV is designed to prevent inadvertent temperature changes of the reactor coolant and consequent impact on reactivity as a result of excess feedwater flow. Reactivity control is a Category A safety function. The SFIVs provide the primary means of supporting this safety function and are therefore deemed Class 1. They are also CIVs. Containment isolation is also a Category A safety function. The SFIVs provide the primary means of supporting this safety function and are therefore also deemed to be Class 1 in this role. See Appendix 15A.

Two SFIVs are provided, one each in the startup feedwater lines to SG A and SG B. The requirement against each is that they will close on demand. Both valves have to close to ensure that the safety function is met in all circumstances.

Startup Feedwater Check Valve (SGS-PL-V256A/B)

This valve provides defence in depth against cooldown transients associated with failure of the startup feedwater pipework upstream of the SFCVs. Protection against cooldown transients and the consequent impact on reactivity control is a Category A safety function. The SFCVs support the feedwater isolation and containment isolation functions and are therefore Class 1. See Appendix 15A.

There are two valves, one on the startup feedwater line to each SG. Both are required to close to satisfy the safety function. The requirement is that they will close when they see reverse flow in the startup feedwater lines.

17.4.1.4 Justification of Claims on Components and Equipment

Main Steam Line Isolation Valves (SGS-PL-V040A/B)

The MSIV valve actuator requires that the hydraulic pressure must be held in place to keep the valve open, which means that any leakage or failure of the hydraulic system will result in the valve closing by virtue of the energy stored in the “gas spring”. The system of solenoid valves used to control operation of the hydraulic system is described above. Clearly, this is not fail-safe with respect to the main steam line isolation function; however, given that spurious actuation of this function when not required could, in itself, give rise to safety concerns through the sudden loss of heat sink when at power, it is judged as appropriate.

Both valves are manufactured from alloy steel to ensure compatibility with steam at the conditions at that it passes through them. They are designed to ASME Boiler and Pressure Vessel Code, Section III-2 that has been specifically developed to qualify pressure-retaining components in safety-significant applications on nuclear power stations. The valves are very similar to those already in service for the same function on many operating power stations. As a result, the information from testing these in-service valves offers a high degree of confidence about the reliability to be expected from these valves.

The failure mechanism of concern would involve the valve sticking or jamming. This could be a result of wear, corrosion, or maintenance-induced failure. In addition to being designed to ASME Boiler and Pressure Vessel Code, Section III-2, the valves are also designed and installed to seismic C-I standards, and are qualified for operation in a harsh environment. The combination of the ASME Boiler and Pressure Vessel Code, Section III and other codes for design and manufacture with the test regime described below will minimise the probability of these failure mechanisms occurring. Both solenoids in either pair must energise for the slow close function, but the requirement that only a single solenoid need energise for the fast close and the fact that redundancy is provided, gives extra confidence in the reliability of achieving the required safety function.

The maintenance and testing arrangements for the MSIVs are based on the programmes associated with ASME Boiler and Pressure Vessel Code qualification. The testing is:

- A full stroke operability test is performed every 2 years when the plant is at cold shutdown. This is required to demonstrate that the valve closure time is less than 5 seconds. Even though a test every three months might be specified for this type of service, exercising the valve with the unit at power is deemed to present an unacceptable risk to normal operation and hence, under the ASME Boiler and Pressure Vessel Code, Section III rules, can be varied.

- Visual confirmation of valve operation during the stroke testing is performed every 2 years.

- Given that they are CIVs, leakage testing is performed as part of the containment integrated leak rate test (ILRT). This test will be performed in line with the CIV leak test programme.

- The actuator nitrogen pressure is monitored to ensure that the valve remains operable in accordance with technical specifications (Tech Specs).

MSIV Bypass Isolation Valves (SGS-PL-V240A/B)

The MSIV bypass valves are air operated with the actuators designed to fail closed in the event of a loss of air supply. This is an inherently safe mechanism meaning that only in the event of a valve sticking will there be a failure to a condition other than safe.

The valves are manufactured from alloy steel to provide compatibility with steam at the conditions at that it passes through them. They are designed to ASME Boiler and Pressure Vessel Code, Section III-2.

The valves are very similar to those already in service for the same function on many operating power stations. As a result, the information from testing these in-service valves offers a high degree of confidence about the reliability to be expected from these valves. Data collected from in-service plants (Reference 17.7, Table 5.1) indicate a value to remain closed for an air-operated valve. This is comparable to the value being claimed.

The failure mechanism of concern would involve the valves sticking or jamming. This could be a result of wear, corrosion, or maintenance-induced failure. In addition to being designed to ASME Boiler and Pressure Vessel Code, Section III, the valves are also designed and installed to seismic C-I standards and are qualified for operation in a harsh environment. The combination of the ASME Boiler and Pressure Vessel Code, Section III and other codes for design and manufacture with the test regime described below will minimise the probability of these failure mechanisms occurring.

The maintenance and testing arrangements for the MSIV bypass valves are based on the programmes associated with ASME Boiler and Pressure Vessel Code qualification. The testing is:

- A full stroke operability test is performed every 3 months with the reactor at power.
- Visual confirmation of valve operation during the stroke testing is performed every 2 years.
- Given that they are CIVs, leakage testing is performed as part of the containment ILRT. This test will be performed in line with the CIV leak test programme.

Main Steam Safety Valves (SGS-PL-V030A/B, -V031A/B, -V032A/B, -V033A/B, -V034A/B, and -V035A/B)

The main steam safety valves are of the spring-loaded, self-actuated type; operation depends only upon the pressure difference across them and not on any method of powered actuation. This passive approach offers a high degree of inherent safety and reliability.

The valves are manufactured from carbon steel as they do not normally see a flow of steam and are designed to ASME Boiler and Pressure Vessel Code, Section III-2.

The valves are very similar to those already in service for the same function on many operating power stations. As a result, the information from testing these in-service valves offers a high degree of confidence about the reliability to be expected from these valves.

The failure mechanism of concern would involve the valve sticking or jamming. This could be a result of wear, corrosion, or maintenance-induced failure. In addition to being designed to ASME Boiler and Pressure Vessel Code, Section III, the valves are also designed and installed to seismic C-I standards. The combination of the ASME Boiler and Pressure Vessel Code, Section III and other codes for design and manufacture with the test regime described below will minimise the probability of these failure mechanisms occurring. The provision of six relief valves with staggered lifting pressure also helps to minimise the impact of any one valve failing to open on demand or, having opened correctly, subsequently failing to reseat.

The maintenance and testing arrangements for the main steam safety valves are based on the programmes associated with ASME Boiler and Pressure Vessel Code qualification. The testing is:

- Each valve should be tested as installed, or bench-tested, every 5 years.
- Given the multiple valves present on each steam line, the ASME Boiler and Pressure Vessel Code standard requires that in fulfilling the above requirement, 20 percent of the valves will be tested, either installed or on the bench, every 2 years.

Power Operated Relief Valves (PORV) (SGS-PL-V233A/B)

The main steam PORVs are air operated with the actuators designed to fail closed in the event of a loss of air supply. This is an inherently safe mechanism meaning that only in the event of a valve sticking will there be a failure to a condition other than safe.

The valves are manufactured from alloy steel to ensure compatibility with the steam at the conditions at that it passes through them. Unlike the main steam safety valves, they are expected to pass flow under off-normal operations when providing RCS cooling by steam generation but with the turbine condensers unavailable. They are designed to ASME Boiler and Pressure Vessel Code, Section III.

The valves are very similar to those already in service for the same function on many operating power stations. As a result, the information from testing these in-service valves offers a high degree of confidence about the reliability to be expected from these valves. Data collected from in-service plants (Reference 17.7, Table 5.1) are comparable to the value being claimed.

The failure mechanism of concern would involve the valves sticking or jamming. This could be a result of wear, corrosion, or maintenance-induced failure. In addition to being designed to ASME Boiler and Pressure Vessel Code, Section III, the valves are also designed and installed to seismic C-I standards and are qualified for operation in a harsh environment. The combination of the ASME Boiler and Pressure Vessel Code, Section III and other codes for design and manufacture with the test regime described below will minimise the probability of these failure mechanisms occurring.

The maintenance and testing arrangements for the MSIV bypass valves are based on the programmes associated with ASME Boiler and Pressure Vessel Code qualification. The testing is:

- A full stroke operability test is performed every 3 months with the reactor at power.
- Visual confirmation of valve operation during the stroke testing is performed every 2 years.

PORV Block Valves (SGS-PL-V027A/B)

The PORV block valves are motor operated, which means that inherently they will fail “as is”. Clearly, this is not fail-safe with respect to the function of isolating a stuck-open PORV, but a spurious actuation of this function could inhibit the operation of a correctly operating PORV. In this case, there might be resulting safety concerns with the incorrect isolation of a heat removal path, so the requirement to fail “as is” is judged as appropriate.

The valves are manufactured from alloy steel to ensure compatibility with steam at the conditions they will see. They are designed to ASME Boiler and Pressure Vessel Code, Section III-2.

The failure mechanism of concern would involve a valve sticking or jamming. This could be a result of wear, corrosion, or maintenance-induced failure. In addition to being designed to ASME Boiler and Pressure Vessel Code, Section III, the valves are also designed and installed to seismic C-I standards and are qualified for operation in a harsh environment. The combination of the ASME Boiler and Pressure Vessel Code, Section III and other codes for design and manufacture with the test regime described below will minimise the probability of these failure mechanisms occurring.

The maintenance and testing arrangements for the MSS PORV block valves are based on the ASME Boiler and Pressure Vessel Code programmes appropriate for these types of valves as used in existing nuclear power stations. The testing is:

- A full stroke operability test is performed quarterly in accordance with ASME Boiler and Pressure Vessel Code.
- Visual confirmation of valve operation during the stroke testing is performed every 2 years.
- Given that they are CIVs, leakage testing is carried out as part of the containment ILRT. This test will be performed in line with the CIV leak test programme.

SG Blowdown Isolation Valves (SGS-PL-V074A/B, -V075A/B)

The blowdown isolation valves are air operated with the actuators designed to transfer closed in the event of a loss of air supply. This is an inherently safe mechanism, meaning that only in the event of a valve sticking will there be a failure to a condition other than safe.

The valves are manufactured from alloy steel to ensure compatibility with the SG secondary-side water that passes through them. They are designed to either the ASME Boiler and Pressure Vessel Code, Section III-2 or Section III-3.

The design of the air-operated globe valve is very similar to those valves used for similar functions in PWR reactors already operating. As a result, the information from testing these in-service valves offers a high degree of confidence about the reliability to be expected from these valves. Data collected from in-service plants (Reference 17.7, Table 5.1) indicate a probability of failure comparable to the claim being made.

The failure mechanism of concern would involve the valve sticking or jamming. This could be a result of wear, corrosion, or maintenance-induced failure. In addition to being designed to ASME Boiler and Pressure Vessel Code, Section III, the valve is also designed and installed to seismic C-I standards and is qualified for operation in a harsh environment. The combination of the ASME Boiler and Pressure Vessel Code, Section III and other codes for design and manufacture with the test regime described below will minimise the probability of this occurring. The provision of two valves in series further reduces the probability of failure to provide the safety function.

The maintenance and testing arrangements for the blowdown isolation valves is based on the ASME Boiler and Pressure Vessel Code programmes appropriate for this type of valve as used in existing nuclear power stations. The testing is:

- A full stroke operability test is performed quarterly in accordance with the ASME Boiler and Pressure Vessel Code.
- Visual confirmation of valve operation during the stroke testing is performed every 2 years.
- Given that they are CIVs, leakage testing is carried out as part of the containment ILRT. This test will be performed in line with the CIV leak test programme.

Main Feedwater Isolation Valves (SGS-PL-V057A/B)

The MFIV is held open by a hydraulic actuator and closes using compressed nitrogen stored within the actuator. Any failure or leakage of the hydraulic system will result in the nitrogen pressure closing the valve. The design action of the solenoid valves that control the hydraulic system provides a fail "as is" feature on loss of all electrical supplies. This is not intrinsically fail-safe with respect to main feedwater line isolation; however, spurious closing of the MFIV could cause loss of heat removal capability and other transient effects, so this arrangement is judged to be appropriate.

The MFIV is manufactured from alloy steel to ensure compatibility with the feedwater that passes through it. By design, its trims and seats are constructed of materials to allow the valve to close within 5 seconds against a major feedwater pipe rupture. The bidirectional wedge design is used to ensure that the valve effectively seals in both directions. Because the failure mechanism of concern would involve the valve jamming or sticking, it is designed to the ASME Boiler and Pressure Vessel Code, Section III design code, Class 2, and seismic C-I; and is qualified for harsh environment. Components designed and built to this code have accumulated a vast body of experience in similar applications. This code, with its supporting testing and examination, provides the foundation for performance claims made on these valves. Data collected from in-service plants (Reference 17.7, Table 5.1) provide a probability of failure to close for a hydraulically operated valve of this type.

The maintenance and testing arrangements for the MFIVs are based on the programmes associated with ASME Boiler and Pressure Vessel Code qualification. The testing is:

- A full stroke operability test is performed every 2 years when the plant is at cold shutdown. This is required to demonstrate that the valve closure time is less than 5 seconds. Even though a test every 3 months might be specified for this type of service, exercising the valve with the unit at power is deemed an unacceptable risk to normal operation; therefore, under the ASME Boiler and Pressure Vessel Code, rules, the frequency can be varied.

- Visual confirmation of valve operation during the stroke testing is performed every 2 years.

- Given that they are CIVs, seat leakage limits will be tested to verify leak tightness. This test will be performed in line with the CIV leak test programme (Reference 17.11).

Monitoring of the actuator nitrogen pressure is performed to ensure that the valve remains operable in accordance with Tech Specs.

Main Feedwater Control Valves (SGS-PL-V250A/B)

The MFCVs are air operated with the actuators designed to fail closed in the event of a loss of air supply. This is an inherently safe mechanism meaning that only in the event of a valve sticking will there be a failure to a condition other than safe.

The MFCVs are manufactured from alloy steel to ensure compatibility with the feedwater that passes through them. By design, their trims and seats are constructed of materials to allow them to close within 5 seconds against a major pipe rupture upstream or downstream. Because the failure mechanism of concern would involve the valves jamming or sticking, they are designed to ASME Boiler and Pressure Vessel Code, Section III-3 and seismic C-I, and are qualified for a harsh environment. Components designed and built to this code have accumulated a vast body of experience in similar applications. This code, with its supporting

testing and examinations, provides the foundation for performance claims made on these valves. Data collected from in-service plants (Reference 17.7, Table 5.1) provide a probability of failure to close for an air-operated valve of this type.

The maintenance and testing arrangements for the MFCVs are based on the programmes associated with ASME Boiler and Pressure Vessel Code qualification. The testing is:

- A full stroke operability test is performed every 2 years when the plant is at cold shutdown. This is required to demonstrate that the valve closure time is less than 5 seconds. Even though a test every 3 months might be specified for this type of service, exercising the valve with the unit at power is deemed an unacceptable risk to normal operation; therefore, under the ASME Boiler and Pressure Vessel Code, the frequency can be varied.

- Visual confirmation of valve operation during the stroke testing is carried out every 2 years.

Main Feedwater Check Valves (SGS-PL-V058A/B)

The operation of the main feedwater check valves depends only upon the pressure difference across them and not on any method of powered actuation. This passive approach offers a high degree of inherent safety and reliability.

The valves are manufactured from stainless steel to ensure compatibility with the RCS chemistry conditions and are designed to ASME Boiler and Pressure Vessel Code, Section III-2 that has been specifically developed to qualify pressure-retaining components in safety-significant applications on nuclear power stations. The code, with its supporting testing and examination, provides the foundations for performance claims made on the accumulator check valves.

The valves are very similar to those already in like service on many operating power stations. This provides a good level of confidence that the valve performance will remain consistent.

Startup Feedwater Control Valves (SGS-PL-V255A/B)

These valves are air operated with the actuators designed to fail closed in the event of a loss of air supply. This is an inherently safe mechanism, meaning that only in the event of a valve sticking will there be a failure to a condition other than safe. The presence of an auxiliary air accumulator to provide a “ride-through” capability against temporary interruption of the air supplies supports reliability during normal operation.

The valves are manufactured from carbon steel and are designed to ASME Boiler and Pressure Vessel Code, Section III.

The valves are very similar to those already in like service on many operating power stations. As a result, the information from testing these in-service valves offers a high degree of confidence about the reliability to be expected from these valves. Data collected from in-service plants (Reference 17.7, Table 5.1) indicate a value that is comparable to the value being claimed.

The failure mechanism of concern would involve the valves sticking or jamming. This could be a result of wear, corrosion, or maintenance-induced failure. In addition to being designed to ASME Boiler and Pressure Vessel Code, the valves are also designed and installed to seismic C-I and are qualified for operation in a harsh environment. The maintenance and testing arrangements for the SFCVs are based on the programmes associated with ASME Boiler and Pressure Vessel Code, qualification. The testing is:

- A full stroke operability test is performed every 3 months with the reactor at power.
- Visual confirmation of valve operation during the stroke testing is performed every 2 years.

Startup Feedwater Isolation Valves (SGS-PL-V067A/B)

These valves are motor operated with the actuators designed to fail "as is" in the event of a loss of power supply. This is not an inherently safe mechanism but the complications associated with ensuring that an air-operated system is protected from spurious failure (for example, the SFCVs) were felt to make for a less reliable solution than a straightforward motor-operated valve.

The valves are manufactured from mild steel and are designed to ASME Boiler and Pressure Vessel Code, Section III-2. The valves are very similar to those already in like service on many operating power stations. As a result, the information from testing these in-service valves offers a high degree of confidence about the reliability to be expected from these valves. Data collected from in-service plants (Reference 17.7, Table 5.1) indicate that this is comparable to the value being claimed.

The failure mechanism of concern would involve the valves sticking or jamming. This could be a result of wear, corrosion, or maintenance-induced failure. In addition to being designed to ASME Boiler and Pressure Vessel Code, Section III, the valves are also designed and installed to seismic C-I and are qualified for operation in a harsh environment. The maintenance and testing arrangements for the SFIVs is based on the programmes associated with ASME Boiler and Pressure Vessel Code, qualification. The testing is:

- A full stroke operability test is performed every 3 months with the reactor at power.
- Visual confirmation of valve operation during the stroke testing is performed every 2 years.

Startup Feedwater Check Valves (SGS-PL-V256A/B)

The operation of these check valves depends only upon the pressure difference across them and not on any method of powered actuation. This passive approach offers a high degree of inherent safety and reliability. The nozzle-type check valve is able to close very rapidly and was selected to minimise the potential for water hammer if there is a flow reversal in the pipework.

The valve is manufactured from mild steel and is designed to ASME Boiler and Pressure Vessel Code, Section III-3.

The valve is very similar to those already in like service on many operating power stations. As a result, the information from testing these in-service valves offers a high degree of confidence about the reliability to be expected from the valve proposed for the AP1000 design. Data collected from in-service plants (Reference 17.7, Table 5.1) indicate that this is conservative with respect to the value being claimed.

17.4.2 Steam Generator Blowdown System

17.4.2.1 Role

A detailed description of the steam generator blowdown system (BDS) is given in Section 6.5.

The BDS sole safety function is preventing the release of radioactive waste material from onsite radioactive waste systems. As dicussed in section 17.1 components that have no other safety function other than a pressure boundary are not discussed in this chapter. As delineated in Table 15A BDS valves achieve the aforementioned function but are not discussed here. Further design details of this system and its constituent components are delineated in Reference 17.18.

17.4.3 Turbine Bypass and Other MSS and Main Turbine System (MTS) Valves

17.4.3.1 Role

A detailed description of the turbine bypass function is given in Section 6.5.

The role of the turbine bypass is to provide an alternative route to handle steam generated when the main turbine is unable to accept it. There are six turbine bypass valves, two exhausting into each turbine condenser pass. These valves allow the station to handle up to 100 percent electrical load rejection and maintain primary and secondary circuit conditions so that demands on the main steam safety valves and pressuriser safety valves are eliminated. This means that the turbine bypass system is effectively providing a defence in depth function even though it is the preferred system to manage these transients.

The system does, however, contribute to the reactivity control and heat transfer/residual heat removal primary safety functions. Incorrect operation of the turbine bypass system when, for example, a bypass valve is opened, will result in increased heat removal and a cooldown transient. To combat this, the turbine bypass valves have a function to isolate on demand. Whilst the main steam isolation valves are the principal means of providing this function, under certain circumstances, isolating the turbine bypass valves is also claimed as defence in depth.

Similarly, there are other valves in the MSS and MTS where isolation is required to provide backup protection against increased heat removal due to excess steam demand events or to limit steam backflow into containment following a postulated steam line break inside containment. These locations are the auxiliary steam supply isolation valves, the steam supply isolation valves to the second stage of the moisture separator reheaters (MSR), and the high pressure turbine stop and control valves. These valves are required to isolate their respective steam paths to meet their defence in depth function.

All the above valves are supported by the PMS and PLS in achieving their safety functions. These valves support the SGS as their safety functions.

Further design details of this system and its constituent components are delineated in Reference 17.20 and Reference 17.8.

17.4.3.2 System Components and Equipment Contributing to Safety Function

The pipework and valve design of the turbine bypass system is to ASME Standard, B31.1. The following components contribute to the turbine bypass system and other steam supplies performing their safety function:

- **Turbine Bypass Control Valves (MSS-PL-V001, -V002, -V003, -V004, -V005, -V006)** – These are 400-mm DN (16-inch), air-operated angle globe valves. The actuators are designed to fail closed on the loss of air supplies. They are required to close on receipt of a main steam line isolation signal from the PMS. This stops any steam flow through the bypass line and terminates the contribution to RCS cooldown; therefore, the isolation of the steam path on demand is a safety requirement.

- **MSR 2nd Stage Reheat Supply Steam Isolation Valves (MSS-PL-V015A/B)** – These are 250-mm DN (10-inch), air-operated globe valves. The actuators are designed to fail closed on loss of air supply. They are required to close on receipt of a main steam line isolation signal that stops any steam flow into the reheater and terminates the contribution to RCS cooldown. This is a safety requirement. They are also required to close on receipt of a main steam line isolation signal to stop any steam flow from the reheater back into the containment in order to limit the mass and energy contribution to the containment atmosphere following a steam line break inside the containment. This is a safety requirement.

- **Auxiliary Steam Supply Header Isolation Valve (MSS-PL-V020)** – This is a 400-mm (16-inch) nominal-bore, air-operated globe valve. The actuator is designed to fail closed on the loss of air supplies. The valve is required to close on receipt of a main steam line isolation signal to prevent any flow into the auxiliary steam systems and terminate the contribution to RCS cooldown. This is a safety requirement.

- **High Pressure Turbine stop valves (MTS-PL-V001A/B and V003A/B) and Control Valves (MTS-PL-V002A/B, and V004A/B)** – The high pressure turbine stop valves and control valves are 700 mm DN (28-inch) valves with electro-hydraulic actuators that can function to quickly shut off steam flow to the turbine under emergency conditions, and control the main steam flow from the steam generator to match electrical power output demand, respectively. Furthermore, the control valves help control heat transfer of the steam generator. The main stop valves are located in the main steam piping directly ahead of the control valves with the outlet of each main stop valve welded directly to the inlet of a separate control valve casing. The valves are required to close on receipt of a main steam line isolation signal to prevent any flow into the high pressure turbine and terminate the contribution to RCS cooldown. As a result, this is a safety requirement. The valves are also required to close on receipt of a main steam line isolation signal to prevent any back flow from the high pressure turbine and MSR into the containment following a steam line break inside containment. This is also a safety requirement.

17.4.3.3 Claims on Components and Equipment

Turbine Bypass Control Valves (MSS-PL-V001, -V002, -V003, -V004, -V005, -V006)

The turbine bypass control valves, when closed, enable the isolation of secondary-side steam flows and so help to prevent cooldown of the RCS. The most immediate concern with

cooldown is the control of reactivity. Control of reactivity is a Category A safety function. The turbine bypass control valves are not the primary means of providing this function as this rests with the main steam isolation valves. The turbine bypass control valves therefore perform a Category C safety function and are Class 3 (Ref. 17.21). See Appendix 15A.

The requirement against these valves is that they will close on demand. Each steam flow path into its associated condenser pass has a single control valve. As a result, all six valves must close to fulfil the safety function.

The valves are very similar to those already in service for the same function on many operating power stations. As a result, the information from testing these in-service valves offers a high degree of confidence about the reliability to be expected from these valves. Data collected from in-service plants (Reference 17.7, Table 5.1) indicate a value to remain closed for an air-operated valve. This is comparable to the value being claimed.

MSR 2nd Stage Reheat Supply Steam Isolation Valves (MSS-PL-V015A/B)

The MSR second-stage reheat steam isolation valves, when closed, enable the isolation of secondary-side steam flows and thus help to prevent cooldown of the RCS. The most immediate concern with cooldown is the control of reactivity that is a Category A safety function. The MSR second-stage reheat steam isolation valves are not the primary means of providing this function as this rests with the main steam isolation valves. The MSR second-stage reheat steam isolation valves therefore perform a Category C safety function and are Class 3 (Reference 17.21). See Appendix 15A.

The requirement against these valves is that they will close on demand. Two MSRs are associated with the turbine generator and a single isolation valve is associated with the second-stage reheat on each MSR. This means that both second-stage reheat steam isolation valves must close to fulfil the safety function.

Auxiliary Steam Supply Header Isolation Valve (MSS-PL-V020)

The auxiliary steam supply header isolation valve, when closed, enables the isolation of secondary-side steam flows and thus helps to prevent cooldown of the RCS. The most immediate concern with cooldown is the control of reactivity that is a Category A safety function. The auxiliary steam supply header isolation valve is not the primary means of providing this function as this rests with the main steam isolation valves. The auxiliary steam supply header isolation valve therefore performs a Category C safety function and is Class 3 (Reference 17.21). See Appendix 15A.

There is one isolation valve associated with auxiliary steam supply and the safety requirement is that the valve will close on demand.

High Pressure Turbine Stop Valves (MTS-PL-V001A/B and V003A/B) and Control Valves (MTS-PL-V002A/B, and V004A/B)

The high pressure turbine stop valves and control valves, when closed, enable the isolation of secondary-side steam flows and so help to prevent cooldown of the RCS or back flow into the containment following a steam line break inside containment. The concern with cooldown is the control of reactivity. Control of reactivity is a Category A safety function. The concern with back flow is containment integrity which is also a Category A safety function. The high pressure turbine stop valves and control valves are not the primary means of providing this function as this rests with the main steam isolation valves. The high pressure turbine stop and

control valves therefore perform a Category C safety function and are Class 3 (Reference 17.21). See Appendix 15A.

The requirement against these valves is that they will close on demand. Each of the four steam flow paths into the high pressure turbine has a single stop valve and control valve in series. All eight valves receive a signal to close when the PMS generates a main steam isolation signal. As a result, either of the stop and control valves in each pair in each of the high pressure turbine steam inlet paths must close to fulfil the safety function.

17.4.3.4 Justification of Claims on Components and Equipment

Turbine Bypass Control Valves (MSS-PL-V001, -V002, -V003, -V004, -V005, -V006)

The turbine bypass control valves are designed to fail closed on loss of air supply. This function is provided by springs within the actuator and, because it does not depend on any external actuation, it is an inherently safe approach.

The air supply to each turbine bypass control valve is provided through three solenoid-operated valves, each of that has to remain energised for the air supply to be maintained and the valve open. Two of these solenoid valves are de-energised to close by signals from the PMS. Either solenoid valve opening will dump the air supply pressure and cause the associated turbine bypass control valve to close. Clearly, this arrangement also means that any failure in the electrical supplies to the solenoid valves will also result in loss of air supply and closure of the associated turbine bypass control valve.

The valves are designed to ASME Section B16.34. The maintenance and testing arrangements for the turbine bypass control valves are based on the programmes that demonstrate both the ability of the valves to stroke through their full operating range and to meet the maximum closure time assumed in the response to faults. The testing is:

- A stroke test to confirm that each valve closure time is within a 5-second limit is performed with the unit at normal operating temperature and pressure but before return to power, after each refuelling outage.

- A full stroke test of each valve is performed during each cold shutdown to confirm that the valve is moving correctly within its position limits.

MSR 2nd Stage Reheat Supply Steam Isolation Valves (MSS-PL-V015A/B)

The MSR second-stage reheat steam isolation valves are designed to fail closed on loss of air supply. This function is provided by springs within the actuator and, because it does not depend on any external actuation, is an inherently safe design.

The air supply to each MSR second-stage reheat steam isolation valve is provided through a solenoid-operated valve that has to remain energised for the air supply to be maintained and the valve open. The solenoid valve is de-energised to close by signals from the PMS. This will dump the air supply pressure and cause the MSR second-stage reheat steam isolation valve to close. Clearly, this arrangement also means that any failure in the electrical supplies to the solenoid valves will also result in loss of air supply and closure of the associated MSR second-stage reheat steam isolation valve.

The valves are designed to ASME Section B16.34. The maintenance and testing arrangements for the MSR second-stage reheat steam isolation valves are based on the programmes that demonstrate both the ability of the valves to stroke through their full

operating range and to meet the maximum closure time assumed in the response to faults. The testing is:

- A stroke test to confirm that each valve closure time is within a 5-second limit is performed with the unit at normal operating temperature and pressure but before return to power, after each refuelling outage.

- A full stroke test of each valve is performed during each cold shutdown to confirm that the valve is moving correctly within its position limits.

Auxiliary Steam Supply Header Isolation Valve (MSS-PL-V020)

The auxiliary steam supply header isolation valve is designed to fail closed on loss of air supply. This function is provided by springs within the actuator and, because it does not depend on any external actuation, is an inherently safe design.

The air supply to the auxiliary steam supply header isolation valve is provided through a solenoid-operated valve that has to remain energised for the air supply to be maintained and the auxiliary steam supply header isolation valve open. The solenoid valve is de-energised to close by signals from the PMS. This will dump the air supply pressure and cause the auxiliary steam supply header isolation valve to close. Clearly, this arrangement also means that any failure in the electrical supplies to the solenoid valve will also result in loss of air supply and closure of the associated auxiliary steam supply header isolation valve.

The valves are designed to ASME Section B16.34 (Reference 17.19).

The auxiliary steam supply header isolation valve performs a defence in depth function.

High Pressure Turbine Stop Valves (MTS-PL-V001A/B and V003A/B) and Control Valves (MTS-PL-V002A/B, and V004A/B)

The valve actuator for the high pressure turbine stop and control valves requires that the hydraulic pressure must be held in place to keep the valve open. Each of the eight valves has two, fail open solenoid valves, one of which is required to open for the valve to close. Each of these solenoid valves is controlled by two pilot valves which both have to be de-energised for the solenoid valve to open. Once, either of the two solenoid valves opens, the steam flow in the valves causes the valve to quickly close. This system of solenoid valves used to control operation of the hydraulic system provides a fail close feature for loss of all electrical supplies.

The valves are manufactured from alloy steel to ensure compatibility at the conditions at which steam passes through them. They are specially designed and manufactured valves that do not fall under any industry standard; however, they are tested to ASME Power Piping Code B31.1 test pressures.

The valves are very similar to those already in service for the same function on many operating power stations. As a result, the information from testing these in-service valves offers a high degree of confidence about the reliability to be expected from these valves.

The failure mechanism of concern would involve the valve sticking or jamming. This could be a result of wear, corrosion, or maintenance-induced failure. The rigorous design and manufacture requirements for these valves, the normal operation of the valves during plant operation, together with the test regime described below will minimise the probability of these failure mechanisms occurring. The requirement that only a single solenoid need

de-energise for the fast close and the fact that redundancy is provided, gives extra confidence in the reliability of achieving the required safety function.

The maintenance and testing arrangements for these valves are based on manufacturer's recommendations including:

- Visual confirmation of valve operation during the stroke testing is performed.
- The electro-hydraulic actuators and supporting equipment are monitored during valve operation to ensure proper operation.

17.4.4 Main Feedwater System

17.4.4.1 Role

A detailed description of the main feedwater system is given in Section 6.5.

In normal operation, the role of the main feedwater system is primarily associated with normal power operation and is required to deliver water at the correct flow rate, pressure, temperature, and chemical composition to each SG.

Further design details of this system and its constituent components are delineated in Reference 17.23.

17.4.4.2 System Components and Equipment Contributing to Safety Function

The main feedwater system comprises two parallel main feedwater lines, designated A and B. Each main feedwater line from the deaerator up to the turbine building wall is designed and constructed to the Power Piping Code B31.1. From the turbine building wall but excluding the MFIV (SGS-PL-V057A/B), the lines are constructed to ASME Boiler and Pressure Vessel Code, Section III-3 in the auxiliary building. Each main feedwater line from the MFIV (SGS-PL-V057A/B) to the SG is constructed to ASME Boiler and Pressure Vessel Code, Section III Class 2.

As dicussed in section 17.1 components that have no other safety function other than a pressure boundary are not discussed in this chapter. As delineated in Table 15A Main Feedwater components are Category C and Class 3.

17.4.5 Startup Feedwater Portion of the Feedwater System

17.4.5.1 Role

A detailed description of the startup feed water portion of the FWS is given in Section 6.5.

In normal operation, the startup feedwater system (SFW) is required to provide and control the flow of feed water to each of the two SGs during low-load operation. It performs the same role when the SGs are steaming with the reactor shut down and the main feedwater system unavailable. The SFW can draw water from either a connection with the main feedwater system or via its own dedicated supply from the condensate storage tanks (CST).

The SFW contributes to the reactivity control, heat transfer/residual heat removal, and containment primary safety functions.

The SFW provides a defence in depth (Class 2) function to support heat transfer/residual heat removal primary safety function by providing feedwater from the CST so the SGs can be used for decay heat removal post reactor trip. This flow is fed to the SGs via the SFIVs and SFCVs.

The SFW is supported by the on-site ac electrical power system (ECS) with standby power provided by the onsite standby power system (ZOS), if needed. The SFW supports the SG system.

Further design details of this system and its constituent components are delineated in Reference 17.23 and Reference 17.24.

17.4.5.2 System Components and Equipment Contributing to Safety Function

The SFW pipework between the startup feedwater isolation valves and the SGs is designed and constructed to the requirements of ASME Boiler and Pressure Vessel Code, Section III-2 and seismic C-I. The section in the auxiliary building is designed and constructed to the requirements of ASME Boiler and Pressure Vessel Code, Section III-3 and seismic C-I. The portion of the SFW in the turbine building is designed and constructed to section B31.1 of the power piping code. The following components contribute to the SFW fulfilling its safety requirements:

- **Condensate storage tank (DWS-MT-02)** – This is a vertical, stainless-steel, cylindrical tank with a capacity greater than that required for its safety function. Level and temperature instrumentation are provided and the tank level is maintained by the makeup valve. Freeze protection is supplied by immersion-type electric heaters. The location of the tank and the arrangements for the off take of condensate ensure that an adequate net positive suction head is provided for the startup feedwater pumps. The safety requirement is that the tank be a reliable source of water for the startup feedwater pumps.

- **Startup Feedwater Pumps (FWS-MP-03A/B)** – These are multistage centrifugal pumps designed to Hydraulic Institute standards. They are driven by an ac induction motor. The pump lubrication subsystems are self-contained and do not require external cooling. The startup feedwater pumps are tripped on high SG-level by signals from the PMS. The safety requirement is to provide feedwater for low and no power operations at appropriate pressure and flow.

- **Startup Feedwater Flow Venturi (FWS-FE-015A/B)** – This is fitted to the pump discharge pipework and is designed so that, at high flow conditions, flow will cavitate in the venturi. This results in the flow choking in the throat and is used to limit flow to prevent pump runout at low pressures. The safety requirement is to limit flow at low discharge pressure.

- **Startup Feedwater Pump Automatic Recirculation Check Valves (FWS-PL-V012A/B)** – These are 100-mm DN (4-inch) combination check and bypass valves (Automatic Ricurculation Valves (ARC)). The valves incorporate a spring-loaded check valve in the SFW pump discharge flow path and a bypass flow control device. Mini-flow recirculation is controlled by the bypass flow control device and the valve also functions as a check valve to prevent reverse flow through the pump when it is not operating and the pump discharge valve has not yet closed. This valve requires no external power and modulates flow through the recirculation path based on pressure-sensing capability. If forward flow to the system drops below approximately 47.7 m^3/hr (210 gpm), the

control valve automatically modulates open to maintain the total pump flow (forward flow plus recirculation flow) at this value. Most of the pressure breakdown of the recirculated flow is accomplished internally in the control valve. The safety requirement is to ensure that minimum flow requirements for the pump are met.

- **Main Feedwater Pump to Startup Feedwater Header Crossflow Valve (FWS-PL-V097)** – This 200-mm DN (8-inch), air-operated globe valve fails closed on loss of air supply. Its normal role is to open to allow the main feedwater pumps to supply the startup feedwater header at low power operation. The valve is normally closed during full-power operation and provides positive isolation of main feedwater to avoid potential thermal stratification effects in the startup feedwater piping. The valve is closed by the PLS on receipt of a main feedwater isolation signal. The safety requirement is to isolate the SFW from main feedwater on demand.

- **Main feedwater to Startup Feedwater Header Check Valve (FWS-PL-V096)** – This 250-mm (10-inch) nominal-bore swing check valve ensures that during operation of the startup feedwater pumps, they cannot inadvertently discharge back into the main feedwater system. The safety requirement is to prevent flow from the SFW into the main feedwater system.

17.4.5.3 Claims on Components and Equipment

Condensate Storage Tank (DWS-MT-02)

The CST provides the source of water to enable the SFW to provide feedwater to the SGs to remove decay heat. Removal of decay heat is a Category A safety function. The use of startup feedwater and SGs for decay heat removal is a defence in depth function, the passive residual heat removal (PRHR) system being the primary method. As such, the CST is Class 2. See Appendix 15A.

The requirement is that the CST capacity is sufficient to maintain steam generator cooling for at least 24 hours following a loss of normal ac power. The CST capacity is also sufficient to cool the RCS to safe shutdown conditions such that the RNS can be put into service. This includes 8 hours for the RCS to be borated and 6 hours to cool the RCS from hot standby to RNS initiation temperature. The single tank provides the supply to both startup feedwater pumps.

Startup Feedwater Pumps (FWS-MP-03A/B)

The startup feedwater pumps provide the motive force to get water from the CSTs to the SGs to remove decay heat. Removal of decay heat is a Category A safety function. The startup feedwater pumps are considered Class 2. See Appendix 15A.

Two pumps are arranged in parallel, and each can supply the required flow to provide the full system duty. They are required to start on demand and continue to run as required.

Startup Feedwater Flow Venturi (FWS-FE-015A/B)

The venturi is designed to cavitate at a flow near but less than the pump runout point; the choked flow in the throat of the venturi under such conditions prevents further flow increase. Thus, the venturi prevents the startup feedwater pump from running beyond its designed maximum flow rate. This device provides essential protection to the startup feedwater pump that supports a Category A safety function. The pump is Class 2, so the venturi must also be Class 2. See Appendix 15A.

The requirement is that the venturi will limit pump flow to a safe level.

Startup Feedwater Pump Automatic Recirculation Check Valves (FWS-PL-V012A/B)

These valves are provided to recirculate flow automatically from each pump discharge back to the CST to ensure a minimum flow through the pump when no flow is supplied forward to the SG. The pumps are supporting a Category A safety function and are Class 2 equipment, so the startup feedwater pump automatic recirculation valves must also be Class 2. See Appendix 15A.

Two valves are provided, one for each pump. Each valve can only support the pump with that it is associated. These valves are required to open on demand.

Main Feedwater Pump to Startup Feedwater Header Crossflow Valve (FWS-PL-V097)

This is required to close when startup feedwater is needed to fulfil the segregated safety function of decay heat removal in lieu of main feedwater. Decay heat removal is a Category A safety function and the startup feedwater system provides defence in depth and is Class 2. This valve supports the startup feedwater system and is therefore also Class 2. See Appendix 15A.

This valve is required to close on demand.

Main Feedwater to Startup Feedwater Header Check Valve (FWS-PL-V096)

This valve is required to close when startup feedwater is supplied for decay heat removal. Decay heat removal is a Category A safety function, and startup feedwater provides defence in depth and is Class 2. This valve supports the startup feedwater and is therefore also Class 2. See Appendix 15A.

This valve is required to close on demand.

17.4.5.4 Justification of Claims on Components and Equipment

Condensate Storage Tank (DWS-MT-02)

The CST contains at least sufficient capacity to meet cooling needs to achieve cold shutdown following a loss of main feedwater.

The CST is fabricated in stainless steel to ensure compatibility with the stored condensate and is vented, to prevent pressurisation. The tank is constructed to API-650 Code standards (Table 15A-1). The design is very similar to that of tanks like on currently operating PWRs and other nuclear power stations. This gives considerable confidence that the tank will be able to perform as expected.

Data collected from in-service plants (Reference 17.7, Table 5-1) indicate that the probability of a minor leak in an unpressurised tank is conservative relative to the value being claimed.

Startup Feedwater Pumps (FWS-MP-03A/B)

The startup feedwater pumps are similar to the pumps performing this duty on currently operating PWRs. As a result, the information from the operation of these in-service pumps offers a high degree of confidence about the reliability to be expected from the pumps

proposed for the AP1000 design. Data collected from in-service plants (Reference 17.7, Table 5-1) indicate that the claims being made are in line with operational experience.

Potential failure mechanisms of overloading, overheating, and lubrication failure are overcome by providing a venturi flow-limiting device, mini-flow flow capability, and cooling directly from the flowing medium.

Although there is no formal surveillance testing of the startup feedwater pumps, they can be tested using the mini-flow facility to verify performance. Routine maintenance and testing of the SFW pumps will be performed according to the manufacturer's recommendations and testing will be carried out to verify that performance has been maintained.

Startup Feedwater Flow Venturi (FWS-FE-015A/B)

A venturi is a passive device with proven performance. The suitability of the detailed design of this device will be established early during commissioning tests. It needs minimal maintenance and testing and, because it has no moving parts, is inherently able to perform its safety function.

Startup Feedwater Pump Automatic Recirculation Check Valves (FWS-PL-V012A/B)

The operation of the startup feedwater pump automatic recirculation check valves depends only upon the pressure difference across them and not on any method of powered actuation. This passive approach offers a high degree of inherent safety and reliability.

The valves are designed and manufactured to the ASME Standard B16.34. The valves are similar to those already in like service on many operating power stations. As a result, the information from testing these in-service valves offers a high degree of confidence in the reliability to be expected from these valves. Data collected from in-service plants (Reference 17.7, Table 5.1) indicate that the claim is conservative.

The failure mechanism of concern would involve a valve sticking or jamming. This could be a result of wear, corrosion, or maintenance-induced failure. Compliance with ASME Standard B16.34, along with the testing, should minimise the probability of these failure mechanisms being present.

Main Feedwater Pump to Startup Feedwater Header Crossflow Valve (FWS-PL-V097)

This valve is air operated with the actuators designed to fail closed in the event of a loss of air supply. This is an inherently safe mechanism, meaning that only in the event of a valve sticking will there be a failure to a condition other than safe.

The valve is designed and manufactured to ASME Standard B16.34 The valves are similar to those already in like service on many operating power stations. As a result, the information from testing these in-service valves offers a high degree of confidence about the reliability to be expected from these valves. Data collected from in-service plants (Reference 17.7, Table 5.1) indicate that the claim is in line with operational experience.

Main Feedwater to Startup Feedwater Header Check Valve (FWS-PL-V096)

The operation of this check valve depends only upon the pressure difference across it and not on any method of powered actuation. This passive approach offers a high degree of inherent safety and reliability.

The valve is designed and manufactured to ASME B16.34 that is well established for power station plants. The valve is similar to those already in like service on many operating power stations. As a result, the information from testing these in-service valves offers a high degree of confidence about the reliability to be expected from these valves. Data collected from in-service plants (Reference 17.7, Table 5.1) indicate that the claim is conservative.

17.5 Passive Core Cooling System and Associated Systems

17.5.1 Accumulators

17.5.1.1 Role

A detailed description of the PXS accumulators (PXS-MT-01A/B) is contained in Section 6.6. Further design details of this system and its constituent components are delineated in Reference 17.25.

The accumulators contribute to the provision of two primary safety functions: reactivity control and heat transfer/residual heat removal. It supports the heat transfer and residual heat removal safety function by providing large quantities of water to ensure that the reactor core is reflooded as quickly as possible following a LOCA. The reactivity control function is supported through this water being borated to cold shutdown levels.

The plant design provides for two independent accumulator tanks, each with its own line connecting to a direct vessel injection line to deliver coolant directly into the reactor vessel. These tanks are partially filled with borated water and contain pressurised nitrogen that acts as the motive force for injecting the water. A single accumulator is claimed to provide sufficient water to mitigate all but the largest LOCAs without core damage. For the largest LOCA, both accumulators are credited to discharge to limit core damage.

At power, the accumulators are maintained between minimum and maximum levels of borated water, between minimum and maximum pressure levels, and between minimum and maximum boron concentrations. Each injection line contains two check valves arranged in series and both must open to permit the injection of water. The accumulator check valves are held closed by the greater pressure under normal operating conditions in the RCS. All that is required for the system to operate is for the check valves to open when the differential pressure across them is reversed as the RCS depressurises. There is also a normally open motor-operated isolation valve in the injection line to allow the accumulator to be isolated when the reactor is shut down and the RCS is depressurised.

To ensure that accumulator pressure is maintained at all times, an accumulator nitrogen makeup isolation valve allows pressure to be increased, and a vent valve vents surplus nitrogen to containment and thus reduces accumulator pressure. To ensure that the volume of water in the accumulator can be controlled, system makeup and drain valves are also incorporated into the design.

The Category A safety function of the accumulators requires no supporting systems and they are Class 1 components. Their actuation requires only opening of check valves, which is discussed in Section 17.5.1.3.

The accumulator system does not support any other systems in their safety functions.

17.5.1.2 System Components and Equipment Contributing to Safety Function

The accumulator vessels themselves are discussed within the structural integrity section (Chapter 20). The associated pipework is designed to ASME Boiler and Pressure Vessel Code, Section III standards. The following components contribute to the accumulator system performing its safety function:

- **Accumulator Discharge Check Valves (PXS-PL-V028A/B and -V029A/B)** – These 200-mm DN (8-inch) swing check valves are required to remain closed when the RCS pressure is higher than the accumulator pressure and to open when the differential pressure across them is reversed. Being straightforward check valves, there is no requirement for any actuation signal, but the requirement to open when the differential pressure is reversed is a safety function.

- **Accumulator Discharge Isolation Valves (PXS-PL-V027A/B)** – These 200-mm DN (8-inch), motor-operated gate valves are required to close to enable controlled RCS pressure reduction to take place without accumulator injection, but are maintained open when the reactor is at power. The valves are not required to move as part of the accumulators achieving their safety function, but they must be open. The valve position will be checked during routine 12-hourly operational surveillances; whilst in this condition, the power supplies to the actuator will be isolated to prevent inadvertent operation. To support the achievement of the accumulator safety function, these administrative arrangements are backed up by the initiation of an open signal to these valves, from the PLS, whenever a safeguards actuation signal is generated. It is felt that these arrangements are sufficiently robust that further analysis is not required.

- **Accumulator Nitrogen Makeup/Vent Isolation Valves (PXS-PL-V021A/B)** – These 25-mm (1-inch) nominal-bore, solenoid-operated globe valves are set up to fail closed. The makeup isolation valve gives the ability to add nitrogen and increase accumulator pressure. The vent valve permits release of nitrogen to the containment atmosphere, and hence a reduction in accumulator pressure, to maintain its nominal set pressure. These operations will be performed in response to routine 12-hourly operational surveillance checks and the valves are not required to change state for the accumulator to perform its safety function.

- **Accumulator Fill/Drain Isolation Valves (PXS-PL-V232A/B)** – These 25-mm (1-inch) nominal-bore, air-operated globe valves are set up to fail closed. They provide the facility to fill or drain the accumulator to correct the level as required. These operations will be performed in response to routine 12-hourly operational surveillance checks and the valves are not required to change state for the accumulator to perform its safety function. Further analysis is therefore not required.

17.5.1.3 Claims on Components and Equipment

Accumulator Check Valves (PXS-PL-V028A/B and -V029A/B)

The accumulator system is provided to help mitigate the consequences of a LOCA. Maintenance of coolant inventory is a Category A safety function. See Appendix 15A. The check valves themselves are fundamental to the operation of the accumulators and failure to operate on demand would compromise the performance of the accumulator. The accumulators are a primary means of meeting the maintenance of RCS inventory is a Category A safety function, and therefore the check valves are Class 1 components. See Appendix 15A.

Both check valves on each accumulator are required to open for the accumulator to perform its safety function, because either one sticking closed would block the injection flow.

Whilst achievement of safety injection through the correct opening of the accumulator check valves is clearly the principal safety requirement, there is an implicit requirement that under normal operation, the accumulator check valves operate with minimal leakage from the RCS back into the accumulator itself. But unless this happens because of a gross failure, that is not considered credible, the changes in accumulator level that result from the leakage will be observed during the 12-hourly routine operational surveillance checks. Any in-leakage would also be detected by the resultant increase in accumulator pressure. The design ensures that in-leakage will result in a high nitrogen cover gas pressure alarm prior to exceeding the maximum permissible water level.

Accumulator Isolation Valves (PXS-PL-V027A/B)

The accumulator system is provided to help mitigate the consequences of a LOCA. Maintenance of coolant inventory is a Category A safety function. See Appendix 15A. The isolation valves themselves are fundamental to the operation of the accumulators and failure to operate on demand or spurious closure would compromise the performance of the accumulator. The accumulators are a primary means of meeting the maintenance of RCS inventory is a Category A safety function, and therefore the isolation valves are Class 1 components. See Appendix 15A.

The valves are not required to move as part of the accumulators achieving their safety function, but they must be open. The valve position will be checked during routine 12-hourly operational surveillances; whilst in this condition, the power supplies to the actuator will be isolated to prevent inadvertent operation.

Accumulator Nitrogen Makeup/Vent Isolation Valves (PXS-PL-V021A/B)

The accumulator system is provided to help mitigate the consequences of a LOCA. Maintenance of coolant inventory is a Category A safety function. See Appendix 15A. The isolation provided by the valves themselves are fundamental to the operation of the accumulators and the valves are not required to change state for the accumulator to perform its safety function. The accumulators are a primary means of maintaining the RCS inventory is a Category A safety function, and therefore the isolation valves are Class 1 components. See Appendix 15A.

The valves are not required to move as part of the accumulators achieving their safety function, but they must be closed. The valve position will be checked during routine 12-hourly operational surveillances; whilst in this condition.

Accumulator Fill/Drain Isolation Valves (PXS-PL-V232A/B)

The accumulator system is provided to help mitigate the consequences of a LOCA. Maintenance of coolant inventory is a Category A safety function. See Appendix 15A. The isolation provided by the valves themselves are fundamental to the operation of the accumulators and the valves are not required to change state for the accumulator to perform its safety function. The accumulators are a primary means of meeting the maintenance of RCS inventory is a Category A safety function, and therefore the isolation valves are Class 1 components. See Appendix 15A.

17.5.1.4 Justification of Claims on Components and Equipment

Accumulator Check Valves (PXS-PL-V028A/B and -V029A/B)

The operation of the accumulator check valves offers a high degree of inherent safety and reliability.

The valves are manufactured from stainless steel to ensure compatibility with the RCS chemistry conditions and are designed to ASME Boiler and Pressure Vessel Code, Section III-1.

The valves are very similar to those already in like service on many operating power stations. As a result, the information from testing these in-service valves offers a high degree of confidence about the reliability to be expected from these valves. Data collected for in-service plants (Reference 17.7, Table 5.1) indicate a probability of failure to open is an order of magnitude better than the value assumed in the PSA and indicates that the claims against these valves are conservative.

The operating mechanism for the valve is very simple and, aside from gross mechanical failure, some form of "sticking" might be considered the principal mechanism for valve failure. There are four reasons for believing this risk to be low, as listed below:

- Given that the valves are not normally called upon to operate, the moving parts do not experience significant wear.

- The materials of design have been specifically chosen to maximise compatibility with the RCS fluid, thus minimising the risk of chemical corrosion interfering with valve operation.

- The valves sit in a region where the RCS fluid is stagnant, this being true even under accident conditions until safety injection from the accumulators begins. As such, they will normally see constant temperatures, and temperatures can only change significantly once the valves have opened and therefore completed their safety function.

- Even if some small amount of "sticking" were to occur in the valve mechanism, the differential pressure across the valve that is generated during fault conditions is substantial. The force available to open the valve is directly proportional to differential pressure and will, therefore, be more than adequate.

The first three of the four reasons above help justify why the accumulator check valves are very unlikely to stick. The same reasoning also provides support for the implicit requirement that back-leakage through the accumulator check valves will be minimal. In addition, the presence of two valves in series provides a significant enhancement to the claim.

Testing of the accumulator check valves is precluded when the reactor is at power and, as a result, routine testing is all carried out during shutdowns. Two types of tests are proposed:

- A flow test of the accumulator performed with the RCS and accumulators at predetermined pressures and injection initiated by opening the motor-operated isolation valve. This should result in a full stroke of the check valve and, through the measurement of achieved flow rate tests, the degree of opening can be determined. Because of the disturbance to RCS operation, this test can only be performed when the

RCS is depressurised during refuelling (Mode 6) every 2 years. This test demonstrates ongoing capability to meet the full safety requirement.

- A partial-flow test makes use of test connections around the check valves and injection of small quantities for fluid to confirm that the valve does, in fact, begin to open at the correct pressure. During this test, it will not be possible to see significant check valve movement, so it cannot confirm full freedom of operation, but it does allow confirmation that the valve is not stuck on its seat. Because of the much smaller quantities of fluid involved, this test can be performed with the RCS intact in Mode 5. It is suggested that this test be performed approximately every 2 years.

Accumulator Isolation Valves (PXS-PL-V027A/B)

The low probability of spurious closure valves offers a high degree of inherent safety and reliability.

The valves are manufactured from stainless steel to ensure compatibility with the RCS chemistry conditions and are designed to ASME Boiler and Pressure Vessel Code, Section III-3.

The valves are very similar to those already in like service on many operating power stations. As a result, the information from testing these in-service valves offers a high degree of confidence about the reliability to be expected from these valves. Data collected for in-service plants (Reference 17.7, Table 5.1) indicate a probability of spurious closure value assumed in the PSA and indicates that the claims against these valves are conservative.

Accumulator Nitrogen Makeup/Vent Isolation Valves (PXS-PL-V021A/B)

The low probability of spurious actuation offers a high degree of inherent safety and reliability.

The valves are manufactured from stainless steel to ensure compatibility with the RCS chemistry conditions and are designed to ASME Boiler and Pressure Vessel Code, Section III-3.

The valves are very similar to those already in like service on many operating power stations. As a result, the information from testing these in-service valves offers a high degree of confidence about the reliability to be expected from these valves. Data collected for in-service plants (Reference 17.7, Table 5.1) indicate a probability of spurious actuation value assumed in the PSA and indicates that the claims against these valves are conservative.

Accumulator Fill/Drain Isolation Valves (PXS-PL-V232A/B)

The low probability of spurious actuation offers a high degree of inherent safety and reliability.

The valves are manufactured from stainless steel to ensure compatibility with the RCS chemistry conditions and are designed to ASME Boiler and Pressure Vessel Code, Section III-3.

The valves are very similar to those already in like service on many operating power stations. As a result, the information from testing these in-service valves offers a high degree of confidence about the reliability to be expected from these valves. Data collected for

in-service plants (Reference 17.7, Table 5.1) indicate a probability of spurious actuation value assumed in the PSA and indicates that the claims against these valves are conservative.

17.5.2 Core Makeup Tanks

17.5.2.1 Role

A detailed description of the core makeup tanks (CMTs) is given in Section 6.6. Further design details of this system and its constituent components are delineated in Reference 17.25.

The PXS CMTs have three primary safety functions: reactivity control, heat transfer/residual heat removal, and actuation of the ADS valves. They support the heat transfer/residual heat removal safety function by providing large quantities of coolant to maintain the reactor coolant inventory/reflood to the core following a LOCA. The reactivity control safety function is supported by the borated water in the CMTs. The positioning of the CMTs in relation to the rest of the primary circuit also allows for natural circulation to feed the contents of the CMTs into the primary circuit. This can take place with the RCS pressure at any value and thus provides the capability to borate the RCS and consequently reduce reactivity. Sensing a reduction in the CMT level provides information used to actuate the ADS valves.

The plant design makes provision for two independent CMTs, each connected to one of the two sets of direct vessel injection pipework to deliver coolant directly to the reactor vessel. The CMTs can operate in two different modes, depending on the RCS conditions. If the cold legs are filled with water, CMTs operate in a water recirculation mode with the driving force based on the density difference between the hot reactor coolant in the CMT balance line and the colder water in the CMT. The pressure balance line is well insulated and routed continuously upward from the top of the cold leg to a high point close to the top of the CMT. This arrangement ensures that the water in the line will remain hot, that aids natural circulation injection of the CMT water. This mode of operation can be relied upon to circulate the borated CMT water into the RCS and reduce reactivity.

If the cold legs become voided, as they do during LOCAs, the CMTs will operate in a steam-displacement injection or steam drain down mode. In this mode, the driving force is generated by the density difference between steam from the cold legs and water in the CMTs.

Each CMT is designed to work in tandem with the associated accumulator connected to the same direct vessel injection line. For small-break LOCAs, the CMTs are the initial source of safety injection, whilst for large-break LOCAs, they supplement safety injection when the accumulators have discharged. The CMTs are sized to ensure that the full safety function can be performed even if one of the direct vessel injection lines is the postulated break.

The positions of the CMT connections to the RCS mean that if the RCPs are running, the pressure difference is such that the CMT recirculation will be impeded if the discharge isolation valves are opened. The RCPs, therefore, are shut down to enable the CMT to function correctly.

At power, the CMTs remain filled with cool water in that a minimum boron concentration is maintained. Each CMT injection line contains two check valves in series. A portion of each injection line has parallel paths, each with a normally closed air-operated isolation valve to prevent reverse flow back into the CMT. For the system to operate one of the two air-operated isolation valves must open and the check valves must allow flow.

The CMTs are not supported by other safety systems in performing their safety function.

The CMTs do not support any other systems in the provision of their safety functions.

17.5.2.2 System Components and Equipment Contributing to Safety Function

The CMT vessels themselves are discussed in the structural integrity section (Chapter 20). The associated pipework and systems are constructed to ASME Boiler and Pressure Vessel Code, Section III-1. The following components contribute to the CMTs performing their safety function:

- **CMT Discharge Isolation Valves (PXS-PL-V014A/B and -V015A/B)** – These are 200-mm DN (8-inch), air-operated globe valves. The valves fail open on loss of air supply and are signalled to open on receipt of a safeguards signal. Each valve has its own solenoid-operated air valve that is driven from the PMS and de-energises to dump the air supply and open the valve. There is also a separate single solenoid-operated air valve, driven from the diverse actuation system (DAS) that is required to energise to dump the air supply and provides an alternate method to open all CMT outlet isolation valves. The CMT outlet isolation valve safety requirement is to enable the CMTs to inject to the RCS.

- **CMT Discharge Check Valves (PXS-PL-V016A/B and -V017A/B)** – These are 200-mm DN (8-inch), inline nozzle check valves. They are required to be normally open and remain open to facilitate injection from the CMT unless there is a reverse flow. This could happen when the accumulators are discharging into a depressurised RCS. Under these circumstances, the safety requirement is for the valve to isolate the line back to the CMT.

- **CMT Inlet Isolation Valve (PXS-PL-V002A/B)** – These are 200-mm DN (8-inch), motor-operated gate valves. They are required to be open for their respective CMTs to perform their safety function. With the reactor at power, they are left in their open position with the actuator power supplies isolated. This condition is then checked on a 12-hourly basis as part of the routine operational surveillances. They do, however, also receive a confirmatory open signal from the PMS. Further analysis is therefore not required.

- **CMT Fill Header Isolation Valves (PXS-PL-V230A/B)** – These are 25-mm DN (1-inch), air-operated globe valves set up to fail closed. They provide the facility to add and remove CMT fluid to ensure that the correct boron concentration is maintained. These operations will be performed in response to routine operational surveillance checks on boron concentration that are performed every 7 days. The valves are not required to change state for the CMT to perform its safety function. Further analysis is therefore not required.

17.5.2.3 Claims on Components and Equipment

CMT Discharge Isolation Valves (PXS-PL-V014A/B and -V015A/B)

The CMT outlet isolation valves open to provide makeup to the RCS in the event of a LOCA and control of core radioactivity. Maintenance of RCS inventory and control of reactivity is a Category A safety function. The CMTs are a primary method of maintaining RCS inventory under fault conditions and as such, these valves are Class 1. See Appendix 15A.

There are two CMT outlet isolation valves arranged in parallel for each CMT. At least one of the two valves is required to open to ensure that the safety function is performed.

CMT Discharge Check Valves (PXS-PL-V016A/B and -V017A/B)

The CMT discharge check valves are provided to ensure that during the injection phase from the accumulators, all fluid is discharged through the direct vessel injection piping and none can find a route through the CMTs. This safety function is associated with maintenance of RCS inventory and control of core reactivity is a Category A safety function. These valves are the primary means of ensuring that injection from the accumulators is properly injected and therefore maintaining RCS inventory. As such, the CMT discharge check valves are Class 1. See Appendix 15A.

There are two CMT discharge check valves in series for each CMT, either one of the two closing will achieve the safety function.

The probability of having the check valves closed and not detected is essentially the same as the probability of the check valves failing to remain open on demand.

Whilst the prevention of incorrect routing of accumulator safety injection flow is the primary safety requirement, there is an implicit requirement that the valves remain open and do not impede any safety injection flow from the CMTs into the RCS when this is required.

CMT Inlet Isolation Valve (PXS-PL-V002A/B)

They are required to be open for their respective CMTs to perform their safety function. With the reactor at power, they are left in their open. This safety function is associated with maintenance of RCS inventory and control of core reactivity is a Category A safety function. As such, the CMT discharge check valves are Class 1. See Appendix 15A.

CMT Fill Header Isolation Valves (PXS-PL-V230A/B)

They are required to be closed for their respective CMTs to perform their safety function. With the reactor at power, they are left in the closed. This safety function is associated with maintaining the integrity of the integrity of RCS which is a Category A safety function. As such, the CMT discharge check valves are Class 1. See Appendix 15A.

17.5.2.4 Justification of Claims on Components and Equipment

CMT Discharge Isolation Valves (PXS-PL-V014A/B and -V015A/B)

The CMT outlet isolation valves are air operated with the actuators designed to fail open in the event of loss of air supply. This is an inherently safe mechanism, meaning that only in the event of a valve sticking will there be a failure to a condition other than safe.

The valves are manufactured from stainless steel to ensure compatibility with the borated RCS fluid that is in contact with them. They are designed to ASME Boiler and Pressure Vessel Code, Section III-1.

The valves are very similar to those already in like service on many operating power stations. As a result, the information from testing these in-service valves offers a high degree of confidence about the reliability to be expected from these valves. Data collected from in-service plants (Reference 17.7, Table 5.1) indicate a probability of a failure to open that is comparable to the value being claimed.

The failure mechanism of concern would involve a valve sticking or jamming. This could be a result of wear, corrosion, or maintenance-induced failure. In addition to being designed to ASME Boiler and Pressure Vessel Code, Section III, the valves are also designed and installed to seismic C-I and are qualified for operation in a harsh environment.

The maintenance and testing arrangements for the CMT outlet isolation valves are based on the ASME Boiler and Pressure Vessel Code programmes appropriate for these types of valves as used in existing nuclear power stations. The testing is:

- A full stroke operability test is performed quarterly in accordance with ASME Boiler and Pressure Vessel Code.
- Visual confirmation of valve operation during the stroke testing is performed every 2 years.
- A system flow test is performed every 10 years and will confirm valve operating performance.

CMT Discharge Check Valves (PXS-PL-V016A/B and -V017A/B)

The operation of the CMT discharge check valves depends only upon the pressure difference across them and not on any method of powered actuation. This passive approach offers a high degree of inherent safety and reliability.

The valves are manufactured from stainless steel to ensure compatibility with the borated RCS fluid that is in contact with them. They are designed to ASME Boiler and Pressure Vessel Code, Section III-1.

The design of this valve has seen some, although not extensive, previous service in nuclear applications. As a result of the limited operating experience in nuclear applications, there is little service data to support the PSA claims. There are, however, a number of reasons to support the claim that they will be highly reliable in service:

- The valve design exhibits a very low pressure drop, and so offers minimum impediment to the establishment of flow from the CMT through natural circulation.
- The valve provides a very rapid response to closure with reverse flow. This minimises the reverse flow velocities seen and consequent water hammer when the valve closes.
- The valve is easy to design so that it sits in the fully open position when there is no flow. This means that there is no requirement for it to open during small LOCAs when the CMT makeup provides the first stage of safety injection.
- In normal operation, there is no flow through the valve and so there will be no wear of moving parts.
- Because there is no flow, the fluid sitting in the valve does not change and so there is no credible opportunity for boric acid to precipitate out and accumulate. This minimises the risk of seizure.
- Any movement of the valves takes place with the valve still containing fluid at ambient containment conditions. The valve only sees large changes in temperature when it has

moved to its fully open position and flow has been established. At this point, the safety requirement is that it remains open so any seizure would not be a safety issue.

Full-stroke checks of the CMT discharge check valves are precluded when the reactor is at power because significant flow is required to force the valves to the closed position, and it is felt that this might generate unacceptable transients. The testing is therefore treated as an exemption to the normal ASME Boiler and Pressure Vessel Code rules. The testing is:

- Verification, from the valve position indication, that the valve is open will be performed quarterly.

- Full valve exercising will be performed during refuelling outages when the RCS boron concentration is much closer to that of the CMTs, and also when the Tech Specs do not require the CMTs to be operable.

- A system flow test is performed every 10 years and will confirm valve operating performance.

CMT Inlet Isolation Valve (PXS-PL-V002A/B)

The low probability of spurious closure valves offers a high degree of inherent safety and reliability.

The valves are manufactured from stainless steel to ensure compatibility with the RCS chemistry conditions and are designed to ASME Boiler and Pressure Vessel Code, Section III-1.

The valves are very similar to those already in like service on many operating power stations. As a result, the information from testing these in-service valves offers a high degree of confidence about the reliability to be expected from these valves. Data collected for in-service plants (Reference 17.7, Table 5.1) indicate a probability of spurious closure value assumed in the PSA and indicates that the claims against these valves are conservative.

CMT Fill Header Isolation Valves (PXS-PL-V230A/B)

The low probability of spurious closure valves offers a high degree of inherent safety and reliability.

The valves are manufactured from stainless steel to ensure compatibility with the RCS chemistry conditions and are designed to ASME Boiler and Pressure Vessel Code, Section III-2.

The valves are very similar to those already in like service on many operating power stations. As a result, the information from testing these in-service valves offers a high degree of confidence about the reliability to be expected from these valves. Data collected for in-service plants (Reference 17.7, Table 5.1) indicate a probability of spurious opening value assumed in the PSA and indicates that the claims against these valves are conservative.

17.5.3 Automatic Depressurisation System

17.5.3.1 Role

A detailed description of the automatic depressurisation system (ADS), which is part of the RCS, is given in Section 6.4. Further design details of this system and its constituent components are delineated in Reference 17.1.

The ADS, in addition to its RCS pressure boundary function, contributes to the provision of the heat transfer/residual heat removal primary safety function by providing the means to carry out a controlled depressurisation of the RCS to allow the passive core cooling system to function and deliver the required quantities of water to refill the reactor vessel.

The plant design makes provision for four stages of depressurisation. The stages of the ADS operate sequentially to depressurise the RCS so that safety injection takes place as required by the plant design. Specifically, the reactor coolant system will depressurize to the pressure at which the accumulators begin to deliver core cooling flow, and eventually the reactor coolant system is depressurised to the in-containment refuelling water storage tank (IRWST) pressure. Each ADS Stage 1, 2, and 3 has two sets of depressurisation valves. ADS Stage 1 valves open when an ADS signal is generated on CMT low level. ADS Stage 2 and 3 valves are given the signal to open in line with a timed sequence following the initiation of the ADS signal (ADS stage 1 opening). ADS Stages 1, 2, and 3 discharge through spargers to the IRWST. ADS Stage 4 has four depressurisation valves which open sequentially with Stages 1, 2, 3 or on a CMT low-low level signal. The ADS Stage 4 piping connects directly to each RCS hot leg and discharges directly into their respective loop compartment.

The ADS is supported by the essential electrical system in performing its safety function.

The ADS does not support any other systems in performing their safety functions.

17.5.3.2 System Components and Equipment Contributing to Safety Function

The following components contribute to the ADS performing its safety function:

- **ADS Stage 1 Control Valves (RCS-PL-V001A/B)** – These are 100-mm (4-inch) nominal-bore, slow–opening, motor-operated globe valves. The valves fail “as is” upon loss of power supplies and are signalled to open by the stage 1 ADS signal. The auto-initiation of this function is derived from the PMS using CMT level transmitters. Manual actuation is available via both the PMS and DAS. The stage 1 valves are connected to the pressuriser via isolation valves and discharge via a sparger to the IRWST. The valves are closed during normal operation. The safety requirement is for them to open to provide a flow path on demand.

- **ADS Stage 2 Control Valves (RCS-PL-V002A/B)** – These are 200-mm DN (8-inch), slow-opening, motor-operated globe valves. The valves fail “as is” upon loss of power supplies and are signalled to open by the stage 1 ADS signal following a time delay. The auto-initiation of this function is derived from the PMS. Manual actuation is available via both the PMS and DAS. The stage 2 valves are connected to the pressuriser via isolation valves and discharge via a sparger to the IRWST. The valves are closed during normal operation. The safety requirement is for them to open to provide a flow path on demand.

- **ADS Stage 3 Control Valves (RCS-PL-V003A/B)** – These are 200-mm DN (8-inch), slow-opening, motor-operated globe valves. The valves fail "as is" upon loss of power supplies and are signalled to open by the stage 1 ADS signal following a further time delay beyond stage 2. The auto-initiation of this function is derived from the PMS. Manual actuation is available via both the PMS and DAS. The stage 3 valves are connected to the pressuriser via isolation valves and discharge via a sparger to the IRWST. The valves are closed during normal operation. The safety requirement is for them to open to provide a flow path on demand.

- **ADS Stage 4 Control Valves (RCS-PL-V004A/B/C/D)** – These are 350-mm DN (14-inch), squib-type valves. The valves are opened by actuating a propellant charge that requires an electrical firing signal and once opened, there is no mechanism for closure. The valves can therefore be considered to fail "as is" in either open or closed positions. The firing signal is generated from the stage 4-ADS signal. The auto-initiation of this function is derived from the PMS. Manual actuation is available via both the PMS and DAS. The stage 4 valves are connected to the RCS hot leg via normally open isolation valves and discharge directly into the containment loop compartments. The safety requirement is for them to open to provide a flow path on demand.

- **ADS Stage 1 Isolation Valves (RCS-PL-V011A/B)** – These are 100-mm DN (4-inch) nominal-bore, motor-operated, flex wedge gate valves. The valves fail "as is" upon loss of power supplies and are signalled to open by the PMS prior to the opening of the stage 1 ADS control valves. The valves are closed during normal operation. The safety requirement is for them to provide reliable isolation but also open to provide a flow path on demand.

- **ADS Stages 2 and 3 Isolation Valves (RCS-PL-V012A/B and -V013A/B)** – These are 200-mm DN (8-inch) , motor-operated, flex wedge gate valves. The valves fail "as is" upon loss of power supplies and are signalled to open by the PMS prior to the opening of their respective ADS control valves. The valves are closed during normal operation. The safety requirement is for them to provide reliable isolation but also open to provide a flow path on demand.

- **ADS Stage 4 Isolation Valves (RCS-PL-V014A/B/C/D)** – These are 350-mm DN (14-inch), motor-operated, wedge gate valves. The valves fail "as is" upon loss of power supplies and are open during normal operation. The safety requirement is for them to be open so that a flow path is provided when ADS 4 is demanded.

17.5.3.3 Claims on Components and Equipment

ADS Stage 1 Control Valves (RCS-PL-V001A/B)

The ADS stage 1 control valves provide the initial depressurisation capability in response to a loss of coolant from the RCS which results in a decrease in CMT level to the ADS actuation setpoint. This RCS pressure reduction is in preparation for the opening of the larger ADS stages 2, 3, and 4 valves, all of which serve to enable continued injection by gravity from the CMTs, accumulators and the IRWST. Maintenance of RCS inventory is a Category A safety function. The valves are a principal means of achieving the function and are therefore Class 1. See Appendix 15A. There are two parallel sets of two series ADS stage 1 valves. Following a LOCA, they are claimed to receive their open signal at a set time after a CMT low-level setpoint is reached. During this period, controlled by a programmed time delay, the stage 1 isolation valves are expected to reach their full open position. The ADS stage 1

control valves are expected to open against the full differential pressure from the RCS to the IRWST.

The ADS stage 1 valves are also designed to provide the operator with the facility to manually depressurise the RCS in response to events such as SGTR where the natural depressurisation rate of the RCS is small, but the leak rate from the RCS to the faulted SG secondary side can be terminated by reducing the RCS pressure. The ADS stage 1 control valves are therefore claimed to have a throttling duty in addition to traversing to fully open in response to the automatic ADS signal. If the operator takes no action following an SGTR, the PXS will be actuated and the operation of the CMTs and PRHR HX will result in a decrease in RCS pressure and the RCS pressure will equalise with the SG pressure. This automatically will terminate the RCS to SG break flow without actuation of the ADS stage 1 valve.

ADS Stage 2 Control Valves (RCS-PL-V002A/B)

The ADS stage 2 control valves provide the second stage of blowdown to support RCS depressurisation. As with the stage 1 valves, this is in support of maintenance of RCS inventory and hence is in support of a Category A safety function. The stage 2 valves are also, as part of the depressurisation sequence, a primary contributor to this function and are therefore Class 1. See Appendix 15A.

There are two parallel sets of ADS stage 2 valves. They receive their open signal a set time after the stage 1 control valves receive their open signal that is longer than the time to open stage 1 valves. These ADS stage 2 control valves are sequenced to open after their associated ADS isolation valves reach their full open position and are expected to do so against the full differential pressure from the RCS to the IRWST.

ADS Stage 3 Control Valves (RCS-PL-V003A/B)

The ADS stage 3 control valves provide the third stage of blowdown to support RCS depressurisation. As with the stage 1 and 2 valves, this is in support of maintenance of RCS inventory and hence is in support of a Category A safety function. The stage 3 valves are also, as part of the depressurisation sequence, a primary contributor to this function and are therefore Class 1. See Appendix 15A.

There are two parallel sets of ADS stage 3 valves. They receive their open signal at a set time after the stage 2 control valves actuate.

ADS Stage 4 Control Valves (RCS-PL-V004A/B/C/D)

The ADS stage 4 control valves provide the final stage of RCS depressurisation. As with the other ADS valves, this is in support of maintenance of RCS inventory and hence is in support of a Category A safety function. The stage 4 valves are also, as part of the depressurisation sequence, a primary contributor to this function and are therefore Class 1. See Appendix 15A.

There are four ADS stage 4 control valves arranged in parallel with two attached to each hot leg. Three stage 4 valves opening will provide the safety function, as discussed in the Squib Valve Safety Case (Reference 17.36). They receive their open signals in a staggered sequence. One stage 4 control valve connected to each hot leg receives its open signal upon the later of the following conditions: a) a set time after the stage 3 control valves receive their open signal, or b) signal receipt from the CMT lowest-level setpoint (CMT level at approximately 20 percent). The second set of stage 4 control valves receives its open signal at a set time after the first set. The valves are claimed to reduce the RCS pressure to allow

gravity injection from the IRWST to take place and subsequently containment recirculation to be established.

As discussed in the Squib Valve Summary Report (Reference 17.2), the AP1000 design includes squib valves because of their high reliability and suitability to a function where there is a one-time need for the valve to actuate. This reputation is supported by the use of squib valves in many designs where the valve cannot fail to perform its function. Examples of these designs include boiling water reactor safety systems, weapons systems, and space systems. The squib valve design is simple and there are few ways for the valve to fail to actuate. This type of design contrasts with the designs of air-operated or motor-operated valves, which have more moving parts that can fail and prevent the valve from actuating.

The advanced light water reactor (ALWR) Utility Requirements Document (URD) indicates a low failure probability (failure to operate) for squib valves. This failure rate does not indicate a valve design with extremely high reliability, as would be expected. This may be because the basis for the URD value is a small population of valves and extrapolation from older, less relevant data.

Section 17.5.3.4 provides the additional details on the design and function of the ADS stage 4 squib valves. Chapter 6 provides discussion on the RCS which contains the ADS valves and references the system specification documents. Table 8A-2 presents faults that credit ADS stage 4 actuation for mitigation of the initiating events; associated fault analyses are referenced, with all design basis analyses presented in Chapter 9. The plant PSA (Chapter 10) includes consideration of the valves to actuation upon demand, as well as the consequences associated with spurious operation. The valve resilience to applicable internal hazards is discussed in Chapter 11. Additional detail on the interfacing C&I systems (PMS and DAS) is provided in Chapter 19, with the spurious operation blocker devise being discussed in Section 19.4.1.2.13. The electrical systems that provide power for actuation are discussed in Chapter 18.

ADS Stage 1, 2, and 3 Isolation Valves (RCS-PL-V011A/B, -V012A/B -V013A/B)

The upstream valve in each ADS path is designated as an ADS isolation valve. The functional requirements for these valves specify each to be leak tight to prevent operational and safety complications arising from an RCS pressure boundary leak. Each ADS stage 1, 2, and 3 isolation valve opens ahead of its corresponding control valve to support RCS depressurisation. As with the other ADS valves, support of the maintenance of RCS inventory is a Category A function. The isolation valves have a primary role in this and hence are Class 1. See Appendix 15A.

Following ADS stage 1, 2, and 3 system-level actuation, these normally closed isolation valves are sequenced to reach their full open position prior to their corresponding control valves receiving their open signals. The failure of an isolation valve to open yields the same results as a failure of its corresponding control valve to open. Although the valves are designed to open against differential pressures up to the maximum RCS operating pressure at blowdown conditions, their design-basis safety requirement is to open with no flow and high differential pressure. When the ADS is then demanded to operate, these valves are required to open and this forms an additional safety claim.

ADS Stage 4 Isolation Valves (RCS-PL-V014A/B/C/D)

Given the high confidence in the leak tightness of the squib valves used on ADS stage 4, it is not necessary to have the stage 4 isolation valves normally closed as is required for the other stages of ADS. Because of this, the stage 4 isolation valves are normally open and are not

required to change state at any time during the ADS sequence. The valves exist to provide an isolation facility to permit maintenance of the ADS stage 4 valves and also can be used to terminate stage 4 ADS operation at the commencement of recovery operations. There is therefore no safety requirement against these valves themselves except to serve as a RCS pressure boundary; however, because the stage 4 isolation valves are situated in the stage 4 ADS blowdown path, there is a requirement that the valves can be confirmed open, so there is a safety requirement against their position indication. As with the other ADS valves, support of the maintenance of RCS inventory is a Category A function. The isolation valves have a primary role in this and hence are Class 1. See Appendix 15A.

17.5.3.4 Claims on Components and Equipment

ADS Stage 1, 2 and 3 Control Valves (RCS-PL-V001A/B, -V002A/V, -V003A/B)

The ADS stage 1, 2, and 3 control valves are all motor operated globe valves, which means they will inherently fail “as is”. To understand why this is appropriate, it is instructive to consider the implications of other failure modes.

If the valves were designed to fail open, then if this happened during normal operation, it would constitute initiation of a substantial LOCA and therefore would not be appropriate. If this happened during the phase of a blowdown sequence when the valves were controlling, it would increase the blowdown rate sharply and potentially invalidate the assumptions used to justify maintenance of adequate coverage of the core; consequently, this would not be appropriate. If the valves failed open following completion of the blowdown sequence, they effectively would fail “as is”.

If the valves were designed to fail closed, then if this happened during normal operation, they would effectively fail “as is”. If this happened during the phase of a blowdown sequence when the valves were controlling, it would decrease the blowdown rate sharply and hence could delay either the introduction or the rate of safety injection that would not be appropriate. If the valves failed closed following completion of the blowdown sequence, it might complicate the plant recovery procedures or lead to stage 4 ADS initiation, even though the plant operators had stabilised the plant after stage 3. This would also be inappropriate.

In addition, the ADS isolation valves can be used to close the flowpath in the event of an ADS control valve failing “as is” in an open condition. On the basis of these arguments, the selection of valves that fail “as is” is considered appropriate.

Globe valves are used for the stage 1, 2, 3 control function because they are better suited to handle the high flow / differential pressure conditions that occur during ADS flow initiation. They are also better suited to handle the gradual flow initiation requirement.

The stage 1, 2, 3 isolation valves use gate valve bodies because they are better suited to providing leak tight service that the globe valve used for the control function.

Both the isolation and control valves on all three stages of ADS are manufactured from stainless steel to ensure compatibility with the reactor coolant water that passes through them. They are designed to ASME Boiler and Pressure Vessel Code, Section III-1. The valves are very similar to those already in like service on many operating power stations. As a result, the information from testing these in-service valves offers a high degree of confidence about the reliability to be expected from these valves. Data collected from in-service plants (Reference 17.7, Table 5.1) indicate a probability of a failure to open that is comparable to the value being claimed.

The failure mechanism of concern would involve the valves sticking or jamming. This could be a result of wear, corrosion, or maintenance-induced failure. In addition to being designed to ASME Boiler and Pressure Vessel Code, Section III, the valves are also designed and installed to seismic C-I and are qualified for operation in a harsh environment (17.1, Table 2.1.2-1).

The requirement of these valves is not to provide the primary isolation from the RCS under normal operating conditions, but to provide the controlled blowdown under fault scenarios. This control function is felt to be met best through the use of globe valves. There are two limiting failures with respect to the ADS. The limiting valve failure is for one ADS stage 4 control valve (V004A, B, C, or D) to fail to open. The limiting electrical failure would cause pairs of stage 1 and 3 control and isolation valves to fail to open (while the other pairs of stage 1 and 3 valves functioned as designed). Safety analyses show the depressurisation function to be met given either failure (Table 9.0-11).

The maintenance and testing arrangements for the ADS stage 1, 2, and 3 valves comply with ASME Boiler and Pressure Vessel Code and are based on the programmes appropriate for these types of valves as used in existing nuclear power stations. The testing is:

- Exercise full stroke at cold shutdown frequency. These tests are not intended to be conducted at power due to risk of inadvertent ADS operation. They are intended to be performed during shutdown conditions with no flow and no differential pressure across the valve. These ADS valves are tested during cold shutdowns when the RCS pressure is reduced to atmospheric pressure so that mispositioning of a single valve during this in-service testing (IST) will not cause a LOCA. Testing these valves at every cold shutdown is consistent with the AP1000 PSA.

- Operability testing will be performed with the reactor shut down. Each valve will be tested through its full range. Because the RCS is depressurised when this is performed, there is no significant flow and no differential pressure. The test frequency is the longer of every three refuelling cycles or 5 years, until sufficient data exist to determine if a longer test frequency is appropriate. The maximum test interval will be once every 10 years provided there is sufficient experience to justify this longer interval.

- Local observation of valve position will be performed during stroke tests at a 2-year frequency to confirm that the remote position indication is operating correctly.

ADS Stage 4 Control Valves (RCS-PL-V004A/B/C/D)

The ADS stage 4 control valves are all squib-type valves, which means they will inherently fail “as is”. Clearly, this is not fail-safe with respect to the automatic depressurisation function, but given that spurious actuation of this function when not required could, in itself, create a substantial transient, effectively a large-break LOCA, it is judged appropriate.

The valves are manufactured from stainless steel to ensure compatibility with the reactor coolant water. They are designed to ASME Boiler and Pressure Vessel Code, Section III-1.

The design of squib valves is such that the firing of a propellant charge is used to build gas pressure above a piston. At a prescribed pressure, a tension bolt fractures, releasing the piston; the piston travels down and impacts the end of the shear cap, shearing off the end. There is a very high level of confidence that the propellant charge and the subsequent actions will happen successfully and the valve will open correctly. The arguments and evidence that the squib valves are designed adequately to reliably perform their necessary safety fuction are provided in the Squib Valve Safety Case (Reference 17.36). The valve reliability depends

heavily on the firing reliability of the propellant charge. This reliability is enhanced by providing each stage 4 squib valve with two PMS igniters actuated from separate Class 1 Divisions. Each squib valve also has a DAS igniter. Actuation of any one of these three igniters will open the valve. As a consequence, the squib valve is believed to be highly reliable. Valve reliability is discussed further in the squib valve summary report (Reference 17.2).

The presence of four valves gives redundancy and, with the design being significantly different from the valves used in ADS stages 1, 2, and 3, provides diversity within the ADS.

The maintenance and testing arrangements for the ADS stage 4 valves comply with ASME Boiler and Pressure Vessel Code and are based on the programmes appropriate for these types of valves as used in existing nuclear power stations. The testing (Reference 17.2) is:

- Given that correct firing of the propellant charges is the primary concern for squib valve reliability, 20 percent of the charges installed on the plant will be replaced and fired every 2 years. These tests will be performed in a test fixture away from the valve, and the positions they occupied in valves on the plant will be taken by replacement charges.

ADS Stage 1, 2, and 3 Isolation Valves (RCS-PL-V011A/B, -V012A/B -V013A/B)

All isolation valves on ADS stages 1, 2, and 3 are motor operated, which means they will inherently fail “as is”. Clearly, this is not fail-safe with respect to the blowdown isolation function, but given that spurious actuation of this function when not required could, in itself, give rise to safety concerns, effectively a significant LOCA, failure “as is” is judged appropriate.

The valves are manufactured from stainless steel to ensure compatibility with the reactor coolant water that passes through them. They are designed to ASME Boiler and Pressure Vessel Code, Section III-1.

The valves are very similar to those already in like service on many operating power stations. As a result, the information from testing these in-service valves offers a high degree of confidence about the reliability to be expected from these valves. Data collected from in-service plants (Reference 17.7, Table 5.1) indicate a probability of a failure to open that is comparable to the value being claimed.

The failure mechanism of concern would involve the valves sticking or jamming. This could be a result of wear, corrosion, or maintenance-induced failure. In addition to being designed to ASME Boiler and Pressure Vessel Code, Section III, the valves are also designed and installed to seismic C-I and are qualified for operation in a harsh environment.

The requirement of these valves is to provide the primary isolation from the RCS under normal operating conditions, not to provide the controlled blowdown under fault scenarios. This isolation function is considered to be met best through the use of gate valves. Each stage of ADS has redundant valves and there is also redundancy between stages. When considering the ADS valves in series with the associated isolation valves, no single failure would prevent the isolation of the ADS stages nor the minimum required flowpaths. The limiting electrical failure would cause pairs of stage 1 and 3 control and isolation valves to fail to open (while the other pairs of stage 1 and 3 valves functioned as designed). Safety analyses show the depressurisation function to be met given either failure (Chapter 9).

The maintenance and testing arrangements for the ADS stage 1, 2, and 3 isolation valves comply with the ASME Boiler and Pressure Vessel Code and are based on the programmes appropriate for these types of valves as used in existing nuclear power stations. The testing is:

- Exercise full stroke at cold shutdown frequency. These tests may be conducted at power but are intended to be performed with no flow and no differential pressure across the valve. These ADS valves are tested during cold shutdowns when the RCS pressure is reduced to atmospheric pressure so that mispositioning of a single valve during this IST will not cause a LOCA. Testing these valves at every cold shutdown is consistent with the AP1000 design PSA.

- Operability testing will be performed with the reactor shut down, and each valve will be tested through its full range. Because the RCS is depressurised when this is performed, there is no significant flow and no differential pressure. The test frequency is the longer of every three refuelling cycles or 5 years until sufficient data exist to determine if a longer test frequency is appropriate. The maximum test interval is once every 10 years provided there is sufficient experience to justify this longer interval.

- Local observation of valve position will be performed during stroke tests at a two-year frequency to confirm that the remote position indication is operating correctly.

ADS Stage 4 Isolation Valves (RCS-PL-V014A/B/C/D)

All four isolation valves on ADS stages 4 are motor operated, which means they will inherently fail "as is". Given that the valves are normally open and have no safety requirement on any change of state, this arrangement is inherently safe.

As indicated above, it is the position indication equipment on this valve that carries the safety requirement. The testing performed on the valve is important for the demonstration of the correct operation of this equipment.

The maintenance and testing arrangements for the ADS stage 4 isolation valves comply with the ASME Boiler and Pressure Vessel Code and are based on the programmes appropriate for these types of valves as used in existing nuclear power stations. The testing is:

- Local observation of valve position will be performed during stroke tests to confirm that the remote position indication is operating correctly.

- A check will be made every 12 hours, as a part of routine operational Tech Spec surveillances, to ensure that the valves are open.

17.5.4 In-Containment Refuelling Water Storage Tank

17.5.4.1 Role

A detailed description of the IRWST (PXS-MT-03) is given in Section 6.6. Further design details of this system and its constituent components are delineated in Reference 17.25.

In normal operation, the PXS IRWST provides borated water to flood up the refuelling cavity when the reactor vessel head is removed for refuelling. During faults, however, it contributes to the heat transfer/residual heat removal and reactivity control primary safety functions.

The contribution of the IRWST to the heat transfer/residual heat removal primary safety function is summarised below:

- Forms the initial heat sink when the PRHR system is actuated. The PRHR HX is situated in the IRWST and transfers heat from the RCS by natural circulation.

- Is the final source of water for injection into the RCS when the RCS has been almost fully depressurised. The IRWST injection isolation valves allow the flow of water from the IRWST into the direct vessel injection lines of the reactor vessel.

- Is the major source of water used to flood the containment and provide the long term source of core cooling through natural circulation into the reactor vessel.

- Accepts steam released from ADS stages 1, 2, and 3 and condenses it with the aid of the depressurisation spargers pipework inside the tank.

- Is the source of water for the defence in depth safety function performed by the normal residual heat removal system (RNS) pumps for low-pressure safety injection.

- Collects water condensed on the inside of the containment shell by operation of the passive containment cooling system (PCS) and the PXS gutter for use as PXS low pressure safety injection.

The IRWST consists of the tank itself, vents to ensure that the tank pressure remains in equilibrium with the containment atmosphere, over flow paths to prevent overfilling the tank, the ADS spargers and lines, and screens that filter out debris during the final stage of safety injection.

The IRWST components are entirely passive in nature and are not supported by other systems.

The IRWST provides support to the PRHR HX and the ADS; and for the RNS when performing its defence in depth safety injection function.

17.5.4.2 System Components and Equipment Contributing to Safety Function

The IRWST is constructed as part of the in-containment structures (Section 6.6). The following components contribute to it fulfilling its safety function:

- **Storage Tank (PXS-MT-03)** – This large, stainless-steel-lined, concrete and steel tank in containment is required to contain borated water. The tank is vented to the containment atmosphere and so there are no pressure retention claims on it. It is constructed as a part of the in-containment structure at a level sufficiently elevated above the RCS to ensure that it can drain by gravity to provide the final stage of safety injection. The safety requirement is to provide the assumed heat sink capability and the assumed safety injection capability.

- **IRWST Vents** – These are an arrangement of vents installed in the roof of the storage tank around its periphery. There are several types of vents that prevent the tank from becoming pressurised from either internal or external pressurisation sources. They provide a sufficient combined release area. They are normally closed to prevent debris from falling into the tank and also to contain water vapour and radioactive gases during normal operation (Section 6.6). The vents are opened by the generation of a slight

positive pressure inside the tank with respect to the containment atmosphere. There are also vents that are opened by the generation of slight positive pressure in containment with respect to the IRWST. The safety requirement is to ensure that significant over pressure or negative pressure compared to the containment pressure does not develop in the IRWST that exceeds the IRWST design pressure.

- **IRWST Overflows –** These are an arrangement of openings at the top of the IRWST vertical wall adjacent to the refuelling cavity. The openings have hinged covers which are opened by the generation of a slight positive pressure inside the tank. These overflows operate to prevent overfilling of the IRWST and ensure that sufficient space is maintained above the IRWST water level. The overflows can also act as additional vent area to prevent IRWST overpressure.

- **Spargers (PXS-MW-01A/B)** – These are two, four-armed, cruciform-type, stainless-steel spargers with outlet holes (Section 6.6). They sit in the IRWST. The spargers receive steam and water discharged through the first three stages of automatic depressurisation and distribute the ADS discharge into the IRWST water. The spargers enable the ADS steam to be condensed to minimise any immediate effects of ADS on the containment environment. The safety requirement is that the ADS discharge does not result in large hydro-dynamic loading on the IRWST structure

- **Screens (PXS-MY-Y01A/B/C)** – These pocket-type screens use a perforated sheet as the filter medium. They are situated at the base of the tank and ensure that injection from the IRWST into the RCS can take place without the accumulation of debris in the reactor vessel, since such debris may inhibit core cooling.

- **IRWST Injection Squib Valves (PXS-PL-V123A/B and -V125A/B)** – These are 200-mm DN (8-inch), squib-type valves. They effectively fail "as is" on loss of control supplies and are signalled to open on receipt of a stage 4 ADS signal from the PMS. The safety requirement is that the valves will enable direct injection from the IRWST into the RCS, as discussed in the Squib Valve Safety Case (Reference 17.36). These squib valves are similar to the containment recirculation isolation valves discussed in Section 17.5.5.2. However, there are a number of design features that create diversity between the two sets of valves as described in Reference 17.2.

  Section 17.5.4.3 provides the additional details on the design and function of the IRWST injection squib valves. Chapter 6 provides discussion on the PXS which contains the IRWST injection valves and references the system specification documents. Table 8A-2 presents faults that credit IRWST injection actuation for mitigation of the initiating events; associated fault analyses are referenced, with all design basis analyses presented in Chapter 9. The plant PSA (Chapter 10) includes consideration of the valves to actuation upon demand, as well as the consequences associated with spurious operation. The valve resilience to applicable internal hazards is discussed in Chapter 11. Additional detail on the interfacing C&I systems (PMS and DAS) is provided in Chapter 19, with the spurious operation blocker devise being discussed in Section 19.4.1.2.13. The electrical systems which provide power for actuation are discussed in Chapter 18.

- **IRWST Injection Line Isolation Valves (PXS-PL-V121A/B)** – These are 200-mm DN (8-inch), motor-operated gate valves. They are designed to fail "as is" on loss of electrical supplies. They are normally open and are only required to be closed to allow maintenance on the IRWST injection isolation valves. The valves are not required to move as part of the IRWST achieving its safety function, but they must be open. The valve position will be checked during routine 12-hourly operation surveillances and

whilst in this condition, the power supplies will be isolated to prevent inadvertent operation. To support the achievement of the IRWST safety function, these administrative arrangements are backed up by the initiation of an open signal from the PLS when a safeguards actuation signal is generated. It is felt that these arrangements are sufficiently robust so that further analysis is not required.

- **IRWST Injection Line Check Valves (PXS-PL-V122A/B and -V124A/B)** – These are 200-mm (8-inch) nominal-bore, swing-check valves. These valves exist to prevent reverse flow if the IRWST opens during a LOCA sequence with the RCS pressure slightly above the IRWST pressure or in the event of an inadvertent actuation of the associated IRWST injection isolation valve. Their safety function is to open on demand to enable direct injection from the IRWST into the RCS.

17.5.4.3 Claims on Components and Equipment

Storage Tank (PXS-MT-03)

The IRWST provides the source of water to enable the final stage of safety injection to take place (prior to containment recirculation injection), provides the heat sink for the PRHR, and quenches the ADS discharge flow. Maintenance of RCS coolant inventory and removal of decay heat are both Category A safety functions. The IRWST storage tank is integral to the PXS designed as the principal methods of providing this safety function and therefore is Class 1. See Appendix 15A.

The requirement is that the tank will provide sufficient water to complete containment sump floodup to a high enough level to initiate containment recirculation flow.

IRWST Vents and Overflows

The vents and overflows on the IRWST ensure that its integrity is not compromised through inadvertent internal or external pressurisation. This supports the maintenance of equipment performing a Category A safety function and so is also in itself a Category A safety function. The vents and overflows are the principal means of ensuring that the internal and external design pressures of the IRWST with respect to the containment atmosphere cannot be exceeded, and therefore are Class 1. See Appendix 15A.

The requirement is that the vents will open when the IRWST pressure begins to deviate from the containment pressure.

Spargers (PXS-MW-01A/B)

The spargers in the IRWST ensure that steam from the ADS is condensed and that the ADS discharge does not result in excessive loads on the IRWST structure. Maintenance of RCS inventory is a Category A safety function. The spargers support the primary method of achieving this by depressurising the RCS sufficiently to enable the PXS to provide safety injection flow into the RCS and therefore are Class 1. See Appendix 15A.

There are two spargers in the IRWST (Section 6.6). The requirement is that each sparger will accommodate steam and water flow from its associated set of ADS stage 1, 2, and 3 valves and distribute it within the IRWST without producing excessive dynamic loads on the IRWST.

Screens (PXS-MY-Y01A/B/C)

The screens ensure that injection from the IRWST into the RCS can take place without the accumulation of debris in the reactor vessel, since such debris may inhibit core cooling. Maintenance of heat removal from the core is a Category A safety function and because the screens are the primary means of ensuring that debris does not block core cooling flow, they are Class 1. See Appendix 15A.

There are three screens available and the requirement is that they will allow adequate flow for gravity injection even when half-blocked.

IRWST Injection Squib Valves (PXS-PL-V123A/B and -V125A/B)

The IRWST injection line isolation valves open to initiate gravity injection from the IRWST into the RCS. Maintenance of RCS inventory is a Category A safety function and as these valves are the primary means of enabling the gravity injection flow, they are Class 1. See Appendix 15A.

There are two injection routes available and each route has two parallel IRWST injection isolation valves. For each injection route, either of the IRWST injection isolation valves operating will establish the full safety function, provided that the associated isolation line check valve has opened. The requirement is therefore that one IRWST injection valve will open, as discussed in the Squib Valve Safety Case (Reference 17.36).

IRWST Injection Line Isolation Valves (PXS-PL-V121A/B)

They are designed to fail “as is” on loss of electrical supplies. They are normally open and are only required to be closed to allow maintenance on the IRWST injection isolation valves. The valves are not required to move as part of the IRWST achieving its safety function, but they must be open. They are Category A, Class 1. See Appendix 15A.

IRWST Injection Line Check Valves (PXS-PL-V122A/B and -V124A/B)

The check valve is required to open to enable the gravity injection from the IRWST to the RCS to take place. Maintenance of RCS inventory is a Category A safety function and as these valves are the primary means of enabling the gravity injection flow, they are Class 1. See Appendix 15A.

There are two injection routes available and each route has two parallel IRWST injection line check valves. For each injection route, either of the IRWST injection line check valves operating will establish the full safety function, provided that the associated injection isolation valve has opened. The requirement is therefore that one IRWST injection line check valve will open.

17.5.4.4 Justification of Claims on Components and Equipment

Storage Tank (PXS-MT-03)

The IRWST provides a large quantity of water in containment and is available as a heat sink to quench steam in the initial stages of RCS depressurisation and for injection by gravity into the RCS. It is entirely passive in nature and requires no pumps or mechanical fluid circulation devices to operate. This confers a high degree of inherent safety.

The tank is manufactured from concrete and carbon steel and lined with stainless steel to ensure maximum compatibility with the borated water it contains. It is designed as a seismic C-I structure with sufficient structural strength for expected pressure differentials to the containment pressure.

Other than its location, the storage tank is very similar to tanks used in currently operating PWRs. As a result, the information from the performance of these in-service tanks offers a high degree of confidence about the reliability to be expected from the tank design as applied to the AP1000 design. Data collected from in-service plants (Reference 17.7, Table 5-1) indicate that the probability for a major or minor leak in an unpressurised tank is conservative relative to the value being claimed.

It should also be noted that even in the event of a leak; the contents of the IRWST would drain into the containment sumps and so would still be available for long-term RCS cooling duty.

IRWST Vents and Overflows

The vent and overflow designs are based around a simple flap arrangement that will inherently lift when the tank internal pressure begins to rise and will close again under the influence of gravity. Similarly, some of the vents are designed to also open inward when the containment pressure begins to rise and will close again under the influence of gravity. These movements are entirely passive in nature and offer a high degree of inherent safety.

The principal failure mechanism is likely to be disruption of the vent area due to excessive loads, etc., during operation. The vents are constructed to a manufacturer's standard and are seismic C-I. A comprehensive finite element model has been analysed to ensure that there are adequate design margins.

Spargers (PXS-MW-01A/B)

The spargers are situated in the IRWST and are consequently always covered with water. This inherently ensures that the spargers will be able to fulfil their function with high reliability.

The sparger design has benefited from experience gained from suppression pool design for boiling water reactors and full sized, full flow prototype testing. This has resulted in the spargers arm and arm hole arrangement that results in acceptable hydrodynamic effects and loads during ADS discharge into the IRWST. The spargers are constructed to ASME Boiler and Pressure Vessel Code, Section III-3 and are seismic C-I. They are manufactured from stainless steel to ensure compatibility with the borated water in the IRWST.

Screens (PXS-MY-Y01A/B/C)

The screens are passive devices that offer an inherently high reliability for filtration. In addition, the following design features are intended to minimise the risk of the screens blocking:

- Three screens are provided and cross-connected so that flow leaving either IRWST injection line pulls flow through all three screens.

- The screens are mounted vertically to minimise the risk of particle accumulation on them.

- The design features of the IRWST precludes debris from entering it.

- There is a large margin between the minimum required surface area and the actual surface area provided.

- The screen area is large enough that the expected debris loading found in the IRWST will only cause a minor differential pressure across the screen surface.

- The screens are arranged such that the lowest screening surface is above the floor of the IRWST. This design feature prevents high-density debris from being swept across the floor and into the screen face.

The screens are manufactured from stainless steel to ensure maximum compatibility with RCS coolant. A number of tests have been done to better understand the performance of the screens, and these are discussed further in Reference 17.12. The above design improvements give confidence that the reliability will be as good as, or better than, experience on operating power stations. Data collected from in-service plants (Reference 17.7, Table 5.1) indicate the probability of filter blockage used in analyses is conservative.

IRWST Injection Squib Valves (PXS-PL-V123A/B and -V125A/B)

The IRWST injection isolation valves are squib-type valves which means they will inherently fail “as is”. Clearly, this is not fail-safe with respect to the IRWST injection function but these valves have demonstrated high reliability. Given the importance of their actuation, it is judged appropriate.

The valves are manufactured from stainless steel to ensure compatibility with the reactor coolant water that passes through them. They are designed to ASME Boiler and Pressure Vessel Code, Section III-1.

The design of squib valves is such that the firing of a propellant charge is used to drive a piston onto the valve shear cap. The shear cap, that is designed to accommodate normal service loads, is broken off by the piston. The piston comes to rest with an opening aligned with the flow path to allow full flow through the valve. Provided that the propellant charge fires correctly, there is a very high level of confidence that the subsequent actions will happen successfully and the valve will open correctly. Consequently, the valve reliability depends almost entirely on the firing reliability of the squib. This issue is discussed further in the squib valve summary report (Reference 17.2).

The maintenance and testing arrangements for the IRWST injection isolation valves comply with ASME Boiler and Pressure Vessel Code and are based on the programmes appropriate for these types of valves as used in existing nuclear power stations. The testing is:

- The inservice testing of the squib valves requires that 20 percent of the charges installed on the plant will be removed from the squib valves, placed in test fixtures and actuated every 2 years. These tests will be performed in a test fixture away from the valve, and the positions they occupied in valves on the plant will be taken by replacement charges.

IRWST Injection Line Isolation Valves (PXS-PL-V121A/B)

They are designed to fail "as is" on loss of electrical supplies. They are normally open and are only required to be closed to allow maintenance on the IRWST injection isolation valves. The valves are not required to move as part of the IRWST achieving its safety function, but they must be open.

The valves are manufactured from stainless steel to ensure compatibility with the RCS chemistry conditions and are designed to ASME Boiler and Pressure Vessel Code, Section III-1.

The valves are very similar to those already in like service on many operating power stations. As a result, the information from testing these in-service valves offers a high degree of confidence about the reliability to be expected from these valves. Data collected for in-service plants (Reference 17.7, Table 5.1) indicate a probability of failure to open an order of magnitude better than the value assumed in the PSA and indicates that the claims against these valves are conservative.

The operating mechanism for the valve is very simple and, aside from gross mechanical failure, some form of failure to open might be considered the principal mechanism for valve failure. There are two particular reasons for believing this risk to be low and they are:

- Under normal operating conditions, the valves sit without differential pressure across them in a relatively clean fluid environment. This, along with the specified seat materials, is judged to reduce the probability of seizure due to corrosion or self-welding to a very low level.

- The valves only see flow for very limited periods during testing. As a result, they are not subject to degradation due to the vibration resulting from fluid flow of impact loads caused by sudden flow reversal and seating.

The maintenance and testing arrangements for the IRWST injection line check valves are based on the programmes appropriate for these types of valves as used in existing nuclear power stations. The testing is:

- Visual confirmation of valve position indication operation during the stroke testing is performed every 2 years.

IRWST Injection Line Check Valves (PXS-PL-V122A/B and -V124A/B)

The operation of the IRWST injection line check valves depends only upon the pressure difference across them and not on any method of powered actuation. This passive approach offers a high degree of inherent safety and reliability.

The valves are manufactured from stainless steel to ensure compatibility with the RCS chemistry conditions and are designed to ASME Boiler and Pressure Vessel Code, Section III-1.

The valves are very similar to those already in like service on many operating power stations. As a result, the information from testing these in-service valves offers a high degree of confidence about the reliability to be expected from these valves. Data collected for in-service plants (Reference 17.7, Table 5.1) indicate a probability of failure to open an order of magnitude better than the value assumed in the PSA and indicates that the claims against these valves are conservative.

The operating mechanism for the valve is very simple and, aside from gross mechanical failure, some form of failure to open might be considered the principal mechanism for valve failure. There are two particular reasons for believing this risk to be low and they are:

- Under normal operating conditions, the valves sit without differential pressure across them in a relatively clean fluid environment. This, along with the specified seat materials, is judged to reduce the probability of seizure due to corrosion or self-welding to a very low level.

- The valves only see flow for very limited periods during testing. As a result, they are not subject to degradation due to the vibration resulting from fluid flow of impact loads caused by sudden flow reversal and seating.

The maintenance and testing arrangements for the IRWST injection line check valves are based on the programmes appropriate for these types of valves as used in existing nuclear power stations. The testing is:

- Stroke testing of Class 1 check valves would ideally be performed quarterly. However exercising the valve with the unit at power is deemed to present unacceptable risk to normal operation. Therefore, a full stroke operability test is performed every 2 years as allowed by the ASME Boiler and Pressure Vessel Code in such circumstances.

- Visual confirmation of valve position indication operation during the stroke testing is performed every 2 years.

- A determination of the initial opening differential pressure will be performed every 2 years.

17.5.5 Containment Recirculation Function

17.5.5.1 Role

A detailed description of the PXS containment recirculation function is given in Section 6.6. Further design details of this system and its constituent components are delineated in Reference 17.25.

Containment recirculation does not play a part in normal operations but is key to maintaining the heat transfer/residual heat removal primary safety function during long term recovery from faults. Containment recirculation functions in two ways:

- If the RCS remains intact, then decay heat is transferred to the IRWST by the PRHR HX. The IRWST water temperature rises and ultimately begins to boil. The steam produced escapes through the IRWST vents and condenses on the inner surface of the containment. Under these circumstances, passive containment cooling, gutters, and downspouts ensure that the condensate on the inner surface of the containment building is returned to the IRWST to maintain its inventory and consequent cooling capability. Note that in the long-term (greater than 14 days) the fact that the return rate back into the IRWST is not 100% can lead to uncover of enough of the PRHR HX that the RCS temperature will rise and ADS valves would have to be actuated transitioning the RCS into a passive feed and bleed cooling mode.

- If the RCS has been breached, the IRWST contents are injected into the RCS. When the IRWST water level reaches its low-low level, the containment recirculation paths to the

direct vessel injection lines are opened. In this situation a steam / water mixture is vented from the RCS breach and the ADS lines. The steam rises into the containment and condenses on the inner surface of the containment. This condensate is returned to the IRWST through a series of gutters. From the IRWST, the condensate is returned to the RCS through the IRWST injection lines. The water vented from the RCS falls down into the containment and is recirculated through containment recirculation screens into the IRWST injection lines and the RCS.

The containment recirculation system functions through the provision of valves that control the drainage path of condensate from the containment inner wall, and by the opening of the recirculation flowpaths from the containment recirculation screen intakes. These recirculation screens are arranged in parallel and filter out debris from the containment floodup water. Water that passes through the screens is available for recirculation through any of the recirculation routes.

Containment recirculation is supported in providing its safety functions by the essential electrical system and also implicitly by the IRWST and its debris screens.

The PXS containment recirculation does not support any other systems in providing their safety functions.

17.5.5.2 System Components and Equipment Contributing to Safety Function

The following components contribute to containment recirculation performing its safety function:

- **IRWST Gutter Drain Isolation Valves (PXS-PL-V130A/B)** – These are 50-mm DN (2-inch), air-operated ball valves that fail closed on loss of air supply. The valves are normally open and are closed on receipt of a PRHR HX actuation signal from either the PMS or the DAS. This isolates the drain line to the containment radwaste sump and diverts the water collected by the IRWST gutter into the IRWST. The safety requirement is to ensure that injection from the IRWST into the RCS can take place without the accumulation of debris in the reactor vessel, since such debris may inhibit core cooling.

- **Containment Recirculation Screens (PXS-MY-Y02A/B)** – These pocket-type screens use a perforated sheet as the filter medium. There are two sets of screens which are situated in the East loop compartment (Loop 2) adjacent to the reactor vessel biological shield wall and ensure that particles are prevented from entering the RCS. The safety requirement is to prevent debris from entering the RCS through the recirculation lines.

- **Containment Recirculation Isolation Valves (PXS-PL-V118A/B & PXS-PL-V120A/B)** – These are 200-mm DN (8-inch), squib-type valves. They effectively fail "as is" on a loss of control supplies and are signalled to open by an open containment recirculation valves signal by the PMS. Opening the valves establishes a gravity injection route from the flooded containment into the RCS and hence a long-term stable heat removal path post-accident. The requirement to establish a flow path is therefore a safety requirement, as discussed in the Squib Valve Safety Case (Reference 17.36). These squib valves are similar to the IRWST injection isolation valves discussed in Section 17.5.4.3. However, there are a number of design features that create diversity between the two sets of valves as described in Reference 17.2.

  Sections 17.5.5.3 and 17.5.5.4 provide additional details on the design and function of the containment recirculation squib valves. Chapter 6 provides discussion on the PXS

which contains the containment recirculation valves and references the system specification documents. Table 8A-2 presents faults that credit containment recirculation actuation for mitigation of the initiating events; associated fault analyses are referenced, with all design basis analyses presented in Chapter 9. The plant PSA (Chapter 10) includes consideration of the valves to actuation upon demand, as well as the consequences associated with spurious operation. The valve resilience to applicable internal hazards is discussed in Chapter 11. Additional detail on the interfacing C&I systems (PMS and DAS) is provided in Chapter 19, with the ADS blocker devise being discussed in Section 19.4.1.2.13. The electrical systems that provide power for actuation are discussed in Chapter 18.

- **Containment Recirculation Isolation Valves (PXS-PL-V117A/B)** – These are 200-mm (8-inch) nominal-bore, motor-operated gate valves that fail "as is" on loss of supplies. These normally open valves are not required to move in order for containment recirculation to achieve its safety function because they are already in their proper position. The valve position will be checked during routine 12-hourly operation surveillances and whilst in this condition the power supplies will be isolated to prevent inadvertent operation. To support the achievement of the containment recirculation safety function, these administrative arrangements are backed up by the initiation of an open signal from the PMS when an open containment recirculation valves signal is generated. It is considered that these arrangements are sufficiently robust that further analysis is not required.

- **Containment Recirculation Check Valves (PXS-PL-V119A/B)** – These are 200-mm DN (8-inch), swing check valves. These valves exist to prevent reverse flow in the event of an inadvertent actuation of the associated containment recirculation isolation valve. Their safety function is to open on demand to enable direct injection from the containment sumps into the RCS.

17.5.5.3 Claims on Components and Equipment

IRWST Gutter Drain Isolation Valves (PXS-PL-V130A/B)

The normal IRWST gutter drain lines are isolated to ensure that condensate from the containment walls is returned to the IRWST to maintain its water inventory and decay heat removal capability via the PRHR HX. Removal of decay heat is a Category A safety function. These valves are the primary means of diverting the containment drainage into the IRWST and are therefore Class 1. See Appendix 15A.

There are two valves in series and either one closing will fulfil the required safety function.

Recirculation Screens (PXS-MY-Y02A/B)

The recirculation screens ensure that recirculation flow from the flooded containment into the RCS can take place without the accumulation of debris in the reactor vessel, since such debris may inhibit core cooling. Maintenance of heat removal from the core is a Category A safety function and because the screens are the primary means of ensuring that debris does not block core cooling flow, they are Class 1. See Appendix 15A.

There are two screens available and the requirement is that they will allow adequate flow for gravity recirculation even when they have captured a conservative amount of debris.

Containment Recirculation Isolation Valves (PXS-PL-V118A/B & PXS-PL-V120A/B)

The containment recirculation isolation valves open to initiate gravity injection from the flooded containment into the RCS. Maintenance of RCS inventory is a Category A safety function and as these valves are the primary means of enabling the gravity injection flow, they are considered to be Class 1. See Appendix 15A.

There are two recirculation routes available and each has two parallel lines containing containment recirculation isolation valves. For sufficient recirculation flow, either of the containment recirculation isolation valves in either operating recirculation route will establish the full safety function, provided that the associated isolation valve in series has opened, as discussed in the Squib Valve Safety Case (Reference 17.36). The reliability for operation of the valves is given in the Squib Valve Summary Report (Reference 17.2).

Containment Recirculation Check Valves (PXS-PL-V119A/B)

The check valve is required to open to enable the gravity injection from the flooded containment to the RCS to take place. Maintenance of RCS inventory is a Category A safety function and as these valves are the primary means of enabling the gravity injection flow, they are considered to be Class 1. See Appendix 15A.

There are two recirculation injection routes available and each has two parallel lines with one line containing a containment recirculation line check valve. For each route, either of the two containment recirculation check valves operating will establish the full safety function, provided that their associated injection isolation valve has opened. It is noted that either of the two other parallel lines that do not contain check valves will also establish the full safety function, provided that their associated injection isolation valve has opened.

17.5.5.4 Claims on Components and Equipment

IRWST Gutter Drain Isolation Valves (PXS-PL-V130A/B)

The IRWST gutter drain isolation valves are air operated with the actuators designed to fail closed in the event of loss of air supply. This is an inherently safe mechanism, meaning that only in the event of a valve sticking will there be a failure to a condition other than safe.

The valves are manufactured from stainless steel to ensure compatibility with the borated RCS fluid that is in contact with them. They are designed to ASME Boiler and Pressure Vessel Code, Section III-3.

The valves are very similar to those already in service on many operating power stations. As a result, the information from testing these in-service valves offers a high degree of confidence about the reliability to be expected from these valves. Data collected from in-service plants (Reference 17.7, Table 5.1) are comparable to the value being claimed.

The failure mechanism of concern would involve a valve sticking or jamming. This could be a result of wear, corrosion, or maintenance-induced failure. In addition to being designed to ASME Boiler and Pressure Vessel Code, Section III, the valves are also designed and installed to seismic C-I and are qualified for operation in a harsh environment (Table 15A-1).

The maintenance and testing arrangements for the IRWST gutter drain isolation valves are based on the programmes appropriate for these types of valves as used in existing nuclear power stations. The testing is:

- A full stroke operability test is performed quarterly in accordance with ASME Boiler and Pressure Vessel Code.

- Visual confirmation of valve operation during the stroke testing is performed every 2 years.

Recirculation Screens (PXS-MY-Y02A/B)

The recirculation screens are passive devices that offer an inherently high reliability for filtration. In addition, the following design features are intended to minimise the risk of the screens blocking:

- The screens are mounted vertically to minimise the risk of particle accumulation on them.

- The design of the containment structures, coatings, and piping insulation minimises the amount of debris that can be created by a postulated fault, as well as the amount of debris which can travel to the screens by providing low flow velocity (large flow areas) approaching the screens to allow high density debris to settle out.

- There is a large margin between the minimum required surface area and the actual surface area provided.

- The screen area is large enough that the expected debris loading found in the containment will only cause a minor differential pressure across the screen surface.

- The screens are arranged such that the lowest screening surface is above the floor of the containment. This design feature prevents high-density debris from being swept across the floor and into the screen face.

The screens are manufactured from stainless steel to ensure maximum compatibility with RCS coolant. A number of tests have been done to better understand the performance of the screens, and these are discussed further in Reference 17.12. The above design improvements give confidence that the reliability will be as good as or better than experience on operating power stations. Data collected from in-service plants (Reference 17.7, Table 5.1) indicate a probability of filter blockage so that the claim is conservative.

Containment Recirculation Isolation Valves (PXS-PL-V118A/B & PXS-PL-V120A/B)

The containment recirculation isolation valves are squib-type valves which means they will inherently fail “as is”. Clearly, this is not fail-safe with respect to the containment recirculation function, but given that the high actuation reliability of these valves, it is judged appropriate.

The valves are manufactured from stainless steel to ensure compatibility with the reactor coolant water that passes through them. They are designed to ASME Boiler and Pressure Vessel Code, Section III-1.

The design of squib valves is such that the firing of a propellant charge is used to drive a piston onto the valve shear cap. The shear cap, that is designed to accommodate normal service loads, is broken off by the piston. The piston comes to rest with an opening aligned with the flow path to allow full flow through the valve. There is a very high level of confidence that the propellant charge and the subsequent actions will happen successfully and

that the valve will open correctly. The arguments and evidence that the squib valves are design adequately to reliably perform their necessary safety function are provided in the Squib Valve Safety Case (Reference 17.36). The valve reliability depends heavily on the firing reliability of the propellant. This issue is discussed further in the squib valve summary report (Reference 17.2).

The maintenance and testing arrangements for the IRWST injection isolation valves comply with ASME Boiler and Pressure Vessel Code and are based on the programmes appropriate for these types of valves as used in existing nuclear power stations. The testing is:

- Twenty percent of the charges installed on the plant will be fired every 2 years. These tests will be performed in a test fixture away from the valve and the positions they occupied in valves on the plant will be taken by replacement charges.

Containment Recirculation Check Valves (PXS-PL-V119A/B)

The operation of the containment check valves depends only upon the pressure difference across them and not on any method of powered actuation. This passive approach offers a high degree of inherent safety and reliability.

The valves are manufactured from stainless steel to ensure compatibility with the RCS chemistry conditions and are designed to ASME Boiler and Pressure Vessel Code, Section III-1.

The valves are very similar to those already in like service on many operating power stations. As a result, the information from testing these in-service valves offers a high degree of confidence about the reliability to be expected from these valves. Data collected for in-service plants (Reference 17.7, Table 5.1) indicate a probability of failure to open that is an order of magnitude better than the value assumed in the PSA and indicates that the claims against these valves are conservative.

The operating mechanism for the valve is very simple and, aside from gross mechanical failure, some form of failure to open might be considered the principal mechanism for valve failure. There are two particular reasons for believing this risk to be low:

- Under normal operating conditions, the valves sit without differential pressure across them in a relatively clean fluid environment. This, and the specified seat materials, is judged to reduce the risk of seizure due to corrosion or self-welding to a very low level.

- The valves only see flow for very limited periods during testing. As a result, they are not subject to degradation due to vibration resulting from fluid flow of impact loads caused by sudden flow reversal and seating.

The maintenance and testing arrangements for the containment recirculation check valves are based on the programmes appropriate for these types of valves as used in existing nuclear power stations. The testing is:

- A full stroke operability test is performed every 2 years in accordance with ASME Boiler and Pressure Vessel Code. Even though a test every three months might be specified for this type of service, exercising the valve with the unit at power is deemed to present an unacceptable risk to normal operation and hence, under the ASME Boiler and Pressure Vessel Code rules, can be varied.

- Visual confirmation of valve position indication operation during the stroke testing is performed every 2 years.

- A check of the initial opening differential pressure will be performed every 2 years.

17.5.6 Passive Residual Heat Removal

17.5.6.1 Role

A detailed description of the PRHR HX and associated piping and valves is given in Section 6.6. Further design details of this system and its constituent components are delineated in Reference 17.25.

The PRHR HX is located within the PXS IRWST and is submerged in the IRWST water which serves as the heat sink for heat transferred from the RCS via the heat exchanger tube surfaces. The PRHR HX has no function during normal operation but serves as the primary Class 1 decay heat removal path during fault conditions with the RCS intact, when the normal heat removal path via the SGs is unavailable. As such, it contributes to the heat transfer/residual heat removal primary safety function.

The system is purely passive in operation with loop pipes and associated valves connecting the PRHR HX inlet to the RCS hot leg and outlet to the RCS cold leg by means of the SG channel head.

The PRHR is supported in the provision of its safety function by the IRWST and the essential electrical system.

The PRHR does not support any other systems in the provision of their safety functions.

17.5.6.2 System Components and Equipment Contributing to Safety Function

All the PRHR pipework, along with the HX (PXS-ME-01) itself, is constructed to ASME Boiler and Pressure Vessel Code, Section III, Class 1 and is also seismic C-I.

- **PRHR HX (PXS-ME-01)** – This comprises Inconel™ 690 tubes arranged in a single-pass, horizontal "C" arrangement. The remaining HX components are manufactured from stainless-steel-lined carbon steel and/or stainless steel. The design limiting heat removal requirement is met with approximately 5-percent tube plugging. The heat transfer duty is a safety requirement.

- **PRHR HX Inlet Isolation Valve (PXS-PL-V101)** – This is a 350-mm DN (14-inch), motor-operated gate valve designed to fail "as is" on loss of electrical supplies. It is normally open and is only required to be closed to allow IST of the outlet valves and for shutdown maintenance on the PRHR HX. The valve is not required to move as part of the PRHR achieving its safety function since it is normally open. The valve position will be checked during routine 12-hourly operation surveillances and whilst in this condition, the power supplies will be isolated to prevent inadvertent operation. To support the PRHR safety function, these administrative arrangements are backed up by the initiation of an open signal from the PMS when a PRHR actuation signal is generated. It is felt that these arrangements are sufficiently robust that further analysis is not required.

- **PRHR HX Control Valves (PXS-PL-V108A/B)** – These are 350-mm DN (14-inch) air-operated ball valves that fail open on loss of air supplies. The valve is normally

closed and is signalled to open on receipt of a PRHR actuation signal from either the PMS or the DAS to separate air control solenoids. The valve opening sets up the natural circulation flow path from the RCS through the PRHR and enables passive cooling of the RCS. The establishment of this flow path is a safety requirement.

17.5.6.3 Claims on Components and Equipment

PRHR Heat Exchanger (PXS-ME-01)

The PRHR HX is the primary post-fault means of removing RCS decay heat with the RCS intact. Decay heat removal is a Category A safety function. The PRHR is deemed to be Class 1.

There is a single HX and it must operate correctly for the system to perform its safety function. The requirement is that the HX will provide adequate heat transfer capability to accommodate RCS decay heat generation and thus cool the RCS.

PRHR HX Inlet Isolation Valve (PXS-PL-V101)

PRHR HX inlet isolation valve must be open to allow decay heat removal from the RCS but is in the open position during operation. Decay heat removal is a Category A safety function. The valves are Class 1. See Appendix 15A.

PRHR Heat Exchanger Control Valves (PXS-PL-V108A/B)

The PRHR HX control valves open to allow decay heat removal from the RCS. Decay heat removal is a Category A safety function. The valves are Class 1. See Appendix 15A.

There are two PRHR HX control valves arranged in parallel. At least one of them is required to open to ensure that the safety function is performed. The requirement is therefore that at least one of the PRHR HX control valves will open.

17.5.6.4 Justification of Requirements on Components and Equipment

PRHR Heat Exchanger (PXS-ME-01)

The PRHR HX is a passive component. Given that it is mounted in the IRWST beneath the water level, and provided that hot fluid is able to circulate through the tubes, heat transfer is inherently going to take place.

The HX is manufactured to ensure maximum compatibility with the RCS coolant and IRWST contents. It is built to ASME Boiler and Pressure Vessel Code, Section III-1.

A number of design features support the reliability claimed for the PRHR HX:

- The tubes are constructed from Inconel 690, a material selected because of its resistance to stress-corrosion cracking. It has been well proven as an SG tube material in current PWRs.

- The use of stainless-steel-lined channel heads is similar to the cladded carbon steel design utilised in the RCS major components, including the reactor vessel and vessel head.

- The PRHR is maintained pressurised during normal operations so that it can be placed into service without water hammer.

- The connections onto the RCS are placed to ensure a strong initial natural circulation driving head.

- The inlet line is sloped up to the HX to ensure that internal convection will maintain it in a hot condition. The inlet pipework is also lagged, again to maintain the inlet to outlet temperature difference and enhance the establishment of natural circulation.

- With the RCPs operating, the PRHR HX operates with the flow in the same direction as when only natural circulation exists. This precludes disruption of the thermal driving head on transfer from forced to natural circulation in the RCS.

The tubes are not designed to be replaced and hence the design has an approximately 5-percent tube-plugging margin to adequate surface area after tube plugging following in-service detection of tube corrosion or cracking or leakage.

Although the PRHR HX is a new concept with the AP1000 design, the principle of tubed HXs is well established in PWRs and other nuclear power stations. As such, the reliability experienced by operating stations can contribute to establishing confidence in the expected PRHR reliability. Data collected from in-service plants (Reference 17.7, Table 5.1) indicate the probability of a tube leak in an HX is comparable to the value being claimed.

The maintenance and testing arrangement for the PRHR HX are based on the ASME Boiler and Pressure Vessel Code programmes appropriate for similar equipment as used on existing nuclear power stations. The testing is:

- A system test is performed every 10 years to confirm PRHR heat transfer capability.

- The PRHR closure heads will be accessible for cladding and tube inspection during every refuelling outage, and there will be external access to the tube bank when the IRWST is drained.

PRHR HX Inlet Isolation Valve (PXS-PL-V101)

Must be open to allow decay heat removal from the RCS but is in the open position during operation.

The valves are manufactured from stainless steel to ensure compatibility with the borated RCS fluid that is in contact with them. They are designed to ASME Boiler and Pressure Vessel Code, Section III-1.

PRHR Heat Exchanger Control Valves (PXS-PL-V108A/B)

The PRHR HX control valves are air operated with the actuators designed to fail open in the event of loss of air supply. This is an inherently safe mechanism, meaning that only in the event of a valve sticking will there be a failure to a condition other than safe.

The valves are manufactured from stainless steel to ensure compatibility with the borated RCS fluid that is in contact with them. They are designed to ASME Boiler and Pressure Vessel Code, Section III-1.

The valves are similar to those already in service on many operating power stations. As a result, the information from testing these in-service valves offers a high degree of confidence about the reliability to be expected from these valves. Data collected from in-service plants (Reference 17.7, Table 5.1) indicate a probability of a failure to open is comparable to the value being claimed.

The failure mechanism of concern would involve a valve sticking or jamming. This could be a result of wear, corrosion, or maintenance-induced failure. In addition to being designed to ASME Boiler and Pressure Vessel Code, Section III, the valves are also designed and installed to seismic C-I and are qualified for operation in a harsh environment (Table 15A-1).

The maintenance and testing arrangements for the PRHR HX control valves are based on the ASME Boiler and Pressure Vessel Code programmes appropriate for these types of valves as used in existing nuclear power stations. The testing is:

- A full stroke operability test is carried out quarterly in accordance with ASME Boiler and Pressure Vessel Code.
- Visual confirmation of valve operation during the stroke testing is performed every 2 years.
- A system test is performed every 10 years to confirm PRHR heat transfer capability. This will also confirm valve operating performance.

17.5.7 Normal Residual Heat Removal System

17.5.7.1 Role

A detailed description of the RNS is given in Section 6.4. Further design details of this system and its constituent components are delineated in Reference 17.26.

The RNS contributes to the primary containment isolation safety function and may contribute to the heat transfer/residual heat removal defence in depth safety functions. During normal shut down operation, it supports the heat transfer/residual heat removal through the removal of decay heat generated in the core when the RCS temperatures are below the level where effective heat removal is possible through steaming the SGs. It also provides the motive force to circulate RCS fluid through the CVS system when the RCPs are shut down.

The RNS contributes to heat transfer/residual heat removal through the following Class 2 defence in depth functions:

- The RNS can provide cooling for the IRWST during operation of the PRHR heat exchanger. The system is manually aligned and can be used to prevent the IRWST boiling.
- Following an accident which has resulted in actuation of all stages of ADS, the RNS can be aligned to provide injection flow from inside the containment to the reactor vessel and provide core decay heat removal instead of making use of the PXS containment recirculation capability.
- The RNS can also provide post-accident low pressure make-up taking water either from the IRWST or from the cask loading pit following actuation of ADS stages 1, 2, and 3. This is intended to provide the facility for the plant to be stabilised before the PXS core makeup tanks drain down to their ADS stage 4 actuation level setpoint. Either train of the

RNS can also be used to cool the spent fuel pool during normal plant operation provided it is not being used for core decay heat removal.

The RNS piping connections from and to the RCS pass through the containment boundary and have containment isolation valves for the containment isolation safety function. This feature supports the containment primary safety function.

After an accident which has included fourth stage ADS, long term makeup may be required from outside of containment. The flow path for this long-term (2-4 weeks following the event) supply of water is administratively controlled and water addition is supplied through either of the two RNS heat exchanger channel head drain connections.

The RNS system consists of two separate and independent trains of mechanical equipment. The RNS shares a common connection to one of the RCS hot legs. After this connection the line is split into two separate RNS lines with separate pipe lines, valves, pumps and HX. Each RNS suction line also has a separate connection from the IRWST and suction relief valves. Single connections are provided to and from the CVS purification demineralisers and filter. Each suction line contains inside and outside containment isolation valves and is routed to its corresponding RNS pump suction. Downstream of each outside containment RNS suction isolation valve, each RNS pump suction line has a connection from the spent fuel pool and from the cask wash down pit. Each RNS pump discharges through its own heat exchanger (cooled by the CCS), and each heat exchanger has its own flow control valves and bypass line to control the RCS cooldown rate. Each pump/heat exchanger discharge line has a piping connection to the spent fuel pool; a separate containment penetration with outer and inner containment isolation valves; and connections inside containment to the IRWST and to the CVS purification demineralisers and filter. Each then feeds into its corresponding PXS direct vessel injection line which connects to the reactor vessel downcomer.

The RNS is supported by the ECS and under certain circumstances by the ZOS. Heat removal from the RNS HXs and pump seal cooling is supported by the CCS. Each RNS pump room is equipped with a central chilled water system (VWS) cooler and the operation of the VWS air cooled chiller subsystem is required to support longer-term operation of the pumps (more than 24 hours). Clearly, for low-pressure RCS makeup, the RNS is supported by the IRWST and/or the cask loading pit.

The RNS supports the SFS in providing their safety function when the full core is placed in the SFP or when there is a failure in the SFS. The RNS also provides a defence in depth function to support PXS low pressure safety injection, long-term recirculation function, and shutdown decay heat removal function.

17.5.7.2 System Components and Equipment Contributing to Safety Function

The pressure boundary of the RNS (pipework, pump casing, valves, and HX) outside of containment are designed to ASME Boiler and Pressure Vessel Code, Section III-3. They are capable of accepting full reactor system pressure without bursting, although there may be some plastic deformation. The sections of RNS pipework inside of containment are designed for full RCS design pressure. The RCS pressure isolation portion of the RNS is designed to ASME Boiler and Pressure Vessel Code, Section III-1; the containment isolation portion of the RNS is designed to ASME Boiler and Pressure Vessel Code, Section III-2; and the rest of the RNS piping inside containment is designed to ASME Boiler and Pressure Vessel Code, Section III-3. The whole system is designed to seismic C-I (Table 15A-1).

- **RNS Pumps (RNS-MP-01A/B)** – These are single-stage, vertical, in-line, bottom-suction, centrifugal pumps constructed of stainless steel. They are directly coupled to an ac induction motor. The pumps develop sufficient shutoff head. The pumps are protected by mini-flow pipework from the HX discharge to the pump suction. They have mechanical seals on the drive shaft and these are cooled by the CCS. The pumps are operated solely by manual operator control and there are no automatic signals to initiate operation. The specific safety requirement of the RNS pumps is to provide the required RNS design flow from the RCS, through the RNS, and back to the reactor vessel.

- **RNS HXs (RNS-ME-01A/B) –** These are vertically mounted shell-and-U-tube design HXs with the RCS fluid to be cooled circulating through the tubes and CCS fluid circulating through the shell. The shell is manufactured from carbon steel and the tubes from stainless steel. The HXs are sized to allow the design plant cooldown profile to be achieved in conjunction with the RNS pump design flow rate. The safety requirement of the RNS HXs is to provide adequate heat transfer to remove core decay heat and cool down the RCS during normal shutdown and accident conditions.

- **RNS Hot Leg Suction Isolation - Inner Valves (RNS-PL-V001A/B)** – These are 250-mm DN (10-inch), motor-operated gate valves located inside containment. They fail "as is" on loss of power. The valves are opened manually to initiate RCS cooling by the RNS system, albeit with permissive interlocks based on RCS pressure and IRWST suction valve position, and are signalled closed by the PMS on receipt of an RNS isolation signal. The safety requirement of the valves is to open on demand to allow use of the RNS system in its defence in depth function, and also to isolate the RNS suction lines on demand from an RNS isolation signal.

- **RNS Hot Leg Suction Isolation Valves (RNS-PL-V002A/B)** – These are 250-mm DN (10-inch), motor-operated gate valves. They fail "as is" on loss of power. The valves are opened manually to initiate RCS cooling by the RNS system, albeit with permissive interlocks based on RCS pressure and IRWST suction valve position, and are signalled closed by the PMS on receipt of a manual RNS isolation signal or a RNS containment isolation signal. The safety requirement of the valves is to open on demand to allow use of the RNS system in its defence in depth function, and also to isolate the RNS suction lines on demand from an RNS or containment isolation signal.

- **RNS return from CVS CIVs (RNS-PL-V061A/B) –** These are 75-mm DN (3-inch), air-operated globe valves located inside containment. They fail closed on loss of air supply, and one is normally opened only when the RNS is in service to return flow from the CVS demineralisers and filters to the RNS, with the flow to the CVS provided from an RNS discharge. This flow path contributes to enabling the RNS to pump RCS fluid through the CVS when the RCPs are shut down. Because of where they are connected to the RNS suction pipework, the valves are CIVs and are closed by the PMS on receipt of a containment isolation signal. The safety requirement of the valves is to isolate the RNS containment penetration on demand.

- **RNS Hot Leg Suction Pressure Relief Valves (RNS-PL-V021A/B)** – These are 75-mm DN (3-inch) safety relief valves located inside containment, with one relief valve connected to each RNS train. The valves provide overpressure protection to the RNS at all times and also provide low-temperature overpressure protection to the RCS when either RNS train is in service. This size has been chosen so that the pressure in the RCS and RNS can be kept below the lower value of the RNS design pressure and the low-temperature limit for the reactor vessel, based on ASME Boiler and Pressure Vessel

Code, Section III, Appendix G. The valves do not require separate actuation but opening at the setpoint pressure is a safety requirement.

- **RNS Suction Header CIVs (RNS-PL-V022A/B)** – These are 250-mm DN (10-inch), motor-operated gate valves located inside containment. They fail "as is" on loss of power and are only opened when it is required to put the RNS into service. They are CIVs and are signalled closed on receipt of a containment isolation signal from the PMS. They also close on receipt of a manual RNS isolation signal from the PMS. The safety requirement of the valves is to open on demand to allow use of the RNS system in its defence in depth function and also to isolate the RNS containment penetration on demand.

- **RNS Discharge CIVs (RNS-PL-V011A/B)** – These are 150-mm DN (6-inch), motor-operated gate valves located outside containment. They fail "as is" on loss of power and are only opened when it is required to put the RNS into service. They are CIVs and are signalled closed by the PMS on receipt of an RNS containment isolation signal. The safety requirement of the valve is to open on demand to allow use of the RNS system in its defence in depth function and also to isolate the RNS containment penetration on demand.

- **RNS HX Outlet Flow Control Valves (RNS-PL-V006A/B)** – These are 150-mm DN (6-inch), air-operated globe valves that fail open on loss of air. They are positioned from the MCR to control RCS cooldown rates but are normally set to the fully open position at other times to ensure maximum cooling should the RNS be used for one of its defence in depth functions.

- **RNS HX Bypass Flow Control Valves (RNS-PL-V008A/B)** – These are 100-mm DN (4-inch), air-operated globe valves that fail closed on loss of air. They are positioned from the MCR to control RCS cooldown flow rates (control is integral to the HX flow control valves) but are normally positioned to the fully closed position at other times to ensure maximum cooling should the RNS be used for one of its defence in depth functions.

- **RNS Suction from IRWST CIVs (RNS-PL-V023A/B)** – These are 250-mm DN (10-inch) nominal-bore, motor-operated gate valves located inside containment. They fail "as is" on loss of power and are only opened when it is required to use the RNS to inject IRWST water, or to initiate IRWST cooling, as part of the RNS defence in depth functions. They are also CIVs and are signalled closed by the PMS on receipt of an RNS containment isolation signal. The safety requirement of the valves is to enable flow from the IRWST on demand when IRWST water is required, and to isolate the IRWST to RNS suction line on demand for normal RNS operation or for containment isolation.

- **RNS Discharge to IRWST Isolation Valves (RNS-PL-V024A/B)** – These are 150-mm DN (6-inch), motor-operated gate valves located inside containment. They fail "as is" on loss of power and are only opened to use the RNS to cool the IRWST as part of its defence in depth function. This is done manually and there is no automatic actuation of these valves. The safety requirement is to enable flow from the RNS pump suction to the IRWST on demand.

- **RNS Pump Suction to Cask Loading Pit Isolation Valves (RNS-PL-V055A/B)** – These are 200-mm DN (8-inch), motor-operated gate valves. They fail "as is" on loss of power and are only opened to use the RNS to provide low-pressure injection from the cask loading pit as part of the RNS defence in depth function. This is done manually and

there is no automatic actuation of these valves. The safety requirement is to enable flow from the cask load pit on demand.

- **RNS Discharge CIV - IRC (RNS-PL-V013A/B)** – These are 150-mm DN (6-inch) swing check valves. They are required to remain open to provide heat transfer and residual heat removal but are also required to isolate on reverse flow and serve as CIVs. Both functions are safety requirements.

- **RNS Discharge RCS Pressure Boundary Stop Check Valves (RNS-PL-V015A/B)** – These are 150-mm DN (6-inch) stop check valves. They are required to open for the RNS to be placed into service and serve as the RCS pressure boundary under normal operating conditions. The safety requirement is to maintain the RCS pressure boundary at all times when they are subject to a reverse pressure difference, and to open when this pressure difference is removed to enable the RNS to be put into service.

- **RNS Discharge RCS Pressure Boundary Check Valves (RNS-PL-V017A/B)** – These are 150-mm DN (6-inch) swing check valves. They are required to open for the RNS to be placed into service and serve as the RCS pressure boundary under normal operating conditions. The safety requirement is to maintain the RCS pressure boundary at all times when they are subject to a reverse pressure difference, and to open when this pressure difference is removed to enable the RNS to be put into service.

17.5.7.3 Claims on Components and Equipment

RNS Pumps (RNS-MP-01A/B)

The RNS pumps provide the motive force to either circulate water through the RNS or to inject water from the IRWST/cask loading pit into the RCS. These flows provide a heat transport capability for the removal of decay heat. Removal of decay heat is a Category A safety function. The RNS pump motor and rotating parts are Class 2. See Appendix 15A. When the RNS is in service, it effectively becomes a part of the RCS pressure boundary with a consequent function to contain radioactive material. Maintaining the reactor coolant pressure boundary is a Category A safety function and the RNS component pressure boundaries are Class 1 in this respect. See Appendix 15A.

There are two RNS pumps; both of them are required to be available to provide the full cooling. However, the loss of one RNS pump does not preclude the ability to cool down, but results in longer cooldown times. The requirement on the pumps is that they will start on demand and continue to run reliably as required.

RNS HXs (RNS-ME-01A/B)

The RNS HXs provide the capability to transfer heat to the CCS. Removal of decay heat is a Category A safety function. The RNS HX shells are Class 2. See Appendix 15A. When the RNS is in service, it effectively becomes a part of the RCS pressure boundary with a consequent function to contain radioactive material. Maintaining the reactor coolant pressure boundary is a Category A safety function and the RNS HX channel heads and tubes are Class 1 in this respect. See Appendix 15A.

There are two RNS HXs, both of that are required to provide the full shutdown cooling duty. However, the loss of one RNS heat exchanger does not preclude the ability to cool down the RCS, but results in longer cooldown times. The requirement on the heat exchangers is that they will provide adequate heat transfer and that they will not impair the operation of the

RNS, or will not themselves be unavailable, through leakage.

Hot Leg Suction Isolation Inner – Valves (RNS-PL-V001A/B)

The RCS hot leg to RNS suction inner isolation valves provide isolation for the lower design pressure portion of the RNS from the RCS. They are required to enable flow into the RNS and therefore are enabling the transfer of decay heat. Removal of decay heat is a Category A safety function. The hot leg suction inner isolation valves are considered Class 2. See Appendix 15A. They are also part of the RCS pressure boundary. Maintenance of the reactor coolant pressure boundary is a Category A safety function and the hot leg suction inner isolation valves are Class 1 in this respect. See, Appendix 15A.

There is one valve arranged in series with the hot leg suction outer isolation valve, discussed below, on each RNS train. Closing either the hot leg suction inner isolation valve or the hot leg suction outer isolation valve will isolate the suction line; the second valve provides thus redundancy. The requirement on the valves therefore is that they will close on demand.

RNS Hot Leg Suction Outer Isolation Valves (RNS-PL-V002A/B)

The RCS hot leg to RNS suction outer isolation valves provide isolation for the RNS from the RCS. They are required to enable flow into the RNS system and therefore are enabling the transfer of decay heat. Removal of decay heat is a Category A safety function. The hot leg suction isolation valves are considered Class 2. The valves also perform a containment isolation function and containment is also a Category A safety function. These valves are classified in this function as Class 1. See Appendix 15A. When the RNS is in service, it effectively becomes a part of the RCS pressure boundary. Maintenance of the reactor coolant pressure boundary is a Category A safety function and the hot leg suction outer isolation valves are Class 1 in this respect. See Appendix 15A.

There is one valve arranged in series with the hot leg suction inner isolation valve, discussed above, on each RNS train. Closing either the hot leg suction inner isolation valve or the hot leg suction outer isolation valve will isolate the suction line; the second valve provides redundancy. The requirement on the valves therefore is that they will close on demand.

RNS Return from CVS Containment Isolation Valves (RNS-PL-V061A/B)

The RNS return from CVS CIVs perform a containment isolation function and containment is a Category A safety function. These valves are classified in this function as Class 1. See Appendix 15A. When the RNS is in service, they effectively become a part of the RCS pressure boundary with a consequent function to contain radioactive material. Containment of radioactive material is a Category A safety function, these valves are Class 1 in this respect also. See Appendix 15A.

The requirement on the valves is that they will close on demand to meet their contribution to isolation of their associated containment penetrations.

RNS Hot Leg Suction Pressure Relief Valves (RNS-PL-V021A/B)

Each RNS hot leg suction pressure relief valve provides cold overpressure protection to the RCS and also provides overpressurisation protection to the RNS, whilst the RNS is in service. Protection of the RCS pressure boundary is a Category A safety function, these valves are deemed to be Class 1. See Appendix 15A.

The requirement on the valves is that they will open on demand when their set pressure is exceeded.

RNS Suction Header Containment Isolation Valves (RNS-PL-V022A/B)

Each RNS suction line CIV is required to open to enable flow into its corresponding RNS train and therefore is enabling the transfer of decay heat. Removal of decay heat is a Category A safety function. These valves are Class 2. The valves also perform a containment isolation function and containment is also a Category A safety function. These valves are classified in this function as Class 1. See Appendix 15A. When the RNS is in service, it effectively becomes a part of the RCS pressure boundary. Maintenance of the reactor coolant pressure boundary is a Category A safety function and the pump suction outside containment isolation valves are Class 1 in this respect. See Appendix 15A.

Each valve is on a separate containment penetration and the requirement is that they will open on demand to meet the RNS heat transfer and residual heat removal requirements and will close on demand to meet the containment isolation requirements.

RNS Discharge Containment Isolation Valves (RNS-PL-V011A/B)

The RNS discharge CIVs enable flow through the RNS and back to the RCS, and therefore are enabling the transfer of decay heat. Removal of decay heat is a Category A safety function and the pump discharge header isolation valves are Class 2. The valves also perform a containment isolation function and containment is also a Category A safety function. These valves are classified in this function as Class 1. See Appendix 15A. When the RNS is in service, it effectively becomes a part of the RCS pressure boundary. Maintaining the reactor coolant pressure boundary is a Category A safety function. Therefore, the CIVs are Class 1 in this respect. See Appendix 15A. These valves are also required to open to provide a long-term supply for makeup to containment inventory. Since this function is not needed until at least 2 to 4 weeks after an accident, it is classified as a Category B safety function and the valves are Class 2 for this function.

Each valve is on a separate containment penetration and the requirement is that they will open on demand to meet the RNS heat transfer, residual heat removal and low pressure requirements and will close on demand to meet the containment isolation requirements.

RNS Heat Exchanger Outlet Flow Control Valves (RNS-PL-V006A/B)

These valves provide part of the temperature control arrangements for the RNS under normal shutdown operations. Because the valves sit in the main RNS HX flow paths, it is important that they can be operated to enable cooling and consequent decay heat removal from the fluid passing through the RNS. Removal of decay heat is a Category A safety function and the valves are Class 2 for this function. See Appendix 15A. When the RNS is in service, it effectively becomes a part of the RCS pressure boundary. Maintenance of the reactor cooling pressure is a Category A safety function and the valves are Class 1 in this respect. See Appendix 15A. These valves are also required to open to provide a long-term supply for makeup to containment inventory. Since this function is not needed until at least 72 hours after an accident, it is classified as a Category B safety function and the valves are Class 2 for this function.

Each HX has its own flow control valve and each one will fulfil the temperature control function for its HX. The requirement is that the valve will open on demand to enable full cooling flow.

RNS Heat Exchanger Bypass Flow Control Valves (RNS-PL-V008A/B)

These valves provide part of the temperature control arrangements for the RNS under normal shutdown operations. Because the valves are in a bypass to the main RNS HX flow path, it is important that they can be operated to enable cooling and consequent decay heat removal from the fluid passing through the RNS. Removal of decay heat is a Category A safety function and the valves are Class 2 for this function. See Appendix 15A. When the RNS is in service, it effectively becomes a part of the RCS pressure boundary. Maintenance of the reactor coolant pressure boundary is a Category A safety function and the valves are Class 1 in this respect.

Each HX has its bypass flow control valve and each one will fulfil the temperature control function for that HX. The requirement is that the valve will close on demand to enable full cooling flow.

RNS Suction from IRWST CIVs (RNS-PL-V023A/B)

The IRWST to RNS suction isolation valves provide an isolation facility for the IRWST from the RNS. They are required to open to enable flow from the IRWST into the RNS and therefore are enabling the transfer of decay heat and providing a source for low-pressure injection to the RCS to maintain RCS inventory. Both of these are Category A safety functions and the valves are considered Class 2. These valves also perform a containment isolation function and containment is also a Category A safety function. These valves are classified in this function as Class 1. See Appendix 15A. When the RNS is in service, it effectively becomes a part of the RCS pressure boundary. Maintenance of the reactor coolant pressure boundary is a Category A safety function the valves are Class 1 in this respect. See Appendix 15A.

Each valve is on a separate containment penetration and the requirement is that they will open on demand to meet the RNS low-pressure injection and IRWST decay heat removal requirements, and will close on demand to meet the containment isolation requirements.

RNS Discharge to IRWST Isolation Valves (RNS-PL-V024A/B)

The RNS discharge to IRWST isolation valves provide an isolation facility for the IRWST from the RNS. They are required to enable flow back to the IRWST from the RNS and therefore are enabling the transfer of decay heat. Removal of decay heat is a Category A safety function and the valves are considered Class 2 for this function. See Appendix 15A. When the RNS is in service, it effectively becomes a part of the RCS pressure boundary. Maintenance of the reactor coolant pressure boundary is a Category A safety function and the valves are Class 1 in this respect. See Appendix 15A.

There are two isolation valves, one associated with each RNS train; the requirement is that either one will open on demand in conjunction with its corresponding IRWST suction isolation valve, to meet the RNS IRWST decay heat removal requirements.

RNS Pump Suction from Cask Loading Pit Isolation Valves (RNS-PL-V055A/B)

The cask loading pit to RNS suction isolation valves provide an isolation facility for the cask loading pit from the RNS. They are required to enable a supply of borated water to be taken from the cask loading pit to the RNS and therefore are a source of low-pressure makeup to the RCS. Maintaining reactor coolant inventory is a Category A safety function and the valves are considered Class 2 for this function. See Appendix 15A. When the RNS is in service, it effectively becomes a part of the RCS pressure boundary. Maintenance of the

reactor coolant pressure boundary is a Category A safety function and the valves are Class 1 in this respect.

There are two isolation valves, one associated with each RNS train; the requirement is that either one will open on demand to meet the RNS low-pressure injection requirements.

RNS Discharge Check CIV – IRC (RNS-PL-V013A/B)

The RNS discharge line check valves are required to open to enable the RNS to perform its decay heat removal and low-pressure injection, both of that are Category A functions and these valves are Class 2 for these functions. These valves also perform a containment isolation function and containment is also a Category A safety function. These valves are classified in this function as Class 1. See Appendix 15A. When the RNS is in service, it effectively becomes a part of the RCS pressure boundary. Maintenance of the reactor coolant pressure boundary is a Category A safety function and the valves are Class 1 in this respect. These valves are also required to open to provide a long-term supply for makeup to containment inventory. Since this function is needed no sooner than 72 hours after an accident, it is classified as a Category B safety function and the valves are Class 2 for this function.

Each valve is on a separate containment penetration and the requirement is that they close on reverse pressure with a consequent function to contain radioactive material. Containment of radioactive material is a Category A safety function and they are Class 1 in this respect. See Appendix 15A.

RNS Discharge RCS Pressure Boundary Stop Check Valves (RNS-PL-V015A/B)

The discharge RCS pressure boundary stop check valves are required to open to enable the RNS to perform its decay heat removal and low-pressure injection. These are Category A functions and these valves are Class 2 for these functions. When the RNS is out of service, these valves are the isolation point between the RNS and RCS and as a result, they are part of the RCS pressure boundary. Maintenance of the reactor coolant pressure boundary is a Category A safety function and these valves are Class 1 in this respect. See Appendix 15A. These valves are also required to open to provide a long-term supply for makeup to containment inventory. Since this function is not needed until at least 72 hours after an accident, it is classified as a Category B safety function and the valves are Class 2 for this function.

RNS Discharge RCS Pressure Boundary Check Valves (RNS-PL-V017A/B)

The discharge RCS pressure boundary check valves are required to open to enable the RNS to perform its decay heat removal and low-pressure injection, both of which are Category A functions. The valves are Class 2 for these functions. When the RNS is out of service, these valves are the isolation point between the RNS and RCS and as a result, they are part of the RCS pressure boundary. Maintenance of the reactor coolant pressure boundary is a Category A safety function and these valves are Class 1 in this respect. These valves are also required to open to provide a long-term supply for makeup to containment inventory. Since this function is not needed until at least 72 hours after an accident, it is classified as a Category B safety function and the valves are Class 2 for this function.

17.5.7.4 Justification of Claims on Components and Equipment

Normal Residual Heat Removal System Pumps (RNS-MP-01A/B)

The pressure boundary of the RNS pumps are designed to ASME Boiler and Pressure Vessel Code, Section III-3 and the RNS pump motors are designed to commercial standards. Therefore, these pumps are very similar to the design of pumps performing this duty on currently operating PWRs. As a result, the information from the operation of these in-service pumps offers a high degree of confidence about the reliability to be expected from the pumps proposed for the AP1000 design. Data collected from in-service plants (Reference 17.7, Table 5-1) indicate that the probability of failure to start is low.

The generic design of these pumps should provide high reliability. The design specification requires that manufacturers identify any specific design features that will provide support in this area. Two specific design features that have been identified that aid the achievement of high reliability in operation:

- In order to limit leakage in the unlikely event of an inter-system loss of coolant accident (IS-LOCA), the pump design includes a "disaster bushing" that is fitted adjacent to, and just outside of, the mechanical seal. The bushing provides a close fit between the pump shaft and the bearing housing and will limit any leakage in the event of mechanical seal failure. This ability is maintained even with RNS pressures in excess of normal design.

- The pumps are designed to run with 3-percent air ingestion with the pump suction without loss of performance. The pumps are also designed to accommodate 5-percent air entrainment at the pump suction but with potentially some degradation of performance.

Given the importance of the RNS pumps to the defence in depth safety functions, it is expected that routine full-flow testing will be performed with the pumps aligned to draw from and discharge to the IRWST. This testing will be carried out quarterly in accordance with the surveillance requirements for investment protection short-term availability control. The pumps will also be subject to routine overhaul and maintenance in line with the manufacturer's recommendations.

RNS Heat Exchangers (RNS-ME-01A/B)

The HXs are manufactured with stainless-steel tubes to maximise compatibility with the RCS fluid. They are designed to ASME Boiler and Pressure Vessel Code, Section III on the tube side and Section VIII, Division 1 (Reference 17.9) on the shell side. The tubes are expanded onto the tube sheet over its full depth and seal-welded in addition. This is intended to minimise the chance of leakage from the RNS side into the CCS.

The HX design is very similar to that used for this role on currently operating PWRs and as such the service experience on existing power stations is a good guide to the expected performance in the AP1000 design. Data collected from in-service plants (Reference 17.7, Table 5-1) indicate a low probability of HX fouling leading to blockage. This indicates that the claims being made are in line with operational experience.

Routine maintenance and testing of the RNS HXs will be performed according to the manufacturer's recommendations; this will include routine changeover of the HXs allocated to duty and standby roles. No specific surveillance test requirements are identified.

Hot Leg Suction Isolation – Inner Valves (RNS-PL-V001A/B)

The RCS hot leg to RNS suction inner isolation valves are motor operated, which means they will fail "as is" on loss of power. This is judged appropriate because if the RNS is in service, it is required that the valves fail open to maintain cooling; if the RNS is shut down, it is required that the valves fail closed to maintain RCS pressure boundary integrity.

The valves are manufactured from stainless steel to ensure compatibility with the reactor coolant water that passes through them. They are designed to ASME Boiler and Pressure Vessel Code, Section III-1. This code has been specifically developed to qualify pressure-retaining components in safety-significant nuclear power applications. The code, with its supporting testing and examination, provides the foundations for performance claims made on the hot leg suction inner isolation valves.

The valves are very similar to those already in like service on currently operating PWRs. As a result, the information from testing these in-service valves offers a high degree of confidence about the reliability to be expected from these valves. Data collected from in-service plants (Reference 17.7, Table 5.1) indicate a low probability of failure to open or close. This indicates that the claim being made is conservative.

The failure mechanism of concern would involve the valve sticking or jamming. This could be a result of wear, corrosion, or maintenance-induced failure. In addition to being designed to ASME Boiler and Pressure Vessel Code, Section III, the valves are also designed and installed to seismic C-I; this inside CIV is also qualified for operation in a harsh environment (Table 15A-1). The combination of the ASME Boiler and Pressure Vessel Code, Section III and other codes for design and manufacture with the test regime described below will minimise the probability of these failure mechanisms occurring. The provision of two valves in parallel further reduces the probability of failure associated with opening the valves to initiate the RNS. The presence of the hot leg suction outer isolation valves in series with these valves further reduces the probability of failure associated with isolation of the system on demand.

The maintenance and testing arrangements for the hot leg suction inner isolation valves are based on the ASME Boiler and Pressure Vessel Code, Section III programmes appropriate for these types of valves as used in existing nuclear power stations. The testing is:

- Remote position indication of these valves is observed locally during valve exercising to verify proper operation of the position indication. This position indication test is performed every 2 years.

- Full stroke exercise testing of these valves is performed during cold shutdown conditions. Opening during normal power operation may result in damage to equipment or initiation of a reactor trip. As a result, the ASME Boiler and Pressure Vessel Code rules allow a relaxation of the testing interval and these valves will be exercised only when the RNS is aligned to remove core decay heat.

- Pressure isolation leak testing of these valves is performed on these valves every 2 years. This test will be performed during normal power operation. The maximum leakage requirement for pressure isolation is included in the surveillance requirements for Tech Spec 3.4.15.

- Operability testing of these valves is performed every 10 years as part of the normal valve in-service testing programme.

- As CIVs, these are tested in accordance with the Reference 17.11 to verify seat leakage.

Hot Leg Suction Outer Isolation Valves (RNS-PL-V002A/B)

The RCS hot leg to RNS suction outer isolation valves are motor operated, which means they will fail "as is" on loss of power. This is judged appropriate because if the RNS is in service, it is required that the valves fail open to maintain cooling; if the RNS is shut down, it is required that the valves fail closed to maintain RCS pressure boundary integrity.

The valves are manufactured from stainless steel to ensure compatibility with the reactor coolant water that passes through them. They are designed to ASME Boiler and Pressure Vessel Code. This code has been specifically developed to qualify pressure-retaining components in safety-significant applications on nuclear power stations. The code, with its supporting testing and examination, provides the foundations for performance claims made on the hot leg suction outer isolation valves.

The valves are very similar to those already on currently operating PWRs. As a result, the information from testing these in-service valves offers a high degree of confidence about the reliability to be expected from the valves proposed for the AP1000 design. Data collected from in-service plants (Reference 17.7, Table 5.1) indicate a low probability of failure to open or close. This indicates that the claim being made is conservative.

The failure mechanism of concern would involve the valve sticking or jamming. This could be a result of wear, corrosion, or maintenance-induced failure. In addition to being designed to ASME Boiler and Pressure Vessel Code, Section III, the valves are also designed and installed to seismic C-I (Table 15A-1). The combination of ASME Boiler and Pressure Vessel Code, Section III, and other codes for design and manufacture with the test regime described below will minimise the probability of these failure mechanisms occurring. The provision of two valves in parallel further reduces the probability of failure associated with opening the valves to initiate the RNS. The presence of the hot leg suction inner isolation valves in series with these valves further reduces the probability of failure associated with isolation of the system on demand.

The maintenance and testing arrangements for the hot leg suction outer isolation valves are based on the ASME Boiler and Pressure Vessel Code, Section III programmes appropriate for these types of valves as used in existing nuclear power stations. The proposed testing is as follows:

- Remote position indication of these valves is observed locally during valve exercising to verify proper operation of the position indication. This position indication test is performed every 2 years.

- Full stroke exercise testing of these valves is performed during cold shutdown conditions. Opening during normal power operation may result in damage to equipment or initiation of a reactor trip. As a result, the ASME Boiler and Pressure Vessel Code rules allow a relaxation of the testing interval and these valves will be exercised only when the RNS is aligned to remove core decay heat.

- Pressure isolation leak testing of these valves is performed on these valves every 2 years. This test will be performed during normal power operation. The maximum leakage requirement for pressure isolation is included in the surveillance requirements for Tech Spec 3.4.15.

- Operability testing of these valves is performed every 10 years as part of the normal valve in-service testing programme.

As CIVs, these are tested in accordance with the Reference 17.11 to verify seat leakage.

RNS Return from CVS Containment Isolation Valves (RNS-PL-V061A/B)

The RNS returns from the CVS CIVs are air operated. They fail closed on a loss of motive air supply and hence will inherently move closed and thus fail-safe.

The valves are manufactured from stainless steel to ensure compatibility with the reactor coolant water that passes through them. They are designed to ASME Boiler and Pressure Vessel Code, Section III-2. This code has been specifically developed to qualify pressure-retaining components in safety-significant applications on nuclear power stations. The code, with the testing and examination that supports it, provides the foundations for performance claims made on the RNS return from CVS CIV.

The valves are very similar to those already in service to provide similar functions on currently operating PWRs. As a result the information from testing these in-service valves offers a high degree of confidence about the reliability to be expected from the valve proposed for the AP1000 design. The failure mechanism of concern would involve the valve sticking or jamming. This could be a result of wear, corrosion, or maintenance-induced failure. In addition to being designed to ASME III, the valves are also designed and installed to seismic C-I (Table 15A-1). The combination of ASME Boiler and Pressure Vessel Code, Section III and other codes for design and manufacture with the test regime described below will minimise the probability of these failure mechanisms occurring.

The maintenance and testing arrangements for the return from CVS CIV is based around the ASME Boiler and Pressure Vessel Code, Section III programmes appropriate for these types of valves as used in existing nuclear power stations. The testing is:

- Remote position indication of these valves is observed locally during valve exercising to verify proper operation of the position indication. This position indication test is performed every 2 years.

- Full stroke exercise testing of these valves is performed during cold shutdown conditions. Opening during normal power operation may result in damage to equipment or initiation of a reactor trip. As a result, the ASME Boiler and Pressure Vessel Code rules allow a relaxation of the testing interval and these valves will be exercised only when the RNS is aligned to remove core decay heat.

- Operability testing of these valves is performed every 10 years as part of the normal valve in-service testing programme.

- As CIVs, these are tested in accordance with the “Primary Containment Leakage Rate Test Program” specified in 10 CFR 50, Appendix J (Reference 17.11) to verify seat leakage.

RNS Hot Leg Suction Pressure Relief Valves (RNS-PL-V021A/B)

The RNS hot leg suction pressure relief valves are of the spring-loaded, self-actuated type and operation depends only upon the pressure difference across them and not on any method of powered actuation. This passive approach offers a high degree of inherent safety and reliability.

Each RNS suction line relief valve provides low-temperature overpressure protection for the RCS. Each valve is sized to limit the pressure of the RCS below the minimum pressure limit for the limiting design-basis low-temperature overpressure transients, so that protection is provided even if only one RNS train is in service. The following two limiting transients were identified as the design basis:

- **Mass injection** – Two CVS makeup pumps delivering at the RNS relief valve set pressure at the limiting conditions of circuit temperature.

- **Heat input** – Startup of an RCP with a 27.8°C (50°F) temperature difference between the RCS and the SG secondary side at the limiting conditions of circuit temperature.

The ASME Code has been specifically developed to qualify pressure-retaining components in safety-significant applications on nuclear power stations. The Code, with its supporting testing and examination, provides the foundations for performance claims made on the RNS hot leg suction pressure relief valves.

The valves are very similar to those already in service to provide the same function. The failure mechanism of concern would involve the valve sticking or jamming. This could be a result of wear, corrosion, or maintenance-induced failure. In addition to being designed to ASME Boiler and Pressure Vessel Code, Section III-2, the valves are also designed and installed to seismic C-I (Table 15A-1). The combination of ASME Boiler and Pressure Vessel Code, Section III and other codes for design and manufacture with the test regime described below will minimise the probability of these failure mechanisms occurring. This is reflective in the low temperature over pressure protection (LTOP) operability for the AP1000 design at 135°C (275°F) rather than a higher temperature (177°C [350°F]) typical to existing PWRs.

The maintenance and testing arrangements for the RNS hot leg suction pressure relief valves are based on the programmes associated with ASME Boiler and Pressure Vessel Code, Section III qualification. The proposed testing is as follows:

- Every valve should be tested as installed, or bench-tested, every 5 years.

- As CIVs, these are tested to verify seat leakage.

RNS Suction Header Containment Isolation Valves (RNS-PL-V022A/B)

The RNS suction header isolation valves are motor operated, which means they will fail "as is" on loss of power. This is judged appropriate because if the RNS is in service, it is required that the valves fail open to maintain cooling; if the RNS is shut down, it is required that the valves fail closed to maintain isolation of the containment penetration.

The valves are manufactured from stainless steel to ensure compatibility with the reactor coolant water that passes through them. They are designed to ASME Boiler and Pressure Vessel Code. This code has been specifically developed to qualify pressure-retaining components in safety-significant applications on nuclear power stations. The code, with its supporting testing and examination, provides the foundations for performance claims made on the RNS suction header CIVs.

The valves are very similar to those already in service to provide the same function. The failure mechanism of concern would involve the valve sticking or jamming. This could be a result of wear, corrosion, or maintenance-induced failure. In addition to being designed to ASME Boiler and Pressure Vessel Code, Section III, the valves are also designed and

installed to seismic C-I (Table 15A-1). The combination of ASME Boiler and Pressure Vessel Code, Section III and other codes for design and manufacture with the test regime described below will minimise the probability of these failure mechanisms occurring.

The maintenance and testing arrangements for the pump suction header isolation valve are based on the ASME Boiler and Pressure Vessel Code, Section III programmes appropriate for these types of valves as used in existing nuclear power stations. The proposed testing is as follows:

- Remote position indication of these valves is observed locally during valve exercising to verify proper operation of the position indication. This position indication test is performed every 2 years.

- Full stroke exercise testing of these valves is performed during cold shutdown conditions. Opening during normal power operation may result in damage to equipment or initiation of a reactor trip. As a result, the ASME Boiler and Pressure Vessel Code rules allow a relaxation of the testing interval and these valves will be exercised only when the RNS is aligned to remove core decay heat.

- Operability testing of these valves is performed every 10 years as part of the normal valve in-service testing programme.

- As CIVs, these are tested in accordance with the "Primary Containment Leakage Rate Test Program" specified in 10 CFR 50, Appendix J (Reference 17.11) to verify seat leakage.

RNS Discharge Containment Isolation Valves (RNS-PL-V011A/B)

The RNS discharge CIVs are motor operated, which means they will fail "as is" on loss of power. This is judged appropriate because if the RNS is in service, it is required that the valves fail open to maintain cooling; if the RNS is shut down, it is required that the valves fail closed to maintain isolation of the containment penetration.

The valves are manufactured from stainless steel to ensure compatibility with the reactor coolant water that passes through them. They are designed to ASME Boiler and Pressure Vessel Code, Section III-2. This code has been specifically developed to qualify pressure-retaining components in safety-significant applications on nuclear power stations. The code, with its supporting testing and examination, provides the foundations for performance claims made on the RNS discharge CIV.

The valves are very similar to those already in like service on currently operating PWRs. As a result, the information from testing these in-service valves offers a high degree of confidence about the reliability to be expected from these valves. Data collected from in-service plants (Reference 17.7, Table 5.1) indicate low probability of failure to open or close. This indicates that the claim being made is conservative.

The failure mechanism of concern would involve the valve sticking or jamming. This could be a result of wear, corrosion, or maintenance-induced failure. In addition to being designed to ASME Boiler and Pressure Vessel Code, Section III, the valves are also designed and installed to seismic C-I (Table 15A-1). The combination of ASME Boiler and Pressure Vessel Code, Section III and other codes for design and manufacture with the test regime described below will minimise the probability of these failure mechanisms occurring.

The maintenance and testing arrangements for the pump discharge header isolation valve are based on the ASME Boiler and Pressure Vessel Code, Section III programmes appropriate for these types of valves as used in existing nuclear power stations. The testing is:

- Remote position indication of these valves is observed locally during valve exercising to verify proper operation of the position indication. This position indication test is performed every 2 years.

- Full stroke exercise testing of these valves is performed during cold shutdown conditions. Opening during normal power operation may result in damage to equipment or initiation of a reactor trip. As a result, the ASME Boiler and Pressure Vessel Code rules allow a relaxation of the testing interval and these valves will be exercised only when the RNS is aligned to remove core decay heat.

- Operability testing of these valves is performed every 10 years as part of the normal valve in-service testing programme.

- As CIVs, these are tested in accordance with the "Primary Containment Leakage Rate Test Program" specified in 10 CFR 50, Appendix J (Reference 17.11) to verify seat leakage.

RNS Heat Exchanger Outlet Flow Control Valves (RNS-PL-V006A/B)

The RNS HX flow control valves are air operated and fail open on loss of air. This ensures that they fail to the position providing maximum cooling and so is inherently safe.

The valves are manufactured from stainless steel to ensure compatibility with the reactor coolant water that passes through them. They are designed to ASME Boiler and Pressure Vessel Code, Section III-3. This code has been specifically developed to qualify pressure-retaining components in safety-significant applications on nuclear power stations. The code, with its supporting testing and examination, provides the foundations for performance claims made on the RNS HX flow control valves.

Whilst routine maintenance and inspection of the RNS HX flow control valves will be performed according to the manufacturer's recommendations, no specific surveillance test requirements are specified.

RNS Heat Exchanger Bypass Flow Control Valves (RNS-PL-V008A/B)

The RNS HX bypass flow control valves are air operated and fail closed on loss of air. This ensures that they fail to the position that provides maximum cooling and so is inherently safe.

The valves are manufactured from stainless steel to ensure compatibility with the reactor coolant water that passes through them. They are designed to ASME Boiler and Pressure Vessel Code, Section III-3.

Routine maintenance and inspection of the RNS HX bypass flow control valves will be performed according to the manufacturer's recommendations, no specific surveillance test requirements are specified.

RNS Suction from IRWST Containment Isolation Valves (RNS-PL-V023A/B)

The IRWST suction isolation valves are motor operated, which means they will fail "as is" on loss of power. This is judged appropriate because if the RNS is in service cooling the

IRWST, it is required that the valves fail open to maintain cooling; if the RNS is shut down, it is required that the valves fail closed to maintain IRWST isolation and containment isolation.

The valves are manufactured from stainless steel to ensure compatibility with the reactor coolant water that passes through them. They are designed to ASME Boiler and Pressure Vessel Code, Section III-2.

The valves are very similar to those already in like service on currently operating PWRs. As a result, the information from testing these in-service valves offers a high degree of confidence about the reliability to be expected from these valves. Data collected from in-service plants (Reference 17.7, Table 5.1) indicate that the claim being made is conservative.

The failure mechanism of concern would involve the valve sticking or jamming. This could be a result of wear, corrosion, or maintenance-induced failure. In addition to being designed to ASME Boiler and Pressure Vessel Code, Section III, the valves are also designed and installed to seismic C-I (Table 15A-1).

Although the generic design of these valves should provide high reliability, the design specification requires that manufacturers identify any specific design features that will provide support in this area.

The maintenance and testing arrangements for the IRWST suction isolation valves are based on the ASME programmes appropriate for these types of valves as used in existing nuclear power stations. The testing is:

- Remote position indication of these valves is observed locally during valve exercising to verify proper operation of the position indication. This position indication test is performed every 2 years.

- Full stroke exercise testing of these valves is performed during cold shutdown conditions. Opening during normal power operation may result in damage to equipment or initiation of a reactor trip. As a result, the ASME Boiler and Pressure Vessel Code rules allow a relaxation of the testing interval and these valves will be exercised only when the RNS is aligned to remove core decay heat.

- Operability testing of these valves is performed every 10 years as part of the normal valve in-service testing programme.

- As CIVs, these are tested in accordance with the Reference 17.11 to verify seat leakage.

RNS Discharge to IRWST Isolation Valves (RNS-PL-V024A/B)

The IRWST discharge isolation valves are motor operated, which means they will fail “as is” on loss of power. This is judged appropriate because if the RNS is in service cooling the IRWST, it is required that the valves fail open to maintain cooling; if the RNS is shut down, it is required that the valves fail closed to maintain IRWST isolation.

The valves are manufactured from stainless steel to ensure compatibility with the reactor coolant water that passes through them. They are designed to ASME Boiler and Pressure Vessel Code, Section III-3.

The valves are very similar to those already in like service on currently operating PWRs. As a result, the information from testing these in-service valves offers a high degree of confidence

about the reliability to be expected from these valves. Data collected from in-service plants (Reference 17.7, Table 5.1) indicate that the claim being made is conservative.

The failure mechanism of concern would involve the valve sticking or jamming. This could be a result of wear, corrosion, or maintenance-induced failure. In addition to being designed to ASME Boiler and Pressure Vessel Code, Section III, the valves are also designed and installed to seismic C-I (Table 15A-1).

Routine maintenance and inspection of the IRWST discharge isolation valves will be performed according to the manufacturer's recommendations, no specific surveillance test requirements are specified.

RNS Pump Suction from Cask Loading Pit Isolation Valves (RNS-PL-V055A/B)

The cask loading pit suction isolation valves are motor operated, which means they will fail "as is" on loss of power. This is judged appropriate because if the RNS is in service injecting water from the cask loading pit, it is required that the valves fail open to maintain cooling. If the RNS is shut down, it is required that the valves fail closed to maintain cask loading pit isolation.

The valves are manufactured from stainless steel to ensure compatibility with the reactor coolant water that passes through them. They are designed to ASME Boiler and Pressure Vessel Code, Section III-3.

The valves are very similar to those already in like service on currently operating PWRs. As a result, the information from testing these in-service valves offers a high degree of confidence about the reliability to be expected from these valves. Data collected from in-service plants (Reference 17.7, Table 5.1) indicate that the claim being made is conservative.

The failure mechanism of concern would involve the valve sticking or jamming. This could be a result of wear, corrosion, or maintenance-induced failure. In addition to being designed to ASME Boiler and Pressure Vessel Code, Section III, the valves are also designed and installed to seismic C-I (Table 15A-1).

Routine maintenance and inspection of the cask loading pit suction isolation valves will be performed according to the manufacturer's recommendations, no specific surveillance test requirements are specified.

RNS Discharge Check Valves CIV – IRC (RNS-PL-V013A/B)

The operation of the discharge check valves depends only upon the pressure difference across them and not on any method of powered actuation. This passive approach offers a high degree of inherent safety and reliability.

The valves are manufactured from stainless steel to ensure compatibility with the borated RCS fluid that is in contact with them. They are designed to ASME Boiler and Pressure Vessel Code, Section III-2.

The valves are very similar to those already in like service on many operating power stations. As a result, the information from testing these in-service valves offers a high degree of confidence about the reliability to be expected from these valves. Data collected from in-service plants (Reference 17.7, Table 5.1) indicate a value that is an order of magnitude better than the value assumed in the PSA.

The maintenance and testing arrangements for the discharge check valve are based on the programmes appropriate for these types of valves as used in existing nuclear power stations. The testing is:

- To exercise these valves closed requires draining of the associated piping and performing a backflow leakage test. This testing would impose undue personnel radiation exposure and place the RNS in an undesirable operational configuration. As a result, the ASME Boiler and Pressure Vessel Code rules allow a relaxation and these valves will be fully stroke-tested during refuelling shutdowns.

- As CIVs, these are tested in accordance with the "Primary Containment Leakage Rate Test Program" specified in 10 CFR 50, Appendix J (Reference 17.11), to verify seat leakage.

RNS Discharge RCS Pressure Boundary Stop Check Valves (RNS-PL-V015A/B)

The operation of the RNS discharge RCS pressure boundary stop check valves depends only upon the pressure difference across them and not on any method of powered actuation. This passive approach offers a high degree of inherent safety and reliability.

The valves are manufactured from stainless steel to ensure compatibility with the borated RCS fluid that is in contact with them. They are designed to ASME Boiler and Pressure Vessel Code, Section III-1.

The valves are very similar to those already in like service on many operating power stations. As a result, the information from testing these in-service valves offers a high degree of confidence about the reliability to be expected from these valves. Data collected from in-service plants (Reference 17.7, Table 5.1) do not differentiate between stop check valves and swing check valves, but for check valves indicate values that are an order of magnitude better than the values assumed in the PSA.

The maintenance and testing arrangements for the discharge RCS pressure boundary stop check valve are based on the programmes appropriate for these types of valves as used in existing nuclear power stations. The testing is:

- The maximum leakage requirement for pressure isolation is included in the surveillance requirements for Tech Spec 3.4.15.

RNS Discharge RCS Pressure Boundary Check Valves (RNS-PL-V017A/B)

The operation of the RNS discharge RCS pressure boundary check valves depends only upon the pressure difference across them and not on any method of powered actuation. This passive approach offers a high degree of inherent safety and reliability.

The valves are manufactured from stainless steel to ensure compatibility with the borated RCS fluid that is in contact with them. They are designed to ASME Boiler and Pressure Vessel Code, Section III-1.

The valves are very similar to those already in like service on many operating power stations. As a result, the information from testing these in-service valves offers a high degree of confidence about the reliability to be expected from these valves. Data collected from in-service plants (Reference 17.7, Table 5.1) indicate values that are an order of magnitude better than the values assumed in the PSA and indicate that the claims against these valves are conservative.

The maintenance and testing arrangements for the discharge RCS pressure boundary check valve are based on the programmes appropriate for these types of valves as used in existing nuclear power stations. The testing is:

- To exercise these valves closed requires draining of the associated piping and performing a backflow leakage test. This testing would impose undue personnel radiation exposure and place the RNS in an undesirable operational configuration. As a result, the ASME Boiler and Pressure Vessel Code rules allow a relaxation and these valves will be fully stroke-tested during refuelling shutdowns.

- Pressure isolation leak testing of these valves is performed on these valves every 2 years. The maximum leakage requirement for pressure isolation is included in the surveillance requirements for Tech Spec 3.4.15.

17.6 Containment

17.6.1 Passive Containment Cooling

17.6.1.1 Role

A detailed description of the passive containment cooling system (PCS) is given in Section 6.6. Further design details of this system and its constituent components are delineated in Reference 17.27.

The PCS is designed to limit and reduce containment pressure following a containment pressurisation event and provide the ultimate heat sink for long-term RCS decay heat removal following accidents. The system supports the heat transfer/residual heat removal primary safety function.

For intact RCS faults where the IRWST boils or where a LOCA or steam line break releases steam directly into containment, the steam circulates by natural convection and condenses on the inside surface of the containment shell which is being cooled by the operation of the PCS. Heat is transferred through the containment vessel by conduction and is dispersed to the atmosphere outside by convection. To enhance the external heat transfer process, water is released from the passive containment cooling water storage tank (PCCWST), which contains sufficient water for 72 hours (three days) of operation. This water flows over the external surface of the containment, is heated, and through evaporation provides a high heat transfer rate. The resulting humid air is swept into the atmosphere by the natural circulation.

The passive containment cooling ancillary water storage tank (PCCAWST) exists as an additional, dedicated, on-site source of make-up water to the containment shell or to the PCS PCCWST and hence allow the system to operate beyond the 72 hours for which the PCCWST is sized. The PCCAWST provides enough water for the plant between 72 hours and 7 days. If the PCCAWST is not available or after 7 days condenser cooling water from the river or sea (or other onsite source) can be used to provide PCS makeup.

The PCS is supported by the essential electrical system in the provision of its safety function.

The PCS supports the PXS decay heat removal function by transferring core decay heat to the environment, and condensing steam on the inside containment shell which is returned to the IRWST. The PCS also supports spent fuel cooling since the PCS PCCWST water can be used for makeup to the SF pool when the decay heat of the fuel inside containment is less than or equal to a set amount and no ac electrical power is available. The PCS also provides a

seismically qualified source of water for the fire protection system (FPS) for use on fires in safety Category A, Class 1 equipment in the non-radiological portion of the auxiliary building. This water source is contained in the PCCWST and is a limited quantity to preclude the possibility of the FPS water flooding and disabling the Class 1 SSCs in this portion of the auxiliary building.

17.6.1.2 System Components and Equipment Contributing to Safety Function

The containment vessel itself is a large pressure vessel and is discussed further in the structural integrity section of this PCSR (Chapter 20). The following PCS components contribute to it fulfilling its safety function:

- **PCCWST (PCS-MT-01)** – This is a stainless-steel-lined concrete tank. It is supported by the top of the shield building above the containment vessel and is intended to provide the source of water, by gravity flow, for passive evaporative cooling of the containment vessel outer surface for at least 72 hours. This is a safety requirement.

- **Recirculation Heater (PCS-MB-01)** – This is a 100-kW electrical heater provided in the PCCWST recirculation path. The heater assembly is constructed from stainless steel and the heater element sheaths from Inconel. The safety requirement is to transfer heat to the PCCWST water to ensure that it does not freeze. The heater is required to maintain the water in the PCCWST in a suitable condition to meet its safety requirement but the heater itself is not required to be available for the PCCWST to operate. Further analysis is therefore not required.

- **PCS Recirculation Pumps (PCS-MP-01A/B)** – These are electrically driven centrifugal constructed from stainless steel. They recirculate the water in the PCCWST to ensure that it is maintained in a homogeneous condition (chemistry and temperature). They can also be used as one way to pump water up to the PCCWST to allow it to maintain cooling duty beyond the 72 hours provided for by the tank storage capacity. The safety requirement of the pumps is to provide this capability to maintain PCS cooling duty beyond 72 hours. The recirculation pump is not required to be available for the PCCWST to operate. If it is unavailable after 72 hours, offsite diesel powered pumps can be used in its stead. Further analysis is therefore not required.

- **Water Distribution Bucket and Weir (PCS-MT-03, MT-04)** – The bucket is stainless-steel. There are 16 equally spaced slots around the circumference of the vessel. The bucket is positioned above the centre of the top of the containment dome to ensure that the PCS water flow is evenly distributed into eight radial sectors at the centre of the dome. The PCS includes two water distribution weirs which include a selection of divider plates and dams secured to the top of the containment dome below the bucket. These are arranged to spread the water flow relatively evenly so that it passes down over the containment outer surface in a thin film. This is a safety requirement as it maximises the heat transfer through evaporation.

- **PCCAWST (PCS-MT-05)** – This is a cylindrical carbon steel tank that is situated at ground level and its contents can be pumped to the PCCWST by the recirculation pumps. The safety requirement for the tank is to provide makeup to extend the operation of the PCS beyond 72 hours. Note that site water (river / sea) can be used for this function if this tank is not available.

- **PCCWST Outlet Air-Operated Isolation Valves (PCS-PL-V001A/B)** – These are 150-mm DN (6-inch), air-operated butterfly valves that fail open on loss of air supplies.

The valves are normally closed and open on receipt of a PMS containment cooling actuation signal. There is also a separate, single solenoid-operated air valve, driven from the DAS that can be energised to dump the air supply and provides an alternate method to open these valves. The safety requirement is to enable the water contained in the PCCWST to be discharged onto the outside surface of the containment vessel.

- **PCCWST outlet motor-operated isolation valve (PCS-PL-V001C)** – This is a 150-mm DN (6-inch), motor-operated gate valve that fails "as is" on loss of power. The valve is normally closed and opens on receipt of a containment cooling actuation signal from either the PMS or the DAS. The safety requirement is to enable the water contained in the PCCWST to be discharged onto the outside surface of the containment vessel.

- **PCCWST outlet motor-operated line isolation valves (PCS-PL-V002A/B/C)** – These are 150-mm DN (6-inch), motor-operated gate valves that fail "as is" on loss of electrical power. The valves are required to be open for their respective PCCWST isolation valves to perform their safety function. With the reactor at power, they are left in their open position with the actuator power supplies isolated. They do, however, also receive a confirmatory open signal from the PMS. Further analysis is therefore not required.

17.6.1.3 Claims on Components and Equipment

Passive Containment Cooling Water Storage Tank (PCS-MT-01)

The PCCWST provides the source of water to enable passive cooling of the containment and is instrumental in establishing a heat sink for decay heat removal. Decay heat removal is a Category A safety function and the tank is Class 1. See Appendix 15A.

The requirement is that the tank will provide enough water to ensure that sufficient evaporative cooling from the external surface of the containment vessel is maintained for at least 72 hours.

Recirculation Heater (PCS-MB-01)

The heater reduces the probability of requiring the use of offsite SSCs to maintain Category A safety functions after 72 hours following an accident by precluding freezing of the PCCAWST tank after 72 hours following an accident. This a category B function and the heater is Class 2.

PCS Recirculation Pumps (PCS-MP-01A/B)

The pumps provide means to supply water to Containment and/or the Spent Fuel Pool after 72 hours following an accident. Maintenance of a Category A safety function beyond 72 hours is a Category B safety function and the pumps are Class 2. See Appendix 15A.

Water Distribution Bucket and Weir (PCS-MT-03, MT-04)

The water distribution bucket and weirs ensure that water from the PCCWST is correctly distributed on the surface of the containment vessel to ensure that adequate cooling by evaporation is available for removal of decay heat. Decay heat removal is a Category A safety function and the water distribution bucket and weirs are Class 1. See Appendix 15A.

Passive Containment Cooling Ancillary Water Storage Tank (PCS-MT-05)

The PCCAWST provides the source of water to enable passive cooling of the containment, for decay heat removal, to be provided beyond 72 hours. Maintenance of a Category A safety function beyond 72 hours is a Category B safety function and the PCCAWST is Class 2. See Appendix 15A.

PCCWST Outlet Air-Operated Isolation Valves (PCS-PL-V001A/B)

The PCCWST outlet air-operated, fail-open, isolation valves open to initiate flow from the PCCWST over the outside surface of containment to establish cooling and decay heat removal. Decay heat removal is a Category A safety function. These valves are Class 1. See Appendix 15A.

There are three isolated flow paths from the PCCWST that supply water to the distribution bucket from a common PCCWST outlet discharge header. As such, any one of the three PCCWST outlet isolation valves (these two air operated valves or the diverse motor operated isolation valve, discussed below) opening will satisfy the safety function, provided its associated line isolation valve is also open.

PCCWST Outlet Motor-Operated Isolation Valve (PCS-PL-V001C)

The PCCWST outlet motor-operated isolation valve opens to initiate flow from the PCCWST over the outside surface of containment to establish cooling and decay heat removal. Decay heat removal is a Category A safety function. This valve is Class 1. See Appendix 15A.

There are three isolated flow paths from the PCCWST that supply water to the distribution bucket from a common PCCWST outlet discharge header. As such, any one of the PCCWST outlet isolation valves opening (this motor-operated valve or the diverse air-operated valves, discussed above) will satisfy the safety function, provided its associated line isolation valve is also open.

PCCWST outlet motor-operated line isolation valves (PCS-PL-V002A/B/C)

With the reactor at power, they are left in their open position with the actuator power supplies isolated. They must maintain their position to allow flow to initiate flow from the PCCWST over the outside surface of containment to establish cooling and decay heat removal. Decay heat removal is a Category A safety function. This valve is Class 1. See Appendix 15A.

There are three isolated flow paths from the PCCWST that supply water to the distribution bucket from a common PCCWST outlet discharge header. As such, any one of the PCCWST outlet isolation valves opening (this motor-operated valve or the diverse air-operated valves, discussed above) will satisfy the safety function, provided its associated line isolation valve is also open.

17.6.1.4 Justification of Claims on Components and Equipment

Passive Containment Cooling Water Storage Tank (PCS-MT-01)

The PCCWST provides a large quantity of water above the containment vessel that can be released to flow by gravity and provide evaporative heat transfer to the ultimate heat sink. It is entirely passive in nature and requires no pumps or mechanical fluid circulation devices to operate. This confers a high degree of inherent safety.

The tank is manufactured from concrete and is lined with stainless steel. It is built to American Concrete Institute (ACI) standards.

The tank has four connections to the outlet pipework arranged at different levels within the tank. All the outlet pipes have separate screens that protect the pipe from being blocked by debris. When recirculated, the water in the tank is very slowly circulated which will result in foreign objects settling in the tank. When activated for containment cooling, the outlet flow from the tank only results in very slow water velocity in and at the bottom of this large tank Settled debris will not be swept to even the lowest of the four outlets. This lowest outlet is elevated above the bottom of the tank to prevent debris from directly flowing into the outlet. Therefore, loss of water flow due to blockage within the PCCWST is considered to be highly unlikely. In the unlikely event that the lower screen becomes plugged, it is estimated that the PCS water will be supplied from the higher level pipes at a lower flow rate for at least 40 hours even with a completely blocked lower screen.

The maintenance and testing programme is fulfilled through the Tech Spec surveillance requirements:

- The PCCWST stored water volume and stored water temperature will be verified every 7 days.

- The capability of the tank to meet water supply requirements will be demonstrated as part of the surveillance testing programme every 10 years.

PCS Recirculation Pumps (PCS-MP-01A/B)

These are industry standard pumps constructed to Hydraulic Standards Institute with a long history of reliability. These components included in the design reliability assurance programme (D-RAP) program (see Chapter 5). which provides confidence that availability is designed into the plant and that availability is maintained throughout plant life. The PCS Reciculation Pumps are intended to provide water to support the PCS in the period beyond 72 hours from its initiation. This timescale is considered to provide adequate time to address issues associated with operation of the pumps and therefore no specific justification is required to support this requirement.

Water Distribution Bucket and Weirs (PCS-MT-03, MT-04)

The water distribution bucket and weirs are passive fixtures above and on the top of the containment vessel. Their function is based entirely on the inherent physical properties of water and water flow and therefore there is a very high confidence that they will function as designed.

The PCS water distribution weirs are used to ensure effective wetting of the dome and vertical sides of the containment shell. The weirs are of limited height and would, in a relatively short time (minutes), be flooded and overflow; therefore, they cannot completely block water flow. The weirs are sectored such that partial blockage of one weir will only affect at most 1/16 of the shell. The nature of the system, and thus sensitivity to shell coverage, is not significant; hence, loss of heat transfer capacity due to a reduction in wetted area as a result of water blockage of the weir is considered to be highly unlikely. The maintenance and testing programme is fulfilled through the Tech Spec surveillance requirements:

- The capability of the water bucket and weirs to meet water supply requirements will be demonstrated as part of the surveillance testing programme every 10 years.

Passive Containment Cooling Ancillary Water Storage Tank (PCS-MT-05)

The PCCAWST is intended to provide water to support the PCS in the period beyond 72 hours from its initiation. This timescale is considered to provide adequate time to address issues associated with operation of the PCCAWST and therefore no specific justification is required to support this requirement.

17.6.1.5 Passive Containment Cooling Water Storage Tank Outlet Air-Operated Isolation Valves (PCS-PL-V001A/B)

The PCCWST outlet air-operated isolation valves are designed to fail open in the event of loss of air supply. This is an inherently safe mechanism, meaning that only in the event of a valve sticking will there be a failure to a condition other than safe.

The valves are manufactured from stainless steel to ensure compatibility with PCCWST water that is in contact with them. They are designed to ASME Boiler and Pressure Vessel Code, Section III-3.

The valves are very similar to those already in like service in many operating power stations. As a result the information from testing these in-service valves offers a high degree of confidence about the reliability to be expected from these valves. Data collected from in-service plants (Reference 17.7, Table 5.1) indicate a probability of a failure to open is comparable to the value being claimed.

The failure mechanism of concern would involve a valve sticking or jamming. This could be a result of wear, corrosion, or maintenance-induced failure. In addition to being designed to ASME Boiler and Pressure Vessel Code, Section III, the valves are also designed and installed to seismic C-I.

The maintenance and testing arrangements for the PCCWST outlet air-operated isolation valves are based on the programmes appropriate for these types of valves as used in existing nuclear power stations. The testing is:

- A full stroke operability test is performed quarterly in accordance with ASME Boiler and Pressure Vessel Code.
- Visual confirmation of valve operation during the stroke testing is performed every 2 years.
- A system flow test is performed every 10 years and this will confirm valve operating performance.

PCCWST Outlet Motor-Operated Isolation Valve (PCS-PL-V001C)

The PCCWST outlet motor-operated isolation valve is designed to offer a diversity of actuation to its air operated counterparts. It is a gate valve as opposed to butterfly valves to offer diversity of valve design also. This serves to maximise the reliability such that the PCCWST water supply function can be provided.

The valve is manufactured from stainless steel to ensure compatibility with PCCWST water that is in contact with them. It is designed to ASME Boiler and Pressure Vessel Code, Section III-3.

The valve is very similar to those already in like service on many operating power stations. As a result, the information from testing these in-service valves offers a high degree of confidence about the reliability to be expected from the valve proposed for the AP1000 design. Data collected from in-service plants (Reference 17.7, Table 5.1) indicate a probability of failure to open is comparable to the value being claimed.

The failure mechanism of concern would involve a valve sticking or jamming. This could be a result of wear, corrosion, or maintenance-induced failure. In addition to being designed to ASME Boiler and Pressure Vessel Code, Section III, the valve is also designed and installed to seismic C-I.

The maintenance and testing arrangements for the PCCWST outlet motor-operated isolation valve are based on the programmes appropriate for these types of valves as used in existing nuclear power stations. The testing is:

- A full stroke operability test is performed quarterly in accordance with ASME Boiler and Pressure Vessel Code.
- Visual confirmation of valve operation during the stroke testing is performed every 2 years.
- A system flow test is performed every 10 years and this will confirm valve operating performance.

17.6.2 Containment Isolation

17.6.2.1 Role

A detailed description of the containment isolation system is given in Section 6.7. Further design details of this system and its constituent components are delineated in Reference 17.28.

The provision of a containment structure is key to supporting the primary safety function of containment. The structural integrity issues surrounding the containment vessel are covered in Chapter 20, but the provision of containment isolation facilities for the individual process lines that pass through the containment boundary are discussed here and elsewhere in this PCSR.

Most fluid system penetrations through the containment boundary are equipped with a CIV inside the containment itself, and a CIV situated external to the containment. In some cases, there is a single valve and the pipework itself represents the containment boundary (e.g., the SG and main steam lines). Where pipework branches are adjacent to the penetration, there may be more than one line that requires isolation to achieve the safety function. As a result, on some systems there may be more than one inside CIV or outside CIV. Isolation of the flow path at either the inside or outside location(s), along with integrity of the fluid system pipework, will ensure that the individual contribution to the containment safety function of that penetration is ensured.

For the systems that provide other safety functions and are addressed elsewhere in Chapters 17 and 23, the safety requirement of the CIVs and justification of this requirement are discussed in the individual system sections.

This section addresses the remaining valves where there are CIVs that have a safety function but the rest of the system does not.

The containment isolation system is supported by the essential electrical system in achieving its safety function.

The containment isolation system does not support other systems in the achievement of their safety functions.

17.6.2.2 System Components and Equipment Contributing to Safety Function

The isolation of containment is established with provision of internal and external isolation valves for fluid systems, or by the fitting of an access hatch for personnel and equipment entry points.

The isolation valves are all sized to match the system pipework associated with the containment penetration; the valve type is selected to match the fluid, and conditions under which isolation is required, for each system. A full list of containment penetrations and associated isolation valves is given in Table 15A-1.

17.6.2.3 Claims on Components and Equipment

Isolation Valves

All CIVs are required to close to isolate the respective penetrations and contribute to the establishment of containment integrity. Preventing the release of radioactive material from the containment is a Category A safety function. See Appendix 15A. In all cases, the CIVs are Class 1. See Appendix 15A.

Each penetration has inner and outer isolation valves and closing either valve will achieve the safety function (if there is branched pipework, then all of the valves providing either the inner or the outer isolation must close). The requirement is therefore that for each penetration, at least one valve, or set of valves, must close.

Access Hatches (CNS-MY-Y01, Y02, Y03, Y04)

The access hatches provide the containment boundary for the passage of equipment, maintenance and personnel. Preventing the release of radioactive material from the containment is a Category A safety function. See Appendix 15A. In all cases, the containment access hatches are Class 1. See Appendix 15A.

The two equipment and maintenance hatches will remain in place at all times during power operation and the requirement is that they will have been fitted, following use, in such a way to provide adequate leak tightness. The two personnel hatches are each comprised of two interlocked doors. These hatches may be used during power operation but at least one of the two doors is always closed in order to provide adequate leak tightness.

17.6.2.4 Justification of Claims on Components and Equipment

Isolation Valves

The air-operated CIVs fail closed and so will fail safe. This is justified for systems when inadvertent isolation due to actuator faults can be tolerated. The motor-operated valves will fail “as is” and therefore not in a position that is necessarily safe in respect to containment isolation. This is justified for systems where inadvertent operation due to actuator faults would, in itself, give rise to safety concerns associated with the system involved.

The valves are all designed to ASME Boiler and Pressure Vessel Code, Section III-2. They are also designed to seismic C-I requirements.

The valves are very similar to those already in like service on many operating power stations. As a result, the information from testing these in-service valves offers a high degree of confidence about the reliability to be expected from these valves. Data collected for in-service plants (Reference 17.7, Table 5.1) are comparable to the values being claimed.

Testing of containment isolation equipment is performed in accordance with Reference 17.11:

- A local leak rate test (LLRT) of an individual penetration where test connections are used to pressurise the individual penetration and confirm that leakage remains within acceptable limits.
- An ILRT where the whole containment building is pressurised to confirm that leakage remains within acceptable limits.

The frequency of these tests is governed by Tech Specs.

Access Hatches (CNS-MY-Y01, Y02, Y03, Y04)

The access hatch penetrations are all designed to ASME Boiler and Pressure Vessel Code, Section III, NE (MC). They are also designed to seismic C-I requirements.

Testing of containment isolation equipment is performed in accordance with Reference 17.11:

- LLRT of an individual penetration where test connections are used to pressurise the individual penetration and confirm that leakage remains within acceptable limits.
- ILRT where the whole containment building is pressurised to confirm that leakage remains within acceptable limits.

The frequency of these tests is governed by Tech Specs.

17.7 Light Load Handling Systems

17.7.1 Refuelling Machine (FHS-FH-01)

17.7.1.1 Role

A detailed description of the refuelling machine is given in Section 6.12. Further design details of the Fuel Handling System (FHS) and its constituent components are delineated in Reference 17.29.

The refuelling machine is required to move new and spent nuclear fuel between the reactor vessel and the fuel transfer system in containment. The system contributes to the containment primary safety function by ensuring that all movement of fuel is carried out with minimum risk of damaging fuel cladding directly, or in such a way that damage could become apparent during either further handling or irradiation. In this way, the opportunity for release of radioactive material is minimised.

The refuelling machine is also designed so that, when handling irradiated fuel assemblies during operation, there will always be an adequate depth of water to maintain adequate shielding of staff on the refuelling machine gantry.

The main hazard to containment integrity, and hence to maintenance of the primary safety function, comes from either dropping fuel assemblies or driving them into obstacles through incorrect operation of the handling equipment. The protection from these hazards comes from appropriate design of the handling equipment itself and the provision of appropriate interlocks to control fuel handling movements. The provision of interlocks is through a mixture of electrical and mechanical means.

The refuelling machine is not supported by other systems in the provision of its safety functions. It does not support other systems in the provision of their safety functions.

17.7.1.2 System Components and Equipment Contributing to Safety Function

The refuelling machine is designed in accordance with the guidelines of the American Nuclear Society (ANS) (Reference 17.13). This specifies a number of necessary design features and the following subsystems are critical in ensuring that the system can support its safety function:

- **Mast hoist** – The mast hoist has numerous redundent features complient with Reference 17.14, such as with wire ropes and redundant braking systems designed to hold loads up to 150 percent of the rated load. The safety requirement of the mast hoist is to minimise the risk of fuel assembly damage, and consequently the challenge to fuel cladding integrity, through being dropped.

- **Mast** – The mast itself has two parts: the inner mast and outer mast that together form a telescopic assembly to hold a fuel assembly during transport around the refuelling cavity in containment. Guide bars in the outer mast are designed to restrain a fuel assembly at each corner of the fuel. This effectively “sheaths” the fuel during transit from the reactor to the fuel transfer mechanism. The safety requirement is therefore to protect fuel from any impact during traversing operations. The design of the inner mast provides an attachment point for the gripper assembly. This is also a safety requirement.

- **Gripper** – The gripper engages the mast hoist mechanism onto the top of the fuel assembly. The gripper is designed to “float” so that misalignment with the fuel assembly can be accommodated to allow the four engagement fingers to correctly latch onto the fuel assembly. The design is such that once the weight of the fuel assembly is being born by the gripper; it holds the gripper in the “latched” position and prevents release of the fuel assembly. The safety requirement of the gripper is to minimise the risk of fuel assembly damage, and consequently the challenge to fuel cladding integrity, through it being dropped.

- **Bridge and trolley** – The bridge and trolley provide the capability to move the mast around the refuelling cavity in the containment building. They are designed in accordance with applicable portions of Crane Manufacturers Association of America specification 70 for class A service. The design provides numerous interlocks to prevent traversal into inappropriate areas, and the machine is designed with appropriate restraints to ensure that it remains in position in the event of a seismic disturbance. The safety requirement of the bridge and trolley is to ensure that fuel movements are confined to areas of the refuelling cavity where there is no risk of damage to the fuel assembly by impact.

- **Monorail hoist** – The monorail hoist is used to support the control rod drive shaft unlatching tool and various other long-handle tools. The safety requirement is to ensure that fuel in the reactor vessel is not damaged as a result of this tool being dropped. However, all of the tools are sufficiently light that, even if dropped, it could not cause damage to fuel. There is therefore no further analysis of the monorail hoist.

17.7.1.3 Claims on Components and Equipment

Mast Hoist

The mast hoist is required to ensure that there is no damage to a lifted fuel assembly from being dropped. Protecting against damage to the integrity of spent fuel, and consequent release of radioactive material, is a Category A safety function and the hoist is Class 2. See Appendix 15A.

The requirement against the mast hoist is that any single failure of the redundant components in the hoist equipment train will result in the fuel assembly being held in position.

Mast

The mast itself is required to ensure that there is no damage to a fuel assembly in the fully raised position through side impact as it is being moved around the refuelling cavity. Protecting against damage to the integrity of spent fuel, and consequent release of radioactive material, is a Category A safety function and the mast is considered Class 2. See Appendix 15A.

The mast is also required to ensure that an adequate depth of water to provide adequate shielding is maintained above any irradiated fuel assembly being transported. Minimisation of occupational radiation exposure is a Category C safety function and the mast is considered Class 3 in this respect.

Gripper

The gripper is required to ensure that there is no damage to a lifted fuel assembly by preventing it from being dropped. Protecting against damage to the integrity of spent fuel, and the consequent release of radioactive material, is a Category A safety function and the gripper is Class 2. See Appendix 15A.

The requirement against the gripper is that it will not release a fuel assembly in any position other than when the fuel assembly is correctly lowered into the reactor core, the fuel transfer mechanism, or the in-containment fuel storage rack.

Bridge and Trolley

The bridge and trolley are required to maintain good alignment of the mast during raising and lowering, and also to ensure that the fuel is moved in a controlled fashion within permissible areas, all to minimise the risk of fuel damage including during a seismic event. Protection against damage to the integrity of spent fuel is a Category A safety function and the bridge and trolley are Class 2. See Appendix 15A.

17.7.1.4 Justification of Claims on Components and Equipment

Mast Hoist

Whilst there is no "inherently safe" way to design lifting equipment, the provision of multiple load paths along with substantial factors of safety is generally accepted as the best solution to minimise the risk of dropped loads.

The mast hoist is designed with the following principal provisions to achieve a high level of hoist integrity:

- The minimum design load is approximately 120 percent of the maximum expected working load.
- The hoist has twin redundant brakes, one mechanically actuated and one electrically actuated, either of which can restrain 150 percent of the rated design load.
- Twin wire ropes are used to support the inner mast, either of that is capable of carrying the full load of the inner mast and an associated fuel assembly.
- The design loads on the wire ropes do not exceed 0.2 times the average breaking strength.
- The attachment to the inner mast is through a load-equalising device to ensure that each wire rope always takes an equal share of the load.
- The wire ropes are manufactured from stainless steel to provide corrosion resistance against the high-humidity containment atmosphere and potential contact with boric acid solution.

The design is very similar to that used in currently operating PWRs and there have been no failures of mast system hoists resulting in dropped fuel as discussed further in Appendix 17A. This provides support to the reliability claims.

The maintenance and testing arrangements for the mast hoist are based on both the statutory inspections required for lifting equipment and those aimed at ensuring reliable operation. The testing is:

- At the beginning of each refuelling outage and prior to the handling of irradiated fuel, the mast hoist will be tested to 125 percent of the design rated load.
- Prior to each refuelling outage, there will be an inspection for loose parts and foreign objects.
- Prior to each outage, checks will be carried out to demonstrate full functionality of the mast hoist.

Mast

The mast provides a physical container around the fuel assembly being moved. This is not dependent on any control or actuation systems and does not require any power supplies. As a result, it provides an inherently safe arrangement for the prevention of damage to the fuel during movement.

The mast is manufactured from stainless steel to ensure compatibility with the borated water environment in which it operates. It is also designed as seismic Category II (C-II). The principal provisions in the design for achieving a high level of fuel protection are:

- The guide bars in the outer mast are adjustable to ensure that they can be set up with fine tolerance to the grid straps on the fuel. This allows the fuel to be held tightly and securely within the mast.

- The mast provides physical restraint stops to prevent irradiated fuel from being raised to a point where an inadequate depth of water for shielding remains above it.

- Control interlocks are associated with the mast to ensure that full movement of the refuelling machine bridge and trolley cannot take place unless a fuel assembly is correctly stowed in the mast.

The design is very similar to that used in currently operating PWRs and from a review of NUREG 1774, 30 crane events involving fuel assembly drops or damage were identified during a 34+ year period in the US fleet. None of these events resulted in fuel cladding damage or any release of radioactivity, and only one was associated with the failure of a hoist. This provides support to the reliability claims.

The maintenance and testing arrangements for the mast are based on both the statutory inspections required for lifting equipment and those aimed at ensuring reliable operation. The testing is:

- Prior to each refuelling outage, there will be an inspection for loose parts and foreign objects.

- Prior to each outage, checks will be carried out to demonstrate full functionality of the mast assembly.

Gripper

Whilst there is no “inherently safe” way to design lifting equipment, the provision of multiple load paths along with substantial factors of safety is generally accepted as the best solution to minimise the risk of dropped loads.

The gripper is manufactured from stainless steel to ensure compatibility with the borated water environment in that it operates. It is also designed as seismic C-II. The principal provisions in the design for achieving a high level of lifting integrity are:

- The gripper design has four “fingers” that grip the fuel assembly being lifted. The design ensures that any two of these will adequately support the weight of the fuel assembly.

- The gripper head is designed to float so that it can move to align correctly when engaging a fuel assembly.

- The design of the gripper assembly is such that once a fuel assembly has been latched into position any load on the latches from lifting operations will tend to cause the latch mechanism to engage further. This feature is not dependent on external actuation or the provision of separate power supplies and so inherently supports the requirement of secure lifting.

- The gripper assembly is designed so that the refuelling machine cannot raise a fuel assembly unless the gripper is fully engaged.

The design is very similar to that used in currently operating PWRs. This provides support to the reliability claims.

The maintenance and testing arrangements for the gripper are based on both the statutory inspections required for lifting equipment and those aimed at ensuring reliable operation. The testing is:

- At the beginning of each refuelling outage and prior to the handling of irradiated fuel, the gripper will be tested to 125 percent of the design rated load.

- Prior to each refuelling outage, there will be an inspection for loose parts and checks of the limit switches and limit switch actuators.

- Prior to each outage, checks will be carried out to demonstrate full functionality of the gripper.

Bridge and Trolley

The bridge and trolley run on machined rails with one rail used by guide rollers to control lateral movement as well as for support. This design ensures that movement can be limited to known areas without use of separate protection equipment, and is an inherently safe approach.

The bridge and trolley are constructed from a coated carbon steel to provide protection against the atmospheric environment in the containment building. They are also designed as seismic C-II. The principal provisions to ensure that fuel cannot be damaged during handling operations, especially through contact with fittings in the refuelling cavity, are:

- Positive stops are provided on the trolley rails to prevent the mast from contacting the wall of the refuelling cavity. Energy-absorbing devices are provided to handle impact with the trolley moving at maximum traverse speed.

- Positive stops are provided on the bridge rails to prevent the mast from contacting the wall of the refuelling cavity. Energy-absorbing devices are provided to handle impact with the bridge moving at maximum traverse speed.

- The bridge propulsion motors are designed so that an integral brake is engaged when power is not being supplied to move the bridge.

- The trolley propulsion motors are designed so that an integral brake is engaged when power is not being supplied to move the trolley.

- The speeds of the bridge and trolley have been set such that inertia loads on fuel assemblies during handling operations do not exceed allowable limits.

- Hold-down devices are provided on both the trolley rails and the bridge rails to prevent the bridge or trolley from leaving the rails in the event of a seismic occurrence.

The design is very similar to that used in currently operating PWRs and from a review of NUREG 1774, 30 crane events involving fuel assembly drops or damage were identified during a 34+ year period in the US fleet. None of these events resulted in fuel cladding

damage or any release of radioactivity, and only one was associated with the failure of a hoist. This provides support to the reliability claims.

The maintenance and testing arrangements for the bridge and trolley are based on both the statutory inspections required for lifting equipment and those aimed at ensuring reliable operation. The testing is:

- Prior to each refuelling outage, there will be an inspection for loose parts, an inspection of exposed gears, and checks of the limit switches and limit switch actuators.

- Prior to each outage, checks will be carried out to demonstrate full functionality of the bridge and trolley.

17.7.2 Fuel Handling Machine (FHS-FH-02)

17.7.2.1 Role

A detailed description of the fuel handling machine is given in Section 6.12. Further design details of the FHS and its constituent components are delineated in Reference 17.29.

The fuel handling machine is required to move new and irradiated nuclear fuel within the spent fuel pool and from the spent fuel storage racks in the auxiliary building fuel handling area to the fuel transfer system outside containment. The system contributes to the containment primary safety function by ensuring that all movement of fuel is carried out with minimum risk of damaging fuel cladding directly, or in such a way that damage could become apparent during further handling or irradiation. In this way, the opportunity for release of radioactive material is minimised.

The fuel handling machine is also designed to limit the lift height so that during operation, when handling irradiated fuel assemblies, there will always be an adequate depth of water to maintain adequate shielding of staff on the fuel handling machine gantry.

The main hazard to containment integrity, and hence to maintenance of the primary safety function, comes from either dropping fuel assemblies or driving them into obstacles through incorrect operation of the handling equipment. The protection from these hazards comes from appropriate design of the handling equipment itself and the provision of appropriate interlocks to control fuel handling movements. Interlocks are provided through a mixture of electrical and mechanical means.

The fuel handling machine is not supported by other systems in the provision of its safety functions. It does not support any other systems in the provision of their safety functions.

17.7.2.2 System Components and Equipment Contributing to Safety Function

The fuel handling machine is designed in accordance with the guidelines in Reference 17.13. This specifies a number of necessary design features, the following are critical in ensuring that the system can support its safety function:

- **New Fuel Handing Area Hoist** – This hoist has twin wire ropes and redundant braking systems designed to hold loads in excess of its rated value. The safety requirement of the hoist is to minimise the risk of damage to spent fuel assemblies in the fuel storage racks from the impact of dropped loads. It is also required to ensure that new fuel cannot be

subject to any impact damage that might result in fuel failure during further handling post-irradiation.

- **Spent Fuel Pool Area Hoist** – This hoist also has twin wire ropes and redundant braking systems designed to hold loads in excess of the rated value.. The safety requirement of the hoist is to minimise the risk of damage to spent fuel assemblies from their being dropped during fuel handling operations.

- **Bridge and hoist trolley(s)** – The bridge and hoist trolley(s) provide the facility to move items attached to either the New Fuel Handing Area Hoist or Spent Fuel Pool Area hoists around the fuel handling facility in the auxiliary building. The design provides numerous interlocks to prevent traversal into inappropriate areas and the machine is designed with appropriate restraints to ensure that it remains in position in the event of a seismic disturbance. The safety requirement of the bridge and hoist trolley(s) is to ensure that fuel movements are confined to areas of the refuelling cavity where there is no risk of damage to the fuel assembly from impact.

- **Fuel assembly handling tools** – The fuel assembly handling tools are suspended from the fuel handling machine hoists with an appropriate choice of tool made for each operation. Each tool contains a latching mechanism to connect to the top nozzle box of a fuel assembly. The design is such that once the weight of the fuel assembly is being borne by the mechanism, it holds it in the "latched" position and prevents release of the fuel assembly or a control component. The safety requirement of the handling tools is to minimise the risk of fuel assembly damage, either directly through being dropped, or consequently as a result of dropping on the spent fuel storage racks.

17.7.2.3 Claims on Components and Equipment

New Fuel Handling Area Hoist

This hoist is required to ensure that no loads can be dropped onto the spent fuel storage racks with the consequential risk of damage to the spent fuel and potential release of radioactive material. Protection against damage to the integrity of spent fuel is a Category A safety function and the hoist is Class 2. See Appendix 15A.

This hoist has dual redundant components such that either of the respective components can perform the full duty. Where redundancy is not available, as on the hoist hook, a double design safety factor is employed. The requirement against the New Fuel Handling Area hoist is that any credible single failure in the hoist equipment train will result in the fuel assembly being held in position.

Spent Fuel Pool Area Hoist

The Spent Fuel Pool Area hoist is required to ensure that spent fuel assemblies cannot be dropped whilst they are being handled, leading to either damage to the dropped assembly or consequential damage to fuel in the spent fuel storage racks. Protection against damage to the integrity of spent fuel is a Category A safety function and the hoist is Class 2. See Appendix 15A.

The Spent Fuel Pool Area hoist has some dual redundant components such that there is a measure of redundancy in performing the lifting duty. The requirement against the Spent Fuel Pool Area hoist is that the risk of dropping a fuel assembly is very low and that the results of any drop do not lead to a significant risk of release of radioactive material.

Bridge and Hoist Trolley(s)

The bridge and hoist trolley(s) are required to ensure that the hoists and loads that they may be supporting are moved in a controlled fashion within the permissible area to minimise the risk of damage. Protection against damage to the integrity of spent fuel is a Category A safety function and the bridge and hoist trolley(s) are Class 2. See Appendix 15A.

Fuel Assembly Handling Tools (FHS-FH-52)

The fuel handling tools are required to ensure that there is no damage to a lifted fuel assembly from being dropped. Protecting against damage to the integrity of spent fuel, and consequent release of radioactive material, is a Category A safety function and the spent fuel handling hoist tool is Class 2. The new fuel handling tool is Class 2. See Appendix 15A. New fuel cannot be transported over the spent fuel racks using the fuel handling machine hoist and the new fuel handling tool. This is controlled by interlock.

The requirement against the fuel assembly handling tools is that they will not release a fuel assembly in any position other than when the fuel assembly is correctly lowered into the fuel racks, the fuel transfer mechanism, or the spent fuel storage flask.

17.7.2.4 Justification of Claims on Components and Equipment

New Fuel Handling Area Hoist

Whilst there is no "inherently safe" way to design lifting equipment, the provision of multiple load paths and substantial factors of safety is generally accepted as the best solution to minimise the risk of dropped loads.

The New Fuel Handling Area hoist is designed against NUREG-0554 (Reference 17.14). It is also designed as seismic C-II. The principal provisions to achieve a high level of hoist integrity are:

- The hoist has a mechanical ratchet and pawl brake and two independent electric brakes. Either one is capable of handling 150 percent of rated load.
- The braking arrangements are such that they are automatically set whenever drive power is removed from the hoist motor.
- There are dual lifting cables, each capable of taking the full rated load.
- The hoist ropes are stainless steel to provide compatibility with the expected atmosphere in the fuel handling area.
- The design load on the hoist ropes does not exceed 0.2 times the average breaking load.

The design is very similar to that used in PWRs already operating, and there have been no failures of hoists of this design resulting in dropped fuel. This provides support to the reliability claims.

The maintenance and testing arrangements for the New Fuel Handing Area hoist are based on both the statutory inspections required for lifting equipment and those aimed at ensuring reliable operation. The testing is:

- Prior to dispatch from their manufacturers, the New Fuel Handing Area hoist will be tested to 125 percent of the design rated load.

- Prior to each refuelling outage, there will be an inspection for loose parts, an inspection of hoist cables, and checks of the limit switches and limit switch actuators.

- Prior to each outage, checks will be carried out to demonstrate full functionality of the New Fuel Handing Area hoist.

Spent Fuel Pool Area Proof Hoist

Whilst there is no "inherently safe" way to design lifting equipment, the provision of multiple load paths and substantial factors of safety is generally accepted as the best solution to minimise the risk of dropped loads.

The Spent Fuel Pool hoist, whilst not designed formally against NUREG-0554 (Reference 17.14), however incorporates a number of features from this standard. It is also designed as seismic C-II. The principal provisions to achieve a high level of hoist integrity are:

- The hoist has a mechanical brake and an independent electric brake. Either one is capable of handling 150 percent of rated load.

- The braking arrangements are such that they are automatically set whenever drive power is removed from the hoist motor.

- There are dual lifting cables, each capable of taking the full rated load.

- The hoist ropes are stainless steel to provide compatibility with the expected atmosphere in the fuel handling area.

- The design load on the hoist ropes does not exceed 0.2 times the average breaking load.

The design is very similar to that used in PWRs already operating.

The maintenance and testing arrangements for the Spent Fuel Pool Area hoist are based on both the statutory inspections required for lifting equipment and those aimed at ensuring reliable operation. The testing is:

- Prior to dispatch from their manufacturers, the Spent Fuel Pool Area hoist will be tested to 125 percent of the design rated load.

- Prior to each refuelling outage, there will be an inspection for loose parts, an inspection of hoist cables, and checks to the limit switches and limit switch actuators.

- Prior to each outage, checks will be carried out to demonstrate full functionality of the Spent Fuel Pool Area hoist.

Bridge and Hoist Trolley(s)

The bridge runs on machined rails with one rail being used by guide rollers to control lateral movement as well as for support. This design ensures that movement can be limited to known areas without use of separate protection equipment and is an inherently safe approach. Mounted on the bridge is a superstructure that includes two monorail trolley-hoists. These two trolley-hoists share the same monorail.

The bridge and trolley are constructed from a coated carbon steel to provide protection against the atmospheric environment over the spent fuel storage pond. They are also designed as seismic C-II. The principal provisions to ensure that fuel cannot be damaged during handling operations, especially through contact with fittings in the fuel pools, are:

- Positive stops are provided on the trolley monorail to prevent the trolley-hoist from disengaging the monorail. Energy-absorbing devices are provided to handle impact with the trolley moving at maximum traverse speed.

- Positive stops are provided on the bridge rails to prevent the bridge from rail disengagement. Energy-absorbing devices are provided to cater for impact with the bridge moving at maximum traverse speed.

- The bridge propulsion motors are designed so that an integral brake is engaged when power is not being supplied to move the bridge.

- The trolley propulsion motors are designed so that an integral brake is engaged when power is not being supplied to move the trolley.

- The speed of the bridge and trolley have been set such that inertia loads on fuel assemblies during handling operations do not exceed allowable limits.

- Hold-down devices are provided on the bridge rails to prevent the bridge or trolley from leaving the rails in the event of a seismic occurrence. The monorail I-beam provides the necessary hold-down capability to prevent the hoist-trolleys from disengaging during a seismic event.

The design is very similar to that used in PWRs already operating and from a review of NUREG 1774, 30 crane events involving fuel assembly drops or damage were identified during a 34+ year period in the US fleet. None of these events resulted in fuel cladding damage or any release of radioactivity, and only one was associated with the failure of a hoist. This provides support to the reliability claims.

The maintenance and testing arrangements for the bridge and hoist trolley(s) are based on both the statutory inspections required for lifting equipment and those aimed at ensuring reliable operation. The testing is:

- Prior to each refuelling outage, there will be an inspection for loose parts, an inspection of exposed gears, and checks to the limit switches and limit switch actuators.

- Prior to each outage, checks will be carried out to demonstrate full functionality of the bridge and trolley.

Fuel Assembly Handling Tools

The fuel assembly handling tools are manufactured from stainless steel to ensure compatibility with the borated water in the spent fuel pool. The principal provisions to ensure that they only release fuel assemblies in the correct location are:

- The handling tool latch assembly has four “fingers” that grip the fuel assembly being lifted. The design ensures that any two of these fingers will adequately support the weight of the fuel assembly.

- The design of the latch assembly is such that once a fuel assembly has been latched into position any load on the latches from lifting operations will tend to cause the latch mechanism to engage further. This feature is not dependent on external actuation of the provision of separate power supplies and so inherently supports the requirements of secure lifting.

- The actuating handle of the fuel handling tools has a positive means of locking the actuating shaft to preclude inadvertent release of a fuel assembly.

The design is very similar to that used in PWRs already operating and from a review of NUREG 1774, 30 crane events involving fuel assembly drops or damage were identified during a 34+ year period in the US fleet. None of these events resulted in fuel cladding damage or any release of radioactivity, and only one was associated with the failure of a hoist. This provides support to the reliability claims.

The maintenance and testing arrangements for the fuel handling tools are based on both the statutory inspections required for lifting equipment and those aimed at ensuring reliable operation. The testing is:

- Prior to dispatch from their manufacturers, the fuel handling tools will be tested to 125 percent of the design rated load.

- Prior to each use, there will be an inspection for nicks, burrs, or other physical damage.

- Prior to each use, checks will be carried out to demonstrate full functionality of the fuel handling tools.

17.7.3 Fuel Transfer System (FHS-FH-05)

17.7.3.1 Role

Further design details of the Fuel Handling System (FHS) and its constituent components are delineated in Reference 17.29 and Section 6.12.

The fuel transfer system is required to move new and irradiated fuel between the refuelling pool inside containment and the spent fuel pool in the auxiliary building fuel handling area. The system contributes to the containment primary safety function by ensuring that all movement of fuel is carried out with minimum risk of damaging fuel cladding directly, or in such a way that damage could become apparent during either further handling or irradiation. In this way, the opportunity for release of radioactive material is minimised.

The fuel transfer system is also designed so that during operation, when handling irradiated fuel assemblies, there will always be an adequate depth of water to maintain adequate shielding of staff involved with the operation of the system.

The fuel transfer system contains the equipment that allows fuel assemblies to be turned from the vertical orientation, for handling by the refuelling machine and the fuel handling machine, to the horizontal orientation, for passing through the fuel transfer tube and vice versa.

The main risk to cladding integrity, therefore, comes from the potential for snags between the fuel assembly being transferred and the fixed parts of the transfer mechanism. The particular concern in this area is operation of the up-ender mechanism when a fuel assembly has not been fully released from either the refuelling machine or the fuel handling machine.

Protection from this issue is provided by the design of the equipment itself and also the provision of appropriate interlocks to control the fuel handling movements. The interlocks provided are a mixture of electrical and mechanical systems. There is also a requirement for the transfer system to move fuel without subjecting it to unacceptable physical shocks that could give rise to fuel assembly damage.

The fuel transfer system is not supported by other systems in the provision of its safety functions. It does not support any other systems in the provision of their safety functions.

17.7.3.2 System Components and Equipment Contributing to Safety Function

The fuel transfer system is designed in accordance with the guidelines of an ANS standard, Reference 17.13. This specifies a number of necessary design features, the following features are critical in ensuring that the system can support its safety function:

- **Fuel Container** – This is a stainless-steel container designed to fully enclose the fuel assembly on all sides except for the top. It is intended to provide adequate support for the fuel assembly under transfer and prevent any in-transit damage by positively locating the assembly within the container. The prevention of physical damage is a safety requirement. The container has openings in its sides so that there is a sufficient circulation of water by natural convection to provide adequate heat removal. Adequate cooling is also provided to prevent any localised damage to fuel assemblies and is therefore a safety requirement.

- **Containment Building Up-Ender** – The up-ender mechanism provides the means for change of orientation of the fuel container between horizontal and vertical. It is manufactured from stainless steel with all bearing surfaces self-lubricated by the water in that the mechanism is immersed. The mechanism is designed to ensure that the limits at extremes of travel, to both the horizontal and vertical positions are provided with necessary protection to limit shocks to the fuel assembly being transferred. The controls of the up-ender are interlocked to ensure that the mechanism cannot attempt to move from vertical to horizontal if a fuel assembly is not fully inserted. The safety requirement is prevention of damage from impact shocks during movement or from movement when the fuel is not correctly stowed.

- **Auxiliary Building Fuel Handling Area Up-Ender** – The design is identical to the containment building up-ender.

- **Fuel Transfer Car** – This wheeled vehicle, manufactured from stainless steel, provides support to the fuel container through the latter's pivot and runs on a track between the containment up-ender and the auxiliary building fuel handling area up-ender. The car is driven by a traverse drive system mounted on the operating floor above the water level in the auxiliary building fuel transfer canal. The car runs on a track, also manufactured from stainless steel, bolted to the transfer tube. The safety requirement is to prevent damage either from impact shocks or snagging of the fuel assembly.

17.7.3.3 Claims on Components and Equipment

Fuel Container

The fuel container is required to ensure that there is no damage to a fuel assembly from snagging, or shocks, as it is moved from the containment building to the fuel handling area of

the auxiliary building. Protecting against damage to the integrity of spent fuel, and consequent release of radioactive material, is a Category A safety function and fuel container is Class 2. See Appendix 15A. The fuel container is also required to ensure that an irradiated fuel assembly is adequately cooled whilst in transit. Again, this is protection against damage to the integrity of spent fuel and is consequently a Category A safety function and the container is Class 2. See Appendix 15A.

Containment Building Up-Ender

The containment building up-ender is required to ensure that there is no damage to a fuel assembly from snagging, or shock loading, as its orientation is changed from horizontal to vertical (or vice versa). It shall not allow rotation between horizontal and vertical positions until the fuel assembly is seated and the hoist on the respective machine is clear of the up-ender. There is also a requirement that during translation, the fuel will not be damaged as a result of shock loads from violent movements. Protecting against damage to the integrity of spent fuel is a Category A safety function and the containment building up-ender is Class 2. See Appendix 15A.

Auxiliary Building Fuel Handling Area Up-Ender

The requirements are identical to those on the containment building up-ender.

Fuel Transfer Car

The fuel transfer car is required to ensure that there is no damage to a fuel assembly from shock loading as it traverses through the fuel transfer tube. The requirement is that it shall not generate shock loads that might damage a fuel assembly during transfer from the auxiliary building to the containment building (or vice versa). The protection of spent fuel assembly integrity is a Category A safety function and the fuel transfer trolley is Class 1. See Appendix 15A.

17.7.3.4 Justification of Claims on Components and Equipment

Fuel Container

The fuel container provides a physical container around the fuel assembly being moved. This is not dependent on any control or actuation systems and does not require any power supplies. As a result, it provides an inherently safe arrangement for the prevention of damage to the fuel during movement. The arrangements made for cooling of an irradiated fuel assembly in transit depend only on natural convection of the water inside and around the fuel transfer mechanism. Again, this is an inherently safe arrangement.

The fuel container is manufactured from stainless steel to ensure compatibility with the borated water environment in that it operates. The principal provisions in the design for achieving a high level of fuel protection are:

- The fuel container encloses the fuel assembly on all sides except the top.
- The inside dimensions of the fuel container, along with associated tolerances, finish, and lead-in configuration, are all selected to ensure good matching with fuel assemblies.
- The openings in the sides of the fuel container allow sufficient flow of water to ensure that boiling of the water around the fuel rods is precluded.

- The fuel container provides support for the fuel assembly at all fuel assembly grid locations.

- There is a nominal clearance between the fuel container and the inside of the fuel transfer tube that is adequate to minimise the risk of snagging.

The design is very similar to that used in currently operating PWRs and, as discussed in Appendix 17A, there have been no occurrences of damaged fuel due to failure of the fuel container to give adequate protection, or adequate cooling, to fuel being transported. This provides support to the reliability claims.

The maintenance and testing arrangement for the fuel container is based on ensuring reliable operation. The testing is:

- At the beginning of each outage, prior to the handling of fuel assemblies, visual inspection of the fuel container to ensure that it is free from damage, loose components, and foreign objects.

- Prior to each outage, checks to demonstrate full functionality of the fuel container.

Containment Building Up-Ender

The containment up-ender is manufactured from stainless steel to ensure compatibility with the borated water environment in that it operates. The principal provisions in the design for achieving a high level of fuel protection are:

- The up-ender mechanism is designed to tilt the fuel container and hold it hard against stops to locate it in the correct vertical alignment to allow fuel assemblies to be inserted and withdrawn.

- The up-ender tilt mechanism is sized so that tilting can only occur when the fuel container is properly located at the end of travel through the transfer canal.

The design is very similar to that used in currently operating PWRs and, as discussed in Appendix 17A, there have been no occurrences of damaged fuel due to failure of the up-ender mechanism. This provides support to the reliability claims.

The maintenance and testing arrangements for the containment up-ender are based on ensuring reliable operation. The testing is:

- At the beginning of each outage and prior to the handling of fuel assemblies, visual inspection of the up-ender to ensure that it is free from damage, loose components, and foreign objects.

- Visual inspection of limit switches and limit switch actuators for damage.

- Prior to each outage, checks to demonstrate full functionality of the up-ender.

Auxiliary Building Fuel Handling Area Up-Ender

The justification is identical to that of the containment building up-ender.

Fuel Transfer Car

The fuel transfer car runs on rails and is equipped with guide rollers to control lateral movement as well as for support. This design ensures that movement can be limited to the rail guide path and is an inherently safe approach.

The fuel transfer car is constructed from stainless steel to provide protection against the borated water in the fuel transfer tube. The principal provisions to ensure that fuel cannot be damaged during handling operations are:

- Wheels are mounted on the transfer car on either side of the loaded centre of gravity to promote stability. The wheels are spaced to ensure that gaps in the track, that are adjacent to each up-ender, can be negotiated.
- The transfer car is restrained from leaving the track for the full length of travel.
- The transfer car is mechanically locked to the tracks to prevent traverse once the up-ender moves to the vertical position.
- Positive stops are provided on the system rails to prevent the car from overrunning.
- The traverse drive mechanism is cut off at loads that minimise the risk of shock loadings due to failures in the drive mechanism components.
- The drive propulsion motor is designed so that an integral brake is engaged when power is not being supplied to move the car.
- The design load on the wire rope used in the transfer mechanism drive is less than 0.2 times the average breaking strength of the wire.

The design is very similar to that used in PWRs already operating and, as discussed in Appendix 17A, there have been no occurrences of damaged fuel due to failure of the fuel transfer car mechanism. This provides support to the reliability claims.

The maintenance and testing arrangements for the fuel transfer car are based on ensuring reliable operation. The testing is:

- At the beginning of each outage, prior to the handling of fuel assemblies, visual inspection of the fuel transfer car to ensure it is free from damage, loose components, and foreign objects.
- Visual inspection of limit switches and limit switch actuators.
- Prior to each outage, checks to demonstrate full functionality of the fuel container.

17.8 Heavy Load Handling Systems

17.8.1 Polar Crane (MHS-MH-01)

17.8.1.1 Role

A detailed description of the polar crane is given in Section 11.8. Further design details of this system and its constituent components are delineated in Reference 17.30.

The polar crane is required to move an assortment of heavy assemblies around the containment building, such as the integrated head package, reactor internals, and RCP components. The system contributes to the primary safety function of containment by ensuring that all the movements are carried out in such a way that there is minimum risk of impact damage to nuclear fuel directly and also to any equipment that is part of the systems responsible for other primary safety functions.

The main hazards presented by the polar crane, and hence to maintenance of the primary safety function, are from either heavy loads being dropped or collision with other plant items. The protection from these hazards comes from appropriate design of the handling equipment itself and the provision of appropriate control of lifting movements.

The polar crane is not supported by other systems in the provision of its safety functions. The polar crane does not support any other systems in the provision of their safety functions.

17.8.1.2 System Components and Equipment Contributing to Safety Function

The polar crane is designed to NUREG-0554 (Reference 17.14) supplemented by ASME NOG-1-1998 (Reference 17.15). This specifies a number of necessary design features, the following subsystems are critical in ensuring that the system can support its safety function:

- **Main hoist** – This hoist is designed with twin wire ropes and redundant braking systems designed to hold loads in excess of the rated value. The design is seismic C-I. The safety requirement of the hoist is to prevent uncontrolled lowering of a critical load.

- **Auxiliary hoist** – This hoist is designed with twin wire ropes and redundant braking systems designed to hold loads in excess of the rated value. The design is seismic C-I. The safety requirement of the hoist is to prevent uncontrolled lowering of a critical load.

- **Bridge**– The bridge is designed for a nominal capacity based on the potential application to SG replacement. The design is seismic C-I, but only up to a reduced lifting capacity based upon standard outage lifts. The bridge and trolley are also required to withstand the pressure and temperature transients associated with conditions inside containment following a LOCA. The safety requirement is to ensure that neither the bridge and trolley nor the supported hoists can collapse and cause damage to equipment inside the containment building.

17.8.1.3 Claims on Components and Equipment

Main Hoist

The main hoist is required to ensure that the heavy loads it lifts around the containment building cannot be subject to an uncontrolled lowering and cause consequential damage to either fuel in the reactor vessel or to other plant SSCs. Protecting the integrity of spent fuel is a Category A safety function. Protection against hazards that might affect the operation of other plant supporting a Category A function is also a Category A safety function. The main hoist is Class 1. See Appendix 15A.

The main hoist is a design that has dual redundant respective components such that each can perform the full safety duty. The hook does not have dual redundancy but is designed with a double factor of safety. The requirement against the main hoist is that any single failure in the hoist equipment train will result in the lifted load being held steady.

Auxiliary Hoist

The auxiliary hoist is required to ensure that the loads it lifts around the containment building cannot be subject to an uncontrolled lowering and cause consequential damage to either fuel in the reactor vessel or to other plant SSCs. Protecting the integrity of spent fuel is a Category A safety function. Protection against hazards that might affect the operation of other plant supporting a Category A function is also a Category A safety function. The auxiliary hoist is Class 1. See Appendix 15A.

The auxiliary hoist is of a design that has dual redundant respective components such that each can perform the full safety duty. The hook does not have dual redundancy but is designed with a double factor of safety. The requirement against the auxiliary hoist is that any single failure in the hoist equipment train will result in the lifted load being held steady.

Bridge and Trolley

The bridge and trolley are required to ensure that the hoists they support, and therefore any loads they may be carrying, do not fall onto either the reactor vessel or onto any other associated plant SSCs. This is effectively protecting against a hazard that might affect other plant SSCs from performing a Category A safety function and hence is also a Category A safety function. The bridge and trolley are Class 1. See Appendix 15A.

The requirement against the bridge and trolley is that they will correctly track along their rails and will maintain structural integrity, even through the pressure and temperature transients associated with a LOCA.

17.8.1.4 Justification of Claims on Components and Equipment

Main Hoist

There is no “inherently safe” way to design lifting equipment, the provision of multiple load paths and substantial factors of safety is generally accepted as the best solution to minimise the risk of dropped loads.

The main hoist is designed to the provisions as specified in ASME NOG-1-1998 and NUREG 0554 (Reference 17.14 and 17.15). The principal features for achieving high integrity are:

- There are redundant components in all elements of the lifting path except the hook.
- There are redundant braking systems, as specified in ASME NOG-1-1998 and NUREG 0554 (Reference 17.14 and 17.15).
- The equaliser assembly ensures that load is always shared equally between the two wire ropes, and if one wire rope fails the load is transferred to the remaining wire rope with minimal movement of the load.
- The load bearing hooks are designed with a double design safety factor.
- The assembly is designed to seismic C-I for critical lifts up to a defined load.

The design is very similar to the polar crane main hoists used in currently operating PWRs. There have been no failures to date with any of them that have resulted in a dropped load. This provides support to the reliability claims.

Maintenance and testing for the main hoist is based on UK statutory inspection arrangements and ASME B30.2, as discussed in Reference 17.16.

Auxiliary Hoist

There is no "inherently safe" way to design lifting equipment, the provision of multiple load paths and substantial factors of safety is generally accepted as the best solution to minimise the risk of dropped loads.

The auxiliary hoist is designed to the provisions as specified in ASME NOG-1-1998 and NUREG 0554 (Reference 17.14 and 17.15). The principal features for achieving high integrity are:

- There are redundant components in all elements of the lifting path except the hook.
- There are redundant braking systems, as specified in ASME NOG-1-1998 and NUREG 0554 (Reference 17.14 and 17.15).
- The equaliser assembly ensures that load is always shared equally between the two wire ropes; if one wire rope fails, the load is transferred to the remaining wire rope with minimal movement of the load.
- The load bearing hooks are designed with a double design safety factor.
- The assembly is designed to seismic C-I for critical lifts up to a defined load.

The design is very similar to the polar crane auxiliary hoists used in currently operating PWRs. There have been no failures to date with any of these that have resulted in a dropped load. This provides support to the reliability claims.

Maintenance and testing for the auxiliary hoist are based around UK statutory inspection arrangements and ASME B30.2 (Reference 17.16).

Bridge and Trolley

The bridge is designed for working loads associated with SG replacement. These are far in excess of the loads seen during normal refuelling activities. As such, with the exception of seismic protection, there is a further very large factor of safety on top of those normally included in the design.

Specific design features incorporated to give confidence of high integrity are:

- Positive stops are provided on the trolley rails to prevent the trolley running off the bridge. In addition to this, the physical location of the polar crane within the containment structure ensures that the trolley cannot run off the bridge.
- The assembly is designed to seismic C-I.

- The design has provisions to ensure that in the event of a LOCA or main steam line break inside containment, the consequent disruption cannot lead to either the bridge or trolley being displaced from their installed positions. All enclosed box sections of the bridge/trolley structure are vented to allow pressure equalisation during containment pressurisations. The structural and mechanical integrity of the crane will not be compromised at 216°C (420°F). The calculated crane expansion versus containment expansion during a DBA has been assessed and there is sufficient clearance between the wheels and the rail to allow for the difference. This is clearly protection of the crane structure only, and a significant programme of examination and testing would be required before the crane could actually be used following this type of event.

- Prior to heavy lifts, lifting plans will be prepared to identify safe load paths.

The design is very similar to the polar crane bridge and trolley design used in currently operating PWRs. There have been no failures to date with any of these that have resulted in a dropped load. This provides support to the reliability claims.

Maintenance and testing for the bridge and trolley are based around UK statutory inspection arrangements and ASME B30.2 (Reference 17.16).

17.8.2 Cask Handling Crane (MHS-MH-02)

17.8.2.1 Role

Further design details of this system and its constituent components are delineated in Reference 17.31 and Section 6.12

The cask handling crane is required to move spent fuel casks, and cask lids around the fuel handling area of the auxiliary building. The system contributes to the containment primary safety function by ensuring that all the movements are carried out in such a way that there is minimum risk of impact damage either to the fuel stored in the fuel storage pool or to any equipment that is part of the systems responsible for other primary safety functions.

The main hazards presented by the cask handling crane, and hence to maintenance of the primary safety function, are either from heavy loads being dropped, or by collision with other plant items. The protection from these hazards comes from appropriate design of the handling equipment itself and the provision of appropriate control of lifting movements.

The cask handling crane is not supported by other systems in the provision of its safety functions.

The cask handling crane does not support any other systems in the provision of their safety functions.

17.8.2.2 System Components and Equipment Contributing to Safety Function

The cask handling crane is designed to NUREG-0554 (Reference 17.14) supplemented by ASME NOG-1-1998 (Reference 17.15). This specifies a number of necessary design features, the following subsystems are critical in ensuring that the system can support its safety function:

- **Main Hoist** – This is a design with twin wire ropes and redundant braking systems designed to hold loads in excess of the rated value. The design is seismic C-I. The safety requirement of the hoist is to prevent uncontrolled lowering of a load.

- **Auxiliary Hoist** – This is a design with twin wire ropes and redundant braking systems designed to hold loads in excess of the rated value. The design is seismic C-I. The safety requirement of the hoist is to prevent uncontrolled lowering of a load.

- **Bridge and Trolley** – These are designed to match the nominal rating of the main hoist. The design is seismic C-I. The safety requirement is to ensure that neither the bridge nor trolley, nor the supported hoists, can collapse and cause damage to SSCs or the fuel assemblies in the SFP.

17.8.2.3 Claims on Components and Equipment

Main Hoist

The main hoist is required to ensure that the spent fuel casks and cask lids that it lifts around the auxiliary building fuel handling area cannot be subject to an uncontrolled lowering and cause consequential damage to SSCs or the spent fuel stored in the SFPs. Protection of the integrity of spent fuel is a Category A safety function. The main hoist is Class 1. See Appendix 15A.

Auxiliary Hoist

The auxiliary hoist is required to ensure that the loads it lifts around the auxiliary building fuel handling area cannot be subject to an uncontrolled lowering and cause consequential damage to SSCs or the spent fuel stored in the SFPs. Protection of the integrity of spent fuel is a Category A safety function. The auxiliary hoist is Class 1. See Appendix 15A.

Bridge and Trolley

The bridge and trolley are required to ensure that the hoists they support, and therefore any loads that may be being carried cannot be dropped and cause consequential damage to SSCs or the spent fuel stored in the SFPs. Protection of the integrity of spent fuel is a Category A safety function. The bridge and trolley are Class 1. See Appendix 15A.

The requirement against the bridge and trolley is that they will correctly track along their rails and will maintain structural integrity.

17.8.2.4 Justification of Claims on Components and Equipment

Main Hoist

Whilst there is no “inherently safe” way to design lifting equipment, the provision of multiple load paths along with the provision of substantial factors of safety is generally accepted as the best solution to minimise the risk of dropped loads.

The main hoist is designed to the provisions as specified in ASME NOG-1-1998 and NUREG 0554 (Reference 17.14 and 17.15). The principal features for achieving high integrity are:

- There are redundant components in all elements of the lifting path with the exception of the hook.
- There are redundant braking systems, as specified in Reference 17.15.
- The equaliser assembly ensures that load is always shared equally between the two wire ropes; if one wire rope fails, the load is transferred to the remaining wire rope with minimal movement of the load.
- The load bearing hook is designed with a double design safety factor.
- The assembly is designed to seismic C-I.

The design is very similar to the cask handling crane main hoists used in currently operating PWRs. There have been no failures to date with any of them that have resulted in a dropped load. This provides support to the reliability claims.

Maintenance and testing for the main hoist are based on UK statutory inspection arrangements and ASME B30.2 (Reference 17.16).

Auxiliary Hoist

Whilst there is no "inherently safe" way to design lifting equipment, the provision of multiple load paths and substantial factors of safety is generally accepted as the best solution to minimise the risk of dropped loads.

The auxiliary hoist is designed to the provisions as specified in ASME NOG-1-1998 and NUREG 0554 (Reference 17.14 and 17.15). The principal features for achieving high integrity are:

- There are redundant components in all elements of the lifting path with the exception of the hook.
- There are redundant braking systems, as specified in ASME NOG-1-1998 and NUREG 0554 (Reference 17.14 and 17.15).
- The equaliser assembly ensures that load is always shared equally between the two ropes; if one rope fails, the load is transferred to the remaining rope with minimal movement of the load.
- The load bearing hook is designed with a double design safety factor.
- The assembly is designed to seismic C-I.

The design is very similar to the cask handling crane auxiliary hoists used in currently operating PWRs. There have been no failures to date with any of them that have resulted in a dropped load. This provides support to the reliability claims.

Maintenance and testing for the auxiliary hoist are based on UK statutory inspection arrangements and ASME B30.2 (Reference 17.16).

Bridge and Trolley

Specific design features incorporated to give confidence of high integrity are the following:

- Positive stops are provided on the trolley rails to prevent the trolley from running off the bridge. In addition, the location of the crane within the auxiliary building structure also physically prevents the trolley from running off the bridge.
- Positive stops are provided on the bridge rails to prevent the bridge from running off the support rails.
- The assembly is designed to seismic C-I.
- The crane rails do not extend over the SFP, so it is not physically possible to lift loads over it.

The design is very similar to the cask handling crane bridge and trolley design used in currently operating PWRs. There have been no failures to date with any of them that have resulted in a dropped load. This provides support to the reliability claims.

Maintenance and testing for the bridge and trolley are based on UK statutory inspection arrangements and ASME B30.2 (Reference 17.16).

17.9 Fuel Storage

17.9.1 Spent Fuel Pool Cooling

17.9.1.1 Role

A detailed description of the SFS is given in Section 6.12.4. Further design details of this system and its constituent components are delineated in Reference 17.32.

The SFS contributes to the heat transfer/residual heat removal primary safety function and also the containment primary safety function. It supports the heat transfer/residual heat removal primary safety function through the removal of decay heat generated in the irradiated fuel assemblies stored in the SFP. It supports containment through purification of the pool water to remove any entrained contamination that could ultimately give rise to an airborne hazard. It also supports this primary safety function through the purification of water in the refuelling cavity during refuelling operations.

The SFS consists of two trains of mechanical equipment. Each train includes one SFP pump, one SFP HX, one SFP demineraliser, and one SFP filter. The two trains of equipment have separate suction and discharge connections to the SFP. In addition to the contribution to primary safety functions described above, the SFS also has the capability to provide cleanup and purification to the IRWST, and to control the transfer of water from the IRWST to the refuelling cavity and back. The system is designed so that one train can perform this duty whilst the other continues to provide SFP cooling.

The connections to the IRWST and the refuelling cavity clearly go through the containment boundary and valves are provided for the containment isolation safety function. This feature provides support to the containment primary safety function.

The SFS is supported by the CCS and also by the ECS and the ZOS.

Whilst the SFS supports the operation of other systems, it does not support them in performing any safety functions.

17.9.1.2 System Components and Equipment Contributing to Safety Function

- The pipework of the SFS is designed to ASME Power Piping Code, B31.1 (Reference 17.10) and ASME Boiler and Pressure Vessel Code, Section III-2 (Reference 17.4) where associated with CIVs.

- **Spent Fuel Cooling Pumps (SFS-MP-01A/B)** – These are single-stage, horizontally mounted centrifugal pumps manufactured from stainless steel and driven directly by an ac induction motor. The pumps are designed to supply the required flow and pressure. One pump is normally running and the safety requirement is to have at least one pump continue running to provide adequate flow to meet SFP cooling requirements.

- **Spent Fuel Pool Heat Exchangers (SFS-ME-01A/B)** – These are plate-type HXs, that consist of multiple thin plates mounted in a frame. SFS water is circulated on one side of the multiple thin plates, while CCS water circulates on the opposite side of them. The HX plates and piping connections are manufactured from stainless steel. The safety requirement of the SFS HXs is to provide adequate heat transfer to ensure that the SFP temperature remains stable for the full range of design conditions. See Appendix 17E.

- **Skimmers (SFS-PY-S03A/B, -PY-S04A/B)** – Skimmer assemblies are provided for the SFP and on the refuelling cavity. The skimmers float freely about the surface of either pool and have a flexible hose leading from the skimmer bottom outlet to a hose adapter. The adapter connects to the skimmer piping quick-connect fitting at the SFP or refuelling cavity wall. The operation of the SFS pump(s) draws water into the skimmer(s). The skimmers are designed to collect debris that may be on the water surface. The skimmer function is not a safety requirement and will not be discussed further.

- **Filters (SFS-MV-02A/B)** – These are sized to collect particulates and resin fines passed by the demineraliser and suspended solids. Process flow is side entry and bottom discharge. The vessel top is a flat head with a flange and gasket hinged with a quick-release closure to allow easy filter cartridge replacement and handling. The assembly is constructed of austenitic stainless steel and uses disposable filter cartridges that can be compacted for waste storage. The safety requirement is to remove particulate contamination from pool water to prevent release to atmosphere.

- **Demineralisers (SFS-MV-01A/B)** – These are constructed from stainless steel and are sized to be charged with a mixture of hydrogen-type cation resin and hydroxyl-type anion resin to remove fission and corrosion products. The demineralisers are sized to accept purification flow from the cooling train. This flow is designed to provide two water volume changes of the SFP within 24 hours. The safety requirement for the demineralisers is to remove dissolved contamination from the pool water to prevent potential release to atmosphere.

- **SFS Suction Line CIVs (SFS-PL-V034 and -V035)** –These are 150-mm DN (6-inch), motor-operated butterfly valves designed to fail “as is” on loss of electrical supplies. Both valves are required to close on receipt of a containment isolation signal from the PMS to support the containment integrity function, or on a SFP low-water-level signal from the PMS to protect the stored spent fuel. The safety requirement is to isolate the containment penetration.

- **SFS Discharge Line CIV (SFS-PL-V038)** – This is a 100-mm DN (4-inch), motor-operated butterfly valve designed to fail "as is" on loss of electrical supplies. The valve is required to close on receipt of a containment isolation signal from the PMS to support the containment integrity function, or on a SFP low water-level signal from the PMS to protect the stored spent fuel. The safety requirement is to isolate the containment penetration.

- **Discharge CIV (SFS-PL-V037)** – This is a 100-mm DN (4-inch) swing check valve. The valve is required to close on reverse flow. This prevents reverse flow in the SFS transfer lines and also contributes to the containment integrity function. The safety requirement is to isolate the penetration.

17.9.1.3 Claims on Components and Equipment

Spent Fuel Pool Cooling Pumps (SFS-MP-01A/B)

The SFS pumps provide the motive force to circulate water from the SFP through the HXs and purification system. Removal of decay heat is a Category A safety function. The SFS pumps are Class 2. See Appendix 15A.

Purification prevents release of radioactive material that accumulates in the SFP and is a Category B safety function. The SFS pumps are Class 2. See Appendix 15A.

Two SFS pumps are provided, either of which can provide sufficient flow to ensure the provision of adequate cooling and also to meet the purification requirements. The requirement on the pumps is that they will continue to run reliably as required.

Spent Fuel Pool Heat Exchangers (SFS-ME-01A/B)

The SFS HXs provide the facility for heat transfer into the CCS and consequent control of spent fuel pool water temperature. Removal of decay heat is a Category A safety function. The SFS HXs are Class 2. See Appendix 15A.

There are two component SFS HXs, either of which can provide the full cooling duty during normal plant operation. The requirement on the HXs is that they will provide adequate heat transfer, they will not impair the operation of the SFS, and they will not be unavailable because of leakage.

Skimmers (SFS-PY-S03A/B, -PY-S04A/B)

The skimmers serve to remove particulate contamination from the SFP water. Purification removes radioactive material from the water in the SFP, refuelling cavity, and IRWST, and this is a Category C safety function. The skimmers are Class 3.

Four skimmers are provided, two for the SFP and two for the Refueling Cavity. The requirement on them is that they will capture appropriate particulate and fission products.

Filters (SFS-MV-02A/B)

The SFS filters serve to remove particulate contamination from the SFP water. Purification removes radioactive material from the water in the SFP, refuelling cavity, and IRWST, and this is a Category C safety function. The SFS filters are Class 3. See Appendix 15A.

Two filters are provided, one on each SFS train. Either filter is able to carry out the full design duty. The requirement on them is that they will capture appropriate particulate material.

Demineralisers (SFS-MV-01A/B)

The SFS demineralisers serve to remove dissolved ionic contamination (both radioisotopes and other ionic materials) from the SFP water. Purification limits the radioactivity of the water in the SFP, refuelling cavity, and IRWST, and this is a Category C safety function. The SFS demineralisers are Class 3. See Appendix 15A.

Two demineraliser units are provided, one on each SFS train. Either demineraliser is able to carry out the full design duty. The requirement on them is that they will maintain dissolved solid concentrations below the required limits.

SFS Suction Line CIVs – (SFS-PL-V034 and -V035)

The CIVs serve to support containment integrity and prevention of the release of radioactive material. This is a Category A safety function and they are considered Class 1. See Appendix 15A.

There are two valves and one of them has to function to secure containment isolation. The requirement is that they will close on demand.

SFS Discharge Line Containment Isolation Valve (SFS-PL-V038)

The CIV serves to support containment integrity and prevention of the release of radioactive material. This is a Category A safety function and the valve is considered Class 1. See Appendix 15A.

The valve is partnered with the check valve in isolation of the penetration. The requirement is that this valve will close on demand.

SFS Discharge Line Containment Isolation Check Valve (SFS-PL-V037)

The CIV serves to support containment integrity and prevention of the release of radioactive material. This is a Category A safety function and the valve is considered Class 1. See Appendix 15A.

The valve is partnered with the motor-operated valve in isolation of the penetration. The requirement is that this valve will close on demand.

17.9.1.4 Justification of Claims on Components and Equipment

Spent Fuel Pool Cooling System Pumps (SFS-MP-01A/B)

The pumps are designed to Hydraulic Institute standards and are very similar to the design of like pumps on currently operating PWRs. As a result, the successful operation of these pumps in service offers a high degree of confidence in the reliability to be expected from these pumps.

Routine maintenance and testing of the SFS pumps will be performed according to the manufacturer's recommendations and will include routine changeover of the pumps allocated

to duty and standby roles. No specific surveillance test requirements are identified since these pumps are normally in operation.

Spent Fuel Pool Cooling Heat Exchangers (SFS-ME-01A/B)

The HXs are manufactured with stainless-steel plates to ensure maximum compatibility with the CCS fluid and the service water system (SWS) fluid that passes through. The HXs are manufactured to ASME Boiler and Pressure Vessel Code, Section VIII, Division 1 (Reference 17.9).

The use of plate HX for this type of application is very well established. The use of this type of heat exchanger gives the ability to easily change the number of plates installed and consequently allow variations to be made in heat exchange area, to optimise the performance of the coolers to the system needs. The plate heat exchangers are substantially smaller than conventional shell and tube heat exchangers since they operate in a true counter-current flow arrangement and use turbulent flow to increase the U-value of the heat exchanger.

Routine maintenance and testing of the SFS HXs will be performed according to the manufacturer's recommendations and will include routine changeover of the HXs allocated to duty and standby roles. No specific surveillance test requirements are identified since these heat exchangers are normally in operation.

Filters (SFS-MV-02A/B)

The filter vessel is constructed from stainless steel to provide compatibility with the SFP water. The vessel is constructed to ASME Boiler and Pressure Vessel Code, Section VIII, Division 1 (Reference 17.9). The design is very similar to like filters on currently operating PWRs and other nuclear power stations. This gives considerable confidence that the filter will be able to perform as expected.

Routine maintenance and inspection of the filter vessel will be performed according to the manufacturer's recommendations. No specific surveillance test requirements are identified since these filters are normally in operation.

The filter element will be replaced periodically unless differential pressure indications suggest that a change is required more frequently.

Demineralisers (SFS-MV-01A/B)

The demineraliser vessels are constructed from stainless steel to provide compatibility with the SFP water. The vessels are constructed to ASME Boiler and Pressure Vessel Code, Section VIII, Division 1 (Reference 17.9). The design is very similar to like demineralisers on currently operating PWRs and other nuclear power stations. This gives considerable confidence that the filter will be able to perform as expected.

Routine maintenance and inspection of the demineraliser vessel will be performed according to the manufacturer's recommendations. No specific surveillance test requirements are identified since these demineralisers are normally in operation.

The demineraliser resin will be replaced periodically unless chemical monitoring suggests that a change is required more frequently.

SFS Suction Line Containment Isolation Valves (SFS-PL-V034 and -V035)

The CIVs are both motor operated, which means they will inherently fail "as is," and clearly, this is not fail-safe with respect to the containment isolation function itself. Given that spurious actuation of this function when not required could, in itself, give rise to safety concerns, this arrangement is judged appropriate.

Both valves are manufactured from stainless steel to ensure compatibility with the reactor coolant water that passes through them. They are designed to ASME Boiler and Pressure Vessel Code, Section III-2.

The maintenance and testing arrangements for the SFS CIVs are based on the ASME Boiler and Pressure Vessel Code programmes appropriate for these types of valves as used in existing nuclear power stations. The testing is:

- A full stroke operability test is carried out quarterly in accordance with ASME Boiler and Pressure Vessel Code.

- Visual confirmation of valve operation during the stroke testing is carried out every 2 years.

- Given that they are CIVs, seat leakage limits will be tested to verify leak tightness. This test will be performed as an LLRT in line with the CIV leak test programme (Reference 17.11).

SFS Discharge Line Containment Isolation Valve (SFS-PL-V038)

The CIV is motor operated, which means it will inherently fail "as is," and clearly, this is not fail-safe with respect to the containment isolation function itself. Given that spurious actuation of this function when not required could, in itself, give rise to safety concerns, this arrangement is judged appropriate.

The valve is manufactured from stainless steel to ensure compatibility with the reactor coolant water that passes through it. It is designed to ASME Boiler and Pressure Vessel Code, Section III-2.

The maintenance and testing arrangements for the SFS CIVs is based on the ASME Boiler and Pressure Vessel Code programmes appropriate for these types of valves as used in existing nuclear power stations. The testing is:

- A full stroke operability test is carried out quarterly in accordance with ASME Boiler and Pressure Vessel Code.

- Visual confirmation of valve operation during the stroke testing is carried out every 2 years.

- Given that they are CIVs, seat leakage limits will be tested to verify leak tightness. This test will be performed as an LLRT in line with the CIV leak test programme (Reference 17.11).

SFS Discharge Line Containment Isolation Valve (SFS-PL-V037)

This CIV is a check valve and operation depends only upon the pressure difference across it, and not on any method of powered actuation. This passive approach offers a high degree of inherent safety and reliability.

The valve is manufactured from stainless steel to ensure compatibility with the reactor coolant water that passes through it. It is designed to ASME Boiler and Pressure Vessel Code, Section III-2.

The maintenance and testing arrangements for the SFS CIVs is based on the ASME Boiler and Pressure Vessel Code, Section III programmes appropriate for these types of valves as used in existing nuclear power stations. The testing is:

- A full stroke operability test is carried out quarterly in accordance with ASME Boiler and Pressure Vessel Code.
- Visual confirmation of valve operation during the stroke testing is carried out every 2 years.
- Given that they are CIVs, seat leakage limits will be tested to verify leak tightness. This test will be performed as an LLRT in line with the CIV leak test programme (Reference 17.11).

17.10 Other Supporting Systems

17.10.1 Component Cooling Water System (CCS)

17.10.1.1 Role

A detailed description of the CCS is given in Section 6.11. Further design details of this system and its constituent components are delineated in Reference 17.33.

Whilst the system does not provide a direct contribution to the primary safety functions of reactivity control or heat transfer/residual heat removal in itself, it does support a number of the systems used as defence in depth to contribute to these primary safety functions. The system provides this support through two roles:

- **Role a** − A heat transport mechanism for the transfer of decay heat away from systems directly responsible for cooling the reactor core or spent fuel stored in the SFP.
- **Role b** − A heat transport mechanism for the transfer of heat, such as that from motors, etc., generated within equipment in the supported system.

The system is made up of two CCS pumps, arranged in parallel, either of which can provide 100 percent of the flow requirement during normal plant power operation. Both are required to be in service to achieve target RCS cooldown times in preparation for refuelling, but the availability of a single pump only increases the cooldown time. Each pump has an associated HX that is also able to provide 100-percent heat duty for normal power operation. It is, however, also possible to align either pump with either HX to facilitate maintenance activities.

The rest of the system is the interconnected pipework that links the pumps and HXs to the individual system heat loads. This pipework is arranged so that one or two operating CCS pumps and HXs can cool all the heat loads. However, the CCS can be segregated into two redundant trains, with each pump and HX train cooling one of two trains of defence in depth components; namely, an RNS HX and pump seal, an SFS HX, and a CVS makeup pump mini-flow HX. When segregated, the remaining non-defence in depth heat loads can be isolated or cooled by either CCS train but without full redundancy.

The CCS provides cooling to equipment in containment and therefore has CIVs as part of its system. These valves support the primary safety function of containment.

The CCS provides support to enable the following systems to perform their safety functions:

- RNS (Roles a and b)
- SFS (Role a)
- CVS (Role b)

The CCS also supports the following systems in normal operation but is required to provide isolation of specific equipment as part of the primary safety function of containment:

- RCP high-pressure motor cooler (Role b)
- RCP flywheel jacket cooler (Role b)
- CVS letdown heat exchanger

The CCS also provides cooling to other systems but in these cases does not support any of them in providing primary safety functions, either as the principal system or as defence in depth.

The CCS is supported by the SWS, a portion of the turbine building ventilation system (VTS), the ECS, and the ZOS if needed.

17.10.1.2 System Components and Equipment Contributing to Safety Function

Most of the CCS system pipework is designed and constructed to ASME B31.1 standards with the exception of the CIVs, containment penetrations, and associated pipework. These are designed and constructed to ASME Boiler and Pressure Vessel Code, Section III-2. A small section of the containment supply and return lines just inside the innermost containment isolation valve is designated Class 1. This section of the line contains the relief valves provided to protect the containment isolation valves from excess pressure buildup while being closed automatically to isolate a Reactor Coolant Pump external heat exchanger tube leak. The following components contribute to the CCS performing its safety functions:

- **Component Cooling Water Pumps (CCS-MP-01A/B)** – These pumps are single-stage, horizontal, centrifugal pumps manufactured from carbon steel and driven directly by an ac induction motor. One of the pumps is normally running and the safety requirement is to continue running to provide adequate CCS fluid to meet design cooling requirements.

- **CCS Heat Exchangers (CCS-ME-01A/B)** – These are plate-type, counterflow HXs that transfer heat from the CCS to the SWS. The HXs are each sized to transfer the full heat load on the CCS during normal operation with 10-percent oversurfacing to handle surface fouling during operation. Component cooling water and service water circulate through the alternating channels formed by contiguous plates in the CCS HXs. Component cooling water is maintained at a higher pressure than the service water to

prevent leakage of the service water into the CCS. The HX plates are constructed of austenitic stainless steel for plants with fresh water recirculating cooling-tower SWS. The closure heads are constructed of carbon steel. The safety requirement of the CCS HXs is to provide adequate heat transfer and maintain acceptable CCS temperatures through the full range of design heat loads.

- **CCS Surge Tanks (CCS-MT-01A/B)** – The surge tanks are constructed from carbon steel and have a capacity sufficient to accommodate shrink or swell within the CCS liquid volume due to operational variations in bulk average temperature and to enhance the period of time for operator response in the event of leakage into, or out of, the system. The surge tanks are maintained at atmospheric pressure via a vent line. The safety requirement of the tank is to ensure that the CCS remains primed and, through its facility to accept shrink or swell, to maintain the CCS inventory and pump suction pressure. Two surge tanks are provided in the event that the CCS subsystems are segregated. Normally, only one CCS surge is operated.

- **CCS CIV Relief Valve (CCS-PL-V220) –** A relief valve is provided to prevent overpressurisation of the return component cooling water line containment penetration. This relief valve prevents overpressurisation that might be caused by thermal expansion of the fluid between the containment isolation valves following an event causing containment isolation. This relief valve is located inside the containment.

- **CCS CIVs (CCS-PL-V200, -V207, -V208)** – These are 250-mm DN (10-inch), motor-operated butterfly valves that fail "as is" on loss of supplies. The valves are required to close on receipt of a safeguard signal from the PMS. This is required to provide isolation of the CCS containment penetrations and is a safety requirement. These valves are also required to close on receipt of a reactor coolant pump bearing water high temperature pump trip signal. This is required to provide automatic isolation of the CCS containment supply and return lines in the event of a reactor coolant pump external heat exchanger tube break at power, to prevent leakage of reactor coolant activity outside containment and radioactive release through the CCS surge tank vent into the turbine building.

- **CCS CIV Check Valve (CCS-PL-V201)** – This is a 250-mm DN (10-inch) swing check valve. The valve is required to close on reverse flow. This prevents reverse flow in the CCS inlet line to containment and also contributes to containment integrity. The safety requirement is to isolate the flow of water.

17.10.1.3 Claims on Components and Equipment

Component Cooling Water Pumps (CCS-MP-01A/B)

The component cooling water pumps provide the motive force to circulate water around the system. This flow provides the heat transfer capability to support transfer of decay heat from the reactor core via the RNS, and the SFP via its cooling system. Removal of decay heat is a Category A safety function mini-flow heat exchanger and the CCS pumps are Class 2. See Appendix 15A.

Two CCS pumps are provided, either of which can provide sufficient CCS flow to ensure the provision of adequate cooling. The requirement on the pumps is that they will continue to run reliably as required.

CCS Heat Exchangers (CCS-ME-01A/B)

The component cooling water HXs provide the facility for heat transfer to the SWS and consequent control of temperature. This supports the transfer of decay heat from the RNS and the SFS. Removal of decay heat is a Category A safety function and the CCS HXs support are Class 2. See Appendix 15A.

There are two CCS HXs, either of which can provide the full cooling duty. The requirement on the HXs is that they will provide adequate heat transfer, will not impair the operation of the CCS, and will not be unavailable because of leakage.

CCS Surge Tanks (CCS-MT-01A/B)

The CCS surge tanks provide the facility to accommodate shrink and swell of the CCS fluid due to bulk temperature changes. They also allow the total CCS inventory to be monitored. This allows the CCS to support the transfer of decay heat from the RNS and the SFS. Removal of decay heat is a Category A safety function and the CCS surge tanks are Class 2. See Appendix 15A.

CCS CIV Relief Valve (CCS-PL-V220)

A relief valve is provided to prevent overpressurisation of the return component cooling water line containment penetration. The valve serves to support containment integrity and the prevention of the release of radioactive material. This is a Category A safety function. The valves are considered Class 1. See Appendix 15A.

CCS CIVs (CCS-PL-V200, -V207, -V208)

The CIVs serve to support containment integrity and the prevention of the release of radioactive material. This is a Category A safety function. The valves are considered Class 1. See Appendix 15A.

These valves are also required to close on receipt of a reactor coolant pump bearing water high temperature pump trip signal. This is required to provide automatic isolation of the CCS containment supply and return lines in the event of a reactor coolant pump external heat exchanger tube break at power, to prevent leakage of reactor coolant activity outside containment and radioactive release through the CCS surge tank vent in the turbine building. Prevention of release of radioactive material through the RCS pressure boundary is a Category A safety function. The primary protection against these is through the integrity of the RCP high pressure motor coolers.

Two valves are partnered in isolation of the penetration and the requirement is that at least one of them will close on demand. A third motor-operated valve is partnered with the check valve in isolation of the penetration. The requirement is that this valve will close on demand.

CCS CIV Check Valve (CCS-PL-V201)

The CIV serves to support containment integrity and the prevention of the release of radioactive material. This is a Category A safety function and the valve is considered Class 1. See Appendix 15A.

The valve is partnered with a motor-operated valve in isolation of the penetration. The requirement is that this valve will close on demand.

17.10.1.4 Justification of Claims on Components and Equipment

Component Cooling Water Pumps (CCS-MP-01A/B)

The component cooling water pumps are designed to Hydraulic Institute standards and are very similar to the design of like pumps on currently operating PWRs. As a result, the information from the operation of these in-service pumps offers a high degree of confidence about the reliability to be expected from these pumps. Data collected from in-service plants (Reference 17.7, Table 5-1) indicate the probability of failure to start, the probability of failure within the first hour of operation and the probability of failure to continue operation. This indicates that the claims being made are in line with operational experience.

Given that with the unit at power, at least one of the CCS pumps will be running, the claims applicable to the starting conditions for the majority of fault sequences are considered conservative.

Routine maintenance and testing of the CCS pumps will be performed according to the manufacturer's recommendations and will include routine changeover of the pumps allocated to duty and standby roles. No specific surveillance test requirements are identified.

CCS Heat Exchangers (CCS-ME-01A/B)

The use of HXs for this type of application is very well established. The use of this type of heat exchanger gives the ability to easily change the number of plates installed and consequently allow variations to be made in cooler flow velocity, and heat exchange area, to optimise the performance of the coolers to the system needs. The plate heat exchangers are substantially smaller than conventional shell and tube heat exchangers since they operate in a true counter-current flow arrangement and use turbulent flow to increase the U-value of the heat exchanger.

Routine maintenance and testing of the CCS HXs will be performed according to the manufacturer's recommendations and will include routine changeover of the HXs allocated to duty and standby roles. No specific surveillance test requirements are identified.

Component Cooling Water System Surge Tanks (CCS-MT-01A/B)

The CCS surge tanks are mounted at a high elevation that allows them to be open to atmosphere while still inherently providing acceptable net positive suction head for the CCS pumps.

Whilst the tanks are constructed from carbon steel, the internal surfaces are coated to provide protection against corrosion from the CCS fluid. The tanks are constructed to ASME Boiler and Pressure Vessel Code, Section VIII, Division 1 (Reference 17.9). The design is very similar to like tanks on currently operating PWRs and on other nuclear power stations. This gives considerable confidence that the tank will be able to perform as expected.

Routine maintenance and inspection of the CCS surge tanks will be performed according to the manufacturer's recommendations. No specific surveillance test requirements are identified.

CCS CIV Relief Valve (CCS-PL-V220)

A relief valve is provided to prevent overpressurisation of the return component cooling water line containment penetration. This relief valve prevents overpressurisation that might

be caused by thermal expansion of the fluid between the containment isolation valves following an event causing containment isolation. The valve is manufactured from carbon steel which is compatible with the CCS water with corrosion inhibitor that passes through them. They are designed to ASME Boiler and Pressure Vessel Code, Section III-2.

The maintenance and testing arrangements for the CCS CIVs are based on the ASME programmes appropriate for these types of valves as used in existing nuclear power stations. The testing is:

- Visual confirmation of valve operation during the stroke testing is performed every 2 years.

- Given that they are CIVs, seat leakage limits will be tested to verify leak tightness. This test will be performed as an LLRT in line with the CIV leak test programme (Reference 17.11).

Containment Isolation Valves (CCS-PL-V200, -V207, -V208)

The CIVs are motor operated, which means they will inherently fail "as is" and clearly this is not fail-safe with respect to the containment isolation function itself. Given that spurious actuation of this function when not required could, in itself, give rise to safety concerns, this arrangement is judged appropriate.

All valves are manufactured from carbon steel which is compatible with the CCS water with corrosion inhibitor that passes through them. They are designed to ASME Boiler and Pressure Vessel Code, Section III-2.

The maintenance and testing arrangements for the CCS CIVs are based on the ASME programmes appropriate for these types of valves as used in existing nuclear power stations. The testing is:

- A full stroke operability test is performed in accordance with the ASME Boiler and Pressure Vessel Code.

- Visual confirmation of valve operation during the stroke testing is performed every 2 years.

- Given that they are CIVs, seat leakage limits will be tested to verify leak tightness. This test will be performed as an LLRT in line with the CIV leak test programme (Reference 17.11).

CCS CIV Check Valve (CCS-PL-V201)

This CIV is a check valve and operation depends only upon the pressure difference across it and not on any method of powered actuation. This passive approach offers a high degree of inherent safety and reliability.

The valve is manufactured from carbon steel to ensure compatibility with the water that passes through it. It is designed to ASME Boiler and Pressure Vessel Code, Section III-2.

The maintenance and testing arrangements for the CCS CIVs are based on the ASME Boiler and Pressure Vessel Code, Section III programmes appropriate for these types of valves as used in existing nuclear power stations. Given that they are CIVs, seat leakage limits will be

tested to verify leak tightness. This test will be performed as an LLRT in line with the CIV leak test programme (Reference 17.11).

17.10.2 Onsite Diesel Generator System (ZOS)

17.10.2.1 Role

A detailed description of the onsite diesel generator system is given in Chapter 18. Further design details of this system and its constituent components are delineated in Reference 17.34 and Section 6.10.

While the system does not provide direct support to any primary safety function in itself, the diesel generators do support a number of systems used as defence in depth to fulfil these primary safety functions. This support is through the provision of standby electrical power supplies that can be made available in the event of a loss of offsite power supplies.

The plant design provides for two independent, self-contained standby diesel generator systems. Each has its own diesel engine, electrical generator, control, and fuel systems. Each onsite diesel generator is connected to separate parts of the main electrical power system as described in Section 6.10 and Chapter 18. In the event of a loss of voltage detected on the associated main 11-kV switchboards, both onsite standby diesel generators are started and some loads from the supported systems are reconnected to the supplies by a sequencer that aims to ensure that the addition of load is done in a way that the diesel engines can accommodate. The remaining loads can be connected manually, as required.

The onsite standby diesel generators provide support to the following systems in performing their defence in depth safety functions:

- RNS
- SFW
- CCS
- SWS
- SFS
- CVS
- FWS (start-up portion)

The standby onsite diesel generators are supported by the standby diesel fuel oil system (DOS); however, this system is used to top off a diesel day tank from which the engines draw their immediate supplies. The standby diesel fuel oil system is therefore only needed in its supporting role for any period of extended loss of offsite power that exceeds 24 hours.

17.10.2.2 System Components and Equipment Contributing to Safety Function

The following subsystems contribute to the diesel generator unit performing its safety function:

- **Diesel Generator Engine (ZOS-MS-05A/B)** – This is a 16-cylinder, turbocharged, four-stroke design with a rated power of approximetly 5 MW. The engine is maintained in a standby mode and is automatically started if low voltage is detected on its associated essential switchboard. The engine then runs up to speed. Fuel is supplied to the engine from a day tank situated at a higher elevation to preclude the need for priming pumps. The requirement to start, run up to speed, and then be loaded up is a safety requirement.

- **Diesel Generator Starting Units (Starting Subsystem)** – This consists of an ac-motor-driven, air-cooled compressor; a compressor inlet air filter; an air-cooled after-cooler; an in-line air filter; a refrigerant dryer; and an air receiver with sufficient storage capacity for three diesel engine starts. The interconnecting stainless-steel piping from the compressor to the diesel engine dual air starter system includes air filters, moisture drainers, and pressure regulators to provide clean, dry, compressed air at normal diesel generator room temperature for engine starting. Provision of air for engine starting is a safety requirement.

- **Air Intake and Exhaust Subsystem** – Each engine is provided with two air intake filters. They are dry-type, replaceable-element paper filters, capable of reducing airborne particulate loading to a level acceptable to the engine before it is fed to a turbocharger. The engine exhaust gas circuit consists of the engine exhaust gas discharge pipes from the turbocharger outlets to a single, vertically mounted outdoor silencer that discharges to the atmosphere. Provision of combustion air and management of exhaust gas is essential to ongoing engine operation and hence is a safety requirement.

- **Diesel Generator Radiators (Engine Cooling Subsystem**) – This is an independent closed-loop cooling system, rejecting engine heat through two separate roof-mounted, fan-cooled radiators. The system consists of two separate cooling loops, each maintained at a temperature required for optimum engine performance by separate engine-driven, coolant water circulating pumps. One circuit cools the engine cylinder block, jacket, and head area; and includes an additional separate motor-driven pump for operation with the engine shut down, while the other circuit cools the oil cooler and turbocharger after-cooler. The cooling water in each loop passes through a three-way contained temperature control valve that modulates the flow of water through or around the radiator, as necessary, to maintain required water temperature. Maintenance of the engine at the correct operating temperature is essential to ongoing engine operation and hence is a safety requirement.

- **Engine Lubricating Oil Subsystem** – This includes an engine oil sump, a main engine-driven oil pump, and a continuous engine prelube system consisting of an ac and dc motor-driven prelube pump and electric heater. The prelube system maintains the engine lubrication system in service when the diesel engine is in standby mode. The safety requirement is to circulate lube oil through the engine and various filters and coolers to maintain the lube oil properties suitable for engine lubrication.

- **Engine Speed Control Subsystem** – This consists of an electrohydraulic governor that provides the primary control and a backup. The system interfaces with the diesel engine fuel rack to ensure that when the engine is running independently with the generator disconnected from the grid supplies, its speed is maintained constant as electrical loads are added or removed, so that the frequency of the generated electrical supply remains within acceptable limits. When the engine is running with its generator connected to the offsite grid, this system is used to regulate output load. The electrohydraulic governor also provides control of the engine acceleration following starting to minimise the risk of overspeed during the run-up. The safety requirement is to accelerate the engine to nominal speed and then maintain engine speed within acceptable limits when operated independently from the offsite grid.

17.10.2.3 Claims on Components and Equipment

Diesel Generator Engine (ZOS-MS-05A/B)

The diesel engines provide power for the onsite electrical system which supports the ac electrical power driven defence in depth functions such as removal of decay heat. Removal of decay heat is a Category A function and the diesel engines are Class 2. See Appendix 15A.

Whilst the two engines are connected to different parts of the main ac power system, each engine feeds respective trains of redundant components in the supported systems. As a result, each diesel can have the same end-duty with respect to the primary safety functions. As such, either engine successfully starting and continuing to run will achieve the safety function. The requirement is therefore that one engine will start on demand, and then, having started, will continue to run until offsite power supplies are restored.

Diesel Generator Starting Units (Starting Subsystem)

The starting subsystem supports the diesel engines. The diesel engines are supporting a Class A function. The starting subsystem is Class 2. See Appendix 15A.

The starting air system maintains enough air stored at pressure to attempt three starts of the engine. As a result, there is no claim against the air compressor and associated systems; the claim is that the air storage receivers and air start valves will operate on demand to deliver enough air, at the correct pressure, for three start attempts.

Air Intake and Exhaust Subsystem

The air intake and exhaust subsystem supports the diesel engines. The diesel engines are supporting a Class A function. The air intake and exhaust subsystem are Class 2. See Appendix 15A.

The requirement against the air intake is that it will provide adequate air supply to the engine, both in terms of volume and quality. The requirement against the exhaust system is that the exhaust products are taken away and discharged in a way that does not lead to unacceptable backpressure for the engine and also does not lead to recirculation back into the air intake.

Diesel Generator Radiators (Engine Cooling Subsystem)

The engine cooling subsystem supports the diesel engines. The diesel engines are supporting a Class A function. The engine cooling subsystem is Class 2. See Appendix 15A.

The requirement against the engine cooling system is that it will provide adequate cooling capacity to ensure that the engine temperatures are maintained within acceptable limits.

Engine Lubricating Oil Subsystem

The engine lubricating oil subsystem supports the diesel engines. The diesel engines are supporting a Class A function. The engine lubricating oil subsystem is Class 2. See Appendix 15A.

The requirement against the lubricating oil system is that it will provide oil, at a suitable temperature, pressure, and quality, to ensure that the diesel engine is adequately lubricated.

Engine Speed Control Subsystem

The engine speed control subsystem supports the diesel engines. The diesel engines are supporting a Class A function. The engine speed control subsystem is Class 2. See Appendix 15A.

The requirement is that the engine speed control subsystem will ensure that the ac frequency does not drop below the specified percent of nominal value at any time during the loading sequence and subsequent operation; and that during each step of the load sequencing, the ac frequency will recover to within specification in no more than specified percentage of the sequence step time interval.

17.10.2.4 Justification of Claims on Components and Equipment

Diesel Engine (ZOS-MS-05A/B)

Diesel engines are a well-established form of standby power supply both in the nuclear power industry and elsewhere. Consequently, there is a large body of evidence supporting the expected reliability and significant effort is put into developing maintenance and testing regimes to maximise reliability.

Reliability data collected from in-service plants (Reference 17.7, Table 5-1) indicate that the claims being made are conservative.

Whilst there are many potential failure mechanisms, the routine surveillances and the surveillance programme are intended to minimise the risks associated with them. Routine maintenance will be performed in line with the manufacturer's recommendations. The testing regime is:

- Verification that the day tank contains more than a minimum volume of fuel oil will be performed monthly.
- Verification that the engine starts correctly and can be loaded in excess of 4 MW and run for more than 1 hour will be performed quarterly.
- Verification that the engine starts correctly and can be loaded in excess of 4 MW and run for more than 24 hours will be performed every 10 years.

Diesel Generator Starting Units (Starting Subsystem)

The starting subsystem air receivers are sized to store sufficient air for three start attempts at the coldest possible ambient air conditions. Given that they are charged up to provide this condition during normal operation and can be monitored at all times, this provides inherent assurance of a start capability for the engine.

The air receivers will be manufactured from carbon steel to the ASME Boiler and Pressure Vessel Code, Section VIII pressure vessel code (Reference 17.9) but will be provided with an interior coating to minimise corrosion. A drain valve is provided at the lowest point to allow any condensate that has collected to be drained as required. Two air start motors and associated starting air valves are provided.

There are no separate figures available for the specific reliability of starting system components, and testing is effectively covered by the arrangements identified above for the

engine. Given that the air receivers will be statutory pressure vessels, however, they will be subject to insurance inspection arrangements.

Air Intake and Exhaust Subsystem

The air intake and exhaust subsystem comprises passive components and are therefore of inherently high reliability. They are not required to change state when the engine starts operating and therefore are subject only to gradual degradation through ageing.

There are no separate figures available for the specific reliability of air intake and exhaust system components, and testing is effectively covered by the arrangements for the engine identified in Section 17.10.2.4.1. Ongoing maintenance will be carried out in accordance with the manufacturer's recommendations to minimise the impact of degradation through ageing.

Diesel Generator Radiators (Engine Cooling Subsystem)

The jacket water cooling subsystem has a separate motor-driven pump that allows the system to be operated with the main diesel engine shut down. This feature, along with an associate jacket water system heater, means that the engine can be maintained warm at all times in preparation for starting. The lubricating oil cooling system is effectively kept warm through transfer of heat from the main lubricating oil warming system.

Once the engine is started, the requirement changes from warming to cooling. The cooling radiators are passive components and the temperature control valve design relies on the inherent properties of materials within the valve and not on external control mechanisms. The active radiator fans provide heat removal from the radiators.

There are no separate figures available for the specific reliability of engine cooling subsystem components, and testing is effectively covered by the arrangements for the engine identified in the beginning of Section 17.10.2.4. Ongoing maintenance will be performed in accordance with the manufacturer's recommendations.

Engine Lubricating Oil Subsystem

The lubricating oil subsystem has a separate motor-driven pump that allows the system to be operated with the main diesel engine shut down. This feature, along with the lubricating oil heater, ensures that the engine components are kept warm and the oil is maintained at an appropriate temperature to ease lubrication of the engine during starting. The lubricating oil heater is thermostatically controlled to ensure that the heater element is maintained cool enough to prevent coking of the oil and the consequent risk of blocking filters and cooler tubes.

Once the engine is started, the requirement changes from warming to cooling. The cooling radiators are passive components and the design of temperature control valve relies on the inherent properties of materials within the valve and not on external control mechanisms. The active radiator fans provide heat removal from the radiators.

There are no separate figures available for specific reliability of engine lubricating oil subsystem components, and testing is effectively covered by the arrangements for the engine identified in the beginning of Section 17.10.2.4. Ongoing maintenance will be performed in accordance with the manufacturer's recommendations.

Engine Speed Control Subsystem

The electro-hydraulic governor can be a part of the diesel engine and is therefore covered by the justification in the beginning of Section 17.10.2.4. A supplemental mechanical governor provides diversity in maintaining engine control.

17.10.3 Service Water System (SWS)

17.10.3.1 Role

A detailed description of the SWS is given in Section 6.11 of this PCSR. Further design details of this system and its constituent components are delineated in Reference 17.35.

The system does not directly contribute to any primary safety function in itself, but it does support the CCS; as a consequence, it indirectly supports a number of the systems used as defence in depth to contribute to the primary safety functions. The support is provided through the provision of a heat transport mechanism for the transfer of decay heat, and heat from other sources, away from the CCS.

The system is made up of two interconnected trains that can be segregated into two independent trains each with an SWS pump and independent pipework to a respective CCS HX. The pipework then continues to take each SWS flow to a separate cooling tower. Each train is capable of providing 100 percent of cooling duty during normal operation. There are also cross connections between the two trains that allow either pump to work with either HX, and either HX to work with either cooling tower. Both trains are required to be in service to meet target cooldown rates in preparation for refuelling, but a single train is capable of meeting this duty with extended cooldown times.

The SWS is supported by the ECS and the ZOS in the provision of its safety function.

The SWS supports the CCS in the provision of its safety function.

17.10.3.2 System Components and Equipment Contributing to Safety Function

The SWS pipework is designed and constructed to ASME B31.1 standards. The following components contribute to the SWS performing its safety function:

- **Service Water Pumps (SWS-MP-01A/B)** – These are vertical, centrifugal, constant-speed, electric-motor-driven pumps. The pumping elements of one pump are mounted in each cooling tower basin structure. One pump is normally running and the safety requirement is to continue running to provide adequate SWS fluid flow to meet design cooling requirements.

- **Service Water Cooling Towers (SWS-MA-01A/B)** – These are counter flow, induced-draft towers. Each utilises one fan, located in the top portion of the cell, to draw air upward through the fill counter to the downward flow of water. Each fan is driven by a two-speed electrical motor through a reduction gearbox. The cooling tower cold water temperature is normally automatically controlled by operation of the tower fans. The fan will be on high speed, low speed, or off, depending on the temperature of the heated service water returning to the cooling tower. When necessary, the water flow to each cooling tower cell can be diverted directly to the basin, bypassing the tower internals. This is achieved by opening a full-flow bypass valve and is used to maintain water temperatures within design limits during very cold ambient conditions. The safety

requirement against the service water cooling towers is that they provide adequate heat transfer to ensure that the SWS water temperature to the CCS HXs remains acceptable through the full range of design heat loads.

17.10.3.3 Claims on Components and Equipment

Service Water Pumps (SWS-MP-01A/B)

The service water pumps provide the motive force to circulate water around the system. This flow provides the heat transfer capability to support transfer of decay heat from the reactor core and the SFP via the CCS HXs. Removal of decay heat is a Category A safety function. The SWS pumps are Class 2. See Appendix 15A.

Two service water pumps are provided, either of which can provide sufficient system flow to ensure the provision of adequate cooling. The requirement on the pumps is that they will continue to run reliably as required.

Service Water Cooling Towers (SWS-MA-01A/B)

The service water cooling towers provide the facility for heat transfer to atmosphere. This supports the transfer of decay heat from the reactor core and the SFP via the CCS HXs. Removal of decay heat is a Category A safety function. The SWS cooling towers are Class 2. See Appendix 15A.

Two cooling towers are provided and provide full cooling duty. The requirement on the cooling towers is that the tower fan will start and run as required and that the tower structure breaks the water flow up into a sufficiently fine flow of droplets so that the design heat transfer takes place.

17.10.3.4 Justification of Claims on Components and Equipment

Service Water Pumps (SWS-MP-01A/B)

The service water pumps are designed to Hydraulic Institute standards and are very similar to like pumps on currently operating PWRs. As a result, the information from the operation of these in-service pumps offers a high degree of confidence about the reliability to be expected from these pumps. Data collected from in-service plants (Reference 17.7, Table 5-1) indicate the probability of failure to start and having started, the probability of failure within the first hour of operation and the probability of failure to continue operation thereafter. This indicates that the claims being made are in line with operational experience.

Given that with the unit at power at least one of the service water pumps will be running, the claims applicable to the starting conditions for the majority of fault sequences could be considered conservative.

Routine maintenance and testing of the SWS pumps will be performed according to the manufacturer's recommendations and will include routine changeover of the pumps allocated to duty and standby roles. No specific surveillance test requirements are identified.

Service Water Cooling Towers (SWS-MA-01A/B)

The service water cooling towers enable evaporative heat transfer to the ambient air to take place. Provided that the water supply to the cooling towers has sufficient pressure to pass

through the sprays, the heat transfer will take place and the service water will be cooled. This is an inherently safe approach.

The service water cooling towers as built will be tested to Cooling Tower Institute standards to confirm that performance is in line with design expectations, as discussed in Reference 17.17. While the design of the cooling tower will always ensure some heat transfer, the tower fan must operate correctly to achieve the design rating. Data collected from in-service plants (Reference 17.7, Table 5-1) indicate the probability of failure to start from standby and the probability of failure within the first hour of operation and the probability of failure to continue operation thereafter.

Routine maintenance and testing of the SWS cooling towers will be performed according to the manufacturer's recommendations and will include routine changeover of the towers allocated to duty and standby roles. No specific surveillance test requirements are identified.

17.11 References

17.1 Westinghouse Report APP-RCS-M3-001, Rev. 8, "Reactor Coolant System, System Specification Document," June 2015.

17.2 Westinghouse Report APP-PV70-GER-002, Rev. 2, "Squib Valve (PV70) and Squib Valve Actuator (PV98) Design Project Summary," October 2016.

17.3 Westinghouse Report APP-CVS-M3-001, Rev. 7, "**AP1000**® Chemical and Volume Control System (CVS) System Specification Document," October 2015.

17.4 ASME Boiler & Pressure Vessel Code, Section III, "Rules for Construction of Nuclear Facility Component," American Society of Mechanical Engineers.

17.5 Westinghouse Report APP-SGS-M3-001, Rev. 7, "**AP1000** Steam Generator System (SGS) System Specification Document," March 2016

17.6 Westinghouse Document WCAP-16779-NP, Rev. 1, "Overpressure Protection Report for AP1000 Nuclear Power Plant," August 2010.

17.7 NUREG/CR-6928, "Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants," U.S. Nuclear Regulatory Commission, February 2007.

17.8 Westinghouse Report APP-MSS-M3-001, Rev. 3, "**AP1000** Main Steam System Specification Document," June 2012.

17.9 ASME Boiler & Pressure Vessel Code, Section VIII, Division 1, "Design and Fabrication of Pressure Vessels," American Society of Mechanical Engineers.

17.10 ASME Boiler & Pressure Vessel Code, Section B31.1, "Power Piping," American Society of Mechanical Engineers.

17.11 10 CFR 50, Appendix J, "Primary Reactor Containment Leakage Testing for Water-Cooled Power Reactors," U.S. Nuclear Regulatory Commission.

17.12 Westinghouse Report WCAP-16914-P (APP-MY03-T2C-003), Rev. 6, "Evaluation of Debris Loading Head Loss Tests for AP1000 Recirculation Screens and In-Containment Refuelling Water Storage Tank Screens," April 2015.

17.13 ANS 57.1, "Design Requirements for Light Water Reactor Fuel Handling Systems," American Nuclear Society, 1992.

17.14 NUREG-0554, "Single-Failure-Proof Cranes for Nuclear Power Plants," U.S. Nuclear Regulatory Commission, May 1979.

17.15 ASME NOG-1-1998, "Rules for Construction of Overhead and Gantry Cranes (Top Running Bridge, Multiple Girder)," American Society of Mechanical Engineers, January 1998.

17.16 ASME Boiler & Pressure Vessel Code, Section B30.2, "Below the Hook Lifting Devices," American Society of Mechanical Engineers.

17.17 CTI-ATC-0105, "Acceptance Test Code," Cooling Tower Institute, February 2000.

17.18 Westinghouse Report APP-BDS-M3-001, Rev. 8, "Steam Generator Blowdown System – System Specification Document," April 2015.

17.19 ASME B16.34 - Valves Flanged, Threaded and Welding End.

17.20 Westinghouse Report APP-MTS-M3-001, Rev. 4, "**AP1000** Main Turbine System – System Specification Document," July 2015.

17.21 NUREG-0138, Issue 1, "Staff Discussion of Fifteen Technical Issues," Nuclear Regulatory Commission, November 1976.

17.22 Not Used.

17.23 Westinghouse Report APP-FWS-M3-001, Rev. 7, "**AP1000** Main and Startup Feedwater System – System Specification Document," June 2015.

17.24 Westinghouse Report APP-DWS-M3-001, Rev. 1, "Demineralized Water Transfer and Storage System Specification Document," September 2015.

17.25 Westinghouse Report APP-PXS-M3-001, Rev. 7, "Passive Core Cooling System, System Specification Document," July 2015.

17.26 Westinghouse Report APP-RNS-M3-001, Rev. 5, "Normal Residual Heat Removal System – System Specification Document," May 2015.

17.27 Westinghouse Report APP-PCS-M3-001, Rev. 8, "Passive Containment Cooling System – System Specification Document," September 2015.

17.28 Westinghouse Report APP-CNS-M3-001, Rev. 4, "Containment System: System Specification Document," August 2015.

17.29 Westinghouse Report APP-FHS-M3-001, Rev. 2, "AP1000 Fuel Handling System - System Specification Document," October 2014.

17.30 Westinghouse Report APP-MH01-Z0-101, Rev. 4, "Design Specification for AP1000 Polar Crane for Mechanical Handling System (MHS)," August 2014.

17.31 Westinghouse Report APP-MHS-M3-101, Rev. 2, "AP1000 Mechanical Handling System - System Specification Document," July 2014.

17.32 Westinghouse Report APP-SFS-M3-001, Rev. 8, "**AP1000**® Spent Fuel Pool Cooling System - System Specification Document," March 2016.

17.33 Westinghouse Report APP-CCS-M3-001, Rev. 4, "**AP1000** Component Cooling Water – System Specification," June 2013.

17.34 Westinghouse Report APP-ZOS-E8-001, Rev. 0, "Onsite Standby Power System Specification Document," July 2015.

17.35 Westinghouse Report APP-SWS-M3-001, Rev. 2, "**AP1000** Service Water System – System Specification Document," June 2012.

17.36 Westinghouse Report UKP-GW-GL-200, Rev. 1, "AP1000 Squib Valve Safety Case," December 2016.

17.37 Westinghouse Report APP-RXS-M3-001, Rev. 6, "Reactor System (RXS) System Specification Document (SSD)," May 2014.

APPENDIX 17A
FUEL HANDLING EQUIPMENT OPERATION EXPERIENCE

The fuel handling equipment in the AP1000 design is very similar to the equipment used for the same purpose on previous Westinghouse pressurised water reactors. To understand how well the fuel handling equipment has performed on these older stations, a review of the Institute of Nuclear Power Operations (INPO) operating experience database was carried out. As would be expected, there have been a number of events reported, of varying significance. Four of the most significant are considered to be:

- OE30024 – Fuel Transfer System Up-Ender Weld Failure
- OE30103 – Fuel Transfer System Cart Drive Cable Disconnects During Fuel Movement
- OE30245 – Refuelling Equipment Issues
- OE30315 – Manipulator Crane Hoist Fails to Stop Automatically

For these and the other events that were identified, although there was some failure of one or more components on some part of the fuel handling equipment, none of them have led to fuel assembly cladding breaches. Consequently, the AP1000 fuel handling equipment design is based on extensive operating experience.

TABLE OF CONTENTS

TABLE OF CONTENTS (cont.)

LIST OF TABLES

None.

LIST OF FIGURES

LIST OF ABBREVIATIONS AND ACRONYMS

ac	Alternating Current
ADG	Ancillary Diesel Generator
ADS	Automatic Depressurisation System
ALARP	As Low As Reasonably Practiable
C&I	Controls and Instrumentation
CCS	Component Cooling Water System
CDF	Core Damage Frequency
CMT	Core Makeup Tank
CVS	Chemical and Volume Control System
DAS	Diverse Actuation System
DBA	Design Basis Accident
DBE	Design Basis Event
dc	Direct Current
DiD	Defence in Depth
DG	Diesel Generator
ECS	Main AC Power System
EDS	Class 2 dc and Uninterruptible Power Supply System
EGS	Grounding and Lightning Protection System
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
EPA	Electrical Penetration Assembly
ESF	Engineered Safety Features
FWS	Startup Feedwater System
IDS	Class 1 dc and Uninterruptible Power Supply
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
LRF	Large Release Frequency
MCC	Motor Control Centre
MCR	Main Control Room
MSU	Main Step-Up
PAM	Post-Accident Monitoring
PCCWST	Passive Containment Coolign Water Storage Tank
PCS	Passive Containment Cooling System
PCSR	Pre-Construction Safety Report
PLS	Plant Control System
PMS	Protection and Safety Monitoring System
RAT	Reserve Auxiliary Transformer
RCP	Reactor Coolant Pump
RNS	Normal Residual Heat Removal System
RSW	Remote Shutdown Workstation
SFS	Spent Fuel Pool Cooling System
SSC	Structures, Systems, and Components
SSE	Safe Shutdown Earthquake
SWS	Service Water System
UAT	Unit Auxiliary Transformer
UK	United Kingdom

LIST OF ABBREVIATIONS AND ACRONYMS (CONT.)

UPS	Uninterruptible Power Supply
US	United States
VFD	Variable Frequency Drive
VT	Voltage Transformer
ZAS	Main Generation System
ZOS	Onsite Standby Power System

18 ESSENTIAL ELECTRICAL SYSTEMS

18.1 INTRODUCTION

18.1.1 Architecture

This chapter of the Pre-Construction Safety Report (PCSR) provides a description of the electrical systems for the AP1000 plant, including the main electrical system supply from the grid, the Class 1, 2, and 3 distribution systems, ac and dc supplies, and the standby and ancillary diesel generators. Offsite power is considered general non-safety prior to connection to the high side of the Unit Auxiliary Transformers (UATs). From the low side of the UATs to the medium voltage buses ES3-ES7 are Class 3, ES1 and ES2 are Class 2. A one-line diagram showing the electrical system architecture and classification is provided in the "AP1000 Electrical System Basis of Safety Case," Reference 18.25. Electrical system design principles, equipment layout, installation requirements, and high level safety functions are also described within the arguments and evidence that support the safety claims contained in Reference 18.25.

The AP1000 plant design philosophy uses passive Class 1 structures, systems or components (SSCs) as the principal means of providing Category A safety functions (primarily criticality control, residual heat removal, containment, and spent fuel pool makeup and cooling) with active Class 2 SSCs providing defence-in-depth (DiD). Due to the passive nature of the principal means of providing Category A safety functions, there are no alternating current (ac) motors associated with the AP1000 plant's Class 1 safe shutdown function. The AP1000 plant is designed to achieve safe shutdown in the complete absence of all external or internal ac power supplies, including onsite standby generation, as described in Appendix 9C. Safe shutdown as used in this document is defined in Appendix 9C to be K_{eff} less than 0.99 and an average RCS temperature less than 215.6°C (420°F). The credited electrical systems for a given fault are presented in Chapter 8. Note that DiD considerations result in a plant that is normally operated and shut down utilising available ac power supplies and components.

The AP1000 plant electrical system fulfils a number of electrical functions that are important to nuclear safety and contribute to DiD. To achieve its safety and operational objectives, the AP1000 plant electrical system is subdivided into the following functional units, which are classified in accordance with their importance to nuclear safety using the scheme described in Chapter 6:

- Main grid voltage, 27kV voltage main generator bus and 11kV voltage ac electrical distribution systems (main generation system [ZAS] and main AC power system [ECS] – Classes 1, 2, and 3, note that the only Class 1 portions of this ac power system is the RCP trip breaker.)
- Class 2 Standby 11kV ac diesel generator system onsite standby power system (ZOS)
- Class 1 250V dc electrical distribution system (IDS)
- Class 2 125/250V dc electrical distribution system (EDS)

Safety claims made in regard to the overall electrical system are incorporated in the "Electrical Basis of Safety Case Document", UKP-GW-GL-163 (Reference 18.25).

Simplified one line diagrams of the ac and dc electrical systems are shown in Figures 18-1A, 18-1B, and 18-3 through 18-6. A description of the high, medium, and low voltage ac systems and the low voltage dc systems is provided below.

18.1.2 High Voltage AC Electrical System Interfaces with the Grid

The high voltage system (ZAS and ECS) includes the main generator and its circuit breaker, unit auxiliary transformers, reserve auxiliary transformers (all Class2 and 3 designated SSCs), and the interconnecting busses. The main generation connection (when generator is online) and the plant maintenance connection (when the generator is offline) to the grid is via the main step-up transformers (grid voltage/27kV). An alternate maintenance connection that is also used for fast bus transfer is available to medium voltage busses from the grid via the reserve auxiliary transformers (grid voltage/11kV). The fast bus transfer functionality of the alternate connection is discussed in Section 18.4. This portion of the electrical system includes Class 2 and 3 SSCs.

Seven 11kV busses, including the 11kV standby diesel generators (Class 2), the reactor coolant pumps (RCPs) associated trip circuit breakers (Class 1), and variable frequency drives (VFDs), are connected to the safety SSCs.

The 11kV medium voltage bus ECS ES-1 and ES-2 services the plant DiD loads. These 11kV buses can be supplied by either the unit auxiliary transformers, reserve auxiliary transformers, or the backup standby diesels. The standby diesels are Class 2, and both sets of transformers are Class 3.

18.1.3 Low Voltage AC Electrical Distribution Systems

The low voltage ac electrical distribution system (part of ECS) includes load centres, motor control centres, and distribution panels and interconnecting cables, and are Class 3 electrical systems. The ancillary diesel generators (Class 2) provide means to supply low voltage ac power to selected loads in the post-72 hours Design Basis Event (DBE) scenario of the plant design basis. In the event that the onsite ancillary diesel generators are unavailable, for instance following a seismic event, offsite portable generators can be brought onsite and connected via a Class 1 connection point.

18.1.4 Direct Current Electrical Systems

The dc systems include both the Class 1 250V dc (and the associated 230V ac electrical inverter distribution system [IDS]) and the Class 2 125/250V dc (and the associated 230V ac electrical inverter distribution system [EDS]) that serve plant loads.

Included within IDS are batteries, battery chargers, battery monitors, inverters, transfer switches, regulating transformers, motor control centres, various distribution panels, and interconnecting cables. See Figures 18-3, 18-4, and 18-4A for the IDS functional arrangement diagrams.

Included within the EDS are batteries, battery chargers, battery monitors, inverters, transfer switches, regulating transformers, various distribution panels, and interconnecting cables. Inverters are not included as part of the EDS5 subsystem, however. The EDS functional arrangement diagrams are shown in Figures 18-5 and 18-6.

18.1.5 Human Factors Interface

Human operations of electrical related activities are assessed by the human factors group. As a result of Human Factor analysis, a summary of the human factors is provided for the inputs to the design and safety processes, error identification methodology and classification, and ALARP arguments. The "UK AP1000 Plant Electrical Equipment Maintenance and Surveillance" (Reference 18.24) provides guidance for the human factors input necessary during development of the site specific maintenance procedures for the electrical system. Reference 18.25 provides claims, arguments, and evidence regarding the human factors assessment of human operations in support of the electrical system as well as the development of the site specific procedures.

18.2 ELECTRICAL SYSTEM DESIGN PRINCIPLES

18.2.1 Electrical Equipment Redundancy, Diversity, and Separation Requirements

The design of the AP1000 plant power distribution systems requires physical separation between Class 1 circuits and between Class 1 and Class 2 or 3 circuits. Electrical isolation is also required between Class 1 and interfacing Class 2 or 3 circuits. Redundancy is designed into IDS, EDS, ZOS, and ECS to maintain availability, reliability, and maintainability of these systems.

The diverse mitigation of frequent faults (faults with initiating event frequencies greater than or equal to 1E-3) is assessed in Reference 18.22. Reference 18.22 considers all frequent faults and identifies both a primary and a diverse means of mitigating each fault including the source of electrical power. This assessment provides evidence that the electrical system supports the diversity requirements of the AP1000 safety systems, as claimed in the safety claims of Reference 18.25.

The electrical system supports diversity of PMS and DAS by providing two separate systems. In order to provide a diverse means of performing the necessary safety functions the DAS (powered by the 2 divisions of EDS) requires a different normal input power supply from the PMS (powered by the 4 divisions of IDS). Further detail on the electrical system support of DAS diversity is provided in the claims and arguments made in Reference 18.25. Specific redundancy and separation requirements for the IDS, EDS, ZOS, and ECS are discussed below.

Redundancy (IDS – Class 1)

The IDS has five independent 250V dc battery subsystems organized in four divisions: A, B, C, and D and a full spare battery system. Divisions A and D are each comprised of one battery bank, one switchboard, and one battery charger. Divisions B and C are each composed of two battery banks, two switchboards, and two battery chargers. The battery banks in divisions A through D, designated as a 24-hour battery bank, provide power to the loads required for the first 24 hours following a DBE. The second battery bank in divisions B and C, designated as a 72-hour battery bank, is used for those loads requiring power for the first 72 hours following a DBE. The spare battery system is comprised of one battery bank, one switchboard, and one battery charger. All battery banks in divisions A, B, C, D and Spare are identical.

A fused transfer switch panel is used to connect each battery to its switchboard. Each switchboard connected to a 24-hour battery bank supplies power to an inverter, a dc distribution panel, and a dc motor control centre (MCC). All Class 1 battery banks are

identically sized, including a spare to allow for easy replacement and continued availability of dc power. The batteries have been designed based upon a calculated load profile with margin for thermal aging and other design factors.

Safe shutdown of the reactor at any time can be achieved with any three of the four 24 hour IDS divisions. As described in Appendix 9C, the necessary ADS actuation is driven by a timer to automatically occur within the 24 hour capacity of the IDS batteries. The IDS 72 hour batteries provide the power to support plant monitoring of the safe shutdown state.

The IDS inverter system provides power at 230V ac within each of the four independent divisions, primarily for powering of controls and instrumentation (C&I) loads. Under normal operation, the inverters receive power from the associated charger with the associated battery bank in standby. If an inverter is inoperable, the static switch featuring a make before break contact automatically switches to regain power from the backup AC power source. Backup power is provided by a regulating transformer connected to a low voltage/medium voltage bus arrangement supplied from a standby diesel generator backed Class 2 bus.

To supply power following the post-72-hour period following a DBE, two ancillary ac generators are provided to supply power to the Division B and Division C ac loads via the regulating transformers. This ac power source can be used to power post-accident monitoring (PAM) loads, lighting in the main control room (MCR), and portable ventilation in the MCR and Division B and C C&I rooms. Figure 18-4 shows the post-72-hour power distribution subsystem.

If the permanently installed Class 2 ECS ancillary generators are not available, then temporary portable generators can be used. Power cables from these generators would be connected to the ancillary diesel generator panels or to the secondary of the IDS regulating transformers. The connection details for the portable generators are discussed in detail in the "AP1000 Plant Post-Fukushima Assessment," UKP-GW-GGR-201 (Reference 18.4). These portable generators are assumed to be stored for enough from the plant that they will be isolated from the event, and a Class 1 connection point is provided in order to ensure post-72-hour support is available following a seismic event.

Reference 18.25 contains safety claims relating to post-72 hour support and portable generators.

Figure 18-3 shows the functional arrangement of the 24-hour IDS subsystem for Divisions A and D, which provides the electrical supply to the Class 1 systems. Figure 18-4 shows the functional arrangements of the 24-hour and 72-hour IDS for Divisions B and C. As these figures show, these systems have electrical supplies through the following three alternatives:

- Supply from the battery
- Supply from the main generator or offsite sources through the ECS and the charger
- Supply from the standby diesel generator (ZOS) through the ECS and the charger

Segregation (IDS – Class 1)

Segregation of the divisions within the IDS is incorporated into the design. The AP1000 plant cable and cableway system comprises five distinct and physically separated groups, namely Groups A, B, C, D, and N. Separation Group A contains power, control, and instrument cables connected to Class 1 components of division A only. Likewise, separation of Group B serves Class 1 components of Division B only and similarly for Divisions C and D. Cables and cableway designated as separation Group N serve equipment not assigned to the four

groups performing Class 2 safety functions. Group N cableways are allowed to be routed in the same areas as Groups A, B, C, or D as long as the established horizontal and vertical separation distances, defined in APP-GW-E1-001, "Electrical Systems Design Criteria," (Reference 18.31) are strictly observed. The IDS equipment is physically separated. The IDS ac and dc panels are split up amongst four different rooms at elevation 100 m (100') and 102.134 m (107'). The 72 hour battery racks are located at elevation 94.666 m (82'-6") in two independent rooms. Likewise the four divisions of IDS 24 hour battery racks are located in four individual rooms at elevation 89.789 m (66'-6") along with the spare battery rack in a separate room. The battery chargers and regulating transformers are organized by division at elevation 94.666 m (82'-6") in four separate rooms.

Cableway separation and segregation criteria are defined by Reference 18.1.

Redundancy (EDS – Class 2)

The EDS has four dc battery systems (EDS1 to EDS4) organized in two subsystems, 1 and 2 (Figure 18-5), with another dc system – EDS5 (see Figure 18-6). A spare EDS battery system (EDSS) is also provided and can be used in place of any of the EDS battery subsystems.

Figure 18-1B shows the arrangement of the EDS1, EDS2, EDS3, and EDS4, which provide the electrical supply to the Class 2 systems. Figure 18-5 shows that EDS1, EDS2, EDS3, and EDS4 have three supplies from the following:

- Supply from the battery
- Supply from the main generator or offsite sources through the ECS and the charger
- Supply from the standby diesel generator (ZOS) through the ECS and the charger

Segregation (EDS – Class 2)EDS battery chargers and inverters are separated. The EDS battery racks are located in two rooms in the annex building with EDS2 and EDS4 grouped together and EDS1 and EDS3 together. In the turbine building EDS1 and EDS3 dc distribution panels are located in switchgear room #1, and EDS2 and EDS4 dc distribution panels are located in switchgear room #2. The EDS ac distribution panels are located in the annex building two electrical switchgear rooms.

Redundancy and Segregation (ZOS – Class 2)

Provision for redundancy and segregation within the ZOS/ECS Class 2 standby diesel generator system is as follows:

- Only one of two standby diesel generators is required as each one is rated at 100 percent of the load required to supply the Class 2 DiD loads.

- Redundant sets of Class 2 ac powered equipment (ZOS-MG02A & ZOS-MG02B) are provided – each connected to one of the two diesel generators (DGs).

- The switchgears are in separate rooms within the annex building and the standby diesel generators in separate rooms within the diesel generator building.

Redundancy and Segregation (ECS – Class 2 and Class 3)

Provision has been made in the design of the Class 3 ECS to maintain supplies to the Class 1and 2 inverter systems through the Class 2 switchboards ECS-ES-1 and ECS-ES-2 by having alternative supplies from separate sources to each switchboard (Figures 18-1A and

18-1B). The Class 3 ECS switchboards are located in both the annex and turbine buildings in separate locations to the Class 2 switchboards, providing segregation between the two classes of systems. The Class 1 RCP breakers are located in the auxiliary building and its Class 2 distribution boards are situated in the annex building. Redundancy is provided by the use of two RCP breakers in series with each breaker's control supplied from a different division of IDS (Figure 18-1C). Segregation is provided by having each of the breakers in a pair located in separate areas of the auxiliary building.

There are two ancillary diesels provided for redundancy purposes. Each ancillary diesel is rated to power the necessary systems to support post-72-hour maintenance of safe shutdown including one train of post-accident monitoring. The preferred supply is from the ECS with the alternative supply provided by the corresponding ancillary diesel generator, see Figure 18-7. In addition to the ancillary diesel generators, offsite portable generators can be brought on site in the event the ancillary diesel generators are not available. The offsite diesel generators can be connected to where the ancillary diesel generators connect or directly to the IDS in the auxiliary building.

18.2.2 Cable and Cableway System Design and Installation

18.2.2.1 Cable and Cableway Design Principles

All cables are sized to carry steady state load current and calculated fault current as well as to minimize voltage drop. Class 1 cables are qualified in accordance with the "AP1000 Environmental Conditions for Equipment Qualification," APP-GW-VP-030 (Reference 18.5). This requirement is captured in the design specifications referenced within Reference 18.25. All Class 1 cables are appropriately protected from mechanical damage using cable trays and/or rigid metal conduit. Separation and segregation is in accordance with defined nuclear and conventional installation standards; the standards are referenced in subsection 18.2.1 of the PCSR. Class 2 and 3 designated cables and cableways are electrically and physically isolated from the safety cables, cableways, and Class 1 power sources.

The IDS, EDS, and ECS cables and cableways are routed such that required separation between redundant components and systems is maintained.

Different levels of cable separation are applied for the various safety classes commensurate with the safety category of the component function. Complete electrical isolation and physical separation is applied for Class 1 DC and inverters (IDS) performing Class 1 functions. Physical separation is maintained between the different groups as well as between the IDS and other Class 2 and 3 systems.

Separation is provided for Class 2 electrical cables which provide power to redundant functions required for normal shutdown. The redundant trains are routed in separate raceways with fire protection or fire suppression within the rooms provided between the trains. Individual cables and conduits are used to separate the trains of the ancillary diesel power cables.

18.2.3 Earthing and Lightning Protection System Design and Installation

18.2.3.1 Earthing and Lightning Design Principles

The earthing and lightning protection system (EGS) of the AP1000 plant summarises the functions, design criteria, and design data of the EGS and its components (Reference 18.3). It also includes the layout, instrumentation and control, interfacing system, and

environmental requirements, describes system operations, identifies monitoring, testing, and maintenance guidelines, and summarises the system design compliance with external criteria (Regulatory, Industry, Utility, etc.). Below provides a high level overview of what the schemes the system grounds and its utilization for investment protection and personnel safety.

This scheme includes the following:

- Station earthing grid
- System earthing
- Equipment earthing
- Instrument/computer earthing
- Management of electromagnetic compatibility (EMC)

EGS provides the following principal functions to provide personnel safety and investment protection:

- Maintains safe voltages across the station grid during system transients
- Provides a low impedance return path
- Maintains safe voltages in station structures during system transients
- Minimizes noise interference in instrumentation systems
- Minimizes the effects of lightning surges to equipment and structures

Lightning protection (direct stroke) is provided for all major structures and outdoor electrical equipment. Lightning arresters, main and down conductors, and air terminals are connected directly to the earthing system. The rolling sphere design concept is used for lightning protection.

Reference 18.25 contains the claims, arguments, and evidence relating to resiliency to transients and disturbances.

Detailed earthing design is site specific; evidence of the earthing design will be provided during the site design phase in alignment with Reference 18.3.

18.2.3.2 Earthing and Lightning Installation Requirements

The plant electrical system neutral, equipment, instrumentation, and lightning protection grounding systems shall be connected to the station grounding grid through the equipment grounding subsystem in accordance with international and local standards as identified in Section 7 of Reference 18.2.

18.2.4 Electrical Protection Device Design

18.2.4.1 Neutral Point Arrangements

The neutral point arrangements for the power distribution system are as follows:

AC Power System (ZAS, ECS, ZOS)

- Main Generator – high resistance ground
- Main Step-up Transformer (high voltage side) – solid ground
- Isolated Phase Bus Duct –solid ground
- Unit Auxiliary Transformers (low voltage side) – low resistance ground

- Start-up Unit Auxiliary Transformers (low voltage side) – low resistance ground
- Reserve Auxiliary Transformers (low voltage side) – low resistance ground
- Standby Diesel Generator – high resistance ground
- Ancillary Diesel Generator –solid ground
- Load Centre Transformer – solid ground
- Lighting and Distribution Transformers – solid ground

DC and Inverter Power Systems (IDS, EDS)

- The DC power systems are ungrounded. The neutral of the inverters is solidly grounded.

18.2.4.2 Electrical Protection Devices

Industry-proven, microprocessor-based, multifunction protective relays are used to provide coordinated protection, monitoring, and control of AP1000 plant ECS electrical components. The protective relay directional and non-directional overcurrent functions are used to protect the electric plant feeders, transformers, motors, and generators. The individual protective relays are connected to a centralised server that provides a graphical interface for mapping serial and Ethernet monitoring data between the protective devices. The relays communicate with the central server via one way communications paths. This safeguarding measure prevents common cause failure of the networked relays as claimed in Reference 18.25.

Class 1 and Class 2 electrical protection devices are used for protection of electrical components in the IDS and EDS respectively.

All protective relays which are considered SMART devices will have their software and hardware assessed according to the guidelines described in section 18.8.2.

Refer to the Electrical Basis of Safety Case (Reference 18.25) for arguments on the protective relaying systems.

18.2.5 Electrical Penetration Assemblies (EPAs) Design

EPAs are used to facilitate the passing of electrical conductors for instruments and electrical devices through the containment vessel and auxiliary building walls. They are designed to meet seismic requirements and to maintain containment integrity under DBE conditions, including pressure, temperature, and radiation. Safety claims on the electrical penetration assemblies are provided in Reference 18.25.

The EPA is a canister design containing multiple feed through modules (solid conduits) mounted between two header plates. Field cables are terminated at each end of the EPA in inboard/outboard enclosure assemblies (junction boxes). Each EPA is designed to carry cables of one voltage class only. Note that the EPAs for the AP1000 plant design conform to the same service level as the cables inside them.

EPA protection panels containing two fuses in series are provided for conductor feedthrough to ensure its containment sealing mechanism is maintained in the event of a short circuit on the containment cable inside. Double isolation is provided for all EPAs. At any boundary of Class 1 and Class 2 circuits there must be a qualified isolation device per the AP1000 plant electrical system design philosophy (Reference 18.31). Refer to the Reference 18.25 for the safety claims on the EPAs.

EPAs are separated according to safety classification and voltage.

18.2.6 Electrical Lighting Design

The normal lighting for ELS is provided by ECS through the MCCs for the AP1000 plant except for the remote shutdown workstation (RSW) and MCR which are provided Class 1 power. During the first 24 hour critical period following a loss of normal lighting, illumination is maintained in all areas required for the performance of emergency operations. Power is maintained jointly by the 24 and 72 hour batteries for the zero to 24 hour period and by the 72 hour batteries for the remaining period after 24 hours. During the post-72-hour period, power is delivered to the emergency lighting and to the normal lighting panels in the MCR and RSW by the ancillary or portable diesel generators through the regulating transformers.

Safety claims on adequate lighting for the MCR and RSW are contained in Reference 18.25.

18.2.7 Electromagnetic Compatibility (EMC) Design

EMC is addressed to ensure electromagnetic compliance, particularly the reduction and mitigation of potential electromagnetic interference (EMI) with regard to Class 1, 2, and 3 systems in accordance with "AP1000 Equipment Qualification Methodology" (Reference 18.30).

The approach to EMC is detailed in Reference 18.13. Further details on the management and mitigation of EMI are given in Sections 11 and 12.

18.2.8 Qualification

All Class 1, 2, and 3 equipment is environmentally and seismically qualified in accordance with Reference 18.5. Class 1 equipment is seismically qualified to function following seismic events, while Class 2 and 3 equipment are required to maintain their integrity following a seismic event so that they do not limit the performance of Class 1 equipment.

18.3 ELECTRICAL SYSTEM ARCHITECTURE/LAYOUT

18.3.1 Containment and Shield Buildings

The components that make up the AP1000 plant electrical systems are located in various plant areas as shown in Figure 18-2. The EPAs are installed in containment and pass through to the auxiliary building. These EPAs serve designated Class 1, 2, and 3 electrical loads in containment including the reactor vessel integrated head package, RCPs, motors, heaters, overhead cranes, lighting, communication, and C&I circuits.

18.3.2 Auxiliary Building

18.3.2.1 General Arrangement

Figure 18-2 shows the general arrangement of electrical system equipment components in the AP1000 plant. The Class 1 IDS equipment and the RCP switchgear are located within the auxiliary building which is a seismic Class I structure.

18.3.2.2 Equipment Rooms

Various Class 1 electrical equipment rooms are provided in the auxiliary building.

The walls between the Class 1 equipment rooms are designed with a 3 hour fire rating. Fire detection is provided in each room. Fire safety case information is provided in Chapter 11.

18.3.2.3 Battery Rooms

The Class 1 IDS divisional batteries including Divisions A, B, C, D and spare are located in separate battery rooms. The 24 hour battery divisions are located on the 89.789 m (66'-6") level. The 72 hour battery divisions are located on the 94.666 m (82'-6") level.

Each battery room is provided with a ventilation system. The supply and exhaust duct serving each division can be isolated from other divisions with combination fire/smoke dampers. Failure of a single combination fire/smoke damper serving a division is accommodated by the presence of combination fire/smoke dampers in the ducts serving other divisions. The system design provides for two fire/smoke dampers in series between electrical divisions. A hydrogen detector in each battery room provides an alarm on a high hydrogen concentration, and exhaust airflow monitors provide an alarm on low airflow.

Safety claims on the separation of equipment in terms of external and internal hazards are contained in in Reference 18.25.

18.3.2.4 Equipment Access

Design for personnel access has been incorporated into the auxiliary building and includes:

- Access, egress, and communications are designed to facilitate personnel in undertaking all necessary operational, maintenance, inspection, and testing activities.
- General lighting is provided for all areas. Provisions for access to the components of the IDS for maintenance and operation are in accordance with the requirements of "The Electricity at Work Regulations" (Reference 18.17) and "Requirements for electrical installations, IEE Wiring Regulations, BS 7671:2008 (Reference 18.18), and local fire and safety requirements.
- All IDS equipment is located in the auxiliary building outside of radiological areas requiring controlled access.
- For those facilities and control functions essential to carrying out Class 1 functions and that may require local manual intervention, two alternative means of access are provided.

18.3.3 Annex Building

18.3.3.1 General Arrangement

Figure 18-2 shows the general arrangement of electrical system equipment components in the AP1000 plant. The annex building is a limited seismically rated structure which contains the Class 2 EDS battery systems 1 through 4 (which serve the redundant system loads that are important to plant operation and investment protection), ECS switchgear rooms 1 and 2 and panel boards, and the ancillary diesel generators (see Figures 18-1B and 18-7).

The Class 2 ECS switchboards are mounted in the annex building away from the Class 3 ECS switchboards located in the turbine building, providing segregation between the two classes of systems.

18.3.3.2 Electrical Switchgear Rooms

Two ECS electrical switchgear rooms are located in the annex building. Separation of Class 2 distribution boards ES1 and ES2 and load centres is provided. The two Class 2 ECS switchboards are located in different switchgear rooms in the annex building away from the Class 3 ECS switchboards in the turbine building, providing segregation between the two classes of systems.

The walls between the Class 2 equipment rooms are designed with a 2 hour fire rating. Fire detection and suppression systems are provided in each room. Fire safety case information is provided in Chapter 11.

18.3.3.3 Battery Rooms (EDS)

The Class 2 EDS battery chargers and dc distribution equipment are located in the annex building in two separate rooms next to the two EDS battery rooms. Two separate power supply groups (EDS1 and EDS3, EDS2 and EDS4) are used to supply the Class 2 loads.

Each battery room is provided with a ventilation system. The supply and exhaust duct serving each EDS subsystem is isolated from other subsystems with combination fire/smoke dampers. Failure of a single combination fire/smoke damper serving a division is accommodated by the presence of combination fire/smoke dampers in the ducts serving other divisions. The system design provides for two fire/smoke dampers in series between electrical divisions. A hydrogen detector in each battery room provides an alarm on a high hydrogen concentration, and exhaust airflow monitors provide an alarm on low airflow.

Safety claims on the Class 1 and Class 2 battery room ventilation are contained in Reference 18.25.

18.3.3.4 Equipment Access

Design for personnel access has been incorporated into the annex building and includes:

- Access, egress, and communications are designed to facilitate personnel in undertaking all necessary operational, maintenance, inspection, and testing activities.
- General lighting is provided for all areas. Provisions for access to the EDS equipment for maintenance and operation are in accordance with the requirements of References 18.17 and 18.18, and local fire and safety requirements.
- EDS equipment located in the annex building is outside of radiological areas requiring controlled access.
- For those facilities and control functions essential to the operation of the plant that may require local manual intervention, an alternative means of access is provided.

18.3.4 Turbine Building

18.3.4.1 General Arrangement

Figure 18-2 shows the general arrangement of electrical system equipment components in the AP1000 plant. The turbine building contains the RCP VFDs, the EDS5 and EDSS battery systems and ECS switchgear rooms 1 and 2 (Figure 18-6).

18.3.4.2 Equipment Rooms

The turbine building contains the Class 3 ECS buses (ES3, ES4, ES5, and ES6) that are separated into two switchgear rooms (ES3 and ES5 in one room, ES4 and ES6 in another room). The ECS EK-31 load centre is located in the same equipment room as ES3 and ES5. Similarly, the ECS EK-41 load centre is located in the same equipment room as ES4 and ES6. The VFDs for the RCPs are located at the other end of the turbine building – above the EDS5 and EDSS batteries.

18.3.4.3 Battery Rooms

EDS5 and the spare EDS batteries are located in the same battery room in the turbine building. The Class 2 EDS5 and EDSS battery chargers and their associated dc distribution equipment are located in the turbine building in a separate room next to the EDS5/EDSS battery room.

18.3.4.4 Equipment Access

Design for personnel access has been incorporated into the turbine building including:

- Access, egress, and communications are designed to facilitate personnel in undertaking all necessary operational, maintenance, inspection, and testing activities.
- General lighting is provided for all areas. Provisions for access to the EDS equipment for maintenance and operation are in accordance with the requirements of Reference 18.17 and 18.18, and local fire and safety requirements.
- The EDS equipment located in the turbine building is outside of radiological areas requiring controlled access.
- For those facilities and control functions essential to the operation of the plant that may require local manual intervention, an alternative means of access is provided.

18.3.5 Standby Diesel Generator Buildings

Figure 18-2 shows the general arrangement of system components in the AP1000 plant. Two independent standby diesel generators (ZOS MG-02A and MG02B) and their auxiliaries are located in separate rooms in a separate diesel generator non-seismic building. The contents and location of the standby diesel generator equipment room are shown in Figure 18-8A.

18.3.6 Power Transformer Yard

The power transformer yard containing the main step-up transformers, unit auxiliary transformers, reserve auxiliary transformers, excitation transformer, interconnecting

iso-phase bus and non-segregated bus (part of ZAS) are located outside of the plant adjacent to the turbine building.

18.3.7 Switchyard Interface

Two interfaces to the high voltage switchyards are made to provide the main ac power connection and the maintenance ac power connection to the grid. The main ac power connection ties the main step-up transformers to the transmission lines coming from the 400kV switchyard. The maintenance ac power connection ties the reserve auxiliary transformers to the transmission lines coming from the switchyard.

18.4 MAIN ALTERNATING CURRENT ELECTRICAL SYSTEM (ECS AND ZAS)

18.4.1 Safety Class 2 and Safety Class 3 Functions and Requirements

18.4.1.1 Safety Functions

The ECS supplies ac power to the AP1000 plant in all normal modes of operation.

The ECS utilizes preferred, maintenance, and standby power supplies to distribute power to Class 2 and Class 3 loads. Onsite standby diesel generators are provided as back up supplies to two Class 2 11 kV buses (ECS ES1 and ES2) so that unnecessary actuation of the passive safety system is prevented.

Additional generator capacity is provided for post-72-hour functions that support post-72-hour maintenance of safe shutdown by the Class 2 ancillary diesel generators.

18.4.1.2 Safety Function Requirements

For transients or faults where operation of the core makeup tanks (CMTs) is claimed to provide criticality control via boration and/or residual heat removal, it is necessary to trip the RCPs to enable proper operation of the CMTs.

Upon loss of all offsite power and the standby diesel generators, if it is not possible to restore power to IDS by the end of the 72-hour period, the ECS ancillary diesel generators (ECS MG-01 and MG-02) will provide power to essential 72-hour loads supporting monitoring and habitability safety Category B safety functions via the IDS voltage regulating transformer of IDS Divisions B and C. The ancillary diesels are designated as Class 2 on this basis. In the event that the ancillary diesel generators are unavailable due to a seismic or other event, offsite portable diesels will be brought onsite and connected via the Class 1 IDS regulating transformers to power the necessary loads.

The safety claims made in the Reference 18.25 place the following functional requirements on the ECS:

- ES1 and ES2 (Class 2) have separate onsite sources
- ES1 – ES6 (Class 2 and Class 3) have preferred and maintenance offsite sources
- RCP circuit breakers
  - To trip the RCPs on signals that actuate the CMTs. The RCP breakers must be tripped in response to faults which credit CMT injection as identified in the fault schedule, Table 8A-2, and explained in Chapter 9. The protection and safety monitoring system (PMS) sends the trip signal to the RCP circuit breakers. The RCP circuit breakers, which are part of ECS, therefore, are classified as Class 1 on this basis.

- Onsite Standby Diesel Generators
  - To provide power to selected Class 2 equipment in the event of the loss of offsite power and the main generator

- Ancillary diesel generators
  - To provide power to selected loads for the coping period between 72 hours and 7 days in the event of loss of all ac electrical power. After 7 days re-supply of consumables (fuel oil and water) allow for continued passive system support. Note that the function of these DGs can be provided by DGs brought in from offsite within 72 hours.

18.4.2 Main Connection to Grid via Main Step-Up (MSU) Transformers (Part of ZAS)

18.4.2.1 Description

The connection to the grid via the MSUs is used to support main generator operation:

- Main generator is supplying power, enabling the transmission of electrical power to the grid minus the power used to supply the plant's auxiliary loads and generator excitation.

- Plant in start-up or shutdown mode, it uses the UATs as the preferred source to supply auxiliary loads from the MSU transformer grid connection. The reserve auxiliary transformers (RATs) can be used as an alternate source when the UATs or MSUs are not available. Onsite standby diesel is an alternate for supplying DiD loads.

The main connection to the grid also has the following purposes:

- Coupling the main generator to the grid and connecting the UAT tie bus via the closing of the generator circuit breaker

- Transitioning of the plant from generation to shutdown and from start-up to generation

- Maintaining main generator operation with auxiliary loads during a grid disturbances (with 100% load rejection capability)

The offsite power source is not required in order to achieve safe shutdown of the AP1000 Plant.

18.4.2.2 Operation

Switching of the main grid connection is used for the majority of plant operating regimes. Switching operations typically used for the plant's main connection to the grid are outlined below:

- Removing the main connection to the grid from service by opening the generator circuit breaker. The transmission line and MSU provide power to the plant auxiliary loads via the UATs.

- Placing the main connection to the grid into service by closing the generator circuit breaker. The generator simultaneously provides power to the plant auxiliary loads via the UATs.

- Grid faults:

  1. If the fault is in the plant connected substation, then the line circuit breaker opens and the generator circuit breaker remains closed and continues to provide power to the plant auxiliary loads. The line circuit breaker is reclosed to restore generation from the plant to the grid after the fault has cleared.

  2. If the fault is on the main transmission line from the switchyard or in the MSU, then the substation power circuit breaker(s) open and the generator circuit breaker opens to isolate the fault. The substation and generator circuit breakers are reclosed to restore normal alignment.

Note that the ac voltage and frequency ranges must be maintained within the following limits:

- Rated bus voltage (V ac):
  - 400kV (±5%) – Normal Range
  - 400kV (±10%) – Maximum Range
  - 275kV (±10%) – Normal Range
  - 132kV (±10%) – Normal Range
- Frequency: Continued operation in range (47Hz – 52Hz)
  - Note: The required operation times for particular ranges are specified in the Grid Code (Reference 18.28).

For safety claims on the electrical system to operate within the grid code specified ranges see the Reference 18.25.

18.4.2.3 Design Basis

The electrical design has taken into account the following factors when designing the main connections to the grid:

- Two UATs connected to the 27kV main connection (ZAS) via a tie bus, both having two equally sized auxiliary secondary buses (11kV)

- One UAT connected to the auxiliary boiler loads.

- Two RATs connected to the grid (primary windings) via an alternate grid connection source both having two equally sized auxiliary secondary buses (11kV)

- UAT and RAT transformers are equally sized (except auxiliary boiler UAT)

- MSUs are sized to accommodate maximum generator output without consideration of house loads

- Phasing between grid voltage and ECS 11kV bus voltage for the RATs vs. MSU + UATs must be the same.

- Preference for supplying plant loads through the UATs

- The electrical distribution system (ECS) connects to each of the UATs and RATs equally sized 11kV secondary windings via four Class 3 buses (ES3, ES4, ES5 and ES6) and two Class 2 buses (ES1 and ES2).

- Each UAT and RAT connects to two unique Class 3 ECS buses and one unique Class 2 ECS bus

- Alternate supplies to plant loads via ZOS (standby diesel generators) or RATs.

Other design requirements include the following:

- The main generator has to be able to sync to the grid via its circuit breaker or via switchyard breaker(s)

- The ability to disconnect the main generator by opening its circuit breaker for disturbances to the grid or plant as allowed by the Grid Code. The capability to remain connected during a grid disturbance as specified by the Grid Code is addressed in Reference 18.25. A disconnector is required for isolation during maintenance of the generator circuit breaker. Plant auxiliary loads must continue to be supplied by the grid.

- Short circuit studies are completed determining short circuit impedance, current and MVA requirements for all medium and high voltage electrical equipment (to be completed during site licensing)

- A coordination study be completed for protective relays and fuses equipment (to be completed during site licensing)

- Use of firewalls for large power transformers to prevent damage to adjacent transformers and other equipment during a fire.

- The main step-up transformer consists of three single-phase transformers with a fourth spare transformer installed alongside.

18.4.2.4 United Kingdom (UK) AP1000 Plant Site-Specific Design

The primary voltage of the MSUs and RATs are site specific design requirements. For the UK the MSU and RAT primary voltages are 400 kV, 275kV, or 132kV. The MSUs will have a load tap changer on its primary winding. The RATs will have a load tap changer on the secondary winding.

18.4.2.5 Inspections, Testing and Maintenance

Refer to "UK AP1000 Electrical Equipment Maintenance and Surveillance" (Reference 18.24) for details on Inspections, Testing, and Maintenance in regards to equipment involved with the main connection to the grid.

18.4.3 Unit Auxiliary Connection (ZAS and ECS)

18.4.3.1 Description

The unit auxiliary connection is used in all main generator conditions except for the reserve auxiliary connection:

- The 27kV isophase unit auxiliary connection enables the distribution of electrical power supplied by the generator or the grid to supply the plant's auxiliary loads via the UATs

- The unit auxiliary connection to the UATs supplies plant auxiliary loads from either the generator during normal operation or the preferred MSU transformer grid connection.

The unit auxiliary connection to the main connection also has the following purposes:

- Connects the primary windings (27kV) of the three UATs together via isophase bus
- Connects the three UATs to the main connection (includes the generator circuit breaker, MSUs, and voltage transformers (VTs))
- Connects each UAT secondary (two equally sized secondary windings) to the four Class 3 ECS buses (ES3, ES4, ES5, and ES6), auxiliary boiler bus and to the two Class 2 ECS buses (ES1 and ES2) via physically separated and electrically isolated non-segregated bus.

During power generation, the supplies for the plant auxiliary system are typically drawn from the main generator via the UATs. This is the normal arrangement as it is the most economical and efficient way of providing a stable supply with maximum buffering from external grid perturbations. When the main generator is not running (e.g., during normal start-up and shutdown when the generator circuit breaker is open), auxiliary power is typically drawn from the utility grid, via backfeed through the (MSU and the UATs, as above. In this situation, voltage compensation is mitigated by the use of load tap changers on the main step-up transformer.

This is a Class 3 designated connection.

18.4.3.2 Operation

Switching of the unit auxiliary connection is used for the majority of plant operating regimes. Switching operations typically used for the plant's auxiliary connection to the grid are outlined below:

- 27kV bus faults: A 27kV isophase bus fault, a UAT fault or a potential transformer fault will initiate a fast bus transfer from the UATs to the RATs to enable plant loads to continue to operate.
- Other faults in protective zone.

18.4.3.3 Design Basis

Electrical design has taken into account the following factors in the design of the unit auxiliary connection to the grid:

- Two UATs connected to the 27kV main connection (ZAS), both having two equally sized auxiliary secondary buses (11kV)
- UAT and RAT transformers are equally sized (except auxiliary boiler UAT)
- Phasing between grid voltage and ECS bus voltage for the RATs vs. MSU + UATs be the same.
- Preference for supplying plant loads through the UATs

- The electrical distribution system (ECS) connects to each of the UATs 11kV secondary windings via two Class 3 buses and one Class 2 bus.

- Each UAT connects to a unique ECS high voltage bus

Other design requirements have included:

- Short circuit studies will be updated to determine short circuit impedance, current, and MVA requirements for medium voltage isophase bus and UATs (to be completed during site liensing)

- Coordination studies will be updated for protective relays and fuses (to be completed during site liensing)

- Installation of firewalls for large power transformers to prevent damage to adjacent transformers and other equipment during a fire.

- Installation of fire barriers, deluge systems, and other equipment to minimize the risk for an unplanned power outage

All UATs are three-phase transformers and have the same power rating (except for the auxiliary boiler UAT). Each transformer has a primary winding with dual secondary windings (except for the auxiliary boiler UAT). Primary voltages of the unit auxiliary transformers are set according to their source – the generator voltage. Load tap changers are provided on the low voltage winding of the UATs to mitigate voltage fluctuations.

18.4.3.4 Inspections, Testing, and Maintenance

Refer to "UK AP1000 Electrical Equipment Maintenance and Surveillance" (Reference 18.24) for details on Inspections, Testing, and Maintenance in regards to the unit auxiliary connection.

18.4.4 Reserve Auxiliary Connection (Part of ZAS)

18.4.4.1 Description

The reserve auxiliary connection is used in specific main generator conditions:

- The reserve auxiliary connection from the RATs is an alternate offsite source to supply plant auxiliary loads; supply via the RATs is not used during power operation

- Supplying electric power to the plant auxiliary loads after a fast bus transfer or residual bus transfer has occurred

The components of the reserve auxiliary connection are described as follows:

- The reserve auxiliary connection begins with a high voltage connection to the grid. Connects each RAT secondary (two equally sized secondary windings) to the four Class 3 ECS buses (ES3, ES4, ES5, and ES6) and to the two Class 2 ECS buses (ES1 and ES2) via 11kV non-segregated bus.

This is a Class 3 designated connection.

18.4.4.2 Operation

Switching operations typically used for the reserve auxiliary connection to the grid are outlined below:

- Faults in the protection zone (yard side Power Circuit Breaker to incomer M1 breakers on busses ES1 through ES6) will initiate a fast bus transfer to serve plant loads via the RATs.

- Manual operation: The RATs and their associated ECS buses can be energized separately for maintenance purposes.

Plant auxiliary loads are drawn from either the UATs or the RATs, but not a combination of both. Supplies may be transferred from the UATs to the RATs by manually or automatically initiated switching. There is no provision for the automatic transfer of supplies from the RATs back to the UATs. Manually initiated switching must be used for this purpose. Electrical interlocking is used to ensure that both sets of breakers cannot be manually closed together.

18.4.4.3 Operational Requirements for Fast Bus Transfer

Automatic switching is affected by a detected fault in the protection zone which initiates a fast bus transfer scheme triggered only by the differential protection covering the zone of protection containing the switchyard circuit breaker(s), iso-phase bus, main step-up transformer, excitation transformer, and generator field circuit breaker, UATs, VTs, and their associated non-segregated 11 kV bus bars. Fast bus transfer reduces the reliance on the standby diesels by automatically providing an alternate grid connection in the event the preferred power source is unavailable.

18.4.4.4 Design Basis

Electrical design has taken into account the following factors into in the design of the reserve auxiliary connection to the grid:

- Two reserve auxiliary transformers (RATs) connected to the grid (ZAS) through a second independent source, both having two equally sized (11kV) secondary windings

- RAT and UAT transformers are equally sized

- Phasing between grid voltage and ECS bus voltage for the RATs vs. MSU + UATs be the same.

- The electrical distribution system (ECS) connects to each of the RATs 11kV secondary windings via two Class 3 buses and one Class 2 bus.

- Each RAT connects to a unique ECS high voltage bus

Other design requirements included the following:

- Short circuit studies are completed determining short circuit impedance, current, and MVA requirements for the RATs (to be completed during site licensing). Installation of firewalls for large power transformers to prevent damage to adjacent transformers and other equipment during a fire.

- Installation of fire barriers, deluge systems, and other equipment to minimize the risk for an unplanned power outage.

All RATs are three-phase transformers and have the same power rating. Each transformer has a single primary winding with dual secondary windings. Primary voltages of the reserve auxiliary transformers are set according to their source (grid voltage). The UATs are fed at the main generator voltage, whereas the RATs are fed at an alternative grid connection. Load tap changers are provided on the secondary side of the RATs to mitigate external grid voltage fluctuations.

18.4.4.5 Inspections, Testing, and Maintenance

Refer to "UK AP1000 Electrical Equipment Maintenance and Surveillance" (Reference 18.24) for details on Inspections, Testing, and Maintenance in regards to the reserve auxiliary connection.

18.4.5 Medium and Low Voltage Distribution System (ECS)

18.4.5.1 Description

The design of the ECS system has many components. The ECS represents the electrical distribution system for the AP1000 plant containing 11kV and 400V buses. See Figures 18-1A, 18-1B, and 18-1C. The ECS distributes high voltage station power at 11 kV, and distributes low voltage power through load centres (Class 2) at 400 volts. The 400V ac supply to the IDS and EDS is provided through load centres supplied at 11 kV by the ECS standby diesel-backed switchboards ES1 and ES2.

Several large motors, MCCs, switchgear (including the RCP trip switchgear), panel boards, bus work, and power cables make up the ECS. Six designated buses are included in the ECS. Four are Class 3 buses (ES3, ES4, ES5, and ES6) that connect to the RCPs and two are Class 2 buses that connect to the load centres, standby diesel generators, and the Class 1 and Class 2 IDS/EDS battery systems. A seventh bus serves site specific auxiliary plant loads and the auxiliary boiler.

The RCP trip switchgear consists of two 6.9 kV/60 Hz breakers connected in series downstream of the VFDs fed from ES3, ES4, ES5, and ES6.

ECS provides power to the Plant Control System (PLS) Motor Generator sets.

18.4.5.2 Operation

The ECS contains the ancillary diesel generators and various circuit breakers that can be used to switch various Class 1, Class 2, and Class 3 plant loads. During normal operation the ECS circuit breakers are closed to energize plant loads via the normal UAT source. The Class 2 ancillary diesels generators are switched on after a DBE when post-72-hour ac power is needed to supply power to the passive containment cooling system (PCS) pumps, MCR lighting, MCR, and C&I room ventilation. These loads can also be powered by offsite portable diesel generators in case the ancillary diesel generators are unavailable.

18.4.5.3 Design Basis

Equipment making up the Class 3 ECS is of a design that has been type tested to the specified extremes of environmental and operational conditions.

The RCP switchgear is of a design that is type-tested and qualified to conditions equal to at least the most severe DBE conditions as described in Chapter 11.

The general status and alarms for the ECS are displayed in accordance with the applicable equipment specifications. The monitoring function and equipment are appropriately designated in accordance with the categorisation and classification scheme.

The ECS electrical system has a layout design that facilitates access for necessary operation and maintenance activities. The main aspects of the design are as follows:

- Provisions for access to the components of the ECS for maintenance and operation are in accordance with local fire and safety requirements.
- Access, egress, and lighting are designed to facilitate personnel in undertaking all necessary operational, maintenance, inspection, and testing activities. General and emergency lighting is provided for all areas in accordance with the applicable equipment specifications.
- For those facilities and control functions essential to the operation of the plant that may require local manual intervention, an alternative means of access is provided.

18.4.5.4 Inspection, Testing, and Maintenance

Refer to "UK AP1000 Electrical Equipment Maintenance and Surveillance" (Reference 18.24) for details on Inspections, Testing, and Maintenance in regards to the medium and low voltage distribution system (ECS).

18.4.6 Ancillary Diesel Generators (Part of ECS)

18.4.6.1 Description

The ancillary diesel generators ECS MG-01 and MG-02 are Class 2 equipment (Figure 18-7 and Figure 18-8B) providing alternative supplies to their corresponding PCS recirculation pumps and 72-hour IDSs (Figure 18-4). The PCS recirculation pump supports the Category B safety function of providing post-72-hour heat removal. The ancillary generator supply to the IDS provides an alternative supply to the system monitoring, MCR lighting, RSW, and C&I room ventilation if no other sources of ac power are available and the IDS batteries are discharged.

These loads can also be powered by offsite portable DGs in the case ancillary diesel generators (ADGs) are unavailable. Once brought on site, portable DGs can be connected via the Class 1 IDS voltage-regulating transformers in the dc equipment rooms, or via the Class 2 ECS ancillary diesel distribution panels. The connection of the portable DGs was reviewed in "UK AP1000 Plant Post-Fukushima Assessment" UKP-GW-GGR-201 (Reference 18.4). Resulting enhancements to facilitate the connection of the diesels via the Class 1 IDS are described in Section 18.8.5.

18.4.6.2 Operation

The ancillary diesel generators are provided with necessary controls and indicators for local monitoring of the operation of the units. Generator control is manual from a control integral with the diesel skid package.

18.4.6.3 Design Basis

The ancillary generators are located in the portion of the annex building that is a seismic Category II structure. For additional detail about design basis for external hazards, refer to chapter 12. The ancillary diesel generator's fuel storage tank is located in the same room as the generator. The fuel tank, piping, and valves are analysed to show that they withstand a safe shutdown earthquake (SSE), for additional information on SSEs refer to Chapter 12. The tank includes provisions for venting to the outside atmosphere and for refilling from a truck or other mobile source of fuel. The tank is classified as seismic Category II and holds sufficient fuel for four days of operation.

Each ancillary diesel generator output is connected to a distribution panel located in the same room as the generators. Each distribution panel has an incoming circuit breaker and outgoing feeder circuit breakers.

The distribution panels provide power to:

- The transfer switch that feeds the Class 1 voltage regulating transformers that power the post-accident monitoring loads, emergency lighting in the MCR and the ancillary fans for ventilation of the MCR and C&I rooms.

- The transfer switch that feeds the passive containment cooling system recirculation pumps.

Redundancy for the ancillary diesels is provided by duplicating essential post-72-hour loads on the ECS Class 2 buses and providing each bus with two alternative supplies. The preferred supply is from the ECS with the alternative provided by the corresponding ancillary diesel generator. These loads can also be powered by offsite DGs in case the ADGs are unavailable.

18.4.6.4 Inspection, Testing, and Maintenance

Refer to "UK AP1000 Electrical Equipment Maintenance and Surveillance" (Reference 18.24) for details on Inspections, Testing, and Maintenance in regards to the ancillary diesel generators.

18.4.6.5 Post-72-Hour Operation

During the post-72-hour period following a DBE, power is required for Class 1 post-accident monitoring, lighting in the MCR, ventilation in the MCR, and for the pumps to provide cooling for the PCS. Provisions are made to connect offsite portable diesel generators to the Class 1 voltage regulating transformers (divisions B and C only) when all other sources of ac power are unavailable, including the Class 2 ancillary diesel generators. Figure 18-4 shows the functional diagram for serving post-72-hour loads.

Safety claims, arguments, and evidence regarding post-72-hour operations are provided in Reference 18.25.

18.5 SAFETY CLASS 1 ELECTRICAL DISTRIBUTION SYSTEM

18.5.1 Class 1 Safety Requirements

18.5.1.1 Class 1 Safety Functions

IDS provides power to the PMS to provide and action Class 1 engineered safety features (ESF) actuation signals and for the actuation of a number of Class 1 SSCs providing the Category A safety functions including decay heat removal safety function under different circumstances or at different stages of a Design Basis Accident (DBA).

Claims regarding Class 1 safety functions are contained in Reference 18.25.

18.5.2 Class 1 Electrical Distribution System

18.5.2.1 Description

The roles of the IDS are to provide continuous power supplies to Class 1 loads required for plant instrumentation, control, and monitoring and other vital functions needed for safe shutdown of the AP1000 plant. Class 1 IDS power is supplied to the MCR and RSW for normal lighting; the rest of the normal lighting is provided by ECS through the MCCs. In addition, the IDS provides power to the emergency lighting in the MCR and to the RSW.

The IDS is a battery-backed power supply that provides dc and ac power (via inverters) to Class 1 loads. In the event of loss of power from the ECS, the batteries are sized to provide power for the 24-hour and 72-hour Class 1 loads without any external ac power supply.

Reference 18.25 provides claims regarding the proper sizing and rating of the IDS system and components in Section 8.4.

The IDS is capable of providing power for the safe shutdown of the plant without the support of battery chargers during a loss of all ac power sources coincident with a DBE. The system is designed so that no single failure will result in a condition preventing the safe shutdown of the plant.

The Class 1 IDS consists of ungrounded stationary batteries, battery chargers, dc distribution equipment, and inverters. The functional schematic diagrams for the IDS are shown in Figure 18-3 and Figure 18-4.

The 400V ac supply to the IDS and EDS is provided through load centres supplied at 11kV by the ECS standby diesel-backed switchboards ECS ES1 and ES2.

The IDS includes only safety designated Class 1 components, which are seismically qualified. They are described in the following sections.

18.5.2.2 Batteries

The 24-hour battery banks and the 72-hour battery banks provide adequate power to the load duty cycle requirement for 24 hours and 72 hours, respectively, without support from the battery chargers.

To maximize the availability of DC power supply to the plant safety DC loads for all normal and emergency conditions, the system's design provides for connection of a spare battery bank to any of the six (6) batteries in the four divisions. The availability of this spare battery bank will permit continuous plant operation in accordance with the technical specifications; this is not an indefinite operating condition. The spare battery is normally maintained in a fully charged condition via a separate, dedicated charger.

Each battery bank is installed on a two-step, restraining side braced seismically qualified rack. A liquid tight spill containment area is provided with each rack.

The operating voltage range of the batteries is 210 to 280V dc with a nominal system voltage of 250V dc. The maximum equalising charge voltage for batteries is 280V dc. Each battery bank is connected to a Class 1 dc switchboard through a set of fuses and a disconnect switch.

If offsite power is lost, the batteries will maintain the system while the standby diesel generator (ZOS) starts. Once started, the standby diesels will power the IDS battery chargers maintaining the supply to the Class 1 equipment.

In the event of a loss of offsite power and failure of the standby diesels to start, the batteries are sized to maintain the supplies to the Class 1 actuation for 24 hours and for post-accident monitoring for 72 hours. The design of the AP1000 plant is such that the reactor will go into a safe shutdown state if all external ac electrical power is lost.

18.5.2.3 Fused Transfer Switch Panels

The fused transfer switch panels are provided to facilitate battery testing, off-line recharging and maintenance. The spare fused transfer switch enables the spare IDS battery bank and spare battery charger to be connected to any other fused transfer switch panel (Figure 18-4A). This allows replacement of any battery bank and battery charger during maintenance or testing.

18.5.2.4 Battery Chargers

The battery chargers provide power to Class 1 250 V dc loads and maintain the batteries fully charged. During normal operation, the IDS battery chargers are supplied with power from the ECS. In turn, the battery charger supplies power to the primary 250V dc switchboard while maintaining the battery charged. The battery chargers also restore discharged batteries to a fully charged state. The spare battery charger maintains a fully charged spare battery bank and powers a Class 1 250 V dc bus in the case of a failure or unavailability of its own battery bank or battery charger. The battery chargers provide the required isolation between the Class 2 and 3 ac and Class 1 dc electrical systems. The battery chargers are qualified as isolation devices.

In the event of loss of offsite power, the standby diesel generators will start and provide power to the chargers through the ECS.

Figure 18-4 shows the connections to post-72-hour loads. During normal operation, the IDS battery chargers can be energised either through the offsite power source or from the station's own generation. The inverters and dc equipment are supplied from the battery chargers.

The battery chargers are classified as seismic category I. They are designed and manufactured to withstand the effects of the SSE and to maintain their specified functions.

18.5.2.5 DC Switchboards

The Class 1 250 V dc switchboards employ fused disconnect switches. The main bus bar is braced to withstand mechanical forces expected during a short circuit current event. The switchboards are capable of operating continuously at the maximum equalization voltage of 280 V dc.

The Class 1 250 V dc switchboards provide power to motor control centres, dc distribution panels, and the IDS inverters. The Class 1 250 V dc switchboard is used to interconnect each battery bank to a battery charger. The Class 1 250 V dc switchboards are powered from the battery chargers and battery banks.

Monitoring of the 250 V dc Class 1 System is included in the Class 1 250 V dc switchboard. Each dc switchboard supplied from a 24-hour battery bank (Divisions A through D) supplies power to an inverter, a 250V dc distribution panel, and a 250V dc MCC. Each switchboard supplied from a 72-hour battery bank (divisions B and C) provides power to an inverter.

18.5.2.6 Inverter

The inverters, static transfer and manual by-pass switches provide ac power to distribution panels. Each inverter is powered from its respective battery bank switchboard. If an inverter is inoperable or the Class 1 250V dc input to the inverter is unavailable, the power is transferred automatically to the backup ac source by a static transfer switch featuring a make-before-break contact arrangement. The backup power is received from the ZOS-backed 400V ac bus through the Class 1 voltage-regulating transformer. In addition, a manual mechanical bypass switch is provided to allow connection of a backup power source when the inverter is removed from service for maintenance.

18.5.2.7 Regulating Transformer

The regulating transformers provide a backup source of ac power to the Class 1 inverter through a static transfer switch. The regulating transformers are powered from the diesel generator backed Class 2 motor control centres. Two regulating transformers are used to connect each ancillary or portable diesel generator to the IDS system and power the necessary loads for the post-72-hour scenario. The Class 1 regulating transformers provide the required isolation between the Class 2 and the Class 1 electrical systems. The regulating transformers are qualified as an isolation device.

18.5.2.8 Battery Monitor

A battery monitor system is a design feature used to monitor each Class 1 IDS battery bank. The battery monitors detect and annunciate open-circuit conditions in the IDS dc system. The battery monitoring function is not safety related as it is an additional observation tool for maintenance in between the required surveillance testing activities. Surveillance requirements are already in place to verify and test the batteries on a regular basis as claimed in the Reference 18.24.

18.5.2.9 250V DC Distribution Panels

The Class 1 250 V dc distribution panels provide dc power distribution and protection between the 250V dc power sources and the assigned loads. The Class 1 250 V dc distribution panels are powered from Class 1 250V dc switchboards. The Class 1 250 V dc

distribution panel is capable of operating continuously at the maximum equalization voltage of 280 V dc along with the equipment downstream of the Class 1 250 V dc distribution panel.

18.5.2.10 250V DC Motor Control Centres (MCCs)

The Class 1 dc motor MCCs operate in the 250V dc two-wire, ungrounded distribution system. The loads fed from the MCCs are protected by fusible disconnect switches from short-circuit faults. The MCCs are capable of operating continuously at the maximum equalization voltage of 280 V dc along with the equipment downstream of the MCCs.

18.5.2.11 Operation

During normal operation, the four division battery chargers are supplied with power from the ECS MCCs. In turn, the battery charger will supply power to the primary dc switchboard, powering dc distribution panels, and the ac inverter while maintaining the battery charge. This allows the ac inverter to supply power to the ac distribution boards. In the event of loss of offsite power, the standby diesel generators will start and provide power to the chargers through the ECS. In the event of a loss of offsite power and failure of the standby diesel generators to start, the batteries are sized to maintain Class 1 loads.

The IDS consists of ungrounded stationary batteries, battery chargers, dc distribution equipment, regulating transformers, and inverters. The functional arrangement diagrams for the IDS system is shown in Figure 18-3 and Figure 18-4.

The IDS is divided into four divisions, A, B, C, and D, which are electrically independent and physically separated. Each division uses a Class 1 stationary battery bank connected to a separate Class 1 dc switchboard through a disconnect switch panel. Divisions B and C are each composed of two battery banks, two switchboards, and two battery chargers. The first battery bank in each of the four divisions, designated as a 24-hour battery bank, provides power to the loads required for the first 24 hours following an event of loss of all ac power sources concurrent with a DBE. The second battery bank in divisions B and C, designated as a 72-hour battery bank, is used for those loads requiring power for 72 hours following the same DBE. Following a DBE MCC loads will be supported by the IDS 24 hour batteries, and are not required to be supported by the 72 hour batteries. These loads are not necessary to support plant safety past the first 24 hours following a DBE. The 72-hour battery banks of Divisions B and C contain batteries the same cell size as the 24-hour batteries but they are discharged over a longer time with smaller loads. Battery chargers are powered from ac load centres fed from standby diesel generator-backed buses. An additional battery and charger unit is provided as a full spare. Each switchboard supplied from a 24-hour battery bank (divisions A to D) supplies power to an inverter, a 250V dc distribution panel, and a 250V dc MCC.

Only loads required during the 24 hours following a DBE are supplied by the IDS 24-hour batteries, so no load shedding or load management programme is needed to maintain power during the required 24-hour safety actuation period. Each switchboard supplied from a 72-hour battery bank (Divisions B and C) provides power to an inverter.

The IDS provides power for the safety-designated equipment required for the plant instrumentation, control, monitoring, and other vital functions needed for shutdown of the plant. In addition, the IDS provides power to the emergency lighting in the MCR and at the remote shutdown workstation. The IDS is capable of providing power for the safe shutdown of the plant without the support of battery chargers during a loss of all ac power sources

coincident with a DBE. The system is designed so that no single failure will result in a condition preventing the safe shutdown of the plant.

The IDS is not directly bonded to ground. A single ground fault does not cause immediate loss of the faulted system. Ground detection relays that alarm in the MCR are provided for each division of power so that ground faults can be located and removed before a second ground fault could disable the affected circuit.

The capacity of each battery is determined based upon formally prepared, reviewed, and issued calculations. Conservative measures are taken to ensure that each battery is sized to supply its assigned load profile for the entire postulated (standby) time without the benefit of the battery charger or forced ventilation.

The following methodology, as defined in the nuclear industry standards for batteries, is employed to achieve conservative battery sizing and validate the design:

- Ambient correction factor of 11 percent to account for the assumed minimum temperature of 15.5°C (60°F)
- Battery aging factor of 125 percent to ensure acceptable voltage at the postulated end of life
- Sizing design margin of 110 percent to account for potential future load growth
- All similar batteries specified at the same capacity and the sizing based upon the worst-case battery duty cycle

Claims on the electrical system being designed with margin are made in in the Basis of Safety Case document (Reference 18.25).

A comprehensive formal sizing calculation has been developed to establish the proper size for the worst-case battery, battery charger, and inverter. The largest size, based upon the worst-case load and allowing for aging and other factors, is applied for all Class 1 battery banks.

Reference 18.25 provides claims on the isolation and transient withstand of the battery chargers. Suitably selected and rated protection on both the ac and dc components of the IDS will prevent an electrical fault on one item of equipment from resulting in an excessive electrical disturbance to other equipment.

18.5.2.12 Inspection, Testing, and Maintenance

Refer to "UK AP1000 Electrical Equipment Maintenance and Surveillance" (Reference 18.24) for details on Inspections, Testing, and Maintenance in regards to the Class 1 IDS equipment.

18.5.2.13 Post-72-Hour Operation

During the post-72-hour period following a DBE, power is required for Class 1 post-accident monitoring, lighting in the MCR, ventilation in the MCR, and for the pumps to refill the PCCWST. Provisions are made to connect the offsite portable diesel generators to the Class 1 voltage regulating transformers (divisions B and C only), when all other sources of power are unavailable including the Class 2 ancillary diesel generators. Figure 18-4 shows the

connections to post-72-hour loads. During normal operation, the IDS battery chargers can be energised either through the preferred offsite power source or from the station's own generation. The inverters and dc equipment are supplied from the battery chargers. These loads can also be powered by offsite DGs in case the ADGs are unavailable.

18.6 CLASS 2 ELECTRICAL DISTRIBUTION SYSTEM (EDS)

18.6.1 Class 2 Safety Requirements

18.6.1.1 Class 2 Safety Functions

EDS provides power to a number of Class 2 SSCs which provide a DiD means of providing residual heat removal safety functions, including:

- Startup feedwater system (FWS)
- Normal residual heat removal system (RNS)
- Component cooling water system (CCS)
- Service water system (SWS)
- Spent fuel pool cooling system (SFS)

EDS provides power to a number of Class 2 SSCs, which provide a DiD means of providing criticality control safety functions including the chemical and volume control system (CVS).

Claims regarding the design, qualification and adequacy of the Class 2 systems are made in Reference 18.25.

18.6.1.2 Class 2 Safety Function Requirements

Fail-to-safety criteria specific to the EDS are the following:

- The inverter units serve as isolation for the EDS from faults for the downstream ac system and protect the EDS load group it serves from faults, surges, and backfeeds. This ensures that the operation of the batteries and associated supplies and equipment are preserved, including if the inverter operation fails.

- Overcurrent and fault protection are suitably rated and specified to protect the EDS from faults with downstream ac and dc equipment.

- The inverter dc input protection is set higher than the battery charger trip setpoints to prevent the inverter from tripping before the battery charger.

The safety claims place the following functional requirements on the EDS:

- To supply a continuous power source to the safety designated plant Class 2 and 3 loads.

- In the event of loss of offsite power (normal, preferred, and maintenance sources), the ZOS will provide power to the EDS for up to 7 days without the necessity for offsite fuel supplies.

- In the event of loss of offsite power and failure to start the standby diesel generators, the EDS batteries are to provide power for the priority loads for a minimum of two hours following the loss.

- Through a site-specific transmission switchyard, the EDS will utilise offsite power for startup and shutdown under normal conditions.

18.6.2 Class 2 DC Electrical Distribution System

18.6.2.1 Description

The EDS provides battery backed continuous electric power to the plant Class 2 and 3 C&I loads during normal operation and in the event of loss of offsite power.

EDS provides power to C&I loads important for plant operation and investment protection and to the hydrogen igniters located inside containment. The Diverse Actuation System (DAS) cabinets are located in the auxiliary building. Two sources of ac power from EDS are provided to the DAS. Additional information about the DAS and squib valves are in Chapter 19.

The EDS is divided into five battery systems, identified as EDS1 to EDS4 and EDS5 (turbine bearing oil pump and airside seal oil backup pump).

Divisions EDS1 to EDS4 consist of the following elements:

- Battery bank
- Battery charger
- Fused transfer switch panel
- dc switchboards
- dc distribution boards
- Inverter
- Voltage-regulating transformer
- ac distribution panels

EDS5 consists of the following:

- Battery bank
- Battery charger
- Fused transfer switch panel
- Transfer switch box
- 250V dc switchboard

Normal ac power to the EDS battery chargers and regulating transformers is supplied from the standby diesel generator-backed 400V ac distribution system (ES1 and ES2).

EDS1 and EDS3 are considered as one functional subsystem, with EDS2 and EDS4 forming the second subsystem of the same configuration. Figure 18-5 shows the functional arrangement schematic diagram for these subsystems. Systems EDS2 and EDS4 are arranged in an identical manner. EDS5 and the EDS spare are standalone systems and are outlined in Figure 18-6.

The EDS1 through EDS4 dc buses provide dc power to their associated inverter units that supply the ac power to the associated Class 2 ac system. An alternative regulated ac power source for the inverter buses is supplied from the associated regulating transformers. The EDS5 dc bus supplies dc motors associated with the main generator. The EDS spare battery bank can supply any of the five EDS system (EDS1-EDS5) through a connection in the fused transfer switch panel.

18.6.2.2 Operation

During normal operation, the EDS1-EDS4 battery chargers are supplied with power from the ECS MCCs. In turn, the battery charger will supply power to the primary dc switchboard, powering dc distribution panels and the ac inverter while maintaining the battery charge. This allows the ac inverter to supply power to the ac distribution boards. In the event of loss of offsite power, the standby diesel generators will start and provide power to the chargers through the ECS. In the event of a loss of offsite power and failure of the standby diesel generators to start, the batteries have been sized to maintain supplies to DiD loads.

During normal operation, the EDS5 battery charger is supplied with power from the ECS MCC. In turn, the battery charger will supply power to the primary 250V dc switchboard while maintaining the battery charge. This allows the dc switchboard to supply power to the Class 2 dc loads. In the event of loss of offsite power, the diesel generators will start and provide power to the charger through the ECS. In the event of a loss of offsite power and failure of the generators to start, the batteries have been sized to maintain Class 2 loads and systems that are identified in Reference 18.25.

18.6.2.3 Design Basis

The EDS electrical system design and layout facilitates access for necessary activities and minimises adverse interactions during such activities. The main aspects of the design are as follows:

- Provisions for access to the components of the EDS for maintenance and operation are in accordance with the requirements of References 18.17 and 18.18, and local fire and safety requirements.

- Access, egress, and lighting are designed to facilitate personnel in undertaking all necessary operational, maintenance, inspection, and testing activities. General and emergency lighting is provided for all areas in accordance with the applicable equipment specifications.

- For those facilities and control functions essential to the operation of the plant that may require local manual intervention, an alternative means of access is provided.

A comprehensive sizing calculation has been developed to establish the proper size for the worst-case battery load and battery charger. The largest size, based upon the worst-case load and allowing for aging and other factors, is applied for all EDS battery banks. The batteries are sized to supply the system loads for at least two hours after loss of all ac power sources.

The design of the electrical system provides diverse power supplies to equipment supplied by the EDS. Under normal operating conditions, the supply to the dc switchboards and the inverter units is through the battery chargers. The supply to these battery chargers is from 400V load centres, which in turn derive their supply from the diesel-backed 11 kV distribution boards. Normal supply to the 11 kV boards is from the offsite supply through the UATs. Alternative offsite supplies are available through the RATs. In the event of loss of the offsite supplies, the diesel generators will start to provide power to the 11 kV boards. Should the diesels fail, the batteries are sized to maintain power to the connected loads for a minimum of two hours.

Suitably selected and rated protection on both the ac and dc components of the EDS will prevent an electrical fault on one item of equipment resulting in an excessive electrical disturbance to other equipment.

Claims on the conservative margin of the electrical system and the ability to withstand transients and disturbances are made in Reference 18.25.

18.6.2.4 Inspection, Testing, and Maintenance

Refer to "UK AP1000 Electrical Equipment Maintenance and Surveillance" (Reference 18.24) for details on Inspections, Testing, and Maintenance in regards to the Class 2 EDS equipment.

18.7 STANDBY DIESEL GENERATORS (ZOS – SAFETY CLASS 2)

18.7.1 Safety Requirements

18.7.1.1 Safety Functions

The onsite standby diesel generators provide power to Class 2 loads in the event of loss of normal/preferred (ECS via the UATs) and reserve (ECS via the RATs) ac power supplies.

18.7.1.2 Safety Function Requirements

The safety case places the following functional requirements on the standby diesel generators and their associated distribution equipment:

- Each generator shall be capable of supplying the necessary Class 2 loads.
- Each generator shall be independent.

Claims in regard to the standby diesel generators are made in Reference 18.25.

18.7.2 Standby Diesel Generators (Safety Class 2)

18.7.2.1 Description

In the event of the loss of offsite power and loss of the main generator, power can be provided to the two 11 kV switchboards (ECS ES-1 and ES2) from the onsite standby diesel generators (see Figure 18-1B). Each bus is backed by one of the Class 2 onsite standby diesel generators. Priority loads for DiD functions based on their specific functions (permanent loads) are assigned to buses ES1 and ES2. Plant permanent loads are divided into two functionally redundant load groups. Each load group is connected to either bus ES1 or ES2.

These standby diesel generators are located in their own building, forming part of the onsite power system.

18.7.2.2 Operation

When a successful fast bus transfer from the UATs to the RATs occurs due to a fault in the protective zone, the standby diesel generator (ZOS) will not be connected. The Class 2 standby diesel generators are switched on once the offsite power has been lost and the main generator is offline. This creates an undervoltage on bus ES1 or ES2, allowing the diesel

generators to be automatically started. The diesel generator, however, is capable of being manually paralleled with the preferred or maintenance power supply for periodic testing.

Claims and arguments regarding the conservative margin that is included in the ZOS equipment are provided in Reference 18.25.

An independent air starting system is provided for each standby diesel generator. The standby diesel generators will provide power for up to seven days from the onsite fuel storage tank without the necessity for offsite fuel supplies.

The onsite standby diesel generators are provided with necessary controls and indicators for local or remote monitoring of the operation of the units.

18.7.2.3 Design Basis

Auto sequencing is designed and tested to ensure that the diesel generators are not overloaded. If loads fail to auto sequence onto the generator, loads can be started manually. Refer to Reference 18.25 for claims made on auto sequencing. The control scheme, while protecting the diesel generators from excessive loading, does not compromise the onsite power supplies ability to support the DiD loads.

Upon detection of an under-voltage condition on the medium voltage diesel bus, the under-voltage relays in the ECS system send a start signal to the diesel generator. When the DG ramps up to synchronous speed, the DG control system will send a "ready to load" signal to the PLS via a programmable logic controller or other approved equivalent gateway device). The PLS will provide the sequencing logic to the medium voltage buses.

The standby diesel generator is type-tested to the expected extremes of environmental and operational conditions. Installation is in accordance with manufacturer's recommendations.

Claims on the operating conditions of the equipment are addressed in Reference 18.25.

Provision for redundancy within the ECS Class 2 standby diesel generator system is as follows:

- Only one of two standby diesel generators is required in power modes with SFP decay heat less than the limit defined in the Technical Specifications as each one is rated at 100 percent of the load required to supply all the Class 2 DiD designated systems. If SFP decay heat is higher than the limit defined in the Technical Specifications and during certain times in Modes 5 and 6, 2 of 3 ac power sources are required. The Class 1 batteries provide the necessary power for the safety actuations, while the Class 2 batteries provide power for monitoring. The standby diesel generators provide support for the defence in depth active system functions. Reference 18.25 contains claims made on the electrical system availability.

- To provide redundancy, the Class 2 DiD systems equipment supplied by the ECS is duplicated; for example, the ZOS MG-02A normal loads are also supplied from MG-02B.

18.7.2.4 Inspection, Testing, and Maintenance

Refer to "UK AP1000 Electrical Equipment Maintenance and Surveillance" (Reference 18.24) for details on Inspections, Testing, and Maintenance in regards to the Class 2 ZOS equipment.

18.8 EXTERNAL ELECTRICAL SYSTEM INTERFACES

The Electrical Basis of Safety Case (Reference 18.25) captures all safety claims made on the electrical systems in the PCSR and describes how the electrical system supports those claims. Fault studies for internally initiated faults (Chapter 9) imply claims on the electrical system through their support of SSCs providing Category A and B safety functions listed in that chapter.

Internal and external hazards assessments (Chapters 11 and 12) make claims in reference to the electrical system, for example, considerations of separation and segregation. The equipment forming the IDS, EDS, ECS, and ZOS is designed, specified, qualified, and installed to protect against internal and external events. This includes the dc battery systems, the RCPs, its circuit breakers, the ac distribution system, and the standby diesel generators.

Electrical and EMC hazards are to be managed per the EMC management philosophy (Reference 18.13). Further details are given in Sections 11 and 12, which discuss internal and external hazards, respectively.

18.8.1 Spent Fuel Pool Cooling

The ECS ES1 and ES2 buses supply power to the SFS and RNS pumps, which provide flow for removal of the design basis heat load. DC power is used for safety containment isolation MOVs, and ac power is used for AOVs. Class 1 IDS is provided as control power for the relays/switchgear to start and stop the containment isolation valve motors. Refer to Chapter 6 for details on the operation of the Spent Fuel Pool Cooling System.

In order to provide DiD for decay heat removal, two of three ac power supplies (2 standby diesel generators and offsite power) and their associated switchgear should be available in accordance with the criteria defined in in UKP-GW-GL-502, “Recommendation for the Development of the AP1000 Technical Requirements Manual”(Reference 18.6) and approved design changes. These requirements support the decay heat removal described in Section 9.2.7.

18.8.2 SMART Devices/Verification and Validation of Software

Chapter 5, Section 5.12 provides the criteria for the use of digital and smart devices in the UK AP1000 plant. Per the criteria, digital devices performing Category A functions in the electrical system are required to be compliant with the appropriate International Electrotechnical Commission (IEC) nuclear standards to be justified as Class 1.

Digital devices which are performing Category B and C functions in the electrical system will be identified and the software and hardware will be justified in accordance with the guidelines of the “AP1000 Smart Device Assessment Process,” UKP-GW-J0Y-004 (Reference 18.26) and the “AP1000 SMART-Device Justification Plan,” UKP-GW-GL-017 (Reference 18.7). The assessment performed will be commensurate with the classification of the device. Additionally, should isolation between the smart aspect and a higher class function be required evidence of this isolation will be provided.

In addition to the criteria provided in Section 5.12, additional information on SMART devices can be found in Chapter 19. Reference 18.25 provides the claims, arguments, and evidence relating to digital devices in the Class 1 IDS system including software diversity claims to reduce the potential for common-cause failure. Reference 18.25 also provides the

claims on the justification of smart devices performing Category B and C functions within the electrical systems.

18.8.3 Reactor Trip

When less than three of the four IDS divisions are in service, the reactor will automatically trip.

18.8.4 Post Accident Monitoring

After a DBE, the IDS provides power to the PMS for post-accident monitoring. After 72 hours, if no other sources of power are available, the two ancillary diesels provide ac power for post-accident monitoring. These loads can also be powered by offsite DGs in case the ADGs are unavailable. Post-accident monitoring provides indication for containment pressure, containment water level, containment radiation intensity, and noble gas effluents. ESF actuation signals and Class 1 isolation valves provide the Category A containment safety functions.

18.8.5 Fukushima Electrical System Assessment

Per the results of the internal flooding assessment in "UK AP1000 Plant Post-Fukushima Assessment" UKP-GW-GGR-201 (Reference 18.4), the minimization of potential flooding sources in the safety-related areas (e.g., IDS battery banks), in addition to the physical separation of redundant safety-related components and systems from each other and from non-Class1 related components, reduces the consequences of internal flooding. The Core Damage Frequency (CDF) and Large Release Frequency (LRF) arising from flooding events during shut down operations are not appreciable contributors to overall AP1000 plant design risk.

Design provisions resulting from the post Fukushima assessment for the UK AP1000 increase the ability of the AP1000 electrical system to withstand or mitigate the effects of beyond-design-basis events. These design provisions and the safety claims made on them are contained in Reference 18.25.

18.9 REFERENCES

18.1 Westinghouse Report APP-G1-E1-003, Rev. 3, "Raceway Design Discipline Criteria," September 2012.

18.2 Westinghouse Report UKP-GW-GL-059, Rev. 3, "UK AP1000 Electrical Systems Codes and Standards Analysis," April 2011.

18.3 Westinghouse Report CPP-EGS-E8-001, Rev. 0, "Grounding and Lightning Protection System, System Specification Document," November 2012.

18.4 Westinghouse Report UKP-GW-GGR-201, Rev. 1, "UK AP1000 Plant Post-Fukushima Assessment" July 2016.

18.5 Westinghouse Report APP-GW-VP-030, Rev. 5, "AP1000 Environmental Conditions (for Equipment Qualification)," January 2015.

18.6 Westinghouse Report UKP-GW-GL-502, Rev. 0, "Recommendation for Development of the AP1000 Technical Requirements Manual" February 2016.

18.7 Westinghouse Report UKP-GW-GLR-017, Rev. 4, "AP1000 SMART-Device Justification Plan," December 2016.

18.8 Not Used.

18.9 Not Used.

18.10 Not Used.

18.11 Not Used.

18.12 Not Used.

18.13 Westinghouse Report UKP-GW-GL-062, Rev. 1, "UK AP1000 Electromagnetic Compatibility – Management Philosophy Document," April 2011.

18.14 Not Used.

18.15 Not Used.

18.16 Not Used.

18.17 UK Statutory Instrument No. 635, "The Electricity at Work Regulations," 1989.

18.18 BS 7671:2008, "Requirements for electrical installations. IEE Wiring Regulations," British Standards Institution, January 2008.

18.19 Not Used.

18.20 Not Used.

18.21 Not Used.

18.22 Westinghouse Report UKP-GW-GL-067, Rev. 1, "AP1000 Assessment of Diverse Mitigation of Frequent Faults for the UK," December 2011.

18.23 Not Used.

18.24 Westinghouse Report UKP-GW-GL-065, Rev. 5, "UK AP1000 Plant Electrical Equipment Maintenance and Surveillance," July 2016.

18.25 Westinghouse Report UKP-GW-GL-163, Rev. 2, "Electrical Basis of Safety Case" December 2016.

18.26 Westinghouse Report UKP-GW-J0Y-004, Rev. 2, "AP1000 Smart Device Assessment Process," December 2016.

18.27 Not Used.

18.28 The Grid Code, Issue 5 Revision 15, 3 February 2016.

18.29 Not Used.

18.30 Westinghouse Report APP-GW-G1-002 Rev. 4, "AP1000 Equipment Qualification Methodology," September 2014.

18.31 Westinghouse Report APP-GW-E1-001, Rev. 1, "Electrical Systems Design Criteria," February 2016.

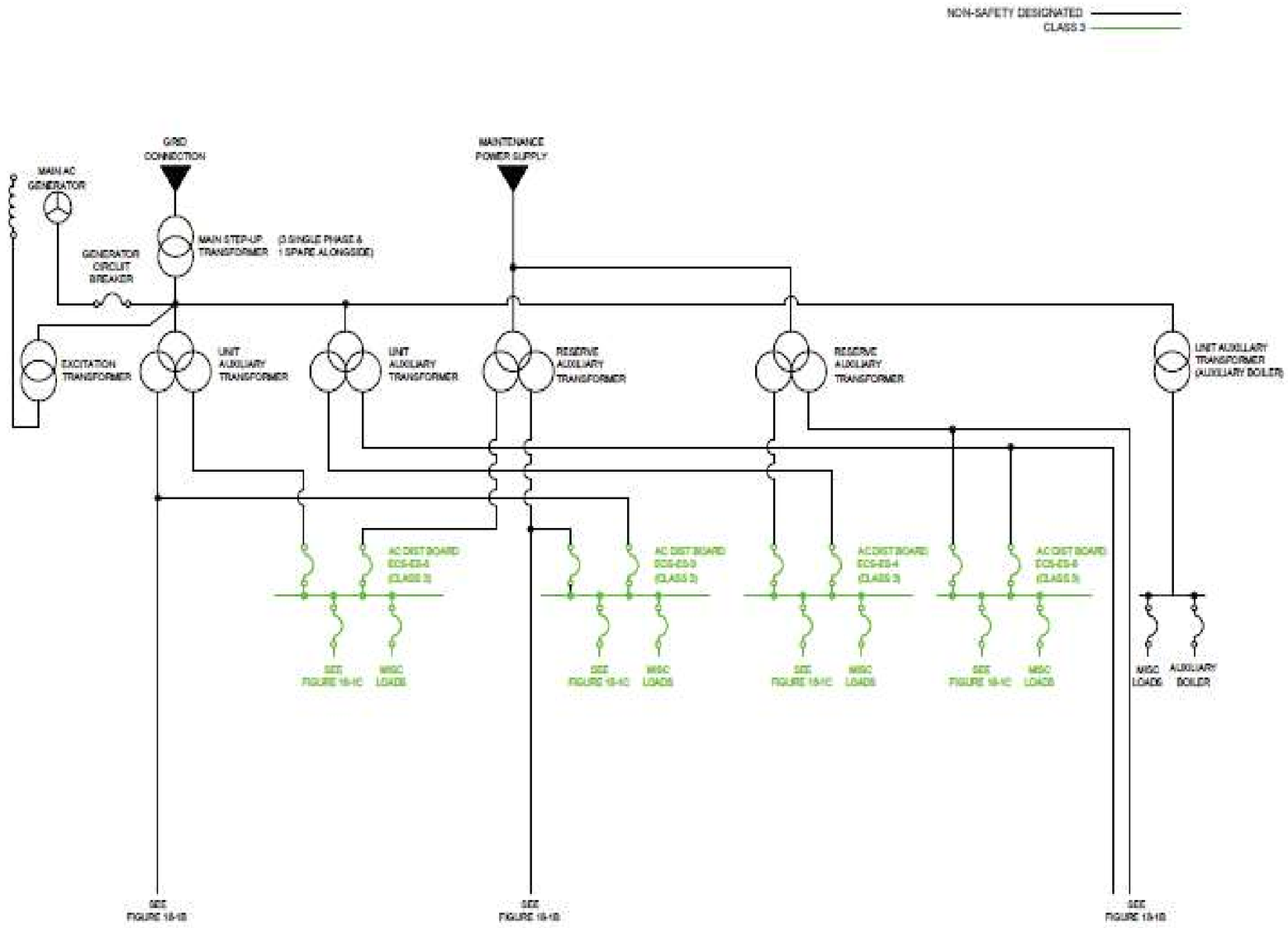


Figure 18-1A. ZAS/ECS Schematic of Electrical System

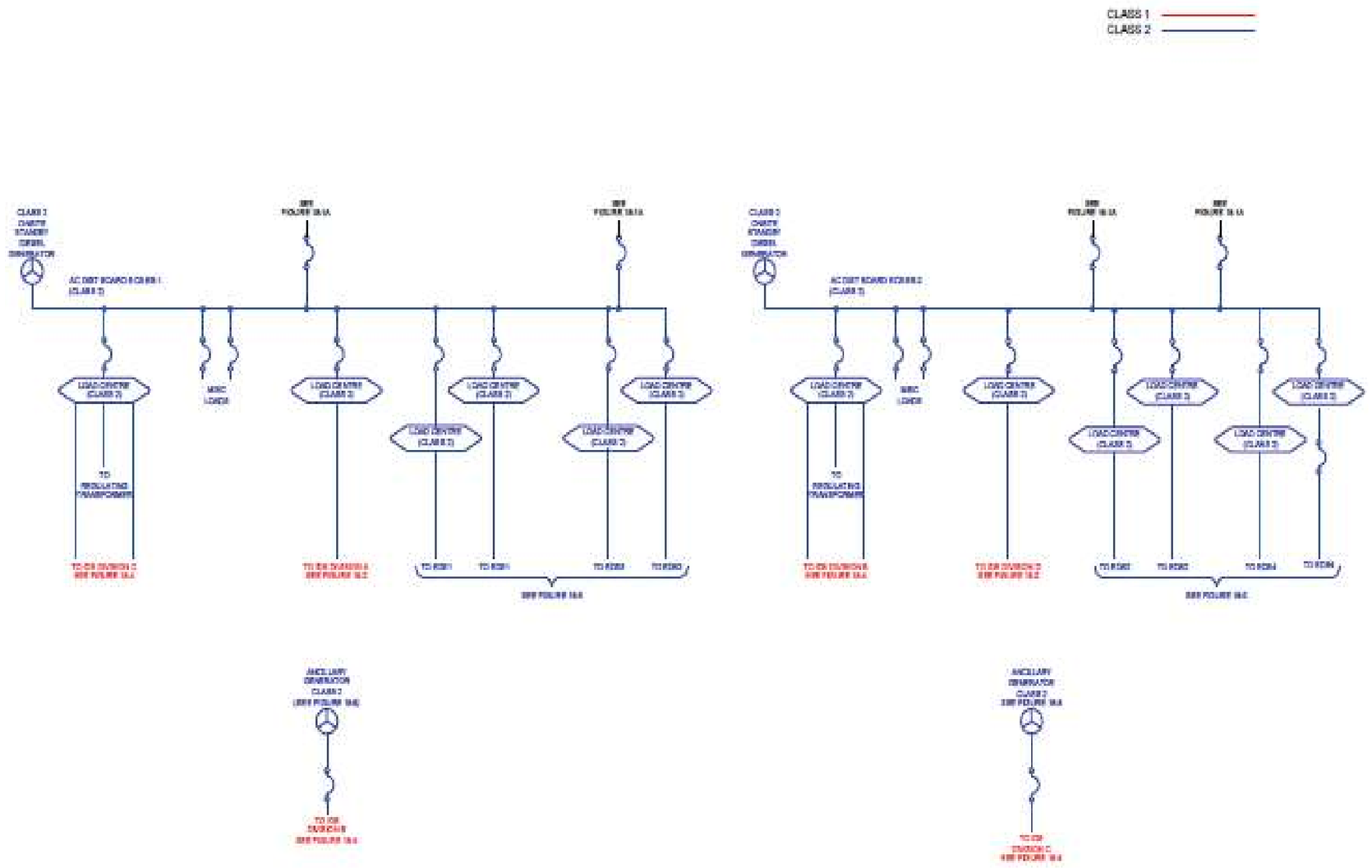


Figure 18-1B. ECS/IDS/EDS Schematic of Electrical System

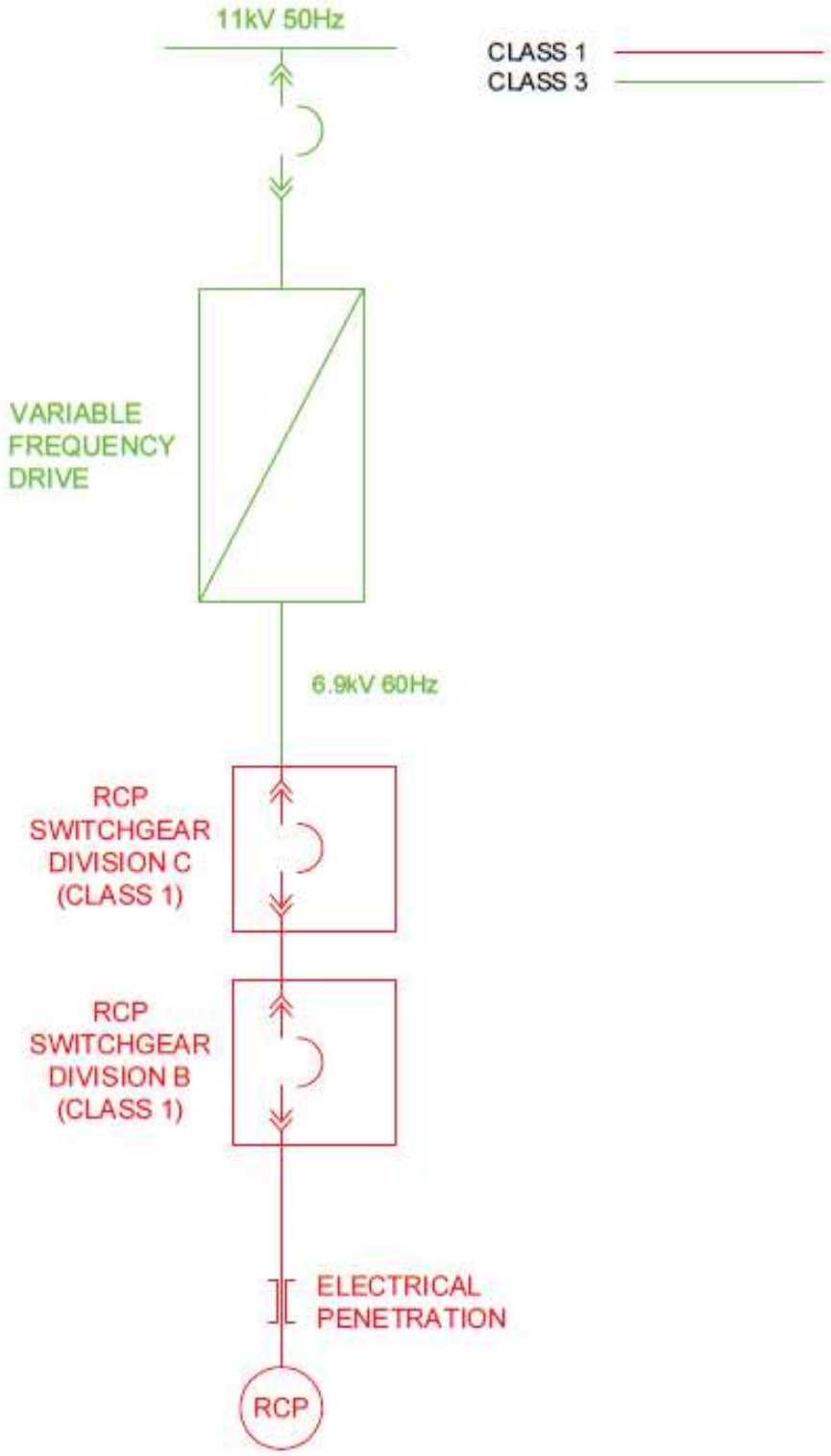


Figure 18-1C. RCP Switchgear Arrangement (ECS)

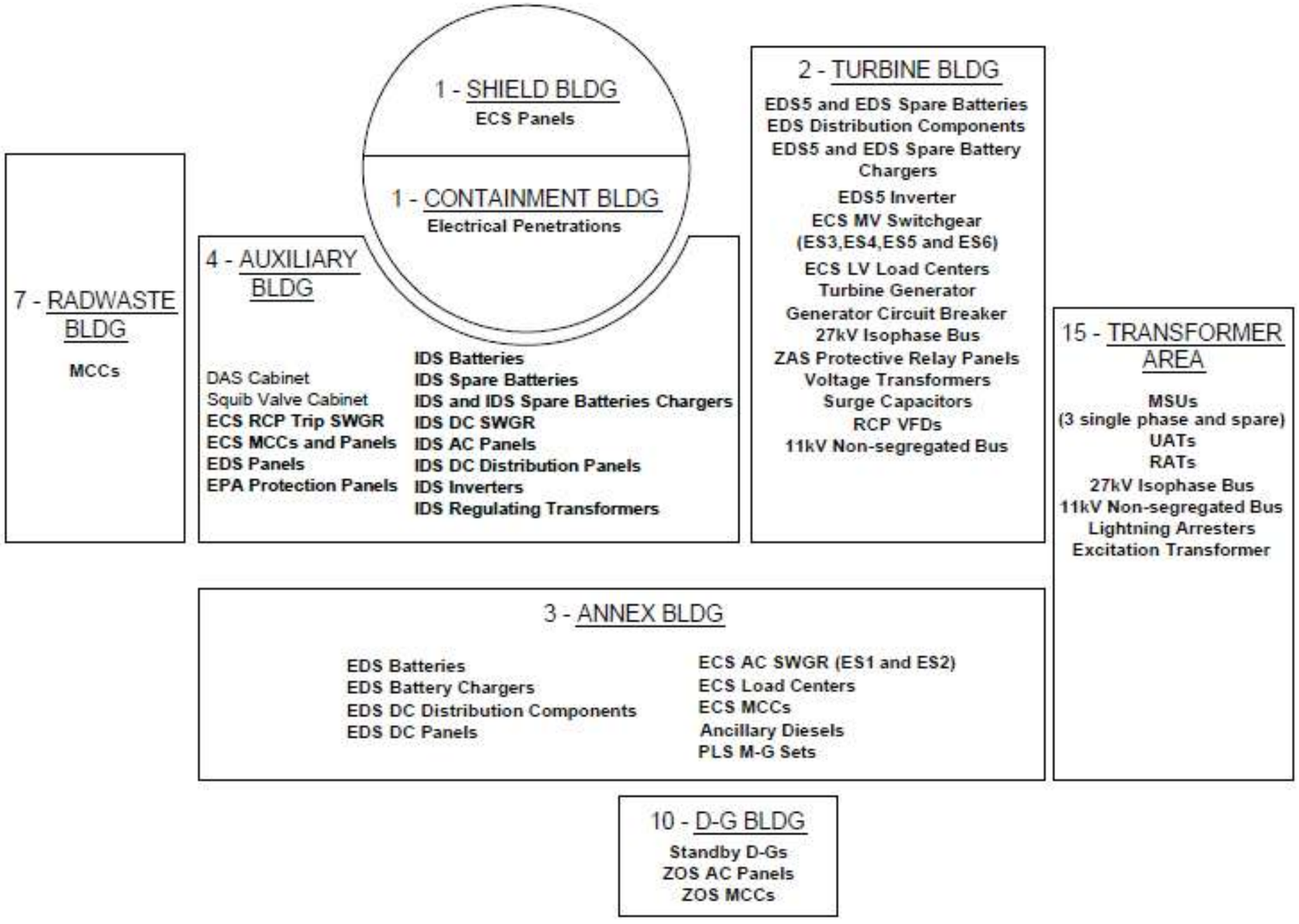


Figure 18-2. Functional Allocation of Electrical System Equipment Components

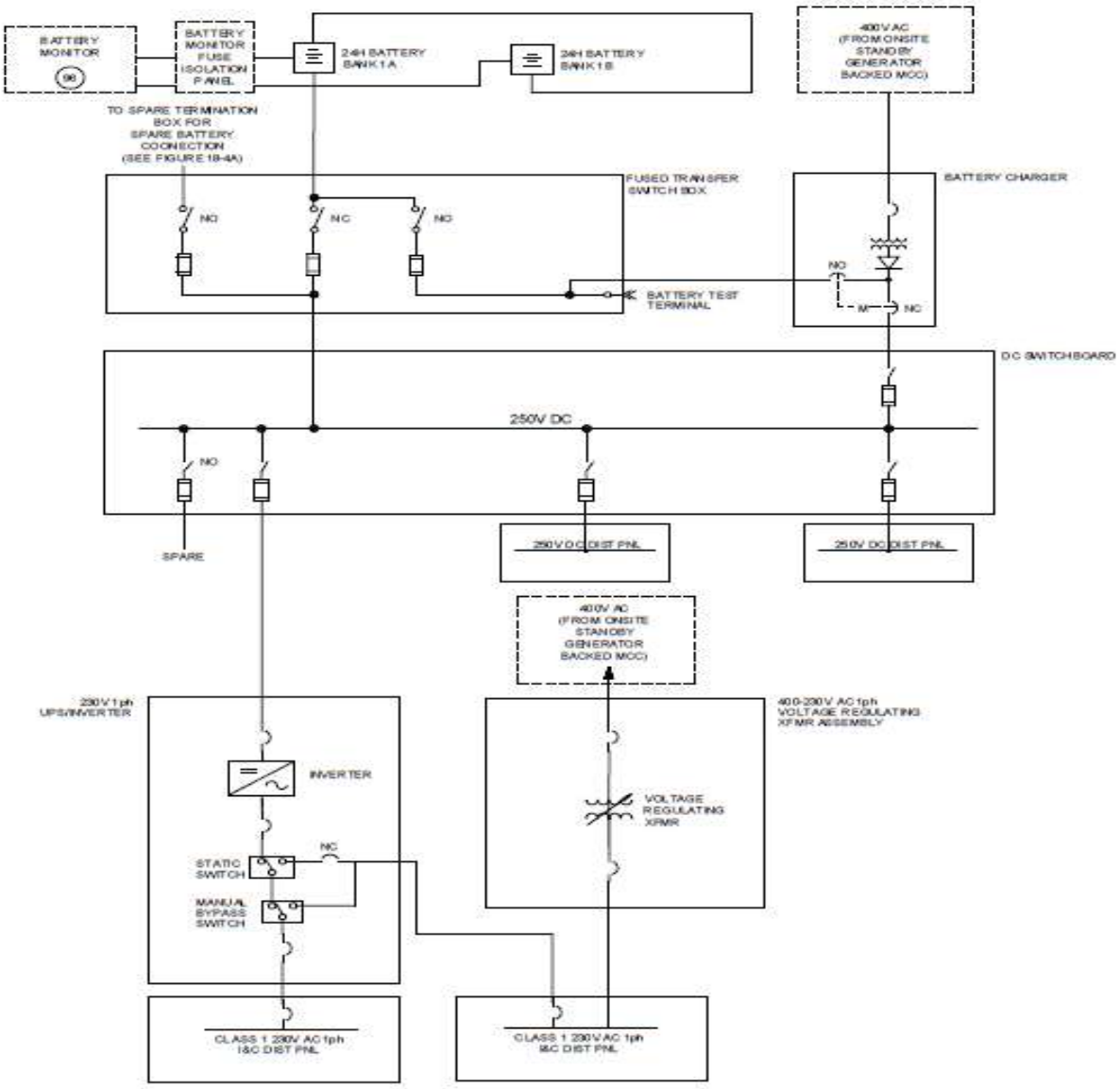


Figure 18-3. Schematic of IDS 24-Hour Uninterruptible Power Supply (UPS) and Battery System – Division A
(Division A/D Similar)

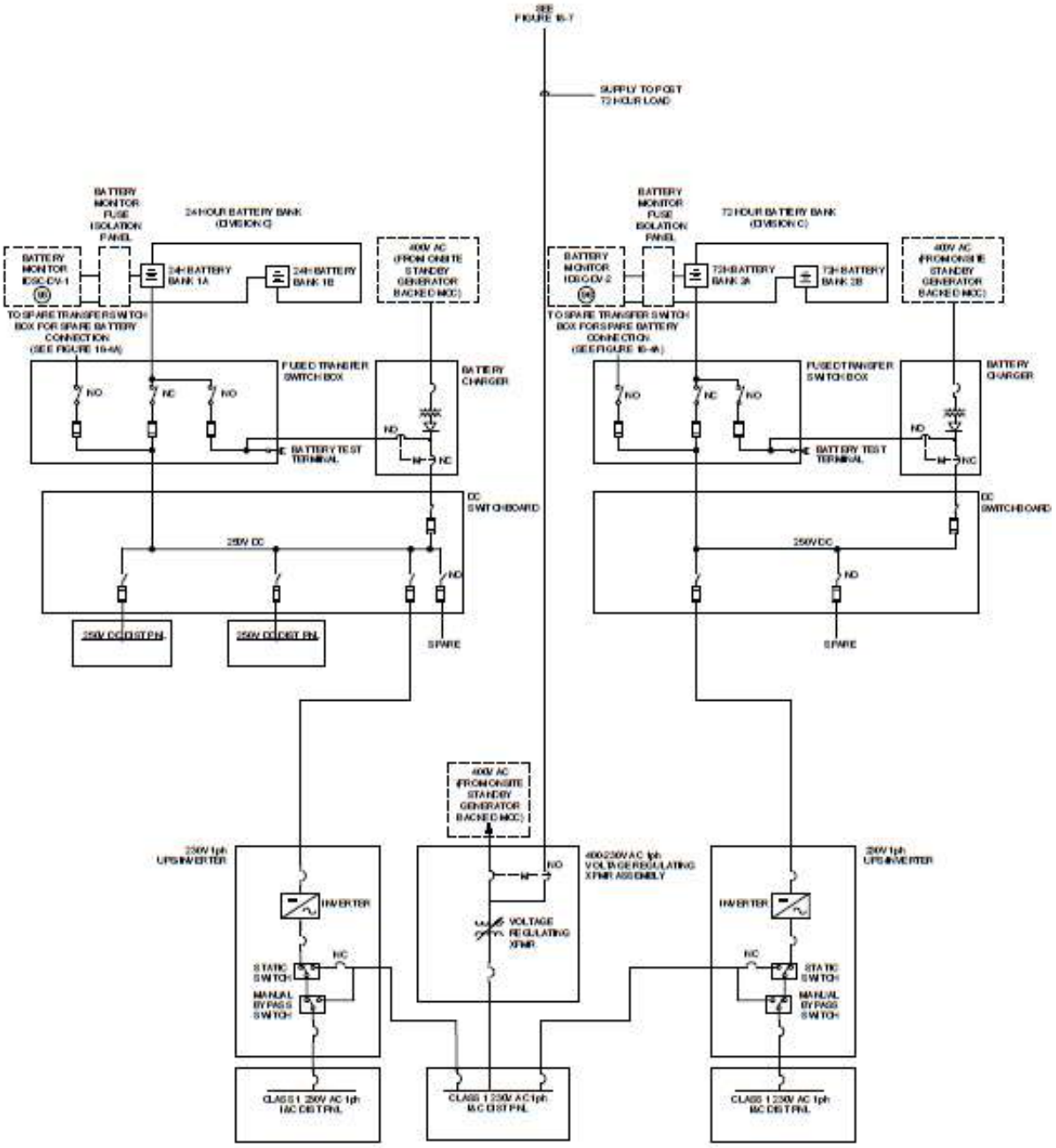


Figure 18-4. Schematic of IDS 24-/72-Hour UPS and Battery System – Division C (Division B/C Similar)

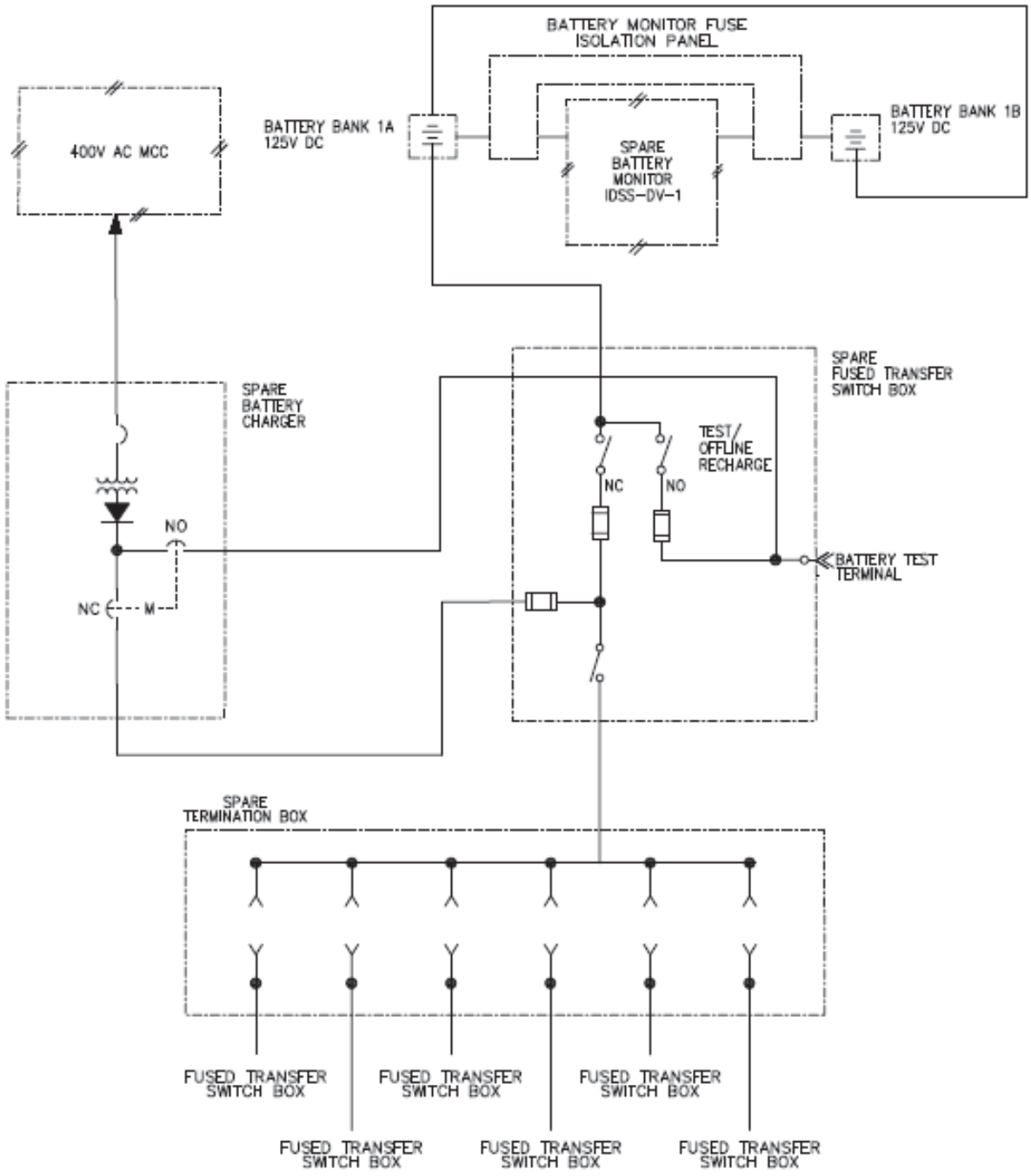


Figure 18-4A. Schematic of Class 1 IDS Spare (IDSS) Battery System

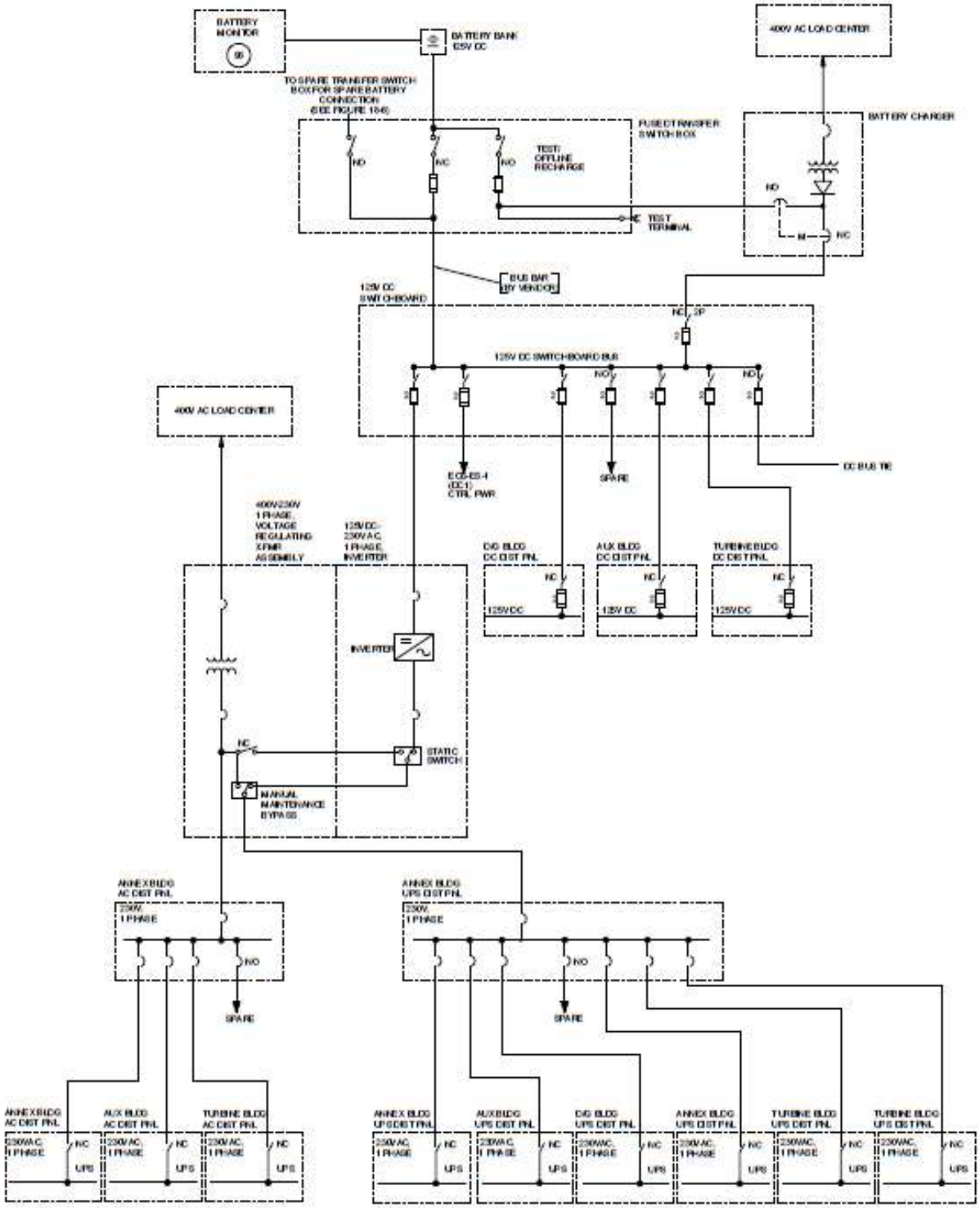


Figure 18-5. Schematic Class 2 EDS Battery and Inverter System EDS1 or EDS3 (EDS 2/EDS 4 Identical)

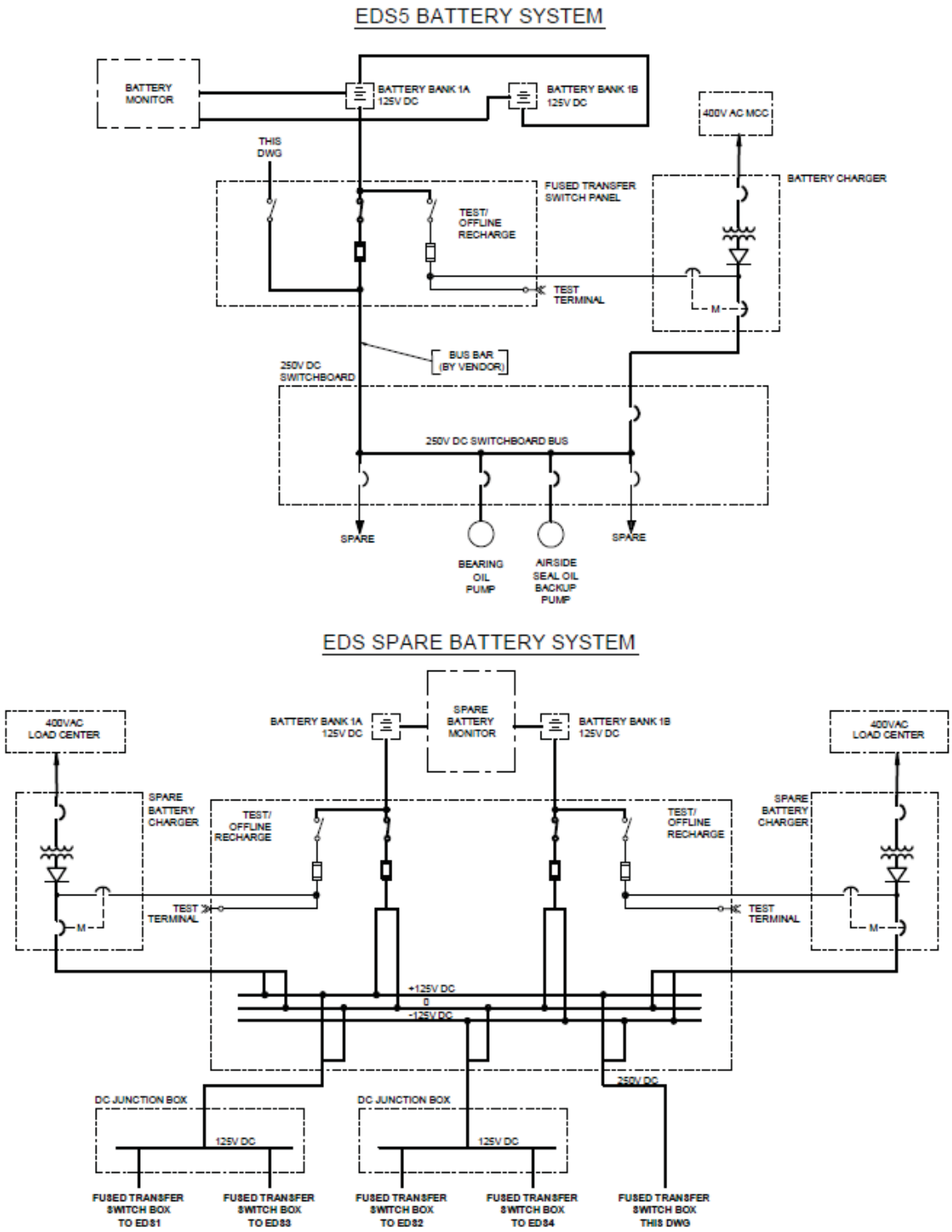


Figure 18-6. Schematic of Class 2 EDS5 and EDS Spare Battery System

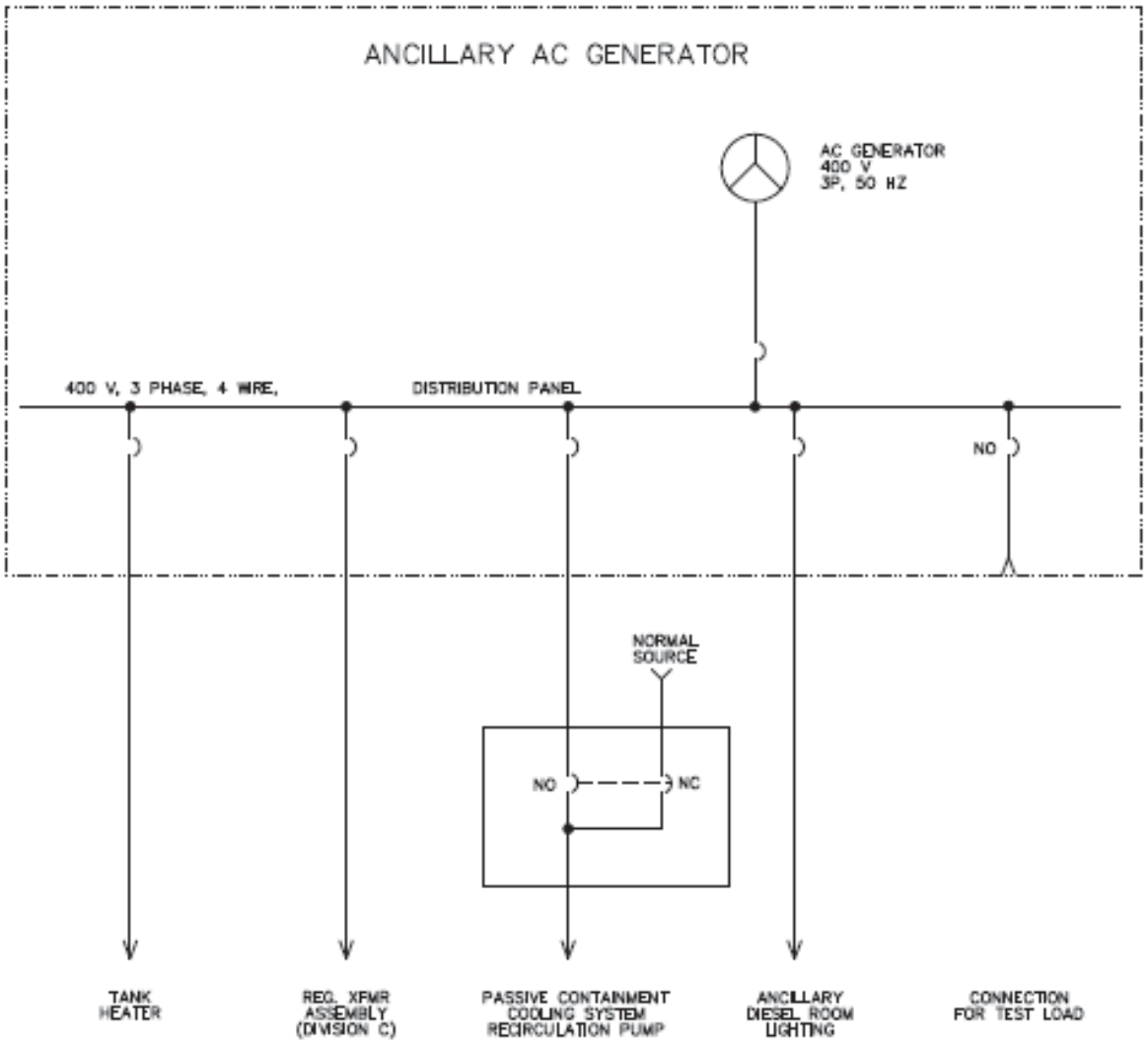


Figure 18-7. One Line Diagram – Ancillary Diesel Generators (ECS Class 2)

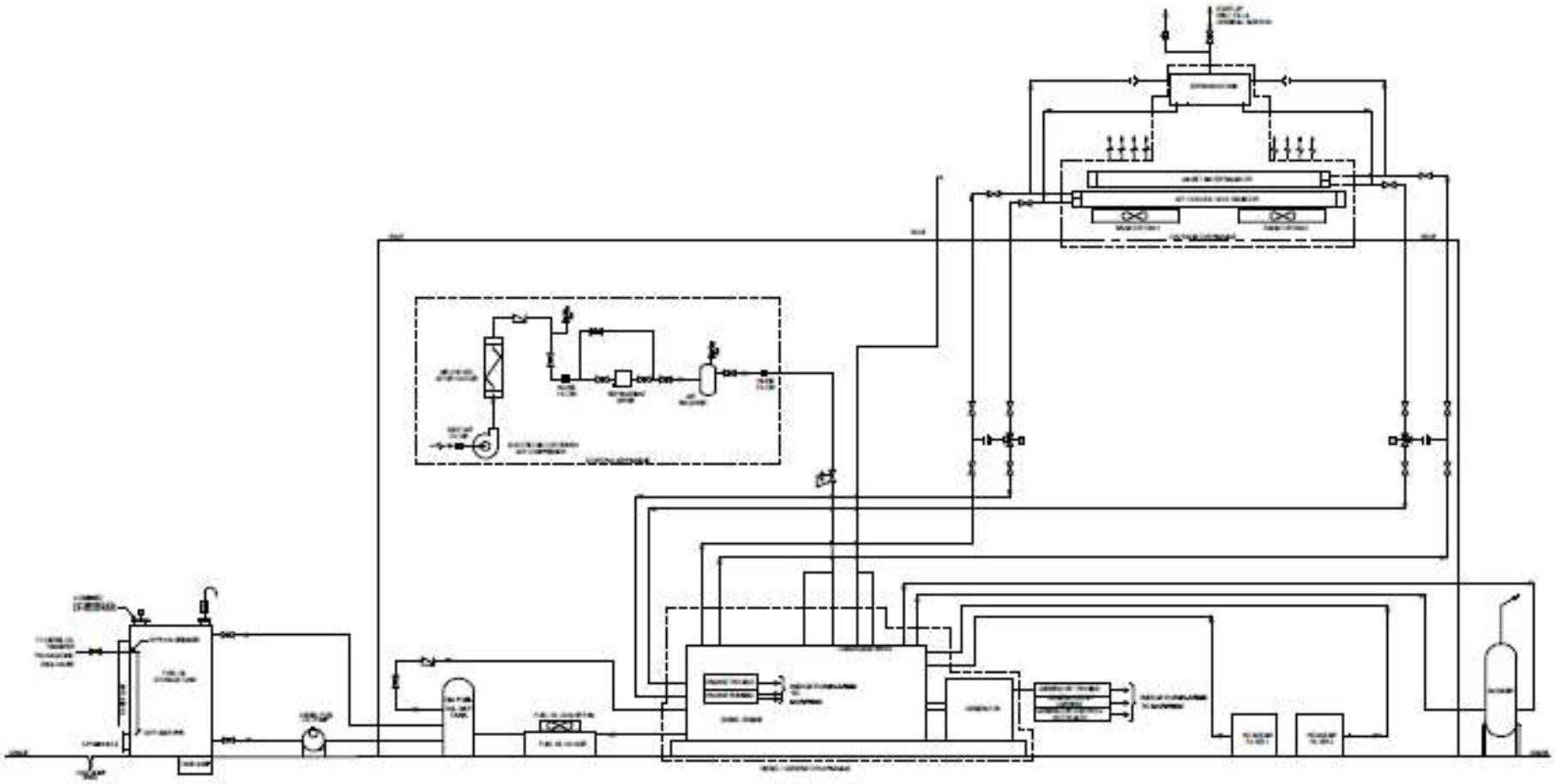


Figure 18-8A. Standby Diesel Generator Functional Arrangement Diagram

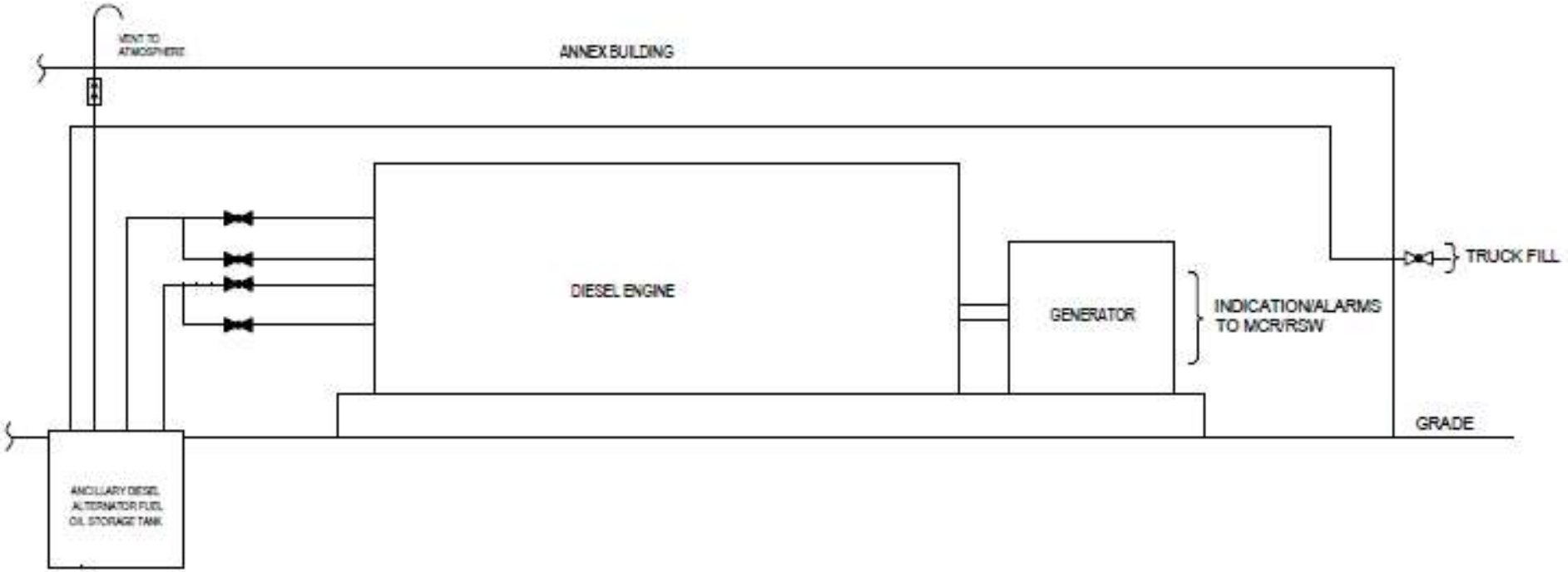


Figure 18-8B. Ancillary Diesel Generator Functional Arrangement Diagram

APPENDIX 18A ELECTRICAL CODES AND STANDARDS

To comply with UK, European, and 50-Hz requirements, Westinghouse has conducted an in-depth analysis of the appropriate codes and standards to be employed in the UK AP1000 plant. The results of this analysis have been reported in Reference 18.2. This report concludes that the majority of the UK AP1000 plant electrical system design and construction can be encompassed by the comprehensive suite of UK and European codes and standards without any significant impact on the standard AP1000 plant design. Where this is so, the appropriate UK and European codes and standards are used. For certain specialised areas, United States (US) standards are applied; these standards are discussed in detail in the appropriate areas of this chapter.

Following completion of the codes and standards analysis, it has been determined that IEC codes and standards are utilised throughout the UK AP1000 plant electrical system except for the following limited applications, where it has been determined that the requirements of the Institute of Electrical and Electronics Engineers (IEEE) standards equal or exceed those of the equivalent IEC standards:

- Class 1 and 2 dc systems, including the switchgear supplying the essential loads from the dc system, are IEEE-qualified equipment
- RCP isolation breakers
- Reactor electrical penetrations
- Generator circuit breakers

To fully accommodate the translation of the AP1000 plant to 50 Hz and the use of 11 kV and 400V auxiliaries, all ac motors are subject to individual assessment during the detailed design phase.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS, ACRONYMS, AND TRADEMARKS

AC	alternating current
ADS	automatic depressurisation system
AFD	automatic fire detection
ALARP	as low as reasonably practicable
APS	alarm presentation system
BSC	basis of safety case
BEACON™	best-estimate analysis core optimisation
BOP	balance of plant
BPL	bistable processor logic
C&I	control and instrumentation
CCF	common-cause failure
CFVMS	CRDM fan vibration monitoring system
CIM	component interface module
CMT	core makeup tank
CPS	computerised procedures system
CRDM	control rod drive mechanism
CVS	chemical and volume control system
DAS	diverse actuation system
DB	design basis
DBA	design basis accident
DC	direct current
DDS	data display and processing system
DiD	defense in depth
DMIMS-DX	digital metal impact monitoring system
EDS	Class 2 DC and uninterruptible power supply system
EMC	electromagnetic compatibility
EQ	equipment qualification
ESF	engineered safety feature
FB	function block
FID	fixed in-core detector
FMEA	failure modes and effects analysis
FWVMS	feedwater vibration monitoring system
GDA	generic design assessment
GNS	general non-safety
HSI	human-system interface
IAEA	international atomic energy agency
IDS	class 1 dc and uninterruptible power supply
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IIS	in-core instrumentation system
ILP	integrated logic processor
I/O	input/output
IRWST	in-containment refuelling water storage tank
LAN	local area network
LCO	limiting conditions for operation
MCR	main control room
MDEP	multi-national design evaluation programme
MG	motor generator
MTP	maintenance and test panel
NAPs	nuclear application programmes
NIS	nuclear instrumentation system
NPP	nuclear power plant

LIST OF ABBREVIATIONS, ACRONYMS, AND TRADEMARKS (cont.)

NRC	Nuclear Regulatory Commission
NSSS	nuclear steam supply system
OCS	operation and control centre system
ONR	office for nuclear regulation
PCS	passive containment cooling system
PCSR	pre-construction safety report
PDSP	primary dedicated safety panel
PIE	postulated initiating event
PLC	programmable logic controller
PLS	plant control system
PMS	protection and safety monitoring system
PRHR	passive residual heat removal
PSA	probabilistic safety assessment
QDPS	qualified data processing system
RCP	reactor coolant pump
RCPVM	reactor coolant pump vibration monitoring
RCS	reactor coolant system
RGP	relevant good practice
RMS	radiation monitoring system
RSR	remote shutdown room
RTCB	reactor trip circuit breaker
SAPs	safety assessment principles
SG	steam generator
SIS	systems important to safety
SMS	special monitoring system
SOE	Sequence of Events
SSC	system, structure, or component
SyDS	system design specification
SyRS	system requirements specification
TAG	technical assessment guides
TSM	technical specification monitoring
UK	United Kingdom
US	United States
VAC	Volts Alternating Current
VIMS	vibration integrity monitoring system
WGMS	Westinghouse global management system
WENRA	western European nuclear regulators association

TRADEMARKS

Advant is a registered trademark of ABB Process Automation Corporation.

BEACON is a trademark of Westinghouse Electric Company LLC.

DMIMS-DX is a trademark of Westinghouse Electric Company LLC.

Ovation is a registered trademark of Emerson Process Management. Other marks are the property of their respective owners.

19 CONTROL AND INSTRUMENTATION

19.1 Introduction

19.1.1 Purpose and Scope

The objective of this Pre-Construction Safety Report (PCSR) chapter is to give a high-level description and provide engineering substantiation of the control and instrumentation (C&I) systems that deliver nuclear safety as part of the overall Westinghouse Electric Company AP1000 reactor. Chapters 1 and 2 of the PCSR provide information on the overall PCSR production process and its relationship to the Office for Nuclear Regulation (ONR) Generic Design Assessment (GDA).

In terms of the C&I systems, the AP1000 reactor is controlled by a Class 2 plant control system (PLS), which maintains the plant within its defined operational limits and conditions. Should there be a failure to control the plant within these limits and conditions, there are systems important to safety (SIS) that respond to the fault conditions and allow the safe shutdown of the reactor before unacceptable conditions occur. Other C&I systems will also be available on the reactor to provide support functions during fault conditions. There are also C&I control and protection systems associated with non-reactor based operations, e.g. the fuel route.

The key objective of this engineering substantiation is to demonstrate that the safety requirements placed onto the C&I systems have been delivered and to an appropriate level of integrity. It is also a requirement to demonstrate that the engineering principles (Chapter 5) have been followed in the development of the safety led design solutions. The safety requirements specified for the C&I systems include safety functions and performance/design requirements of the structures, systems or components (SSCs) that deliver the safety functions. The source documentation for the C&I safety requirements, including the relevant sections of the safety case, are given within this chapter. Evidence is also provided in this chapter or referenced lower tier documentation to show that the safety requirements have been delivered at the correct level of integrity.

In addition to the individual C&I systems, justification and substantiation of the overall C&I architecture is provided, i.e. how the individual systems are configured to provide the plant with sufficient defense in depth (DiD) to meet the requirements of the safety case and the expectations for a modern nuclear power plant (NPP). This chapter, therefore, provides a demonstration that the design of the C&I systems and their interfaces within the AP1000 reactor are fit-for-purpose to deliver their nuclear safety functions and use technology and modes of operation that are commensurate with applicable standards. Reference is made in this chapter to the detailed descriptions and substantiation of the individual systems that are provided in, amongst other documents, the relevant Basis of Safety Case (BSC) documents. A number of BSCs also refer to lower tier BSCs where specific aspects of the systems require detailed substantiation.

Due to the fundamental importance of the overall architecture, justification of the architecture takes prominence in this chapter. The overall AP1000 design and manner of operation are described in Chapter 6.

This chapter demonstrates that the design of the AP1000 C&I systems helps to reduce radiological risks to as low as reasonably practicable (ALARP), which is a legal requirement within the United Kingdom (UK). This is achieved by making reference to Westinghouse Electric Company's ALARP guidance (Reference 19.37) and demonstrating that:

- the potential for control system faults to be initiated has been reduced as far as reasonably practicable and C&I protection consists principally of automated protection systems, i.e. the position of the C&I design in the safety hierarchy;

- relevant good practice (RGP) has been applied in the design and is applied in detailed design, installation and operation. Where necessary, this is with respect to established codes and standards that are considered to represent RGP;

- safety functions have been substantiated and that required reliability requirements have been satisfied (or that there is a programme of work to complete the analysis); and

- suitable optioneering has been undertaken to underpin design and configuration selection.

Section 19.1.4 describes how ALARP has been met for the C&I architecture. The supporting ALARP document produced for this chapter (Reference 19.61) provides further supporting evidence that the design of the C&I architecture, its systems and sub-systems contribute to the reduction of radiological risk to the public and workers to a level that is considered to be ALARP. The system BSC documents also support the high level claim that ALARP principles have been applied in the development of the systems.

In terms of the C&I systems themselves, this chapter primarily focuses on the overall architecture of the C&I systems, i.e. how they are configured and interface with each other to ensure an operable and maintainable plant that delivers security and safety requirements. Figure 19-1 illustrates the control and instrumentation architecture for the AP1000 plant. Detailed engineering substantiation of the architecture is provided in this PCSR chapter in lieu of lower tier documentation. However, the principal C&I systems themselves are described at a summary level in this PCSR chapter due to the detailed substantiation being available in the individual BSCs, i.e. the following systems:

- Plant control system (PLS);

- Protection and Safety Monitoring system (PMS);

- Diverse Actuation System (DAS);

- Data Display and Processing Systems (DDS).

Note that full compliance is not claimed within the system safety case documents or the supporting documents for this Chapter 19. The safety plans within these documents identify the gaps in compliance and the associated compensating measures which will be completed during the Nuclear Site Licensing Phase.

Figure 19-8 shows the scope boundary for coverage between the PCSR and system BSCs.

In addition, a number of supporting C&I systems are also briefly mentioned. Detailed safety specifications for these systems have yet to be fully developed as they are outside the scope of the GDA and the BSCs for these systems (where appropriate) have not been written. Further safety specification and design of the following systems, together with production of BSCs, are anticipated to be developed during the Nuclear Site Licensing Phase:

- Special Monitoring System (SMS);

- In-core Instrumentation System (IIS);
- Radiation Monitoring System (RMS);
- Other C&I.

The scope of the engineering substantiation undertaken for the C&I systems in this chapter at this phase of GDA only includes the logic components of the systems. The other aspects required to deliver the relevant safety functions, i.e. detection and termination is anticipated to be included at the Nuclear Site Licensing Phase PCSR submission. The Nuclear Site Licensing Phase will also substantiate the use of smart devices within systems. The methodology for justification of smart devices for the AP1000 SSCs is in Chapter 5. Chapter 11 (Internal Hazards) and its supporting references justify how C&I safety functions (particularly Category A) will be delivered through design basis internal hazards that may affect multiple systems, e.g. fire and flooding. Chapter 11 describes how this delivery will be achieved by use of segregation and separation, e.g. via redundant divisions being within segregated fire compartments or separated by distance. Therefore, the layout of the systems to deliver internal hazard requirements is not discussed in this chapter and reference should be made to Chapter 11 and its supporting fire barrier matrix (Reference 19.54). The C&I systems that are required to be seismically qualified will be fully substantiated at the Nuclear Site Licensing Phase.

It is important to note that where reliability requirements for C&I systems have been specified, this chapter demonstrates that the requirements have been achieved or that there is a programme of work to complete this demonstration. The overall adequacy of the configuration with respect to meeting overall radiological fault risk reduction (the purpose of probabilistic safety assessment (PSA) and the modelling of the PLS/PMS/DAS as a conglomerate) is provided within Chapter 10. It is important to note that the C&I design process has been iterative to ensure that the C&I configuration supports the overall qualitative and quantitative radiological risk reduction required.

A key aspect of design standards is the concept of a safety life cycle, which includes planning, requirements, design, installation, commissioning, operations and maintenance. Whilst the UK AP1000 is still at the requirements stage, this chapter outlines how the latter aspects of the design life is anticipated to be managed via application of the relevant codes and standards.

The chapter is structured to facilitate an understanding of the C&I architecture and give evidence that the required safety functions of the systems are understood and delivered, i.e. that that they are fit-for-purpose. Therefore, this chapter includes sections that describe:

- how the safety case has been constructed and the categorisation and classification of safety functions and the C&I systems that deliver the safety functions;
- the codes and standards that have been used in the design process and how these reflect RGP, e.g. comparison of the original Institute of Electrical and Electronic Engineers (IEEE) design standards with those of the International Electrochemical Commission (IEC) of which the latter are considered to represent RGP in the UK;
- the high level requirements of the individual systems and their overall architecture;
- the individual systems and how they deliver the safety functions and required reliability; and

- how ALARP is demonstrated for the overall C&I architecture and the individual systems.

As necessary, this chapter makes reference to

- operations and maintenance philosophy;
- security; and
- life-time records.

19.1.2 Control and Instrumentation Architecture Safety Case Overview

There are a number of key interfaces between this Chapter 19 and other chapters within the PCSR. In particular:

- Chapter 5 (Engineering Principles) describes the safety led design approach to ensure that the provision of design solutions is based upon good engineering solutions, hence meeting the requirements of RGP.
- Chapter 8 (Fault and Accident Analysis) includes the methodology for the assessment of design basis (DB) and beyond design basis. The chapter also includes a fault schedule defining the DB class of the fault groups, the relevant safety functions/categories and the classification (e.g., PMS is Class 1 and DAS is Class 2) that deliver the safety functions. The C&I systems must be demonstrated to be delivered in this chapter;
- Chapter 9 (Internally Initiated Faults) includes design basis accident analysis for internally generated faults;
- Chapter 10 (Reactor Faults Probabilistic Safety Analysis and Severe Accident Analysis) confirms the adequacy of the C&I configuration with respect to overall risk reduction requirements;
- Chapter 11 (Internal Hazards) specifies faults for which the C&I systems are to be tolerant (e.g. fire or flooding);
- Chapter 12 (External Hazards) specifies faults for which the C&I systems are to be tolerant (e.g. seismic);
- Chapter 13 (Human Factors) describes the human factors engineering programme, the integration of human factors in the AP1000 design, and the verification and validation of the design. Chapter 13 also examines the role of the operator and how the potential for error has been minimised through design and specifies specific design standards to be applied, for example for the control room layout;
- Chapter 15 (Engineering Schedule) consolidates safety functions and system classifications. Therefore, the C&I SSCs and their classification identified within Chapter 15 form the basis of the descriptions and engineering substantiation provided in this Chapter 19.

The above analyses presented in Chapters 8 to 15 reflects one input into the derivation of safety requirements for the C&I systems substantiated in this chapter. Designation of systems

as Class 1, 2 or 3 in line with IEC 61513 (Reference 19.16) drive safety design/performance requirements that may complement or be in addition to those specified explicitly in Chapters 8 to 15. Moreover, the original design process for the AP1000 C&I systems was undertaken in line with Nuclear Regulatory Commission (NRC) endorsed IEEE standards. The specification of safety requirements via this design route was via the production of documents such as a System Requirements Specification (SyRS) and System Design Specification (SyDS).

19.1.3 Overall Control and Instrumentation High Level Claims

As outlined above, the fault assessment presented within Chapter 8 identifies specific safety functions delivered by the C&I SSCs (summarised in Chapter 15). The requirements of the safety case influences the overall C&I architecture. Chapters 8 to 15 of the PCSR make the following fundamental claims that influence the C&I architecture:

- The reactor is controlled by the PLS, which can initiate faults that if uncorrected can lead to unacceptable consequences (Chapters 8 and 9).

  An unacceptable consequence, as defined in IEC 61226 (Reference 19.22), is a consequence of an operational state or of a postulated initiating event (PIE), that exceeds specified limits for the corresponding plant states, in terms of releases at the site or to the wider environment.

- The DB requirements require two independent safety measures to protect against defined reactor faults, as detailed in the Fault Schedule (Chapter 8). One measure must be Class 1 and the other is specified as Class 2 in the Engineering Schedule (Chapter 15);

- A Remote Shutdown Room (RSR) is required should the Main Control Room (MCR) (Chapter 11) need to be evacuated and there is an Automatic Fire Detection (AFD) system (Chapter 11);

- The operator receives input from the operation and control centre system (OCS) that interfaces with the PMS, DAS, IIS, and RMS, as specified in the Engineering Schedule (Chapter 15);

- The RMS provides monitors to enable action to maintain habitability of the MCR (Chapter 15).

In simple terms, the safety case requires a plant protection system with two independent safety measures to satisfy DB requirements to prevent significant consequences potentially associated with a design basis event. There must be a remote shutdown facility in case of a MCR evacuation and operator interface systems to provide feedback to the operator on the normal plant control condition and the status of the two independent safety measures. These fundamental requirements are shown schematically in Figure 19-7.

It is important to note that the schematic in Figure 19-7 represents the basic building blocks of the C&I architecture. The development of the architecture is explained and justified in Section 19.3. Additional architecture requirements are sourced from the use of the relevant C&I design standards, e.g. IEC 61513 (Reference 19.16).

In addition to the architectural requirements stemming from the safety case, the safety functions require consideration. Table 19-1 summarises the principal safety functional claims made upon the individual C&I SSCs (classification 1 and 2 only), which are further expanded

in the relevant sections with more detail on the definition of the classification numbers and the implication for C&I design in Section 19.2.

It is important to note that for the PLS/PMS/DAS in particular, the design basis analyses place requirements on independence, segregation and diversity between the systems. This ensures that the plant is fault tolerant (i.e., can withstand an unrevealed failure in a safety measure), and the potential for common cause failure (CCF) between the PLS, PMS, and DAS is minimised. Thus, in developing the fundamental C&I architecture, an understanding of these aspects is required.

19.1.4 Overall Control and Instrumentation ALARP Demonstration

19.1.4.1 Introduction

Demonstration that the AP1000 design is ALARP is a stated aim within Chapter 1 of the PCSR. To support the demonstration of ALARP, Westinghouse has produced specific ALARP guidance (Reference 19.37). An outline of how Chapter 19 is structured to provide ALARP arguments, in line with the Westinghouse Electric Company guidance, is given below.

19.1.4.2 ALARP Demonstration

The principal purpose objective of Chapter 19 is to present the C&I architecture and its component systems to demonstrate that they meet the requirements placed upon them from the overall safety case. There is a clear ALARP hierarchy to be demonstrated in terms of architecture, systems and sub-systems. Therefore, the sections associated with the overall C&I architecture and systems make reference to the explicit safety case demands (e.g. from the Engineering Schedule), which include the:

- origin of the demand;
- demand itself, i.e. the safety function and performance requirement where specified (e.g. reliability).

A supporting C&I architecture ALARP justification document has been produced for Chapter 19. It provides justification that the safety case requirements specified in the relevant fault analysis (Chapters 8 to 12), the human factor programme (Chapter 13), fault analysis conclusions (Chapter 14) and the Engineering Schedule (Chapter 15) have been included in the design.

The Plant C&I Architecture ALARP Justification, (Reference 19.61) summarises the ALARP justification. This in addition to the supporting documents and system BSCs provide positive demonstration that the safety case requirements have been satisfied.

19.2 Codes and Standards

19.2.1 Introduction

The AP1000 plant C&I systems were originally designed to United States (US) codes and standards. Subsection 19.2.2 describes this further.

In order to demonstrate that the AP1000 plant C&I design conforms with appropriate UK codes and standards, a conformance exercise has been carried out to provide an evidence

trail of how the UK requirements have been addressed and mapped against the Westinghouse design.

The UK codes and standards requirements can be considered to constitute three main groups:

- the high level guidance provided by the international atomic energy agency (IAEA), augmented by material published by Western European Nuclear Regulators Association (WENRA), Multi-National Design Evaluation Programme (MDEP) and other similar technical bodies;

- the more detailed requirements and recommendations contained in the IEC SC45A series of nuclear sector standards for which IEC 61513 (Reference 19.16) is the head document;

- the UK regulatory expectations as embodied in the ONR safety assessment principles (SAPs), the associated technical assessment guides (TAG) and other documents referenced from the SAPs and TAGs.

Subsections 19.2.3 through 19.2.5 provide further details on the above 3 groups and discusses the conformance of the AP1000 C&I design to their requirements.

19.2.2 Design to US Codes and Standards

The control and instrumentation systems were designed in accordance with guidance provided in applicable portions of the following standards:

- IEEE 379-2000; "IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems"

- IEEE 383-1974; "IEEE Standard for Type Test of Class IE Electric Cables, Field Splices, and Connections for Nuclear Power Generating Stations"

- IEEE 384-1981; "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits" (Reference 19.11)

- IEEE 420-1982; "IEEE Standard for the Design and Qualification of Class 1E Control Boards, Panels, and Racks Used in Nuclear Power Generating Stations"

- IEEE 603-1991; "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations" (Reference 19.5)

- IEEE 627-1980; "IEEE Standard for Design Qualification of Safety Systems Equipment Used in Nuclear Power Generating Stations"

- IEEE 1050-1996; "IEEE Guide for Instrumentation and Control Equipment Grounding in Generating Stations"

- IEEE 1074-1995; "IEEE Standard for Developing Software Life Cycle Processes"

- EPRI TR-102323, Revision 1, "Guidelines for Electromagnetic Interference Testing in Power Plants"

19.2.3 Conformance to UK high level principles

19.2.3.1 Relevant guidance documents

The Safety Guides that record the most applicable guidance provided by the IAEA in relation to the design of C&I architectures are:

- IAEA SSR-2/1 (Reference 19.34)
- IAEA SSG-39 (Reference 19.35)

Other publications of specific relevance include:

- WENRA RHWG Report "Safety of new NPP designs" (Reference 19.38);
- MDEP Common Position № DICWG-09 (Reference 19.3); and
- Licensing of SC software for nuclear reactors (Reference 19.40).

The approach adopted in this PCSR chapter is to conduct an assessment to distil from the above sources, and record in this section, the High Level principles that would be considered Relevant Good Practice. With reference to subsection 19.2.3.2, these High Level principles may be organised into the following 3 broad stages of the C&I design safety life cycle:

- those that constitute "inputs" to the C&I design process;
- those that constitute Engineering Principles to be adopted by the C&I design, including those discussed in Chapter 5 of this PCSR;
- those that mainly (but not exclusively) address the later stages of the safety life cycle.

The Engineering Principles may be further organised into three sub-groups and the full set of principles then used to structure the discussion of the C&I architecture in Section 19.3.

The distilled principles are discussed in subsection 19.2.3.2.

19.2.3.2 High Level Principles

The distilled High Level principles are included below.

1. C&I is designed to be consistent with the Plant Design and Safety Analysis
    a. Constraints from the plant design framework (including Defense-in-Depth (DiD) concept)
    b. Constraints from the plant operational and maintenance philosophies
    c. Functional requirements arising from safety analysis
    d. Performance requirements arising from safety analysis
    e. Safety importance (categorisation) arising from safety analysis
    f. Reliability requirements arising from safety analysis

2. C&I is designed to provide DiD
    a. Functional allocation to levels of defense and specific systems
    b. Independence (between levels of defense and redundant parts)
    c. Diversity (of systems in response to frequent PIE)

d. Separation (to prevent hazard spread) / isolation (to prevent failure propagation)
e. C&I supporting systems adhere to requirements arising from the above considerations

3. C&I conforms to standards appropriate to the category and class
   a. Categorisation of functions
   b. Classification of C&I systems
   c. Conformance to codes and standards
   d. Qualification (environmental and functional)
   e. Validation / commissioning

4. C&I is designed to be robust and reliable
   a. Identification of faults (within C&I systems)
   b. Actions upon fault identification (within C&I systems)
   c. Application of single failure criterion
   d. Communication between C&I systems / prevention of fault propagation
   e. Defense against CCF (within C&I systems)
   f. Avoidance of complexity
   g. Demonstration of reliability
   h. Defense against malicious attack

5. C&I is designed to be safely operated and maintained
   a. Human-system interface (HSI) design
   b. Testability
   c. Maintainability
   d. Ageing and obsolescence management
   e. Design for ease of modification / replacement
   f. Establishment / maintenance of lifetime records

19.2.4 Conformance to UK codes and standards

19.2.4.1 Relevant Codes and Standards

As stated in subsection 19.2.1, IEC 61513 (Reference 19.16) is the head document for the IEC SC45A standards series. In particular, IEC 61513 (Reference 19.16) describes the safety life cycle that should be adopted for the C&I design process. This ensures the required level of confidence that the systems will reliably fulfil their design function through their life cycles.

The normative parts of IEC 61513 (Reference 19.16) are clause 2 (references) and clauses 5 to 8 inclusive.

The C&I architecture High Level Claim regarding conformance with IEC 61513 (Reference 19.16) is documented in UKP-GW-GLR-038 (Reference 19.59) and the BSC documents for the individual C&I systems as follows:

- The overall safety life cycle (clause 5): UKP-GW-GLR-038 (Reference 19.59)
- Systems safety life cycle (clause 6): BSC for systems
- Overall integration and commissioning (clause 7): UKP-GW-GLR-038 (Reference 19.59) and BSC for systems

• Overall operation and maintenance: (clause 8)	UKP-GW-GLR-038 (Reference 19.59) and BSC for systems

Reference 19.59 addresses the safety life cycle requirements that are judged to be applicable to the overall C&I architecture in the form of Claims Arguments and Evidence. It also includes a safety plan which identifies any gaps and compensating measures at the overall C&I architecture level. The safety plan within Reference 19.59 has identified several deficiencies and remedial activities respectively, as well as future work in design or safety case development. These gaps are not considered to be significant. The gaps and compensating measures are identified so that all future work (remedial or not yet performed) is captured and planned appropriately.

In addition to IEC 61513 (Reference 19.16), the most important IEC SC45A standards from the point of view of the C&I architecture are judged to be the following:

- IEC 61226 (Reference 19.22) addressing safety categorisation
- IEC 62340 (Reference 19.15) addressing coping with CCF
- IEC 60709 (Reference 19.41) addressing separation

and to a lesser extent:

- IEC 60671 (Reference 19.42) addressing surveillance testing

Other IEC SC45A standards then address:

- Software-reliant systems important to safety:
    - IEC 60987 (Reference 19.23)
    - IEC 60880 (Reference 19.24)
    - IEC 62138 (Reference 19.25)
    - IEC 62566 (Reference 19.43)
    - IEC 62671 (Reference 19.44)
- Suitability for the environment:
    - IEC 60780 (Reference 19.48)
    - IEC 61000 (Reference 19.6)

but these apply to individual C&I systems for which conformance is addressed, where applicable, within the corresponding BSCs.

In addition to the above, other IEC SC45A standards address the control rooms and associated HSI:

- IEC 60964 (Reference 19.45) addressing the (main) control room
- IEC 60965 (Reference 19.46) addressing the supplementary control room
- IEC 61839 (Reference 19.47) addressing assignment of functions

The system-specific aspects of these standards are addressed within the corresponding BSCs, but other aspects apply at the C&I architecture level and are addressed below.

19.2.4.2 Conformance with IEC SC45A standards series

This subsection considers three important standards in terms of the C&I architecture and three other important standards with which conformance has been demonstrated for individual C&I systems.

19.2.4.2.1 C&I architecture

IEC 61513

IEC 61513 (Reference 19.16) sets out the requirements applicable to C&I systems and equipment that perform functions important to safety. In addition to defining the requirements for a safety life cycle, these relate to the following:

- Derivation of C&I requirements from the plant safety basis
- Design of the C&I architecture and assigning safety functions
- Planning
- Integration and commissioning
- Operations and maintenance

Conformance evidence has also been identified in the following documents:

- Reliability, WNA-AN-00038-WAPP (Reference 19.26)
- Defense in depth, APP-GW-J1R-004 (Reference 19.18)
- Allocation of manual and automatic actions, described in the functional requirements.

The system BSCs evaluated the conformance and all gaps are identified in the system BSCs. The gaps for the overall C&I architecture are identified in Reference 19.59.

IEC 61226

IEC 61226 (Reference 19.22) is directly referenced by IEC 61513 (Reference 19.16) and is a second-tier document in the SC45A series that describes the categorisation functions (safety) and classification of C&I systems.

The main references to demonstrate conformance with IEC 61226 (Reference 19.22) are Quality Management System 3.2.1, regarding safety categorisation, and WNA-SQ-00049-GEN (Reference 19.62), regarding classification of C&I systems. These documents are considered to provide good conformance evidence, since in many cases the text is a direct extract from IEC 61226 (Reference 19.22).

IEC 62340

The main purpose of IEC 62340 (Reference 19.15) is to address CCF. This is used in the diversity evaluations that are documented in the system BSCs.

19.2.4.2.2 C&I systems

IEC 60987

IEC 60987 (Reference 19.23) is directly referenced by IEC 61513 (Reference 19.16) and is a second-tier document in the SC45A series that deals with the hardware design of computerised systems.

IEC 60880

IEC 60880 (Reference 19.24) is directly referenced by IEC 61513 (Reference 19.16) and is a second-tier document in the SC45A series that deals with the software aspects for Class 1 systems performing Category A functions.

IEC 62138

IEC 62138 (Reference 19.25) is directly referenced by IEC 61513 (Reference 19.16) and is a second-tier document in the SC45A series that deals with the software aspects for C&I systems performing Category B and C safety functions.

19.2.5 Conformance to UK regulatory expectations

19.2.5.1 Discussion of ONR SAPs

Although not a code or standard, the ONR SAPs (and associated TAGs) may be used as a basis for assessment by licensees as well as regulators.

It is understood that each SAP, together with any explanatory paragraphs, addresses a specific topic for which the ONR require confidence that the design meets their expectations.

It is also understood that the SAPs are aligned with the IAEA guidance and with the more important IEC SC45A standards and so conformance with the SAPs provides useful confirmation that the design is also in conformance with the IAEA guidance and the IEC SC45A standards.

19.2.5.2 Conformance with ONR SAPs

The C&I Architecture SAPs Conformance Assessment (Reference 19.60) demonstrates conformance of the overall C&I architecture with the identified set of applicable SAPs.

UKP-GW-GLR-039 (Reference 19.60) specifically addresses the C&I system architecture and is supported by individual SAP conformance evaluations for the PMS (which includes the component interface module (CIM) and Alternate Spurious Operation Blocker); PLS; DDS and DAS. The SAPs evaluation has not identified any future activities specific to the C&I architecture that is not already planned for the detailed design development during site licensing. The safety plan for the individual C&I systems can be found in the applicable system BSC.

19.3 Overall Control and Instrumentation System Architecture

19.3.1 Design Basis

19.3.1.1 Fundamental Safety Function

In accordance with international consensus C&I is required in the plant to provide information about the plant and control its operation as follows:

(a) To determine the values of all the main variables that can affect the fission process, the integrity of the reactor core, the reactor coolant systems and the containment

(b) To obtain the essential information on the plant that is necessary for its safe and reliable operation;

(c) To determine the status of the plant in accident conditions;

(d) And for making decisions for the purposes of accident management.

Together with the plant systems and structures the C&I assures the accomplishment of the three critical safety functions:

1. Control of reactivity
2. Heat removal from the reactor core
3. Limiting of reactivity release by maintaining the barriers containing radioactive material:
    a. Fuel pellet and fuel elements
    b. Reactor coolant system
    c. Containment

Thus the C&I ensures in all plant conditions and modes of operation that radiation doses to workers and the public do not exceed the dose limits and that they are kept as low as reasonably achievable during, and following, accident conditions as demonstrated by the analysis presented in PCSR Chapter 8 through 11.

19.3.1.2 Functional and Performance Requirements

Functional and Performance requirements of the C&I are derived from the PCSR, the plant design documents and regulations. The C&I System design further receives inputs from industry standards (PCSR Chapter 5), relevant good practice and Westinghouse experience.

PCSR Chapters 8 through 11 (Fault and Accident Analysis) provides an overview of the fault and accident methodology. The C&I functional design implements the essential safety functions credited in the analysis (see the Table 8A-2 of Chapter 8 for a list of those functions). These requirements are captured in the PMS Functional Requirements (Reference 19.122).

The requirements from plant systems design are imposed on the C&I in the following key design documents for plant systems:

- System Specification Document
- System Piping and Instrumentation Diagrams
- System Component Control Requirements
- System Instrumentation and Packaged Mechanical System Interface Requirements

All of the above requirements are collected in the C&I System Requirements Document (Reference 19.21) and SyDS (Reference 19.13) and from there on flow into individual C&I System requirements specifications.

The UK AP1000 process for management of C&I requirements is described in Reference 19.1. Reference 19.1 provides a description and justification for the C&I requirements capture process, including the derivation of C&I requirements from safety analyses into the C&I requirements documents and the management of requirements from sub-system licensing basis documents into lower level C&I documents.

19.3.1.3 Categorisation Resulting from Safety Case

Categorisation is used to identify the safety significance of a C&I function, and defines the class in which the C&I system function must be implemented.

The method for classifying the safety significance of C&I SSCs is primarily based on deterministic methods, complemented where appropriate by probabilistic methods and engineering judgment (see PCSR Chapter 5). This takes account of factors such as:

- Category of safety function(s) to be performed by the SSC;
- Consequences of the failure of the SSC to perform its function;
- Probability that the SSC will be called upon to perform a safety function;
- Time following any initiating fault at which, or the period throughout which, the SSC will be called upon to operate.

The categorisation and classification methodology is further discussed in subsection 19.3.3.1.3.

19.3.1.4 Reliability Requirement Resulting from Safety Case

All SSCs are expected to have a reliability that is commensurate with their safety importance. Class 1 systems, in particular, are expected to have a high level of reliability. The methodology used to assess the reliability of SSCs is described in PCSR Chapter 5.9.

The target probability for failures on demand for each class of system are:

- The reliability claim for Class 1 systems is 1.0×10^{-3} failures/demand
- The reliability claim for Class 2 systems is 1.0×10^{-2} failures/demand
- The reliability claim for Class 3 systems is 1.0×10^{-1} failures/demand

Justification for the reliability claims can be seen in the BSCs for the respective C&I systems.

19.3.2 Overview of Control and Instrumentation Functional Systems

Figure 19-1 illustrates the instrumentation and control architecture for the AP1000 plant. The figure shows two major sections separated by the real-time data network. Figure 19-1 depicts the real-time data highway as a single network. To meet cyber security concerns, the real-time data highway is separated into security levels as described in Reference 19.17.

The lower portion of the figure includes the plant protection, control, and monitoring functions. At the lower right-hand side is the PMS. This system performs the Category A reactor trip functions, the engineered safety features (ESF) actuation functions, and the Qualified Data Processing (QDPS) functions. The C&I equipment performing reactor trip and ESF actuation functions, their related sensors, and the reactor trip switchgear are, for the most part, four-way redundant. This redundancy permits the use of bypass logic so that a division or individual channel out of service can be accommodated by the operating portions

of the protection system reverting to a two-out-of-three logic from a two-out-of-four logic.

The ESF coincidence logic performs system-level logic calculations, such as initiation of the passive residual heat removal system. It receives inputs from the plant protection subsystem bistables and the main control room.

The ESF actuation subsystems provide the capability for on-off control of individual plant loads. They receive inputs from the ESF coincidence logic, remote shutdown workstation and the main control room.

The DAS is a diverse system that provides an alternate means of initiating reactor trip and actuating selected ESF functions, and providing plant information to the operator.

The plant control system performs open and closed loop instrumentation and control functions using both discrete (on/off) and modulating (analogue) type actuation devices. It controls plant within operational limits and conditions. Failure of this function could require directly the actuation or operation of a Category A safety function.

The real-time data network, which horizontally divides Figure 19-1, is a high speed, redundant communications network that links systems of importance to the operator. The PMS is connected to the network through gateways and qualified isolation devices so that the Category A functions are not compromised by failures elsewhere. Plant protection, control, and monitoring systems feed real-time data into the network for use by the control room and the data display and processing system.

The upper portion of the figure depicts the OCS (refer to PCSR Chapter 13) and DDS. The main control room is implemented as a set of compact operator consoles featuring colour graphic displays and soft control input devices. The graphics are supported by a set of graphics workstations that take their input from the real-time data network. An advanced alarm system, implemented in a similar technology, is also provided. The OCS also houses those systems which are required to provide information that allows specified manual actions necessary after the non-hazardous stable state has been reached to prevent a design basis accident (DBA) from leading to unacceptable consequences, or mitigate the consequences of a DBA.

The safe shutdown of the plant can be established and maintained from the RSR should an evacuation of the control room be required.

The data display and processing system is implemented in a distributed architecture. The working elements of the distributed computer system are graphics workstations, although their graphics capability is secondary to their computing performance. The distributed computer system obtains its input from the real-time data network and delivers its output over the network to other users.

The following subsections provide introductions to the functional C&I systems that are covered in this chapter:

- Protection and safety monitoring system
- Diverse actuation system
- Plant control system
- Operation and control centre system
- Data display and processing system
- Special monitoring system

  - Digital metal impact monitoring system (DMIMS-DX™)
  - Reactor coolant pump vibration monitoring (RCPVM) system
- In-core instrumentation system
- Radiation monitoring system
- Fuel handling and storage

19.3.2.1 Protection and Safety Monitoring System

The PMS is a programmable logic controller (PLC) based system that operates on an Advant® AC160 controller. The Advant AC160-based protection system is a digital-process protection system designed for use within both pressurised water reactors and boiling water reactors. The PMS is described in Reference 19.28, PMS Safety Case Basis. It consists of all the necessary equipment to facilitate reliable actuation of the following functions, namely:

- Detection of system transients beyond the normal operational reactor parameters;

- Actuation of the safety protective functions, necessary to achieve and then maintain the plant in a safe shutdown state.

In addition, the PMS provides the equipment necessary to monitor the plant functions during and following any DBA.

Protective functions are those necessary to achieve the system responses detailed in the safety analyses, and those needed to shut down the plant safely. The AP1000 plant protective functions are grouped into two classes:

- Reactor trip
- ESF actuation

The AP1000 plant PMS consists of four redundant divisions, designated as A, B, C, and D, which are depicted in Figure 19-2 (see Reference 19.3, Section 2.1).

The PMS performs the necessary signal acquisition, calculations, setpoint comparison, coincidence logic, reactor trip, and ESF actuation functions, and safety component control functions to achieve and maintain the plant in a safe shutdown condition. The PMS also contains maintenance and test functions to verify correct operation of the system. The PMS includes four redundant safety displays, one for each division, located on the primary dedicated safety panel (PDSP) in the MCR. Four redundant divisions are provided to satisfy single failure criteria and improve plant availability.

19.3.2.2 Diverse Actuation System

The DAS provides a diverse backup to the PMS as described in the DAS BSC (Reference 19.29). The DAS design utilises solid-state hardware that is based on the Westinghouse 7300 series platform. The DAS supports the AP1000 plant risk mitigation by reducing the probability of a severe accident. Without the DAS, a severe accident could occur from the unlikely coincidence of postulated transients and postulated CCF in the protection and control systems.

The specific functions performed by the DAS are selected based on two separate considerations:

- One consideration is PSA-based. In this approach, the DAS provides backup C&I capability in sequences involving CCF of the PMS and PLS that are risk important (subsection 19.4.2.2). Chapter 10.5.15 provides the PSA summary for the DAS.

- Another consideration is deterministic-based. The DAS provides the Class 2 backup for Category A functions required in the mitigation of frequent faults with an initiating event frequency >10-3/yr.

The DAS design is intentionally simple to enhance its reliability. It uses a fault tolerant approach and provides a means for periodic surveillance testing and revealing internal system faults as described in the DAS BSC (Reference 19.29).

The DAS provides, among other things, a diverse means (from the PMS) to achieve the following safety functions:

- Automatic reactor trip
- Automatic turbine trip
- Automatic passive residual heat removal (PRHR) heat exchanger actuation
- Automatic core makeup tank (CMT) actuation and reactor coolant pump trip
- Automatic passive containment cooling system (PCS) actuation
- Automatic containment isolation
- Manual actuations (see Table 19-2)

The DAS operates with different sensors, logic, and electronic hardware from those used by the PMS. It also provides diverse display of its monitored process variables.

19.3.2.3 Plant Control System

The PLS is an Ovation® based distributed control system (described in Reference 19.30) that provides automatic regulation of reactor and other key system parameters to support normal power operations of the plant. The PLS acts to maximise margins according to plant safety limits and to maximise the plant transient performance. The PLS also provides the capability for manual control of plant systems and equipment. Redundant control logic is used in some applications to increase single failure tolerance.

The function of the AP1000 reactor control systems is to establish and maintain the plant operating conditions within prescribed limits while providing control and coordination of the plant in all operating modes. The control systems improve plant safety by minimising the number of situations for which some protective response is initiated and relieves the operator from routine tasks.

The PLS controls components in the plant that are operated from the MCR or RSR. The system integrates the automatic and manual control of the reactor, reactor coolant, and various reactor support processes for required normal and abnormal conditions.

The PLS contains C&I equipment to change reactor power, control reactor coolant system temperature, control nuclear power distribution, control pressuriser pressure and level, control steam generator level (including feedwater flow control), control turbine bypass steam dump, and perform other plant functions associated with power generation.

19.3.2.4 Data Display and Processing System

The DDS (as the PLS) is a distributed Ovation® based system that provides the plant monitoring and control interfaces for the general system and a subset of the SIS, and provides general indication of certain parameters used by the SIS (described in Reference 19.31). The DDS interfacing includes processing, display, trending, and archival of data from the plant. The DDS consists of the plant C&I network, operator and engineer workstations, data link and application servers, process historian, system support workstations and servers, and the communication network gateway.

The DDS interfaces with the OCS to provide the human-system interface for the MCR operators and engineers and includes the alarm presentation system (APS) for indication of pre-set plant parameters that are exceeded. The DDS allows the operators to access all plant procedures via the computerised procedures system (CPS).

The DDS includes the data processing functions such as the nuclear application programmes that perform calculations to monitor AP1000 plant parameters and processes. The DDS logs and archives plant data through the process historian, and provides data links to external plant systems and gateways to interface with the PMS. The DDS also provides system security, system and database maintenance, and system time management functions for the plant C&I systems and the external communications gateway to the site local area network (LAN).

19.3.2.5 Special Monitoring System

The SMS comprises the DMIMS-DX and the RCPVM system.

The SMS provides detection of the presence of metallic debris in the reactor coolant system (RCS) when the debris impacts against the internal parts of the RCS. The DMIMS-DX is composed of digital circuit boards, controls, indicators, power supplies, and remotely located sensors and related signal-processing devices. A minimum of two sensors are located at each natural collection region, connected to separate instrumentation channels, to maintain the impact monitoring function if a sensor fails in service.

The RCPVM system is a continuous monitoring system that provides outputs for diagnostic tools and information to assist in the evaluation of the performance of the reactor coolant pumps (RCPs).

19.3.2.6 In-Core Instrumentation System

The primary function of the IIS is to provide a 3-D flux map of the reactor core. This map is used to calibrate PMS ex-core neutron detectors and to optimise core performance system adjustments using calculations from the best-estimate analysis core optimisation (BEACON™) application. A secondary function of the IIS is to provide the PMS with the thermocouple signals necessary for the post-accident inadequate core cooling monitor. The IIS assemblies house both fixed in-core flux detectors and core-exit thermocouples.

19.3.2.7 Radiation Monitoring System

The RMS provides early indication of a system or equipment malfunction that could result in an excessive radiation dose to plant personnel or lead to plant damage. Radiation monitoring data, including alarm status, are provided to the AP1000 plant operators via the PLS (and in the case of Class 1 monitors, to the PMS).

19.3.2.8 Fuel Handling and Storage

C&I systems are integral to the fuel handling and storage systems. They encompass the handling systems for moving fuel to and from the reactor and the fuel pond. Fuel Handling and Storage is further described in Chapter 17.

The fuel handling system is equipped with machines that are provided with control systems that perform such functions as interlock control, load-weighing functions and control, and boundary zone checking.

19.3.2.9 C&I Network

The plant C&I network is the Ovation® real-time redundant Class 3 network used to interconnect the C&I systems. The network distributes the plant data that is collected by other systems and is the primary communication network for the entire plant. The plant C&I network provides two-way communication between the distributed controllers, and supports both periodic and aperiodic data transfers of general non-safety (GNS) signals and data. The plant real-time data network also provides secure, unidirectional data transfer from the plant real-time network to the plant communication / business network.

19.3.3 Engineering Principles

The purpose of this subsection is to introduce the engineering principles applied in the design of the C&I architecture and its systems (PLS, PMS, DAS, OCS and DDS). The principles explained and the claims made are further detailed and substantiated in the following BSC documents:

- Reference 19.30 - Westinghouse Report UKP-PLS-GLR-001, Rev. 1, "United Kingdom AP1000 Plant Control System (PLS) Basis of Safety Case,"
- Reference 19.28 - Westinghouse Report UKP-PMS-GLR-001, Rev. 2, "United Kingdom AP1000 Protection and Safety Monitoring System Safety Case Basis," December 2016.
- Reference 19.27 - Westinghouse Report UKP-PMS-GLR-002, Rev. 2, "United Kingdom AP1000 Component Interface Module Safety Case Basis,"
- Reference 19.29 - Westinghouse Report UKP-DAS-GLR-001, Rev. 2, "United Kingdom AP1000 Basis of Safety Case for the Diverse Actuation System,"
- Reference 19.31- Westinghouse Report UKP-DDS-GLR-001, Rev. 1, "United Kingdom AP1000 Data Display and Processing System (DDS) Basis of Safety Case,"

These BSC documents are not further referenced in the text below, only additional relevant document are explicitly referenced.

19.3.3.1 Architecture Compliance with Defense in Depth Requirements

19.3.3.1.1 Functions Allocated to Levels of Defense in Depth and Specific Systems

To achieve the required plant safety levels in accordance with international consensus the C&I supports five independent levels of DiD. The DiD concept and approach describe below is based on the ONR/IAEA definitions and associated criteria. The levels of DiD are described below:

DiD Level 1 - The objective of Level 1 is for prevention of abnormal operation and failures by design.

Level 1 is implemented in the PLS which monitors and controls the plant and its systems in order to achieve safe and reliable operation and to maintain plant parameters within prescribed limits. The DDS and OCS provide the means for the operator to monitor plant status.

DiD Level 2 – The objective of Level 2 is for prevention and control of abnormal operation and detection of failures.

Level 2 is implemented in the PLS which is designed to maintain plant parameters under failure conditions in the plant. All of the C&I have self-diagnostics features. Any failures and abnormal plant conditions identified by these features are provided to the operator through the DDS and OCS.

DiD Level 3 – The objective of Level 3 is for control of faults within the design basis to protect against escalation to an accident.

Level 3 is implemented by the PMS and the DAS, which perform the protective functions resulting from the safety analyses, i.e. those needed to shut down the plant safely and mitigate the consequences of design basis accidents. The PMS and DAS are diverse and independent systems.

DiD Level 4 and 5 – The objective of Level 4 is for control of severe plant conditions in which the design basis may be exceeded, including protecting against further fault escalation and mitigation of the consequences of severe accidents.

The objective is Level 5 is mitigation of radiological consequences of significant releases of radioactive material.

Levels 4 and 5 are provided by the PMS, DAS, and PLS. The DDS and OCS, which provide the means for the operator to monitor plant status, alert the operator to off-normal conditions and provide means for manual control plant of equipment. It includes qualified post-accident monitoring/display of variables and manual operator intervention.

Levels of defense are shown in Figure 19-9 where the levels of DiD are mapped to the C&I architecture.

Reference 19.18, “AP1000 Instrument and Control Defense-in-Depth and Diversity Report,” demonstrates the diversity of the C&I architecture and function allocation with respect to the critical functions of:

1. Reactor Shutdown
2. RCS Inventory Control
3. Core Decay heat Removal
4. Containment Cooling
5. Containment Isolation

It should be noted that the DiD concept and approach described in Reference 19.18 is based on US definition and associated criteria.

19.3.3.1.2 Independence between Levels of DiD

Interference between the systems that make up the levels of DiD is prevented by various means such as physical separation, electrical isolation, functional independence, hardware diversity and independence of communication (data transfer).

The PMS (an Advent® PLC based system) is a standalone system, that is electrically, physically and functionally separated from the other systems in the C&I architecture.

Where there are interfaces to other systems the independence of the PMS from the other systems is assured by the following means (see Reference 19.3):

1. Hardwired output signals to the PLS are provided through qualified isolation devices.

2. Information put out to the DDS is provided through unidirectional isolated datalinks.

3. Non-safety manual control of components is electrically isolated through qualified isolation devices and priority logic in CIM provides functional isolation.

The DAS (a hardwired Westinghouse 7300 hardware system) is a standalone system (like the PMS), that is electrically, physically, and functionally separated from the other C&I systems (see subsection 19.4.2.2.6 - Independence).

1. The DAS does not share any of the sensors, operational platforms, or wiring with the PMS or PLS.

2. The DAS has its own independent wiring system from the sensor to the platform (Processor Cabinets PC1 and PC2) and to the actuated field equipment (Squib Valve Controller Cabinet).

3. The DAS includes a dedicated DAS control panel, with indicators and controls, in the MCR, independent from other systems. It also includes a dedicated remote DAS control panel, with indicators and controls, in the DAS cabinets located in the auxiliary building.

The PLS (an Ovation® distributed control platform) has no interfaces to the DAS and is therefore independent from the DAS. The PLS receives hardwired sensor data from the PMS trough qualified isolation devices to control plant variables. Signal selector algorithms in the PLS ensure that faults in the PMS sensors channel cannot cause the PLS control function to fail.

The PLS relies on the DDS (which is part of the Ovation® platform) for communication, however, critical automatic control functions are designed and implemented to be independent of Plant I&C Network signals. Loss of communications on the network shall not cause these critical control functions to malfunction or upset the plant state.

19.3.3.1.3 Supporting Systems Requirements

Chapter 18 of the PCSR (Electrical Power Systems) defines how electrical power is supplied to C&I systems and how the system supports the reliable operation of C&I under normal and accident conditions such as a loss of off-site power. It also defines the power supply conditions that need to be considered for the design of the power supplies to the C&I systems.

The Class 1 C&I is supplied from the Class 1 DC and Uninterruptible Power Supply (IDS) that supplies the Class 1 alternating current (AC) and direct current (DC) loads. This system is normally supplied from the main AC power system, but in case a loss of all on and off-site AC power, the batteries will supply the power to the required Class 1 loads for up to 72 hours.

The Class 2 C&I is supplied from the Class 2 battery backed electrical supply system (EDS). This system is normally supplied from the main AC power system, but in case of a loss of AC power, the batteries are sized to supply the power for up to 2 hours.

The cable and raceway systems requirements such as separation and segregation are also defined in PCSR Chapter 18.

19.3.3.2 Safety Classification

19.3.3.2.1 Categorisation of Functions

Categorisation of functions is used to identify the safety significance of a C&I function. This in turn helps to define the class of the C&I system in which the function must be implemented. Reference 19.4 provides details on the categorisation methodology applied.

C&I functions are categorised as A, B, C in accordance with Reference 19.22. The resulting categorisation can be summarised as follows:

Category A

A Category A safety function is a principal means of maintaining nuclear safety. Category A safety functions are those utilised to achieve and maintain a non-hazardous, stable state within 72 hours of the initiating event. Failure to maintain a Category A safety function has the potential to result in significant core damage and radiation exposure.

Category B

A Category B safety function is a significant contributor to nuclear safety. Category B safety functions are utilized to; 1) to maintain the non-hazardous stable-state after 72 hours following an accident, 2) prevent radiological exposures to onsite personnel and the offsite population from exceeding the design basis limits, or 3) mitigate beyond design basis accidents. Failure to maintain the Category B safety function may reduce safety margins significantly; with radiation exposure less than Category A limits, but greater than normal operating limits.

Plant process control functions that maintain the main process variables within the limits assumed in the safety analysis are Category A. Failure of this could function could lead directly to the actuation or operation of a Category A safety function.

Category C

Category C safety functions are those safety functions that may make a contribution to nuclear safety, but are not categorised as Category A or Category B. Since the removal of nuclear heat during normal operation prevents reactor trips and the actuation of Category A and Category B functions, these normally operating duty systems are recognised as being important to safety.

19.3.3.2.2 Classification of Structures, Systems and Components

Classification of SSCs is used to identify those SSCs that play an important part in ensuring nuclear safety. This in turn helps to define the quality requirements placed on those SSCs during design and manufacture, and through life. In particular, the safety class of a given SSC can be used to determine which codes, standards, and seismic design considerations are appropriate to the design and manufacture of that SSC. Reference 19.4 provides the details on the classification methodology applied.

In summary the classes of C&I systems are as follows:

Class 1 Systems, Structures, and Components

Class 1 SSCs provide the principal means of fulfilling a Category A safety function.

These SSCs are standby or normally operating SSCs required to protect against, or mitigate the consequences of, DBAs (consistent with the DBA analysis). These SSCs provide the principal means for the protection of the health and safety of the public and workforce, and are selected using deterministic methods. The reliability of these features is confirmed using a probabilistic sensitivity analysis.

Class 2 Systems, Structures, and Components

Class 2 SSCs are a principal means of fulfilling a Category B safety function, or are a significant contributor to fulfilling a Category A safety function.

A significant contributor is defined as an SSC that provides a supplementary capability for those SSCs used in the principal response to DBAs. Class 2 SSCs are identified using the AP1000 plant reliability evaluations described in Section 5.9.

Class 3 Systems, Structures, and Components

Class 3 SSCs are all other SSCs that are not Class 1 or Class 2 that provide contributions to maintaining nuclear safety and include SSCs identified to support the operation of Class 1 and Class 2 SSCs.

General Non-Safety Systems, Structures, and Components

SSCs classified as GNS are those SSCs that do not contribute to maintaining nuclear safety as determined by the safety case.

19.3.3.2.3 Protection and Safety Monitoring System Classification

The PMS provides Category A reactor trip and engineered safety functions under differing circumstances or at different stages of a DBA and is therefore a Class 1 system.

The Class 1 SSCs actuated by the PMS include:

- Reactor Trip Breakers
- PRHR heat exchanger air operated valves
- CMT air operated valves
- Automatic depressurisation system (ADS) 1-3 motorised valves
- ADS4 squib valves

- In-containment refuelling water storage tank (IRWST) injection squib valves
- IRWST recirculation squib valves
- PCS air operated and motor operated valves
- Main Steam Isolation Valves
- Main Feed Isolation Valves
- Steam generator (SG) power-operated relief valves
- Class 1 isolation valves providing the Category A containment safety function
- Class 1 control room habitability system

The CIM is the interface between PMS and the SSCs actuated by PMS. CIM therefore has the same safety claims as PMS and is consequently designated as Class 1 on this basis.

19.3.3.2.4 Diverse Actuation System Classification

The DAS is designed as a backup to the PMS in its provision and actuation of reactor trip signals that provide the Category A criticality control safety function, and in its provision and actuation of a number of Class 1 SSCs that provide the Category A residual heat removal safety function under differing circumstances or at different stages of a DBA. On this basis, the DAS is designated as a Class 2 system.

19.3.3.2.5 Plant Control System Classification

The PLS is mainly used for normal operational control of the plant. However, there are a number of safety claims on it where it actuates SSCs which are diverse or DiD means of providing the Category A residual heat removal safety function, including:

- Startup feedwater system
- Normal residual heat removal system
- Component cooling water system
- Service water system
- Spent fuel pool cooling system

PLS also actuates Class 2 SSCs, which are diverse or DiD means of providing the Category A criticality control safety function. On the basis of these functions, the relevant parts of PLS are designated as Class 2.

19.3.3.2.6 Data Display and Processing System Classification

The DDS is a Class 3 system. The safety significant data display and processing functions are included in the PMS or DAS, as appropriate.

19.3.3.3 Conformance to Design and Manufacturing Codes and Standards

The standards to which the C&I systems have been designed and manufactured are defined in the PCSR Chapter 5 – Engineering Principles. C&I design compliance is demonstrated to the standards described in Section 19.2.

19.3.3.4 C&I Reliability and Fault Tolerance

19.3.3.4.1 Functional Reliability

The C&I architecture and its subsystems are designed for high functional reliability to meet and exceed the C&I design basis reliability requirements stated in subsection 19.3.1.3. The

functional reliability is achieved through the application of the entirety of the engineering principles in subsection 19.3.2.9 (e.g., fault tolerance, independence of systems, redundancy, diversity, testability and maintainability, fail-safe design, selection of proven equipment and quality in manufacturing and installation. The BSC documents provide the evidence that the required reliability has been achieved for the systems.

19.3.3.4.2 Single Failure Criterion

Category A functions conform to the Single Failure criterion. A single failure in the system shall not prevent reactor trip nor shall it prevent the required ESF actuation – even with one of the redundant groups bypassed for maintenance or testing. Category A functions are implemented in PMS, and a diverse backup is provided by the DAS. Additional information on this requirement is further detailed in the description of the PMS and DAS – subsections 19.4.1 and 19.4.2.

19.3.3.4.3 Redundancy in the Architecture

The PMS (Class 1 system) is implemented in four safety divisions (A through D). Redundancy and independence is also designed into the system, so that no single failure or removal from service of any component or channel result in the loss of the protection function. Redundancy is provided in the non-Class 1 system such that a single failure will not cause a forced outage.

The DAS (Class 2 system) is implemented in one-out-of-two taken twice or two-out-of-three logic.

The PLS controllers are redundant. One PLS controller operates as primary and the redundant partner operates as backup. Each PLS controller in a redundant controller pair has two connections to the plant C&I network.

The DDS network is dual redundant. Equipment that is used to implement the redundant network is powered from redundant, uninterruptible power sources so that a loss of one power source will not result in the loss of both networks.

Redundancy is maintained in the power sources that feed each set of PLS controllers. Chapter 18.2.1 discusses the means through which redundancy is achieved for electrical equipment.

19.3.3.4.4 Independence

The PMS is independent from the other C&I systems as described in subsection 0.

The PMS conforms to the requirements for channel independence of IEEE 603 (Reference19.7). A discussion of the channel independence is presented in Reference19.9. The signals to initiate a division of the PMS are electrically isolated from the signals to initiate the redundant divisions. Divisions of the PMS are electrically independent and redundant, as are the power supplies for the divisions up to and including the final actuated equipment.

The four PMS divisions exchange partial trip signals for the purpose of voting. To avoid a single component failure or spurious signal causing an inadvertent plant trip while a channel is in test or maintenance, the protection and safety monitoring system uses the bypass logic discussed in Sections 3.4 and 6.1 of the PMS BSC (Reference 19.28).

The PLS is independent from the other C&I systems as described in subsection 19.4.3.2.

The PLS controls the plant from the same measurements which are used by the PMS. This permits the control system to function in a manner which maintains margin between operating conditions and safety limits, and reduces the likelihood of spurious trips.

Compliance to the requirements of IEEE 603 (Reference 19.7) is assured by the provision of isolation devices to guard the protection system against possible electrical faults in the control system.

Functional independence of control and protection is obtained by signal selector algorithms. The purpose of the signal selector algorithm is to prevent a failed signal, caused by the failure of a protection channel, from initiating a control action that could lead to a plant condition requiring that protective action. The signal selector function provides this capability by comparing the redundant signals and automatically eliminating an aberrant signal from use in the control system. This capability exists for bypassed sensors or for sensors whose signals have diverged from the expected error tolerance.

The DAS is independent from the other C&I systems as described in subsection 19.4.2.2.

19.3.3.4.5 Physical Separation

Physical separation and segregation relate to the location of equipment, cable routing, and other factors to limit CCFs of independent circuits and functions. This includes failures from external causes and mutual physical effects between the circuits and functions. The high-level architecture supports the decomposition of the overall functionality into physically separate pieces while allowing the controlled flow of information across the boundaries.

The four PMS divisions are located in four separate rooms, cabling, sensors and actuated devices are physically separated. Separation and segregation for the PMS is discussed in subsection 19.4.1.2.

The DAS is located in a separate area from the PMS as described subsection 19.4.2.2.

Separation and segregation requirements for the PLS is discussed in subsection 19.4.3.2.

19.3.3.4.6 Electrical Isolation

Electrical signal isolation between systems is provided by fibre optic communications and qualified isolation devices. These prevent credible faults (such as open circuits, short circuits, or applied credible voltages) in one circuit from propagating to another circuit.

Electrical isolation of the power supplies is ensured by the use of separate power supplies for separate systems and redundant divisions in the systems

19.3.3.4.7 Functional Independence

The C&I system architecture emphasises functional divisions, rather than divisions based on physical systems or plant layout. Functional divisions in this case refer to major C&I functions such as plant control and protection. Data-gathering hardware and software for digital and analogue input signals ensure that the signal provided meets the requirements for all the assigned uses of that signal.

Signal selector algorithms provide the plant control system with the ability to obtain inputs

from the protection and safety monitoring system. The signal selector algorithms select those protection system signals that represent the actual status of the plant and reject erroneous signals. Therefore, the control system does not cause an unsafe control action to occur even if one of four redundant protection channels is degraded by random failure simultaneous with another of the four channels bypassed for test or maintenance.

Each signal selector algorithm receives data from each of the redundant divisions of the protection and safety monitoring system. The data is received from each division through an isolation device.

The signal selector algorithms provide validated process values to the plant control system. They also provide the validation status, the average of the valid process values, the number of valid process values, an alarm (if one process value has been rejected), and another alarm (if two process values have been rejected).

For the logic values received from the protection and safety monitoring system, such as permissives, two-out-of-four voting is used to provide a valid logic value to the plant control system.

19.3.3.4.8 Diversity – Defense against Common Cause Failures

As demonstrated in Reference 19.32 and Reference 19.55, the DAS is diverse from the PMS and the PLS/DDS. The DAS is based on the Westinghouse 7300 series (analogue) platform, the PMS is based upon the Westinghouse Common Q™ (digital) platform, and the PLS/DDS is based on the Emmerson Ovation™ (digital) platform. These platforms are diverse with respect to:

- Development Processes
- Tools Used
- Development Teams
- Technology
- Hardware Modules
- Components

Diversity analysis of the PLS/DDS and DAS is described in Reference 19.55. Diversity analysis of the PMS and DAS is described in Reference 19.32. Note that the PLS/PMS Diversity Analysis will be developed after GDA as identified in the safety plan for the IEC 61513 compliance document for this chapter (Reference 19.59) and the PMS and PLS BSC (References 19.28 and 19.30 respectively. Diversity for the PMS, DAS and PLS is also discussed in subsections 19.4.1.2.4, 19.4.2.2.5, and 19.4.4.2 .

19.3.3.4.9 Failure Modes

Various features in the C&I design assure a preferred state is obtained in case of equipment (hardware and software) faults and failures. Those features and the definition of the desired safe state may vary from system to system and are described in detail in the BSCs for the systems. The following high level strategies are generally applied (the implementation details vary from system to system):

- Continuous verification of output wiring to actuated devices.
- Definition of preferred failure modes by the system designer in design

documentation.

- Dynamic operation of the systems ensures that hard failures (static failures) are detectable by interfacing systems such that these can take on an appropriate state upon the detection of failure.
- Continuous diagnostics are implemented to reveal faults such that appropriate automatic and manual actions can be taken to prevent a failure of the systems and undertake timely maintenance operations.
- Internal redundancy and comparison between redundant systems parts assures faults are revealed and prevents single faults from leading to a failure of the system.
- Comparison of redundant sensor values.

The fail-safe design for the PMS is justified in subsection 19.4.1.2 of this Chapter and subsection 6.1.9.3 of the PMS BSC (Reference 19.28).

19.3.3.4.10 Environmental Qualification

A qualification program for items important to safety is implemented to verify that items important to safety are capable of performing their intended functions when necessary, and in the prevailing environmental conditions, throughout their design life. The program demonstrates the continued functionality of the systems for design basis events such as earthquake, environmental and electromagnetic compatibility (EMC) events, as required by the system function and classification.

The C&I platforms have undergone generic qualifications programs, but the AP1000 has unique requirements for equipment qualification as described in Section 5.8 of the PCSR. In that section of the PCSR, the standards to be met for equipment qualification are stated. The AP1000 Equipment Qualification Methodology Document (Reference 19.8) describes the implementation of the Equipment Qualification (EQ) program in compliance to the PCSR.

The EQ methodology is based on IEEE standards. The following references demonstrate the equivalence of these IEEE standards to the IEC standards:

- EQ-EV-283, “Electromagnetic Compatibility Standards Evaluation,” Reference 19.33
- EQ-EV-284, “Comparison of IEC Standard 60780-1998 to IEEE Standard 323-1974,” Reference 19.51
- EQ-EV-285, “Comparison of IEC Standard 60980-1989 to IEEE Standard 344-1987,” Reference 19.52

19.3.3.5 C&I Testing and Maintenance

19.3.3.5.1 Defense against Unauthorized Access

Unauthorised access to, or interference with, items important to safety, including computer hardware and software, will be prevented through multiple means as defined in Reference19.3 for the PMS and the BSC for individual systems and the security plans (yet to be produced). Examples of those measures are:

- Procedural control to means of access during installation, commissioning and operation.

- Locked cabinets and key-lock switches to prevent access to maintenance functions.
- Password controlled access to functions.
- Absence of data connections to external systems.
- Cyber security measures as defined in the security plan.

19.3.3.5.2 C&I Testing During Operation

In order to meet the reliability goals and the design standards, the PMS and the DAS are equipped to perform testing and calibration where possible with the plant at power. The frequency/periodicity of these tests vary depending on the reliability goals for the systems. Current typical intervals are defined in the surveillance requirements of the technical specifications.

Periodic surveillance of the PMS through the application of overlapping tests provides an independent means to test system operation (function and response time) and ensure calibration of analogue circuitry is maintained. The testing features of the PMS are discussed in Reference 19.3.

Testing from the sensor inputs of the PMS through to the actuated equipment is accomplished through a series of overlapping sequential tests. The majority of the tests are capable of being performed with the plant at full power. Sensors are generally not accessible, these are calibrated during plant outage. Where testing final equipment at power would upset plant operation or damage equipment, provisions are made to test the equipment at reduced power or when the reactor is shut down. PMS testing is further discussed in subsection 19.4.1.2.

The DAS is provided with the capability for channel calibration and testing while the plant is operating. To prevent inadvertent DAS actuations during online calibration, testing. or maintenance, the normal actuation function is bypassed. DAS testing is performed on a periodic basis, and is further discussed in subsection 19.4.2.2.7.

Testing of the PLS is supported by the inclusion of modular design and built-in diagnostics that assist personnel in routine testing and maintenance, fault finding, and component replacement. Testing for the PLS is covered in subsection 19.4.3.2.

19.3.3.5.3 C&I Maintenance During Operation

Faults in the PMS can be diagnosed and repaired with the plant at power. The redundancy of the PMS combined with the bypass feature for test and maintenance allows for the removal of operation of a redundant protection set (or parts thereof) for repair whilst the minimum required redundancy is maintained. See Reference 19.3 and PCSR subsection 19.4.1.2 for a description of the test and maintenance features of the PMS.

During testing or maintenance, functions are provided to bypass a protection set or individual channel. The coincidence logic is automatically adjusted and the remaining redundant protection sets or channels continue to meet the single failure criterion. The two-out-of- four logic is automatically reinstated when the bypass is removed

The PMS Maintenance and Test Panel provides the means for modifying those setpoints that need to be adjusted during plant operation. Access to this feature is under administrative and

key-lock control.

Test features are provided in the DAS that allow a channel to be bypassed for test or maintenance.

The redundancy built into the PLS supports the maintenance of the system with the plant at power. System status displays aid in fault finding. Redundant controllers can be powered down for repair while the backup controller maintains the functionality of the unit. Input/output (I/O) modules can be replaced while the cabinet is powered and remains operational.

The redundancy in the DDS allows for the repair of the data network in a transparent way without affecting the DDS communication. The redundancy of the OCS workstations allows for taking a workstation out of service without impacting the tasks of the operator.

19.3.4 Overall Planning

19.3.4.1 Management of Safety

Chapter 7 of the PCSR describes the management arrangements associated with the achievement of nuclear safety throughout the design life cycle of the plant considering the design, change control, construction, commissioning, maintenance, ageing, and degradation and decommissioning.

Currently, Westinghouse as the Design Authority for the AP1000 C&I, has an established management system for ensuring that all safety requirements for the design of the C&I are considered and implemented in all phases of the C&I life cycle. The Westinghouse global management system (WGMS) is described in Chapter 3.

At a suitable point, this role is anticipated as being transferred to the licensee, and Westinghouse is anticipated as becoming the responsible designer of the C&I (as described in Chapter 3). Westinghouse will provide support to the licensee until agreed otherwise, and formal procedures are anticipated to be established between Westinghouse and the licensee to define the responsibilities throughout the development of the AP1000 C&I design, procurement, construction, installation, and commissioning phases.

The quality and safety of the C&I is dependent on the abilities and attitudes of the individuals who design, construct, commission, operate, examine, maintain, inspect, test, and modify the equipment. Management is responsible for determining and assuring personnel attains the necessary competencies in terms of skills, education, and experience requirements for the activities affecting quality as directed by the WGMS procedures (as defined in the Chapter 3).

19.3.4.2 Life Cycle Process

The C&I systems are implemented using structured and planned life cycle processes. The integrated C&I design process is described in Reference 19.56. Sections 1, 2, and 3 of Reference 19.56 provide the requirements for the systematic process to be followed for a C&I design, including the following:

- Definition of the phases of the design
- Process for collection and definition of requirements for each design phase

- Development and documentation of requirements for subsequent phases of the design process
- Requirements for configuration management
- Verification and validation of the requirements between the design phases

Section 4 of the PMS BSC (Reference 19.28) provides the requirements and guidance for the system-level requirements engineering phase and the development of a System Requirements Specification (Reference 19.21). The AP1000 requirements documents whether at the overall C&I level or at the subsystem level (e.g., PMS) include both functional and non-functional requirements.

Section 5 of Reference 19.56 provides requirements for the system design process. This process provides the requirements and guidance for the overall C&I system design process, including the development of an C&I SyDS and the allocation of requirements to subsystems. The I&C SyDS (Reference 19.13) is one of the results of this phase of the process.

The processes applied are compatible with the safety classification of the systems and compatible with the relevant IEC standards (IEC 61513 (Reference 19.16), IEC 62138 (Reference 19.25) and IEC 60987 (Reference 19.23).

19.3.4.3 C&I Validation/Testing

C&I is exhaustively validated/tested during manufacturing, installation and plant start-up in accordance with the strategy defined in the I&C test strategy (Reference 19.63). A "bottom-up" approach is applied to the testing, such that test are performed at increasing levels of complexity and integration.

During design and manufacturing, test activities are performed on the parts, components, assemblies, and subsystems that make up the subsystems that comprise the integrated plant C&I system. These activities are associated with the subsystem design organisations or their independent verification and validation organizations when required by regulation. The activities typically include a combination of one-time design tests and recurring manufacturing tests. For SIS, the activities include any required commercial dedication activities.

The scope of these activities includes all functions of the entire subsystem inclusive of all interfaces, both internal and external, and all manufacturing and design requirements (including performance and capacity requirements).

The next level of activities focuses on the interfaces that interconnect the individual subsystems that comprise the integrated C&I system. It validates the interfaces between subsystems from a connectivity or functionality point of view, where testing at earlier levels is not sufficient to provide adequate coverage of the interface.

19.3.4.4 C&I Commissioning - Validation/Testing

C&I testing on site after installation is coordinated with the plant test and commissioning activities described in PCSR Chapter 7. After installation of the equipment validation and testing focuses on cabinet installation verification and initial energisation. Inspection and testing is performed to verify absence of shipping/installation damage, correct equipment and cable and power supply installation. Basic functionality is confirmed for controllers, modules, and workstations after the equipment is powered. Software is anticipated as also being loaded (if needed) during this phase of testing.

Along with construction progress testing focuses on C&I system interface testing as the C&I equipment is installed and progressively interfaced to other C&I equipment as well as field equipment associated with plant systems. The testing then progresses to include component and system-level testing of mechanical and electrical systems utilizing the C&I system for controls and indications.

19.3.4.5 C&I Overall Integrated Commissioning - Validation/Testing

Once plant systems can be put to work testing focuses on preoperational testing of all the plant systems and the emphasis is on integrated system testing with process systems using the C&I systems as a resource. This level of testing is performed prior to initial fuel loading to demonstrate the capability of plant systems to meet performance requirements.

The tests demonstrate that equipment and systems perform in accordance with design criteria so that initial fuel loading, initial criticality, and subsequent power operation can be safely undertaken.

The general objectives of the preoperational test program are the following:

- Demonstrate that C&I systems, including alarms and indications, meet appropriate criteria based on the design;
- Provide documentation of the performance and condition of equipment and systems;
- Provide baseline test and operating data on equipment and systems for future use and reference;
- Operate equipment for a sufficient period to demonstrate performance;
- Demonstrate that C&I and plant systems operate on an integrated basis.

Plant operating, emergency, and surveillance procedures are incorporated into the initial test program procedures. The capability of the C&I to support the procedures is verified through use, to the extent practicable, during the preoperational test program and revised if necessary, prior to fuel loading.

Start-up Testing continues to validate the C&I systems properly perform during integrated plant testing. Final tuning and adjustments of controls are performed based on real-time plant responses to transients. This testing phase will begin during initial fuel load and will not complete until the end of the 100% power accession plateau.

Start-up tests begin with the initial fuel loading and are performed to demonstrate the capability of individual systems, as well as the integrated plant, to meet performance requirements. Start-up test verify that the operating characteristics of the reactor core and associated control and protection equipment are consistent with design requirements and accident analysis assumptions.

These tests facilitate gathering of the required data to calibrate equipment used to control and protect the plant and to verify that the plant is operating within the limits imposed by the Technical Specifications.

19.3.5 Overall Operation

19.3.5.1 Provision of Control Locations

A MCR is provided from which the plant can be safely operated in all operational states, either automatically or manually, and from which measures can be taken to maintain the plant in a safe state or to bring it back into a safe state after anticipated operational occurrences and accident conditions. The MCR is further described in the PCSR Chapter 13.

Instrumentation and control equipment is provided at an alternate location - the Remote Shutdown Room (RSR). This room is so equipped to enable the reactor to be be placed and maintained in a shutdown state, to allow residual heat to be removed, and to allow essential plant variables to be monitored if there is a loss of ability to perform these essential safety functions in the main control room.

The RSR will provide a Safety Panel with Class 1 displays complete with accompanying PMS soft blocks/resets. Class 1 System Level dedicated controls will also be provided that will be hardwired to the PMS cabinets. The RSR is further described in PCSR Chapter 13 (Human Factors).

A SAP compliance document (Reference 19.50) has been produced which provide the claims, arguments, and evidence to demonstrate that the UK AP1000 RSR provides adequately classified displays and controls to comply with the applicable SAPs selected from "Safety Assessment Principles for Nuclear Facilities" (Reference 19. 2). An ALARP document (Reference 19.53) has also been produced which provides the claims, arguments, and evidence to demonstrate that the UK AP1000 RSR design, including Class 1 displays and controls satisfies ALARP principles. Reference 19.53 also documents the optioneering exercised to determine the ALARP design for the UK AP1000.

19.3.5.2 Human-System Interface Design

Chapter 13 (Human Factors) describes the application of human factors engineering in the plant and provides requirements for the application of human factors engineering in the C&I design – particularly in the human-system interface.

19.3.5.3 Operational Limits and Limiting Conditions for Safe Operation

A set of operating rules (operational limits and conditions) for safe operation of the plant is established and applied to the operation of the C&I systems through the application of the surveillance requirements, adherence to the limits for operability, response time and accuracy, and application of the action requirements in the plant Technical Specifications. The development of these operating rules is described in Chapter 5 and Reference 19.58.

Trip setpoints in the C&I will be selected to provide sufficient allowance between the trip setpoint and the analytical limit to account for uncertainties. The safety analysis establishes the analytical limit based on the parameter that is measured and the required time response for the protective action. After the detailed design is completed, the uncertainty in each channel is evaluated based on operating experience, equipment qualification, design specifications, engineering analysis, laboratory tests, and engineering drawings. This evaluation will include process and measurement uncertainties. The results of the evaluation will be used to select the trip setpoint so that the analytical limit will not be exceeded under all conditions.

19.4 Control and Instrumentation System Descriptions

This section provides description of the major C&I systems.

19.4.1 Protection and Safety Monitoring System

19.4.1.1 Protection and Safety Monitoring System Definition

The PMS is a Class 1 PLC based system that operates on an Advant® AC160 controller. The Advant AC160-based protection system is a digital-process protection system designed for use within both pressurised water reactors and boiling water reactors. It was originally developed as a commercial system and has since gone through a qualification regime to achieve Class 1 status as a dedicated nuclear power plant protection system in accordance with European codes and standards.

19.4.1.2 Protection and Safety Monitoring System Design Basis

A basis of safety case for the PMS containing arguments and detailed evidence in support of how the safety principles and standards in relation to the design of the PMS have been met has been produced. See Reference 19.28 "United Kingdom AP1000 Protection and Safety Monitoring System Safety Case Basis."

A detailed description of the design process for the PMS is described in subsection 6.1.5.2 of Reference 19.28.

As a Class 1 system, the PMS plays a principal role in achieving or maintaining a safe state in the reactor and prevents a DBA from leading to unacceptable consequences. The function of the PMS is essential at the beginning of the transient when no alternative actions can be taken, even if unforeseen faults are detected.

The following factors are considered in this design approach section to provide evidence of the design philosophy:

- Separation/segregation
- Manual actuation
- Power
- Diversity
- Redundancy
- Software
- Common Cause Failure Independence
- Independence
- Fail-safe
- Testing
- Operator interfaces
- Safety display functions
- Spurious Actuation

19.4.1.2.1 Separation and Segregation

The PMS provides four divisions of equipment that are in different locations of the plant, which meets the requirement for divisions of equipment to be in areas separated from each other and from other areas in the plant by fire barriers with a minimum 3-hour fire-resistance rating. The cabling is segregated in accordance with Reference 19.7.

Isolation devices are used to maintain independence where redundant equipment is required to communicate with other systems. For example, electrical separation of the IDS and the EDS is maintained through the use of isolation devices in the interconnections between the PMS and the DDS.

There is a gateway in each of the PMS divisions that connects the Class 1 system maintenance and test panel (MTP) to the Class 2 and Class 3 systems, and the flow of information between the two gateway subsystems is strictly from the Class 1 subsystem to the lower class subsystem (i.e., it is unidirectional, and therefore prevents the lower class system from adversely affecting the system).

19.4.1.2.2 Manual Actuations

The PMS allows the "permit manual trip or bypass" function of each individual automatic reactor trip function and permits manual actuation or bypass of each individual automatic ESF actuation function.

The PMS manual trip facility is wired directly to the reactor trip circuit breakers (RTCBs). Therefore, a failure of the automatic system cannot prevent a manual tripping of the reactor (Reference 19.3, Figure 2.2).

The manual reactor trip consists of two controls in the MCR, either of which trip all eight of the RTCBs. There are no interlocks or bypasses associated with the manual trip function.

19.4.1.2.3 Power

The power supply for the PMS is the IDS. The power in a division is converted from IDS power to DC power for the PMS cabinet equipment using power supplies (see subsection 3.4.2.1.4 of Reference 19.28).

The IDS provides power for the Class 1 equipment required for plant instrumentation, control, monitoring, and other vital functions. In addition, the IDS provides power for the emergency lighting in the MCR and at the remote shutdown workstation.

The IDS can provide power for the safe shutdown of the plant for 72 hours without the support of battery chargers during a loss of all AC power sources coincident with a DBA. The system is designed so that no single failure will result in a condition that prevents the safe shutdown of the plant.

The IDS is further described in Chapter 18.

19.4.1.2.4 Diversity

The PMS also provides automatic and manual actuation of ESFs in response to DBAs, particularly those ascribed to CCF.

DiD is provided by the ESFs and the DAS. These systems utilise diverse hardware functions. System diversity is substantiated in Reference 19.18 and provides supporting evidence.

As part of the overall C&I systems, the PMS has been included in Reference 19.18. In addition to this report, Westinghouse has produced a specific diversity analysis between the DAS and PMS for the UK AP1000 C&I that addresses requirements from additional standards including IEC-62340 (see Reference 19.32).

Diversity is addressed by the provision of the DAS for frequent faults as shown in the Fault Schedule of Chapter 8. It is a completely separate system for actuation of Class 1 reactor protection systems. The employment of a completely separate system for reactor protection has been implemented to address the issue of DiD. The DAS is addressed in detail in subsection 19.4.2.

19.4.1.2.5 Redundancy

The PMS includes redundancy to ensure that a single failure of any component part of the system will not cause either a failure to trip or the operational failure of any ESF.

Four redundant measurements using separate sensors are made for each of the reactor trip variables. The processing of these variables is carried out by each of the PMS's four redundant sections (in an identical manner). The outputs are passed to the system logic circuitry; each of the redundant divisions sends its partial trip status to each of the other three redundant divisions over isolated data links. A reactor trip signal is generated if two or more of the redundant channels of a single variable are in the partial trip state. In respect to reactor trip functionality, the PMS employs two-out-of-four logic voting (reduced to two-out-of-three voting with one allowable bypass). This allows for a single equipment failure, or the execution of plant maintenance on a single division, while still ensuring adequate protection by the use of the remaining two-out-of-three voting logic.

Redundancy provides confidence that ESFs are actuated on demand, even when the PMS is degraded by a single sensor failure.

ESF coincidence logic functions are performed by two ESF logic processors per division for more reliable accident mitigation and protection against spurious actuation. The primary functions of the ESF logic processors are to perform the two-out-of-four vote for each ESF safety function and transmit the data to the integrated logic processors (ILP). To perform the ESF coincidence logic calculations, the ESF processors require data from the Bistable processor logic (BPL) subsystems.

The ESF logic processors perform the following functions:

- Receive bistable data supplied by the four divisions of BPL subsystems and perform two-out-of-four voting on this data.
- Implement system-level voting logic and transmit the output to the ILP processors for ESF component fan-out and actuation.
- Process manual system-level actuation commands received from the MCR or RSR.

19.4.1.2.6 Software

The PMS software will be designed, produced and installed in accordance with Reference 19.9, which specifies the process used.

The programming language C is used for the Common Q platform flat panel display system and the custom PC elements. The PMS application software for the AC160 is written in a function block (FB) oriented language. The requirements for FB-oriented software are found in the Common Q coding standard and guidelines document Reference 19.10.

The CIM does not contain software. However, software is used in its design. The development of the CIM is based on IEEE standards and US NRC Regulatory Guides. Subsection 6.1.3 of the CIM BSC Reference 19.27 describes compliance with relevant UK Safety Assessment Principles and Industry Standards.

19.4.1.2.7 Common-Cause Failure

For the PMS to be able to provide high levels of reliability, CCF needs to be minimised.

The PMS and DAS safety features are sufficiently dissimilar and separate that a CCF that fails both need not be considered, e.g., the PMS and DAS achieve reactor trip and required ESF functions by using different functions and diverse equipment.

To minimise CCF mechanisms within the PMS, for example, the following environmental effects have also been taken into consideration:

- **EMC** – Susceptibility and emissions testing of the digital equipment will be carried out to meet the prevailing legislative requirements for both conductive and radiated signals.

- **Separation and isolation requirements** – Physical separation and segregation have been used in the placement of equipment and in the routing of cables to mitigate the effects of external hazards and those effects mutually induced. Particular attention has been paid to the separation of IDS divisions, as well as supply voltage levels within groups. Different signal routing is used to ensure the application of diversity (e.g., by equipment diversity or functional diversity).

19.4.1.2.8 Independence

The PMS meets the requirements of independence in Reference 19.11.

The PMS is a Class 1 PLC-based system. The system is designed to incorporate enough redundancy to mitigate single failure trip operation. The system is divided into four redundant divisions, each housed in separate cabinets with each division in separate rooms.

To ensure that subsystem independence is not compromised, the following features are used:

- Separate DC power sources with output protection to prevent interaction between redundant BPL and local coincidence logic subsystems upon failure of a subsystem.
- Separate input or output circuitry to maintain independence at the subsystem interfaces.
- Dead man signals that force a predefined operating condition upon the cessation of a normally dynamic input parameter to improve the reliability of discrete data crossing the subsystem interface.
- Optical coupling between subsystems. Optical transmission media are employed to meet Class 1 independence requirements between safety divisions and between Class 1 and lower class equipment (Reference 19.13).

- Four separate sensors for each variable.

The PMS independence features are further described in subsection 6.9.16 of the PMS BSC (Reference 19.28).

19.4.1.2.9 Fail-safe

Extensive, detailed failure modes and effects analysis (FMEAs) have been performed on the PMS modules to determine the effectiveness of self diagnostics. In general, the results indicate that a high percentage of faults that could occur will be detected by diagnostics and cause the system to assume a default state. These results are incorporated into unavailability equations as percentages of faults that are detectable or fail-safe or both in Chapter 10 and WCAP-16438-P (Reference 19.14).

The reactor trip coincidence logic provides the logic function to combine the partial trip signals and outputs a fail-safe trip signal to the RTCBs. In the case of the PMS, this results in the release of the control rods into the reactor under gravity resulting from the loss of power to the rod drive mechanism coils. The two-out-of-four voting allows bypass of a single channel or division while still maintaining the single failure criterion. The bypassing of two or more redundant channels or divisions is not permitted.

The PMS is designed such that a loss of power to the system will result in a reactor trip.

The loss of AC power sources (low IDS battery charger input voltage) is detected and initiates ESFs. The ADS timer in the PMS actuates ADS on low battery charger input voltage after 22 hours. The PRHR heat exchanger, and supporting passive features (reactor trip, CMTs, PCS) all self-actuate on loss of all AC and DC. On an extended loss of AC power, the Class 1 systems revert to a fail-safe configuration and the failure is alarmed in the MCR.

The fail-safe design of the PMS is further described in subsection 6.1.9.3 of the PMS BSC Reference 19.28.

19.4.1.2.10 Testing

The PMS includes the features of continuous self diagnostics and on-line verification testing. The system utilises two-out-of-four voting, which allows for the bypass of a single channel or division to allow test and maintenance operations to be carried out without compromise of the safety function, as this leaves the system running in two-out-of-three logic mode. Periodic surveillance is carried out manually to verify that the system is performing its safety function.

Testing is carried out via the four independent MTP subsystems, each located within one of four divisions of the PMS (see Figure 19-3). The divisions are physically separated and electrically isolated from each other. Therefore, an MTP subsystem can only make changes to its associated division and does not require additional physical means of restricting it from accessing other divisions. (i.e., cable disconnects and key lock switches). The following description illustrates the operation of one of the four identical divisions.

The MTP provides the human interface to the system and is used for maintenance and test functions. The MTP provides the means for the technician to perform the following functions (Reference 19.3, subsection 2.2.6):

- Periodic surveillance testing to verify operability

- Corrective maintenance
- Enter and change setpoints and calibration coefficients
- Place a protection function in partial trip mode via key lock switch to prevent unintended action
- Place a protection function in bypass mode via key lock switch to prevent unintended action
- Display partial trip or actuation and bypass status for each bistable trip function in each division
- Display reactor trip status in each division
- View detailed system status and diagnostic messages
- Load software into the Advant Controller 160 processor modules, via key lock switch to prevent unintended action
- Provide interface to the real-time data network

A detailed description of the maintenance, testing, and calibration procedures for the PMS is given in Reference 19.3, Section 6.

19.4.1.2.11 Operator Interfaces

The HSI for the PMS will be situated in the MCR and the RSR and is referred to as the Safety Displays.

19.4.1.2.12 Safety Display Functions

There is one Class 1 safety display associated with each of the four independent divisions of the PMS located in the MCR. The C&I in the MCR contains separate interfaces with the PMS as shown in Figure 19-3, and provides the following functionality:

- Operator access to control the system permissives, blocks, and resets in accordance with the functional requirements documents and functional logic diagrams.
- Provides manual control of safety components with onerous consequences.
- Displays the values of system parameters.
- Provides the capability to trend system parameters that permit operators to select variables for trending and enter the required trend control parameters.
- Provides high-level status of the health of the system.
- Provides the operator with the ability to perform periodic calibration of the nuclear instrumentation system (NIS) and over temperature/ΔT calculations. The purpose of the testing and calibration is to demonstrate that the protection system is operable by verifying that the division is capable of performing its protective function.
- Provides display of QDPS variables.

19.4.1.2.13 Spurious Actuation

Spurious actuation within the PMS software has a potential CCF that could result in the simultaneous activation of the system.

Potential initiating events follow:

- Actuation of CMT isolation valves results in no significant consequence
- Actuation of PRHR isolation valves results in no significant consequence.
- Actuation of PCS isolation valves results in no significant consequence
- Spurious actuation of ADS Stages 1 through 4 resulting in an intermediate to large hot leg loss-of-coolant accident. Stage 4 spurious actuation would expose piping / supports to loads beyond their capability, which could result in degraded ADS vent capacity.
- Actuation of IRWST squib valves would expose piping / supports to loads beyond their capability, which could result in degraded ADS vent capacity.
- Actuation of recirculation squib valves resulting in potential draining of IRWST into sump

The squib valves are discussed in further detail in Chapter 17.5.

The Alternate Spurious Operation Blocker is a diverse Class 1 module physically located within each of the PMS divisions. It accepts the two CMT narrow-range upper-level measurements in that division, two battery charger low input voltage signals and a manual unblock control as inputs, and provides block signals to the outputs that control the ADS valves assigned to that division. To block ESF actuation, it interrupts the arm signal from the CIM outputs to the squib valve termination unit or the open signal to the motor-operated valves motor control centres.

The ADS blocker device provides a reliable capability independent of the PMS computers that significantly reduces the likelihood of spurious actuation while maintaining the safety function of the system. As a result, such spurious signals do not need to be analysed with respect to plant performance and radiation releases.

There is a separate basis of safety case for the PMS Spurious Actuation Blocking Device, Reference 19.49.

19.4.1.3 Protection and Safety Monitoring System Function

The PMS provides detection of system excursions beyond the normal operational limits and automatic actuation of the protective functions necessary to ensure that the plant reaches and remains in a safe shutdown state. The system is designed to incorporate sufficient redundancy to mitigate single failure trip operation. In addition, the PMS includes all the equipment necessary to monitor the plant functions during and following any design basis accident.

The main PMS system functions are:

- Acquire and analyse sensor inputs required for reactor trip and ESF actuation calculations
- Perform computation and logic operations on variables based on acquired inputs

- Perform coincidence logic voting for reactor trip
- Initiate a reactor trip to the RTCBs
- Provide ESF actuation commands to the Class 1 safety components.
- Permit manual trip or bypass of each individual automatic safety function
- Provide data to external systems
- Provide isolation for control functions requiring input from sensors, which are also required for protection functions
- Provide displays on the MCR PDSP

19.4.1.4 Protection and Safety Monitoring Safety Function

The PMS performs the Category A reactor trip functions, the Category A ESF actuation functions, the Category B QDPS functions, and Category C Sequence of Events (SOE) functions. The Category B QDPS is executed on Class 1 equipment. The Category C SOE functions are functionally and electrically isolated from the rest of the PMS. For a more detailed description of the PMS function categorisation and equipment classification, see Section 6.1 of Reference19.28.

The PMS monitors key plant parameters and automatically initiates various protective functions to prevent violation of any of the three barriers, or if violation of a barrier cannot be prevented, to maintain the integrity of the remaining barriers. The system performs its functions by actuating a variety of equipment and by monitoring the plant process using a variety of sensors and operations performing calculations, comparisons, and logic based on those sensor inputs.

The PMS generates an automatic reactor trip for the following conditions and therefore are Category A functions. All of these functions two-out-of-four coincidence functions.

1. High Source Range High Neutron Flux
2. High Intermediate Range High Neutron Flux
3. Power Range High Neutron Flux (Low Setpoint)
4. Power Range High Neutron Flux Trip (High Setpoint)
5. Power Range High Positive Flux Rate
6. Over-temperature ΔT
7. Overpower ΔT
8. Low Pressuriser Pressure
9. Low Reactor Coolant Flow
10. Reactor Coolant Pump Underspeed
11. Reactor Coolant Pump Bearing Water Temperature
12. High Pressuriser Pressure
13. High Pressuriser Water Level
14. Low Water Level in any Steam Generator
15. High Steam Generator Water Level in Any Steam Generator
16. Automatic Depressurization Systems Actuation
17. Core Makeup Tank Actuation
18. Safeguards Actuation
19. Manual Reactor Trip
20. PRHR Actuation

The PMS senses accident situations and initiates ESF functions. The occurrence of a limiting fault, such as a loss of coolant accident or a secondary system break, requires a reactor trip plus actuation of one or more of the ESF functions. This combination of events prevents or mitigates damage to the core and reactor coolant system components and provides containment integrity.

The PMS is actuated when system setpoints are reached for selected plant parameters. The selected combination of process parameter setpoint violations is indicative of primary or secondary system boundary challenges. Once the required logic combination is generated, the PMS equipment sends the signals to actuate the appropriate ESF components.

The following is a list of the ESF system-level actuations initiated by the PMS and these functions are Category A functions:

1. Safeguards Actuation
2. Containment Isolation
3. In-Containment Refueling Water Storage Tank Injection
4. Core Makeup Tank Injection
5. Automatic Depressurization System Actuation (Stages 1-4)
6. Main Feedwater Isolation
7. Reactor Coolant Pump Trip
8. Passive Residual Heat Removal Actuation
9. Turbine Trip
10. Containment Recirculation
11. Steam Line Isolation
12. Steam Generator Blowdown System Isolation
13. Passive Containment Cooling Actuation
14. Startup Feedwater Isolation
15. Boron Dilution Block
16. Chemical and Volume Control System (CVS) Isolation
17. Steam Dump Control
18. Main Control Room Isolation
19. Auxiliary Spray and Purification Line Isolation
20. Containment Air Filtration Isolation
21. Refueling Cavity Isolation
22. CVS Letdown Isolation
23. Pressuriser Heater Block
24. Steam Generator Relief Isolation
25. Normal Residual Heat Removal Containment Isolation
26. Demineralized Water Transfer and Storage System Isolation
27. Reactor Vessel Head Vent Valve Control

The PMS provides signal conditioning, communications, and display functions for post-accident monitoring. The portion of the PMS that is dedicated to providing the post-accident function is referred to as the QDPS. The QDPS calculates post-accident variables for the safety displays in the control room.

The QDPS performs the following functions:

1. Support display of key post-accident variables so that the operator can monitor the effectiveness of the following systems:

    a. RCS
    b. Containment
    c. PRHR
    d. Related systems (Steam Generator (SG), CMT, Radiation, Spent Fuel Pool)

2. Support display of Critical Safety Functions:

    a. Subcriticality
    b. Core Cooling
    c. Heat Sink
    d. Integrity
    e. Containment
    f. Inventory

19.4.1.5 Protection and Safety Monitoring System Architecture

A detailed description of the PMS architecture can be found in Section 3.4 of Reference 19.28. The following subsections provide an overview of the PMS architecture.

19.4.1.5.1 Divisional Architecture

A description of the single-division architecture follows and is shown in Figure 19-3. An overview of the four-division architecture is shown in Figure 19-2.

Each of the divisions of the PMS incorporates the following subsystems:

- NIS, which provides the interface to the ex-core nuclear instrumentation.
- BPL unit that facilitates data acquisition and generates the partial trip signals that are passed to the local coincidental logic of all the divisions.
- Local coincidental logic, which uses two-out-of-four voting logic for generation of both reactor trip and ESF actuation.
- ILP for ESF component fan out and actuation.
- Integrated communications processor for inter-divisional and external interfaces.
- Interface and test processor for testing and diagnostics.
- MTP for maintenance, testing, and calibration, and for communication to the PLS/DDS.
- QDPS, divisions B and C only for support of post-accident safety display.
- Safety Displays in the MCR for system status, post-accident information, control of selected system components, and changing nuclear instrumentation calorimetric constants.

19.4.1.5.2 Platform and Components

The PMS uses two major platforms: the Common Qualified (Q) Platform and the CIM.

1. Common (Q) Platform

The Common Q Platform is comprised of commercially developed components that undergo qualification for use in Class 1 systems. It consists of the following major components that are used in the PMS:

- AC160 with PM646A Processor Module.
- Input and Output Cards
- Power Supply
- Flat Panel Display System.
- AF100 Communication
- High Speed Link Communication

2. Component Interface Module

The CIMs receive component control signals from the PMS and the PLS and arbitrate the signals to the plant component. Signal arbitration is between the PLS and the PMS with the PMS having priority over PLS. The CIM is a field-programmable gate array based Class 1 module for safety critical component control.

Additional features provided by the CIM include the following:

- Continuous controller-to-CIM testing for the system command outputs.
- Continuous CIM diagnostics with local fault indications allow problems to be quickly identified.
- Surge-withstand capability qualified to industry standards.
- Continuous CIM monitoring of the external field relay voltage.
- Ability to disable control system inputs (alarmed) for testing.
- Local manual output relay control (alarmed) for testing.
- Hot swappable; repairs can be accomplished by plug-in module replacement with power on, without disturbing cabling.
- Circuit voltage monitor ensures component control power availability and circuit continuity on a continuous basis. Output relay contact is tested when device is actuated.
- Wetting voltage on field inputs is continuously monitored.

19.4.1.6 Protection and Safety Monitoring System Qualification

The PMS equipment qualification program is a type test that demonstrates the continued functionality of the PMS for design basis events such as earthquake, environmental and EMC events.

Although the Common Q Platform had undergone a generic equipment qualification

program, the AP1000 has unique requirements for equipment qualification as described in the AP1000 Equipment Qualification Methodology Document (Reference 19.8). The EQ methodology is based on IEEE standards. The following references demonstrate the equivalence of these IEEE standards to the IEC standards:

- EQ-EV-283, "Electromagnetic Compatibility Standards Evaluation," Reference 19.33
- EQ-EV-284, "Comparison of IEC Standard 60780-1998 to IEEE Standard 323-1974," Reference 19.51
- EQ-EV-285, "Comparison of IEC Standard 60980-1989 to IEEE Standard 344-1987," Reference 19.52

Details of the justification for the type test for hardware and software Configuration of the PMS can be found in subsection 6.1.8.4 of the PMS BSC Reference 19.28.

The results of the PMS EQ tests are summarised in Reference 19.36.

19.4.2 Diverse Actuation System

19.4.2.1 Diverse Actuation System Definition

The DAS design utilises solid-state hardware that is based on the Westinghouse 7300 series platform. The DAS is a Class 2 system that provides diverse actuation of reactor trip and ESF functions with one-out-of-two taken twice or two-out-of-three logic as specified in the safety case and examination, maintenance, inspection, and testing requirements.

19.4.2.2 Diverse Actuation System Design Basis

The DAS functions contribute to the delivery of Category A safety functions. Since the PMS provides the principal means and DAS provides only a supplemental means, the system is Class 2. The DAS functions are performed using solid-state logic, which has been used in Class 1systems in the past.

The following points are included in this design approach section to provide evidence of the design philosophy:

- Separation and Segregation
- Reliability Requirements
- Manual Trip
- Power
- Diversity
- Independence
- Testing
- Operator Interface

19.4.2.2.1 Separation and Segregation

The DAS provides indicators and manual control capability in the auxiliary building that are physically separated from and independent of the DAS equipment located in the MCR. The purpose of this remote DAS control location is to provide the capability to actuate the DAS functions for a beyond design basis event in which the MCR and the RSR are unavailable.

19.4.2.2.2 Reliability Requirements

To defend against postulated CCF of the PMS, the DAS automatic and manual functions do not interface with other controls for given components.

The DAS design has a maximum unavailability of 1E-2 demands/failure for each of the automatic and manual safety functions. This value includes the unavailability for test and maintenance. The unavailability requirement does not account for failures from sensors or transmitters, output signal conversion devices (such as electromechanical relays and solenoid valves), electrical power sources, or the heating, ventilation, and air conditioning system.

The DAS includes design features that prevent spurious and inadvertent actions. For example the probability of spurious actuation is minimised through the voting logic, such as two-out-of-three, and two-switch operation for manual actuation functions.

19.4.2.2.3 Manual Actuation

The DAS manual functions are listed in Table 19-2.

The DAS provides the capability for manual initiation of reactor trip and ESF functions from a DAS control panel that is located in the MCR. These actions are accomplished by actuating a master enable handswitch to provide DC power to the DAS control panel and then actuating two handswitches on the DAS control panel. The two handswitches are wired so that an actuation signal from both handswitches is required.

The DAS manual actuation functions are implemented by connecting the controls on the DAS control panel in the MCR and the controls on the remote DAS control panel in the DAS cabinets located in the auxiliary building to the actuated field devices, independent of the PMS logic. In addition, the DAS manual actuation relays are separate from and independent of the DAS voter actuation logic and associated automatic actuation relays. (The coils of the DAS manual actuation relays are wired independently from the DAS voter actuation logic and the coils of the associated DAS automatic actuation relays. The contacts of the manual actuation relays and the automatic actuation relays are commonly wired to the actuated field devices.)

The manual controls on the remote DAS control panel are provided in the event of a large catastrophic casualty to the clean portion of the auxiliary building on the nuclear island, which could significantly debilitate the C&I capabilities of the AP1000 plant. The four divisions (A, B, C, and D) of PMS and IDS, all electrical containment penetrations, all methods of PLS instrumentation and control, the MCR, and the remote shutdown workstation are all concentrated in the same region of the auxiliary building. A large, multilevel fire could render all the aforementioned systems/locations unusable for a significant amount of time. The remote DAS control panel provides a means for limited indication and plant control, primarily for the purposes of long-term decay heat removal and plant stability, that is physically separated from the clean auxiliary building. The remote DAS manual controls are a subset of the manual controls located on the DAS control panel.

19.4.2.2.4 Power

The DAS includes two fully redundant, 100% capacity, power supply and distribution subsystems (internal to the DAS cabinets). Each of these subsystems receives a separate and independent power feed from the EDS (see Chapter 18 for a full description of the EDS).

In the event one of the EDS power feeds is lost, the remaining EDS power feed and the associated DAS power supply and distribution subsystem are capable of providing power to the entire DAS. In the event both EDS power feeds are lost, each DAS power supply and distribution subsystem includes a battery-backed uninterruptible power supply that is capable of providing DAS power for up to four hours.

19.4.2.2.5 Diversity

Diversity is addressed by the provision of the DAS for frequent faults as shown in the Fault Schedule of Chapter 8. The DAS is a completely separate system for actuation of Class 1 reactor protection systems. The employment of a completely separate system for reactor protection has been implemented to address the issue of DiD.

19.4.2.2.6 Independence

The DAS is an independent system and does not share any of the sensors, operational platforms, or wiring with the PMS or PLS.

The DAS sensors are shown in Table 19-3. These sensors are used solely to generate inputs to the DAS.

The DAS uses exclusively solid-state hardware. Therefore, the platform is independent of the PMS and PLS.

The DAS has its own independent wiring from the sensor to the platform (via Processor Cabinets PC1 and PC2) and to the actuated field equipment (via the Squib Valve Controller Cabinet).

19.4.2.2.7 Testing

The PSA model assumes that the DAS functionality is tested at power every 92 days, and that capability is provided for testing the DAS instrument channels and testing the DAS voter actuation logic and associated automatic actuation relays. The PSA model also assumes that the DAS is returned to service within 14 days if it is out of service.

Each DAS instrument channel includes manual switches that provide the capability to test the channel (and calibrate, if necessary) by simulating the process input value. During this test, the output of the channel comparators are bypassed so that an actuation signal is not generated, and the likelihood of a spurious actuation is minimised. In addition, during this test, the redundant instrument channels remain operable to support actuation of the DAS functions.

The voter actuation logic and associated automatic actuation relays are tested by bypassing the output of the relays that are associated with the voter to be tested, thereby minimising the likelihood of spurious actuation. All voting logic combinations are then tested using simulated test signals at the output of the instrument channel comparators. The status of the associated automatic actuation relays is monitored locally to ensure correct operation of the voting logic and the relays. During this test, the redundant voter and the associated automatic actuation relays remain operable to support actuation of the DAS functions.

19.4.2.2.8 Operator Interfaces

The DAS HSI is located in the MCR and in the auxiliary building.

Alarms and annunciators are used to alert the operator of excursions beyond the designed safety parameters.

19.4.2.3 Diverse Actuation System Functions

The DAS provides a diverse backup to the PMS to reduce the probability of excessive offsite doses that may occur from the unlikely coincidence of frequent faults and postulated CCFs in the protection and control systems.

The DAS provides automatic reactor trip and automatic actuation of specific ESF functions. It also supports manual reactor trip and actuation of specific ESF functions.

The DAS has its own set of sensors and signal processing equipment, which is located in Processor Cabinets PC1 and PC2 and the Squib Valve Controller Cabinet. Control interface, with indicators and manual controls, is provided on the MCR DAS control panel and on the DAS cabinet remote DAS control panel.

The DAS cabinets are segregated from the PMS cabinets, which are located in Class 1 instrument rooms. This segregation minimises the potential for location-related influences such as radiation, EMC, radio frequency interference, missiles, water spray, fire, and flooding to affect both systems.

19.4.2.4 Diverse Actuation System Safety Functions

The DAS provides a backup to the PMS and provides a diverse means of actuating the Class 1 protective functions (i.e., reactor trip and ESF).

The DAS safety functions are listed in subsection 19.3.2.2.

The DAS reactor trip function opens the rod drive motor generator (MG) set field breakers, de-energising the MG set outputs and the control rod drive mechanism (CRDM) coils. The control rods then drop into the reactor by gravity.

19.4.2.5 Diverse Actuation System Architecture

A detailed description of the DAS architecture is presented in Section 3.4 of the DAS BSC (Reference 19.29). The following subsections provide an overview of the DAS architecture.

19.4.2.6 System Architecture

An overview of the DAS architecture is shown in Figure 19-1. The DAS consists of the following three cabinets and a control panel interface (in the MCR):

- DAS-JD-001 Processor Cabinet PC1
- DAS-JD-002 Processor Cabinet PC2
- DAS-JD-003 Squib Valve Controller Cabinet
- OCS-JC-020 MCR DAS Control Panel

DAS Processor Cabinets PC1 and PC2 process the sensor input signals, generate the associated comparator outputs, perform the voter logic (one-out-of-two taken twice or two-out-of-three), and pass the voter outputs to the automatic actuation relays in the Squib Valve Controller Cabinet. Processor Cabinets PC1 and PC2 also include test switches and indications (that support testing of the 7300 process instrument channels, the voters, and automatic actuation relays), local indicators for each monitored process variable, and manual system-level actuation handswitches for certain functions.The DAS Squib Valve Controller Cabinet includes automatic and manual actuation relays. The automatic actuation relays receive signals from the voters in Processor Cabinets PC1 and PC2. The manual actuation relays receive signals from the manual actuation handswitches in Processor Cabinets PC1 and PC2 and the manual actuation handswitches in the MCR. For non-squib valve field equipment, the automatic and manual actuation relays provide individual actuation signals to the components. For squib valves, the manual actuation relays provide ARM and ACTUATE signals to the squib valve controllers that are also mounted in the cabinet. These controllers, in turn, actuate the squib valves. During normal plant operation, the compartment in which the squib valve controllers are mounted is void of all power as a defensive measure to prevent spurious actuation. The DAS Squib Valve Controller Cabinet also includes the bypass relays that are used to prevent actuation of plant equipment during testing.

The DAS Control Panel is located in the MCR. It contains indicators for each monitored process variable, and manual system-level actuation handswitches for the DAS safety functions.

19.4.2.7 Platform and Components

The DAS is implemented using the Westinghouse 7300 series platform. This platform consists of input signal processing (printed circuit) boards, comparator boards, output boards (for the monitored process variable indicators), test boards, and power supplies.

19.4.2.8 Diverse Actuation System Qualification

Although the 7300 Platform had undergone a generic equipment qualification program, the AP1000 has unique requirements for equipment qualification as described in Section 5.8 of the PCSR. In that section of the PCSR the standards to be met for equipment qualification are stated. The AP1000 Equipment Qualification Methodology Document (Reference 19.8) describes the implementation of the EQ program in compliance to the PCSR.

19.4.3 Plant Control System

19.4.3.1 Plant Control System Definition

The PLS controls the nuclear process, conversion of nuclear energy into heat energy, and the transport of the heat energy from the nuclear reactor to the main steam turbine. The PLS provides automatic regulation of reactor and other key system parameters in response to changes in operating limits (load changes) for required normal (including startup, ascent to power, powered operation, shutdown, and refuelling) and off-normal conditions.

The PLS also acts to maximize the plant transient performance and margins to plant safety limits. Additionally, the PLS provides the capability for manual control of plant systems and equipment. Redundant controllers are used to increase single-failure tolerance, where necessary.

19.4.3.2 Plant Control System Design Basis

The following factors are considered in this design approach section to provide evidence of the design philosophy:

- Independence from Instrumentation and Control Network
- Separation and Segregation
- Maintenance, Diagnostics and Testing
- Power

19.4.3.2.1 Independence from Instrumentation and Control Network

The C&I network is not qualified to Class 2 and cannot be claimed for Category B safety functions. Therefore, all PLS Category B functions must operate correctly without the C&I network (Reference 19.13, Section 12.2).

19.4.3.2.2 Separation and Segregation

In order to eliminate single failures of PLS components the following hardware redundancy has been incorporated into the PLS design:

- Redundant controllers – Category B and Category C functions will be implemented on redundant controllers that do not depend upon each other for operation
- Redundant network connections to each redundant controller
- Redundant power supplies in each PLS cabinet
- Redundant I/O modules (where necessary)
- Two or more Category B function controllers will not share the same input signal.

Class 2 portions and control element of the PLS, which are separated by fire zones or power sources, will be implemented on separate controllers (Reference 19.13, Section 12.2). Fire zones, in many cases, will dictate how plant-based items are physically segregated. This specification requires that the physical separation of any controlling equipment is segregated along the same lines.

Cable separation and segregation requirements are defined in Reference 19.7.

19.4.3.2.3 Maintenance, Diagnostics, and Testing

The requirements for maintenance, diagnostics, and testing are specified in Reference 19.13, Section 3.5. One of the key elements of these requirements is the inclusion of modular design and built-in diagnostics that assist personnel in routine testing and maintenance, fault finding, and component replacement.

Requirement specifications are also in place to facilitate maintenance, diagnostics, and testing whilst the plant is online and without compromising plant control functionality (except those elements that are within the nuclear island that are not accessible while online). This includes the removal of individual inputs and outputs without disturbing field cables.

19.4.3.2.4 Power

Factors concerning the reliability of the power supply to the PLS will not compromise the overall ability of the PLS to deliver its safety duty.

The PLS will be fed from the EDS, as described and substantiated in Chapter 18. The supply will be subject to the requirements of EMC (subsection 19.4.3.6).

The PLS system design will be tolerant to power loss through the following design provisions:

- On loss of power, all outputs are set or driven to a safe state (this may be by keeping the pertaining setting).
- On resumption of power, the system will be set to manual control.

19.4.3.3 Plant Control System Functions

The PLS controls the majority of the AP1000 plant duty control elements through either automatic control or manual operator control. It also has monitoring functions. The following parameters are controlled by the PLS automatic controls:

- Nuclear steam supply, by controlling the reactivity, reactor pressure, coolant and turbine steam demand, and steam and coolant inventory
- Control rod movements, as required by the reactivity control (not including the shutdown banks)
- Control and protection of the turbine
- Various miscellaneous control functions required for subsidiary activities and day-to-day running of the plant

The following are the PLS measurement and monitoring functions:

- Rod position, including facility for rod drop time testing
- Post-accident monitoring of non-Class 1 plant

These functions are described in more detail in the PLS BSC (Reference 19.30)

19.4.3.4 Plant Control System Safety Function

The PLS is composed of individual controllers with local and remote I/O. Each controller communicates point data via the plant C&I network. Details of the functionality are included in PLS BSC (Reference 19.30). The PLS performs the following functions:

- turbine control and protection
- fluid systems control
- diesel generator control and load sequencing
- ventilation systems control
- electrical systems control
- balance of plant system control

- rod position indications
- nuclear steam supply system (NSSS) control

NSSS Control includes the following:

- rod control
- reactor power
- pressuriser pressure
- pressuriser level
- steam generator level
- reactor coolant system inventory
- turbine steam demand control
- T_{avg}
- steam pressure

19.4.3.5 Plant Control System Architecture

A detailed description of the PLS Architecture can be found in the PLS BSC (Reference 19.30). The following subsections provide an overview of the PLS architecture.

The PLS is divided into cells, each comprised of a multiple of cabinets. Cells are selected according to functional groupings to minimize the number of signal interfaces that cross between cells. Cell definitions also support design standardization by collecting site specific applications into one cell. This also enables the through-life design, implementation, manufacturing, and test of the system.

Architectural features for critical functions are:

- all controllers used within the PLS have redundant controllers, cabinet power supplies, network connections, and power feeds. I/O signal redundancy is supported, and is applied as necessary to meet single failure criteria
- the PLS controllers attach to the plant C&I network (the network is part of the DDS) which is based on redundant switches and data paths. Automatic reconfiguration occurs quickly (typically less than one second) following detected switch or media failure
- each controller processor is dual attached to the network so that loss of a network interface will not disrupt operation or require failover to the backup processor
- the controllers in the NSSS cell are distinctly grouped into segments, each responsible for the control of a major plant function (e.g. reactor power, RCS inventory, etc.). This ensures that total failure of a controller will not lead to a plant accident that is more severe than those analysed as design basis events
- critical automatic control functions (Category B) are designed to be independent of plant C&I network signals. Loss of communications on the network will not cause spurious operation of these control functions. This entails hardwired inputs and outputs for all principle signals of the control function. If communication is required between controllers, this is also done by hardwired connections. (Note: network communications may be used for non-critical sub-functions such as manual operator control of the outputs)

19.4.3.6 Plant Control System Qualification

Although the Ovation Platform had undergone a generic equipment qualification program,

the AP1000 has unique requirements for equipment qualification as described in Section 5.8 of the PCSR. In that section of the PCSR the standards to be met for equipment qualification are stated. The AP1000 Equipment Qualification Methodology Document (Reference 19.8) describes the implementation of the EQ program in compliance to the PCSR.

19.4.4 Data Display and Processing System

19.4.4.1 Data Display and Processing System Definition

The DDS is a Class 3 system that provides the plant monitoring and control interface for the duty system and a subset of the SIS. This interface requires the processing, display, and archiving of data gathered from the plant. It contains the equipment necessary to accomplish this purpose, including the plant C&I network, servers, and the operator and engineer workstations.

The DDS provides the main real-time data network (the plant C&I network) for all of the plant data. The data is collected by other systems and distributed through the network by the DDS. The DDS displays the information to the operators through operator displays; this also includes data processing functions. The DDS includes the APS, which alerts the operators when preset parameters are exceeded. The DDS includes the CPS, which allows the operators to access all plant procedures at any operator workstation in the MCR, including those for normal operation and emergency situations. It includes nuclear application programmes (NAPs), logs and archives plant data through the process historian, provides gateways to an interface with balance of plant (BOP) monitoring and control equipment, and provides an interface with external systems.

The DDS consists of operator workstations, engineer workstations, data link server, plant C&I network, process historian/report server, communication network gateway, and wall panel information system .

The DDS resources include the following:

- Plant C&I network to provide communication with the other plant C&I systems
- Operator stations for the human-system interfaces
- Process historians for historical data collection, archiving and report building
- Application servers for the APS, CPS, and BEACON
- Application servers and nuclear application programmes
- Datalink servers for interfacing to external plant C&I systems
- Database servers to provide database management functions for the plant C&I systems
- Engineer stations and system support workstations to provide system security, system maintenance, and time management functions for the plant C&I systems
- Enterprise data servers for external communications to the LAN

Figure 19-5 shows a schematic of the DDS resources and their interfaces to the other functional systems.

The DDS provides the main real-time data network (plant C&I network) for all of the plant data, which includes the following:

- Data processing
- Supporting APS
- Supporting CPS
- Supporting NAPs
- Data collection, archiving, and report building
- Providing gateways to interface with BOP monitoring and control equipment
- Providing an interface with external systems

19.4.4.2 Data Display and Processing System Function

The DDS nuclear application programmes provide plant personnel with information to assure safe plant operations and effective use of the plant equipment. These programmes execute on a redundant application server and monitor AP1000 plant parameters and processes.

The nuclear applications receive their input data from the plant C&I network and output their results onto the plant C&I network. The calculated data is in a form that can be used in plant alarms, displays, trending functions, and historical storage and retrieval.

A modular approach for implementing software applications is used for the development of the application programmes in the DDS. Applications are specified and implemented using basic FBs and sub-applications, or any combination of these three functional units. The use of FBs provides the ability to comprehensively and consistently apply the functional requirements for DDS applications and interfaces to all application programmes using the FBs.

When application programmes execute on a redundant pair of application servers, one application server operates in the primary mode and the other in the backup mode. The application programme software is installed and executes on both application servers. Each application server executes the software independently; however, only the application server operating in the primary mode broadcasts the calculated results to the plant C&I network. Should the primary application server fail, the backup application server assumes the role of primary application server. This redundancy scheme is inherent in the application server operating environment (Reference 19.20, Section 3).

The scope of the DDS application programmes can be subdivided in accordance with the general objectives of an information system, which are to provide plant personnel with information to ensure safe plant operations and effective use of the plant equipment. The following groups of applications are provided to meet these objectives:

- Plant safety:
  - Technical specification monitoring (TSM)
  - Safety functions display support
  - Computerised operation support
- Effective use of equipment:
  - Plant performance assessment

Two additional groups of applications provide support for the above groups of applications:

- Application support functions
- Transform calculations and signal processing

The TSM group of applications is intended to provide information for effective monitoring of DiD functions. The first barrier, which provides DiD, is related to the plant normal operations and translated to monitoring of plant parameters and equipment. The goal is achieved in accordance with plant Technical Specifications. The operator monitors the following parameters:

- Limiting conditions for operation (LCO) entries
- Required actions, if LCOs are violated
- Timing requirements for completion of the required actions
- Surveillance requirements violation, which contributes to violation of the LCO (Reference 19.20, Section 3.1)

The computerised operator support group of applications is intended to support miscellaneous processes required for execution of plant normal operations associated with the plant Technical Specifications and normal operating procedures.

The safety functions display group of applications perform calculations to support safety parameter displays, the display of critical safety function data, and CPS functions (Reference 19.20, Section 3.3).

The plant performance assessment group of applications is intended to provide accurate data related to plant thermal output and effectiveness of the plant systems involved in the plant thermal cycle.

The application support function group of applications support the applications identified in Table 9-4.

The transform calculations and signal processing group of applications perform the following basic functions to support other applications:

- Correction of flow signals
- Compensation of level signals
- Calculation of rates of change
- Calculation of averages of redundant sensors
- Calculation of averages of a signal over time

The application programme software will be capable of executing in either an application server operating environment within the plant C&I system or in a simulator environment without modification.

The application programme software can run in the simulator environment without modification. A base application server configurable parameter may be set to enable the simulator interface when the software is implemented in the simulator environment. This is to ensure that when the software is run in the application environment, the simulator interface cannot be run. If the simulator interface functions when the application programme is installed in an application server, the C&I system could cause erroneous results to be

provided to those using the application programme results (Reference 19.20, subsection 2.1.4.2).

The following are the modes of operation:

- Normal operation
- Initialise
- Update configuration
- Restart with primary application server operating

19.4.4.3 Data Display and Processing System Architecture

19.4.4.3.1 Plant Control and Instrumentation Network

The plant C&I network is a real-time redundant network used to interconnect the controllers, workstations, and communication gateways. The network distributes the plant data that are collected by other systems and is the primary communication network for the entire plant. The plant C&I network provides two-way communication between the distributed controllers, and supports both periodic and aperiodic data transfers of signals and data. The plant real-time data network also provides secure, unidirectional data transfer from the plant real-time network to the plant communication / business network.

The Ovation redundant high-speed network uses Fast Ethernet standards to send input and output data to all DDS workstations and PLS controllers connected to the network.

The plant C&I network is redundant and network segmentation is configured to consider potential network failures and facilitate the various plant commissioning phases (Reference 19.13, Section 8.5).

The EDS electrical power distribution is designed with two load groups to support redundant Class 2 and general equipment. Power connections are critical to the reliable operation of the plant C&I network and to network-attached devices. The load groups are aligned with redundant plant components, and the controls for this equipment should be aligned to the supporting load group. The redundant components of the plant C&I network shall each be powered from separate EDS power sources.

The plant C&I network shall have software tools to configure, modify, and monitor network devices and attachments, and shall provide features to permit the detection and identification of faulty network devices and network attachments.

For analogue input and output values, the engineering unit high- and low-range limits, expressed in engineering units, are used to range-check each analogue calculated or external input value. The PMS shall have quality information for data values it transmits to the Advant to Ovation interface gateway, consistent with Reference 19.19. The plant C&I network data has both signal quality information that is transmitted along with the data, and signal identification information that is associated with the data.

The Ovation distributed control system shall provide the ability to interface to the package local control system through discrete I/O devices and serial data links.

19.4.4.3.2 Application Server

The application server provides general purpose processing functionality to support the needs of nuclear applications processing. The application server provides the platform for the nuclear applications, the APS, the CPS, BEACON, and data link servers. These servers can be arranged in an active/standby configuration or a non-redundant configuration. The application server has an application builder tool, which is a graphical tool for building combination logic.

19.4.4.3.3 Process Historian

The basic role of the process historian is to perform the collection of process values and messages generated by the workstations and controllers into a data-file-based management system. The process historian will execute the collection, summary processing, archiving, and retrieval of data from across the system.

19.4.4.3.4 Reduced Functionality Operator Work Stations

Reduced functionality workstations provide the ability to navigate display pages and to review plant data. This configuration is necessary to limit the ability to control the plant to the operators while allowing the plant status to be reviewed by other personnel (Reference 19.13, Section 8.9).

The senior reactor operator's workstation will have the capability for the soft controls to be normally off, with the capability to activate them.

The DDS will provide workstations with no control capability in plant areas where the only need is to view the plant processes and equipment status.

The technical support centre workstations, and the operations support centre workstation, will have displays consistent with MCR displays but will have no control capability.

Local control operator workstations will only have controls for the plant systems associated with that workstation.

19.4.4.3.5 Computerised Operating Procedures

The CPS is an online system that assists the operational staff in the execution of plant procedures. The CPS may be used for normal, abnormal, and emergency operating procedures. The system guides the operator step by step through the procedures by monitoring the appropriate plant data, processing the data, identifying the recommended course of action, and providing necessary parallel information that allows the operator to assess other plant conditions that may require attention. Computerised plant procedures can be accessed at operator workstations in the MCR (Reference 19.13, Section 8.10).

19.4.4.3.6 Data Link Servers

Data link servers allow the network to communicate with components that do not support Ovation highway interfaces. Data links can provide two-way communication and will comply with cyber security considerations.

19.4.4.4 Data Display and Processing System Qualification

The AP1000 has unique requirements for equipment qualification as described in Section 5.8 of the PCSR. In that section of the PCSR the standards to be met for equipment qualification are stated. The AP1000 Equipment Qualification Methodology Document (Reference 19.8) describes the implementation of the EQ program in compliance to the PCSR.

19.4.5 Special Monitoring System

19.4.5.1 Special Monitoring System Definition

The SMS is a Class 3 system that processes data from specialised sensors. It consists of specialised subsystems that interface with the C&I architecture to provide diagnostic and long-term monitoring functions. The monitoring functions are:

- The DMIMS-DX
- The vibration integrity monitoring system (VIMS), which includes the RCPVM system, the CRDM fan vibration monitoring system (CFVMS), and the feedwater vibration monitoring system (FWVMS)

The SMS uses internal data networks that interface with the C&I networks using dedicated data links.

19.4.5.2 Special Monitoring System Function

19.4.5.2.1 Digital Metal Impact Monitoring System

The DMIMS-DX provides for the detection of the presence of metallic debris in the RCS when the debris impacts against the internal parts of the RCS.

The DMIMS-DX comprises digital circuit boards, controls, indicators, power supplies, and remotely located sensors and related signal processing devices. A minimum of two sensors are located at each natural collection region, connected to separate instrumentation channels, to maintain the impact monitoring function if a sensor fails in service.

The DMIMS-DX uses two methods of detection: automatic data analysis and audio monitoring. For automatic data analysis the system performs impact detection and alarm generation and records the signal waveforms and frequency spectra whenever an impact is detected (Reference 19.13, subsection 10.2.3). Audio monitoring is valuable because the impact signals are in the audio frequency range and knowledgeable listening can identify additional signal characteristics.

The DMIMS-DX provides sensor data for display in the MCR or a printed output for analysis (Reference 19.21, Table A-1).

19.4.5.2.2 Vibration Integrity Monitoring System

The VIMS is a continuous monitoring system that provides information to assist in the evaluation of the performance of the RCPs, CRDM fans, and feedwater pumps.

The RCPVM system uses vibration sensors on each RCP and one phase reference sensor to monitor pump speed and shaft position. At the cabinet, a local display allows for operator

interaction. The instrumentation rack communicates with the DDS to provide process data and alarms for MCR display.

The CFVMS receives signals from vibration sensors on each of the fans. The instrumentation rack communicates with the DDS to provide process data and alarms for the MCR display. The CFVMS will provide a vibration warning alarm for each CRDM fan.

The FWVMS receives signals from vibration sensors on each of the feedwater pump packages, each of which consists of a feedwater booster pump, main feedwater pump, gearbox, and motor.

Data and alarms from the FWVMS are provided to the operator through the Modbus™ connection to the DDS.

19.4.6 In-Core Instrumentation System

19.4.6.1 In-Core Instrumentation System Definition

The primary function of the IIS is to provide a continuous 3-D measured power distribution of the reactor core. The measured power distribution is used to confirm margin to thermal limits as per LCO 3.2.5 and is used to periodically calibrate PMS neutron detectors. A secondary function of the IIS is to provide the PMS with the thermocouple signals necessary for the post-accident inadequate core cooling monitor. The IIS assemblies house both fixed in-core flux detectors and core-exit thermocouples.

19.4.6.2 In-Core Instrumentation System Function

The IIS is a Class 3 system. It has two functions: one is to provide a continuous 3-D measured power distribution of the reactor core; its secondary function is to supply the PMS with thermocouple temperature measurement signals for the post-accident inadequate cooling monitor, as well as to provide the DAS with dedicated indication of core temperature.

The in-core thermocouple signals used for the QDPS are Class 1. Therefore, the fixed in-core detector (FID) signals will be independent from the thermocouple signals for all credible failures of the Class 3 portion of the system.

The in-core instrument thimbles assemblies are inserted into the active core through the upper head and internals of the reactor vessel. During plant operation, the in-core instrument thimble assembly is positioned within the fuel assembly. Thimbles exit through the top of the reactor vessel head to the integrated head package. For each assembly, there is a separate cable for the core-exit thermocouple and the FIDs, which are combined at the reactor vessel head into one cable guide. The FID and core-exit thermocouple cables are then routed to different data conditioning and processing stations. The data are processed, and the results are available for display in the MCR. All power distribution calculations are carried out using the BEACON core monitoring system which resides on dedicated servers. Additional information on BEACON is provided in Reference 19.57.

The IIS cables will be grouped and routed to signal termination equipment in accordance with their associations with different systems. The system will incorporate two independent sets of IIS FID electronics including the cabinets, power supplies and multiplexed data output links, so that the requirements for single failure criteria are met and one failure does not disable the power distribution measurements.

Figure 19-6 shows the IIS system configuration.

19.4.7 Radiation Monitoring System

19.4.7.1 Radiation Monitoring System Definition

The RMS supports safe operation of the plant under normal conditions, and provides DiD capability during fault conditions. It provides signals for automatic actuation functions and information to the plant operating staff so that actions may be taken to protect the health and safety of the public and plant personnel.

- The RMS provides early indication of a system or equipment malfunction that could result in an excessive radiation dose to plant personnel or lead to plant damage.
- Radiation monitoring data, including alarm status, are provided to the AP1000 plant operators via the PLS (and in the case of Class 1 monitors, to the PMS).
- The safety channels are environmentally qualified and are powered from the IDS.

The functions of RMS include the following:

- Providing radioactivity monitoring of selected plant fluid (gaseous and liquid) process streams
- Providing radioactivity monitoring of plant liquid and gaseous effluents
- Providing plant airborne radioactivity monitoring
- Providing area radiation monitoring
- Providing alarms to warn plant personnel of unusual radiological conditions
- Providing alarms to warn of RMS equipment malfunctions
- Providing process effluent radiological data for the effluent measuring and reporting.

19.4.8 Instrumentation

Process instrumentation is used to measure plant status during normal and abnormal conditions. The instruments provide input to all C&I systems, and they will be classified in accordance with the function that is being provided, and will be qualified in accordance with Chapter 5. If smart instrumentation is proposed to be used, additional justification for the use of the smart instrument will be provided using the processes in Chapter 5.

19.5 Conclusions

This chapter has provided justification and substantiation of the overall C&I architecture, i.e. how the individual C&I systems are configured to provide the plant with sufficient DiD to meet the requirements of the safety case and the expectations for a modern NPP. This chapter has, therefore, provided a demonstration that the design of the C&I systems and their interfaces within the AP1000 reactor are fit-for-purpose and use technology and modes of operation that are commensurate with modern standards. Reference has been made in this chapter to the detailed descriptions and substantiation of the individual systems that are provided in, amongst other documents, the relevant BSC documents.

This chapter has also provided evidence that the design of the C&I architecture and systems ensures that the radiological risks to the public and workers are reduced to ALARP. This has been achieved by demonstrating that:

- the potential for control system faults to be initiated has been reduced as far as reasonably practicable and C&I protection consists principally of automated protection systems, i.e. the position of the C&I design in the safety hierarchy;

- RGP has been applied in the design and will be applied in detailed design, installation and operation. Where necessary, this is with respect to established codes and standards that are considered to represent RGP;

- safety functions have been substantiated and that required reliability requirements have been satisfied (or that there is a programme of work to complete the analysis as identified in the safety plans of system BSCs and the PCSR Chapter 19 IEC 61513 and SAP compliance documents); and

- suitable optioneering has been undertaken to underpin design and configuration selection.

Section 19.3 has described and justified the design of the overall C&I architecture. The Engineering Principles described in Chapter 5 were utilised in the design of the architecture and its individual systems. The architecture of the C&I was originally designed to recognised and reputable US NRC standards. Therefore, a benchmarking exercise has been undertaken to compare the design process with IEC 61513 (Reference 19.16), which is considered to represent RGP in the UK. Closure of the compensatory measures will demonstrated that the design of the architecture has followed a process that is aligned with IEC 61513 (Reference 19.16). Thus, a key ALARP test has been demonstrate that RGP has been utilised in the design of the architecture. It is recognised that at this GDA stage not all C&I systems have been designed, e.g. the fuel route control and protection systems. However, the C&I architecture is sufficiently mature to enable these systems to be developed during the licensing phase and feed into the overall configuration.

The development of the architecture of the C&I, as described in Section 19.3, has taken into account a number of key inputs. The design process has ensured that the architecture delivers an operable and maintainable NPP that shall offer secure and safe operations that minimise unavailability of the NPP due to breakdown, maintenance and functional testing. The architecture delivers a PLS that shall have operator oversight and ultimate operator control from the MCR. The PLS is described and substantiated in subsection 19.4.3.

The principles of DiD have been incorporated into the design of the C&I architecture. Together with the passive containment features of the AP1000 and ultimately, the emergency arrangements for severe accidents, the C&I architecture and individual systems ensure that the potential for core damage or large radiological releases is minimised, as far as reasonably practicable. Particular aspects of the C&I that support the provision of DiD include the provision of:

- A robust plant control system (the PLS) that will minimise the potential for control system errors in the first instance and hence minimise the demand on the safety measures;

- Independent, diverse and segregated systems (the PMS and DAS) that will respond to system failures and return the plant to a defined safe state without operator intervention, e.g. reactor trip and provision of cooling functions and provide feedback to the operator (the OCS and DSS);

- A system to ensure MCR habitability (the RMS) in the unlikely event of a severe accident and provision of reactor and environmental diagnostics to facilitate recovery operations;

- An alternative safe shutdown facility should the MCR become uninhabitable (the RSR).

In final conclusion, the C&I architecture and the individual systems utilise proven technology that includes a significant number of design improvements that enhance tolerance to failure and maximise reliability. The requirements of the safety case and the safety requirements of the relevant IEC standards that represent RGP in the UK have been delivered and evidence for this has been provided in the individual BSCs and their supporting references. As far as practicable, conformance with IEC standards that represent RGP in the UK has been achieved by final close out of the compensatory measures. There has been the consideration of options in the selection of technology platforms. In addition, by the use of FMEA and PSA, systems have been optimised to maximise their reliability. The C&I systems contribute to the overall DiD of the AP1000 plant and provide the necessary mixture of engineered protection systems (high in the safety hierarchy) and support functions to facilitate recovery from unlikely severe accidents. It is therefore concluded that due to:

- delivery of safety requirements;

- alignment of the design with RGP;

- use of option selection in the design process; and

- optimising the design to improve reliability (risk reduction),

the design of the C&I architecture and systems is ALARP and shall support the overall demonstration of ALARP for the AP1000 plant as a whole.

19.6 References

19.1. Westinghouse Report UKP-GW-GLR-116, Rev. 0, "United Kingdom AP1000 Plant C&I Requirements Management," November 2016.

19.2. ONR "Safety Assessment Principles for Nuclear Facilities," 2014 Edition, Revision 0.

19.3. Westinghouse Report APP-GW-GLR-071, Rev. 7, "AP1000 Protection and Safety Monitoring System Architecture Technical Report," August 2015.

19.4. Westinghouse Report UKP-GW-GL-044, Rev. 1, "AP1000 UK Safety Categorization and Classification Methodology," April 2010.

19.5. IEEE 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers, 1991.

19.6. IEC 61000, "Electromagnetic Compatibility (EMC) General – Immunity," International Electrotechnical Commission, 2004.

19.7. Westinghouse Document APP-EW21-E1-001, Rev. 3, "AP1000 Standard Raceway and Cable Separation and Segregation," July 2014.

19.8. Westinghouse Document APP-GW-G1-002, Rev. 4, "AP1000 Plant Equipment Qualification Methodology," September 2014.

19.9. Westinghouse Document WCAP-16096-P-A, Rev. 4, "Software Program Manual for Common Q Systems," August 2013.

19.10. Westinghouse Report 00000-ICE-3889, Rev. 16, "Coding Standards and Guidelines for Common Q Systems," December 2014.

19.11. IEEE 384-1992, "IEEE Standard Criteria for Independence of Class 1E Electrical Equipment and Circuits," Institute of Electrical and Electronics Engineers, 1992.

19.12. Westinghouse Document APP-PMS-J1-001, Rev. 12, "AP1000 Protection and Safety Monitoring System Functional Requirements," June 2016.

19.13. Westinghouse Document APP-GW-J4-001, Rev. 11, "AP1000 I&C System Design Specification," April 2014.

19.14. Westinghouse Document WCAP-16438-P, Rev. 6, "FMEA of AP1000 Protection and Safety Monitoring System," April 2014.

19.15. IEC 62340, "Nuclear Power Plants – Instrumentation and Control Systems Important to Safety – Requirements for Coping with Common Cause Failure (CCF)," International Electrotechnical Commission, 2007.

19.16. IEC 61513, "Nuclear power plants. Instrumentation and control important to safety. General requirements for systems," International Electrotechnical Commission, 2011.

19.17. Westinghouse Document APP-GW-GLR-104, Rev. 1, "AP1000 Cyber Security Implementation," June 2008.

19.18. Westinghouse Document APP-GW-J1R-004, Rev. 7, "AP1000 Instrument and Control Defense-in-Depth and Diversity Report," November 2015.

19.19. Westinghouse Document WNA-DB-00103-GEN, Rev. 0, "Standard Design Criteria Document for Data Quality and Redundant Sensor Algorithm Functions," April 2009.

19.20. Westinghouse Document APP-DDS-J4-031, Rev. 1, "AP1000 Data Display and Processing System Application Programs Requirements Specification," May 2013.

19.21. Westinghouse Document APP-GW-J1-010, Rev. 11, "AP1000 I&C System Requirements Specification," April 2014.

19.22. IEC 61226, "Nuclear Power Plants – Instrumentation and Control Important to Safety – Classification of Instrumentation and Control Functions," International Electrotechnical Commission, 2009.

19.23. IEC 60987, "Nuclear Power Plants – Instrumentation and Control Important to Safety – Hardware Design Requirements for Computer Based Systems," International Electrotechnical Commission, 2007.

19.24. IEC 60880, "Nuclear Power Plants – Instrumentation and Control Systems Important to Safety – Software Aspects for Computer-Based Systems Performing Category A Functions," International Electrotechnical Commission, 2006.

19.25. IEC 62138, "Nuclear Power Plants – Instrumentation and Control Important to Safety – Software Aspects for Computer-Based Systems Performing Category B or C Functions," International Electrotechnical Commission, 2004.

19.26. Westinghouse Document WNA-AN-00038-WAPP, Rev. 1, "AP1000 Protection and Monitoring System Reliability Analysis Plan," May 2011.

19.27. Westinghouse Report UKP-PMS-GLR-002, Rev. 2, "United Kingdom AP1000 Component Interface Module Safety Case Basis," November 2016.

19.28. Westinghouse Report UKP-PMS-GLR-001, Rev. 2, "United Kingdom AP1000 Protection and Safety Monitoring System Safety Case Basis," December 2016.

19.29. Westinghouse Report UKP-DAS-GLR-001, Rev. 2, "United Kingdom AP1000 Basis of Safety Case for the Diverse Actuation System," December 2016.

19.30. Westinghouse Report UKP-PLS-GLR-001, Rev. 1, "United Kingdom AP1000 Plant Control System (PLS) Basis of Safety Case," December 2016.

19.31. Westinghouse Report UKP-DDS-GLR-001, Rev. 1, "United Kingdom AP1000 Data Display and Processing System (DDS) Basis of Safety Case," December 2016.

19.32. Westinghouse Report UKP-GW-GLR-023, Rev. 2, "United Kingdom AP1000 Diversity Analysis of the Protection and Safety Monitoring System (PMS) and the Diverse Actuation System (DAS)," December 2016.

19.33. Westinghouse Document EQ-EV-283, Rev. 0, "Electromagnetic Compatibility Standards Evaluation," April 2016.

19.34. IAEA SSR-2/1, Rev 1, "Safety of Nuclear Power Plants: Design."

19.35. IAEA SSG-39, "Design of Instrumentation and Control Systems for Nuclear Power Plants."

19.36. Westinghouse Report APP-PMS-VBR-003, Rev. 5, "Equipment Qualification Summary Report for PMS Cabinets and NIS Auxiliary Panels for Use in the AP1000 Plant," March 2016.

19.37. Westinghouse Report UKP-GW-GL-112, Rev. 0, "ALARP Justification Guidance for GDA Close-Out Phase," August 2015.

19.38. WENRA RHWG Report, "Safety of new NPP designs," March 2013.

19.39. MDEP Common Position № DICWG-09, Version 0, "Safety Design Principles and Supporting Information for the Overall I&C Architecture," July 2015.

19.40. Common position of international nuclear regulators and authorised technical support organisations, "Licensing of safety critical software for nuclear reactors," 2015 Revision.

19.41. IEC 60709, "Nuclear Power Plants – instrumentation and control systems important to safety – separation," International Electrotechnical Commission, 2004.

19.42. IEC 60671, "Nuclear Power Plants – instrumentation and control systems important to safety – surveillance testing," International Electrotechnical Commission, 2007.

19.43. IEC 62566, "Nuclear Power Plants – I&C important to safety – Development of HDL-programmed integrated circuits for systems performing category A functions," International Electrotechnical Commission, 2012.

19.44. IEC 62671, "Nuclear Power Plants - I&C important to safety - Selection and use of industrial digital devices of limited functionality," International Electrotechnical Commission, 2013.

19.45. IEC 60964, "Nuclear Power Plants - Control rooms – Design," International Electrotechnical Commission, 2009.

19.46. IEC 60965, "Nuclear Power Plants - Control rooms - Supplementary control rooms for reactor shutdown without access to the main control room," International Electrotechnical Commission, 2009.

19.47. IEC 61839, "Nuclear Power Plants – design of control rooms – functional analysis and assignment," International Electrotechnical Commission, 2000.

19.48. IEC 60780, "Nuclear Power Plants - electrical equipment of the safety system – qualification," International Electrotechnical Commission, 1998.

19.49. Westinghouse Report UKP-PMS-GLR-003, Rev. 1, "PMS Spurious Blocker Safety Case Basis," December 2016.

19.50. Westinghouse Report UKP-OCS-GLR-001, Rev 1, "United Kingdom AP1000 RSR Control Strategy for Class 1 Displays and Controls - SAPs Compliance," December 2016.

19.51. Westinghouse Report EQ-EV-284, Rev. 1, "Equipment Qualification - Comparison of IEC Standard 60780-1998 to IEEE Standard 323-1974," May 2016.

19.52. Westinghouse Report EQ-EV-285, Rev. 0, "Equipment Qualification - Comparison of IEC Standard 60980-1989 to IEEE Standard 344-1987," April 2016.

19.53. Westinghouse Report UKP-OCS-GLR-002, Rev 1 "United Kingdom AP1000 RSR Control Strategy for Class 1 Displays and Controls – ALARP Justification," December 2016.

19.54. Westinghouse Document UKP-1000-GEC-004, Rev. 1, "AP1000 Barrier Matrix," January 2017.

19.55. Westinghouse Report UKP-GW-GLR-024, Rev. 2, "United Kingdom AP1000 Diversity Analysis of the Plant Control System/Data Display and Processing System (PLS/DDS) and Diverse Actuation System (DAS)," December 2016.

19.56. Westinghouse Document WNA-PD-00055-GEN, Rev. 3, "Standard Integrated System Engineering Process," March 2016.

19.57. Westinghouse Report UKP-GW-GL-162, Rev.1 , "UK AP1000 BEACON Core Monitoring System Basis of Safety Case," October 2016.

19.58. Westinghouse Report UKP-GW-GL-500, Rev 0, "AP1000 UK Limits and Condition Process Description," December 2015.

19.59. Westinghouse Report UKP-GW-GLR-038, Rev. 0, "United Kingdom AP1000 Plant C&I Architecture IEC 61513 Safety Life Cycle Conformance Assessment," September 2016.

19.60. Westinghouse Report UKP-GW-GLR-039, Rev. 0, "United Kingdom AP1000 Plant C&I Architecture SAPs Conformance Assessment," September 2016.

19.61. Westinghouse Report UKP-GW-GLR-037, Rev. 0, "United Kingdom AP1000 Plant Control and Instrumentation Architecture ALARP Justification", August 2016.

19.62. Westinghouse Document WNA-SQ-00049-GEN, Rev. 3, "Classification of I&C Systems," November 2014.

19.63. Westinghouse Document APP-GW-GBH-361, Rev. 2, "Westinghouse AP1000 Integrated I&C Test Strategy," September 2015.

Table 19-1. Principal Claims on C&I Equipment in the Safety Case

System	Highest Cat/ Class	Principal Claims in the Safety Case
PLS	B/2	Controls plant within operational limits and conditions. Failure of this function could lead directly to the actuation or operation of a Category A safety function. Functions that considerably reduce the frequency of an initiating event as identified by the DBA analysis, i.e. the PLS is required to minimise the demand on safety systems.
PMS	A/1	PMS is the primary C&I system to initiate reactor trip and engineered safety functions such as containment isolation, decay heat removal, and safety injection. PMS initiates functions required to reach the non-hazardous stable state, to prevent a DBA from leading to unacceptable consequences or to mitigate its consequences. Initiates reactor trip when plant conditions reach specified limits. The PMS should be independent to the PLS and DAS.
DAS	A/2	DAS is the diverse C&I system to initiate reactor trip and engineered safety functions such as containment isolation, decay heat removal, and safety injection. DAS initiates functions required to reach the non-hazardous stable state, to prevent a DBA from leading to unacceptable consequences or to mitigate its consequences. Initiates reactor trip when plant conditions reach specified limits. The DAS should be independent to the PLS and the PMS and diverse to the PMS.
OCS	A/1	Required to provide information and control capabilities that allow specified manual actions necessary to reach the non-hazardous stable state. The OCS provides the primary hardware used to manually initiate and monitor Class 1 SSCs. The OCS provides the human interface design as well as the location and mounting arrangement for the operator interface equipment necessary to support DiD safety functions.
IIS	B/2	Required to provide information that allows specified manual actions necessary after the non-hazardous stable state has been reached to prevent a DBA from leading to unacceptable consequences, or mitigate the consequences. Core exit temperature measurements are not used for reactor trip or ESF functions. Some of the measurements are inputs to the PMS and DAS for post-accident monitoring.
RMS	A/1	Maintaining the integrity of the containment; thereby minimising the release of radioactive material from the containment. Maintaining habitability of the MCR.

Table 19-2. DAS Manual Functions

Function	MCR DAS Control Panel	Remote DAS Control Panel
Reactor and Turbine Trip	X	X
Passive Containment Cooling Actuation	X	X
CMT Actuation and RCP Trip	X	X
Open Stage 1 ADS Valves	X	
Open Stage 2 ADS Valves	X	
Open Stage 3 ADS Valves	X	
Open Stage 4 ADS Valves	X	X
Open PRHR Discharge Isolation Valves and Close IRWST Gutter Isolation Valves	X	X
Selected Containment Penetration Isolation	X	X
Containment Hydrogen Igniter Actuation	X	
Initiate IRWST Injection	X	X
Initiate Containment Recirculation	X	X
Initiate IRWST Drain to Containment	X	X

Table 19-3. DAS Sensors

Item No	Sensor Tag	Description	Scale	Use
1	RCS-TE300A	Hot Leg 1 Temperature Channel 1	288C° to 343°C (550° to 650°F)	Protection
2	RCS-TE300C	Hot Leg 1 Temperature Channel 2	288C° to 343°C (550° to 650°F)	Protection
3	RCS-TE300B	Hot Leg 2 Temperature Channel 1	288C° to 343°C (550° to 650°F)	Protection
4	RCS-TE300D	Hot Leg 2 Temperature Channel 2	288C° to 343°C (550° to 650°F)	Protection
5	SGS-LT044	Steam Generator 1 Level Channel 1	0 to 100% of span	Protection
6	SGS-LT 045	Steam Generator 1 Level Channel 2	0 to 100% of span	Protection
7	SGS-LT 046	Steam Generator 2 Level Channel 1	0 to 100% of span	Protection
8	SGS-LT 047	Steam Generator 2 Level Channel 2	0 to 100% of span	Protection
9	RCS-LT305A	Pressuriser Level Channel 1	0 to 100% of span	Protection
10	RCS-LT305B	Pressuriser Level Channel 2	0 to 100% of span	Protection
11	RCS-LT305C	Pressuriser Level Channel 3	0 to 100% of span	Protection
12	VCS-TE053A	Containment Temperature Channel 1	0C° to 149°C (32° to 300°F)	Protection
13	VCS-TE053B	Containment Temperature Channel 2	0C° to 149°C (32° to 300°F)	Protection
14	VCS-TE053C	Containment Temperature Channel 3	0C° to 149°C (32° to 300°F)	Protection
15	IIS-TE009	Core Exit Temperature Channel 1	93C° to 1260°C (200° to 2300°F)	Monitoring
16	IIS-TE013	Core Exit Temperature Channel 2	93C° to 1260°C (200° to 2300°F)	Monitoring
17	IIS-TE030	Core Exit Temperature Channel 3	93C° to 1260°C (200° to 2300°F)	Monitoring
18	IIS-TE034	Core Exit Temperature Channel 4	93C° to 1260°C (200° to 2300°F)	Monitoring
19	PLS-ET001	Motor Generator Set Voltage Channel 1	0 to 260 Volts Alternating Current (VAC)	Monitoring
20	PLS-ET002	Motor Generator Set Voltage Channel 2	0 to 260 VAC	Monitoring

Table 19-4. DDS Application Programmes

Programme Identifier	Programme Name
AFD	Axial flux difference monitor
BAP	Best-available parameters
BDP	BEACON data processing
BIS	Bypass and inoperable status indication
BOP	BOP performance calculation
CLR	Containment leak rate monitor
COM	Containment monitor
CPS	Miscellaneous calculations to support computerised procedures system functions
CON	Plant Constants
FLC	Flow correction
HCD	Heatup/cooldown calculation
HSI	Miscellaneous calculations to support human system interface functions
LCO	Limiting conditions for operation
ICR	Inverse Count Rate Ratio
LPO	RCPs and loops in operation monitor
LRM	RCS leak rate monitor
LVC	Level correction
PLM	Plant mode
PLT	Plant state monitor
PPP	Primary plant performance calculations
PSM	Plant system monitor
RFT	Radial flux tilts monitor
ROC	Rate of change
RSA	Redundant sensor algorithm
RSU	Rod supervision
SLM	Sump level monitor
SPD	Safety parameter display calculations
SSF	Shutdown critical safety functions
TAP	Time averaging programme
XYP	XY plot data processing

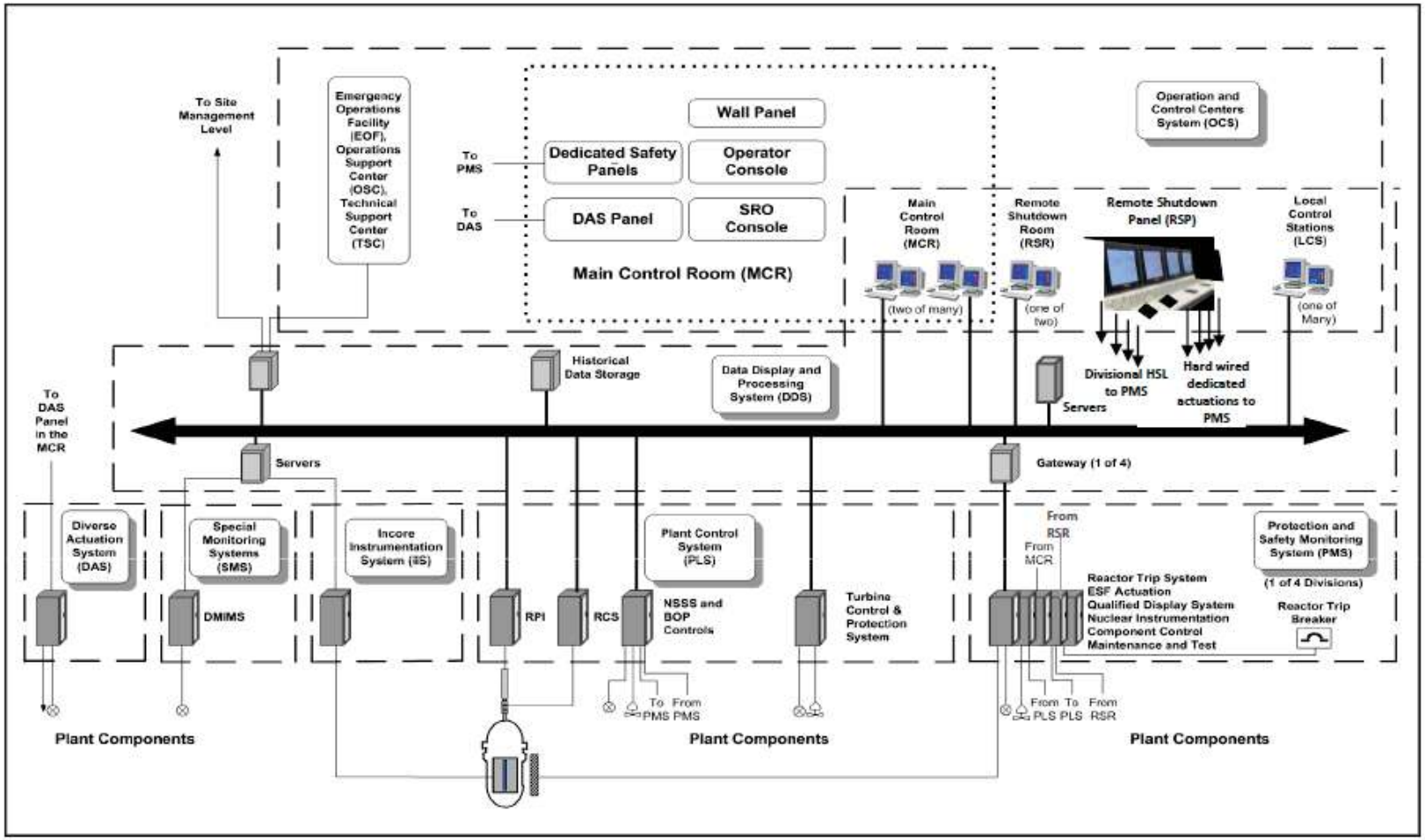


Figure 19-1. C&I Architecture

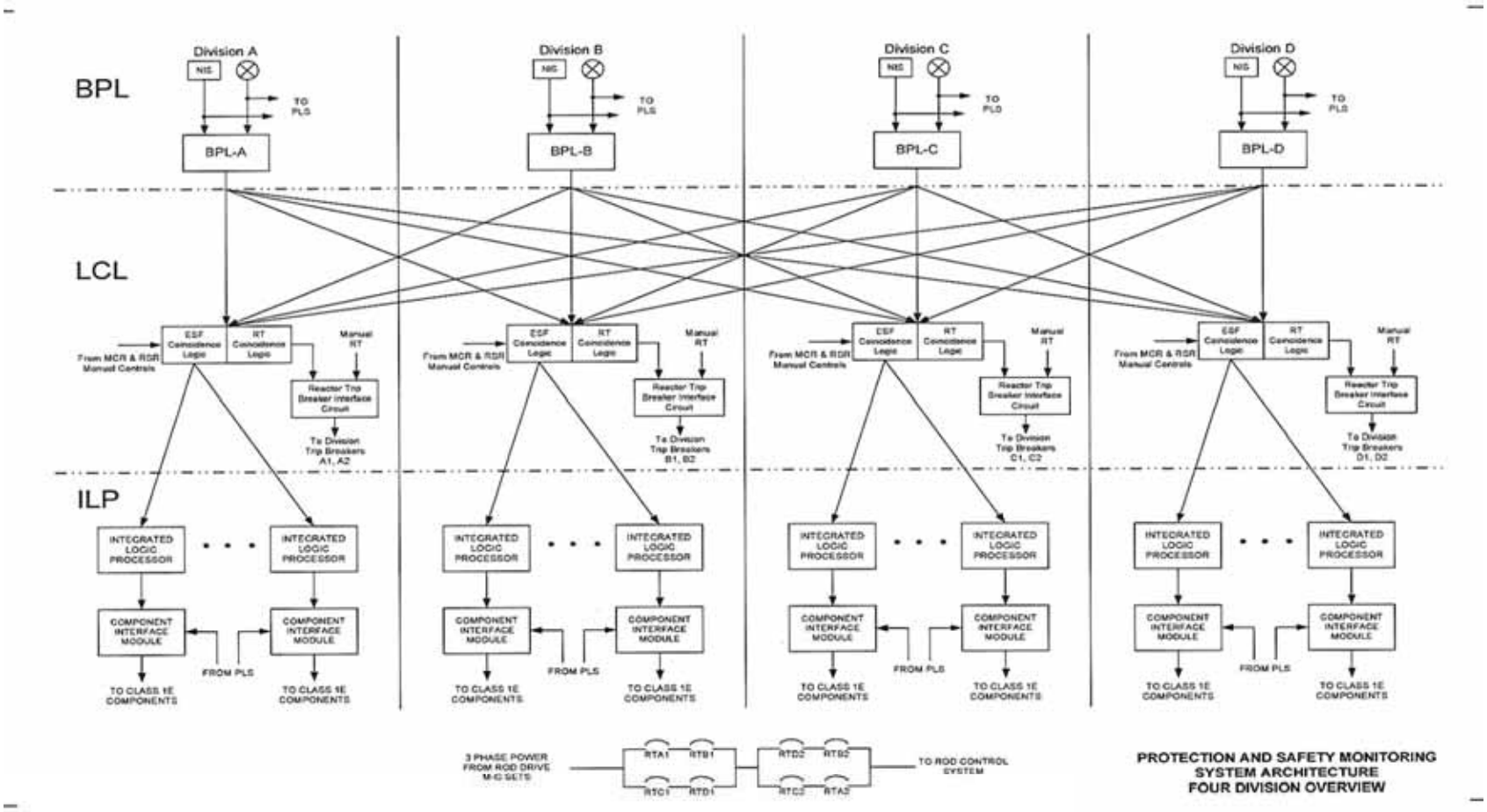


Figure 19-2. PMS Four-Division Overview

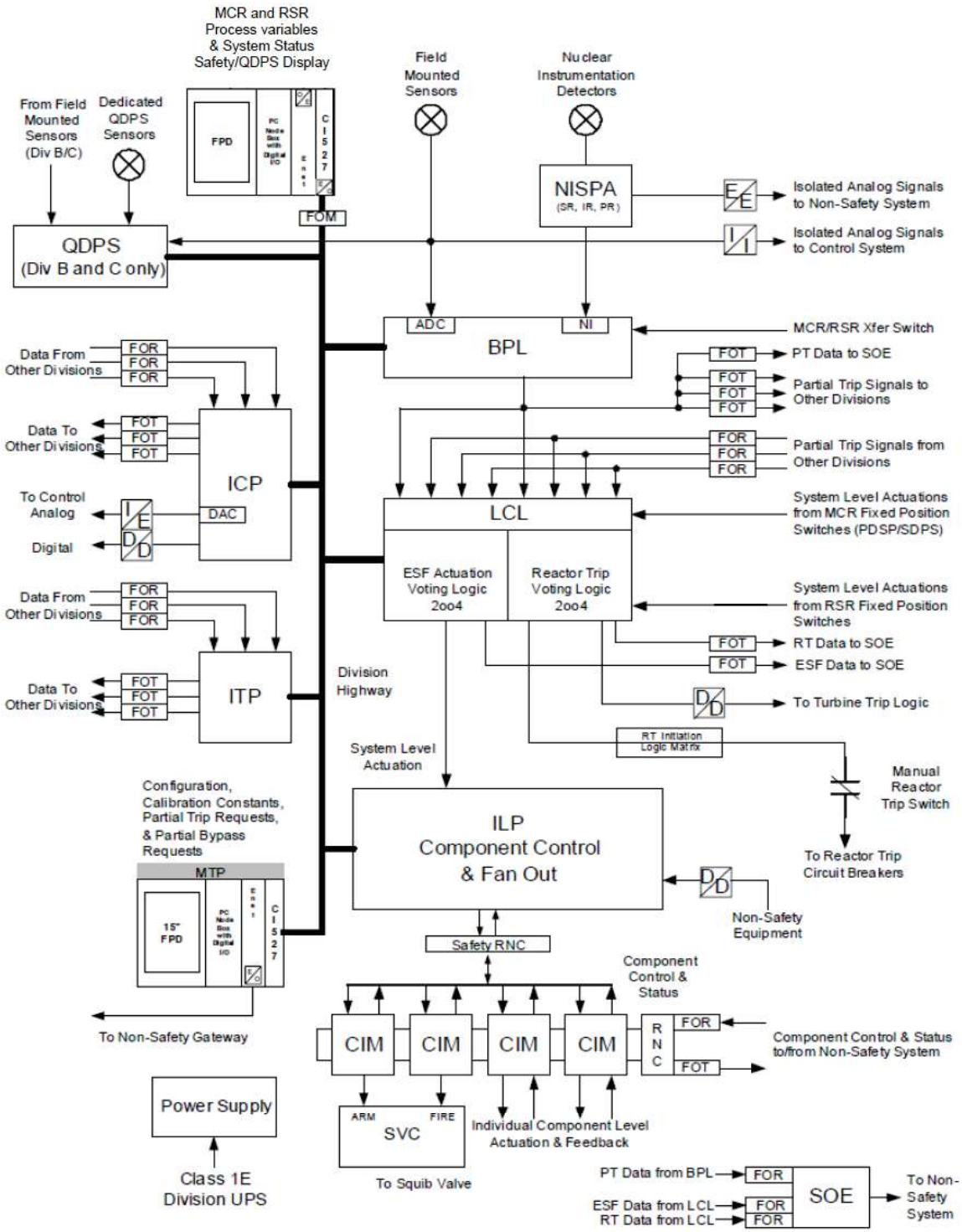


Figure 19-3. PMS Single Division

Figure 19-4. Not Used

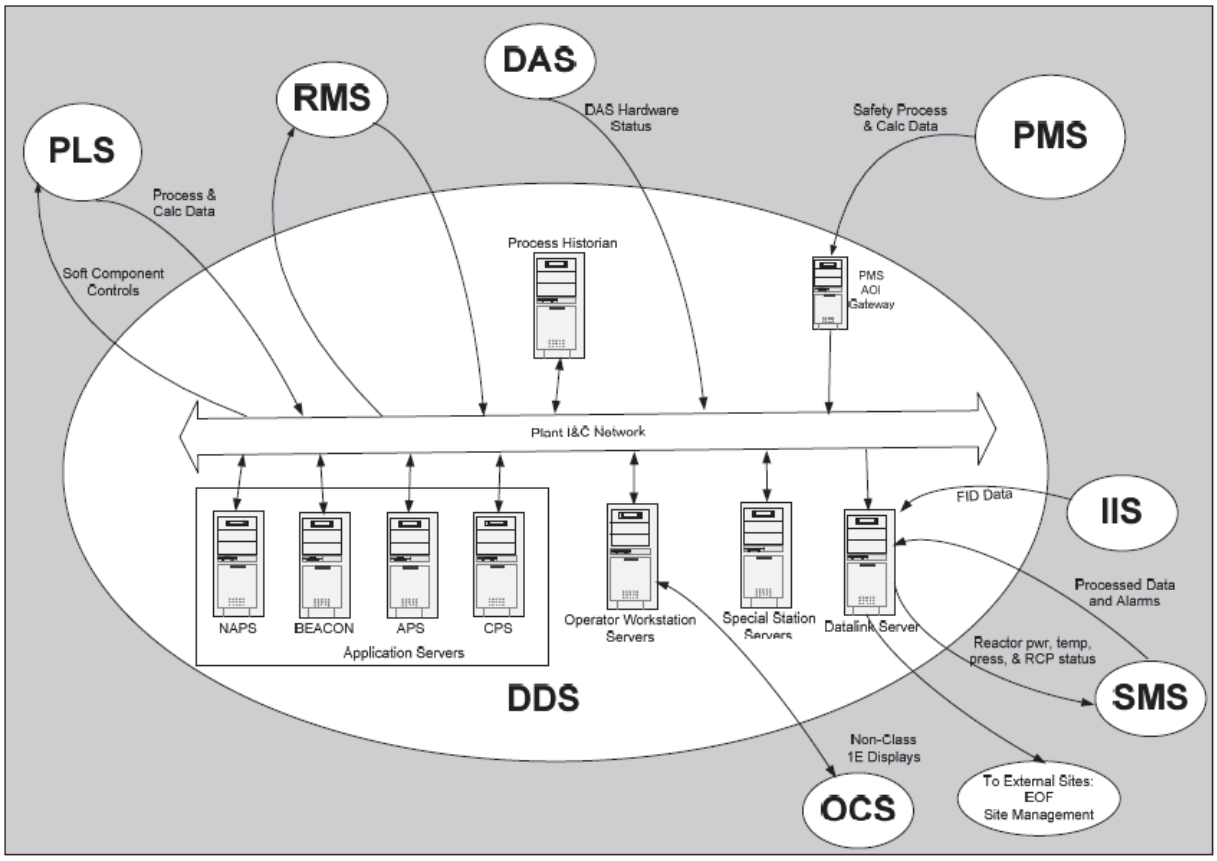


Figure 19-5. Schematic of DDS Resources and their Interfaces

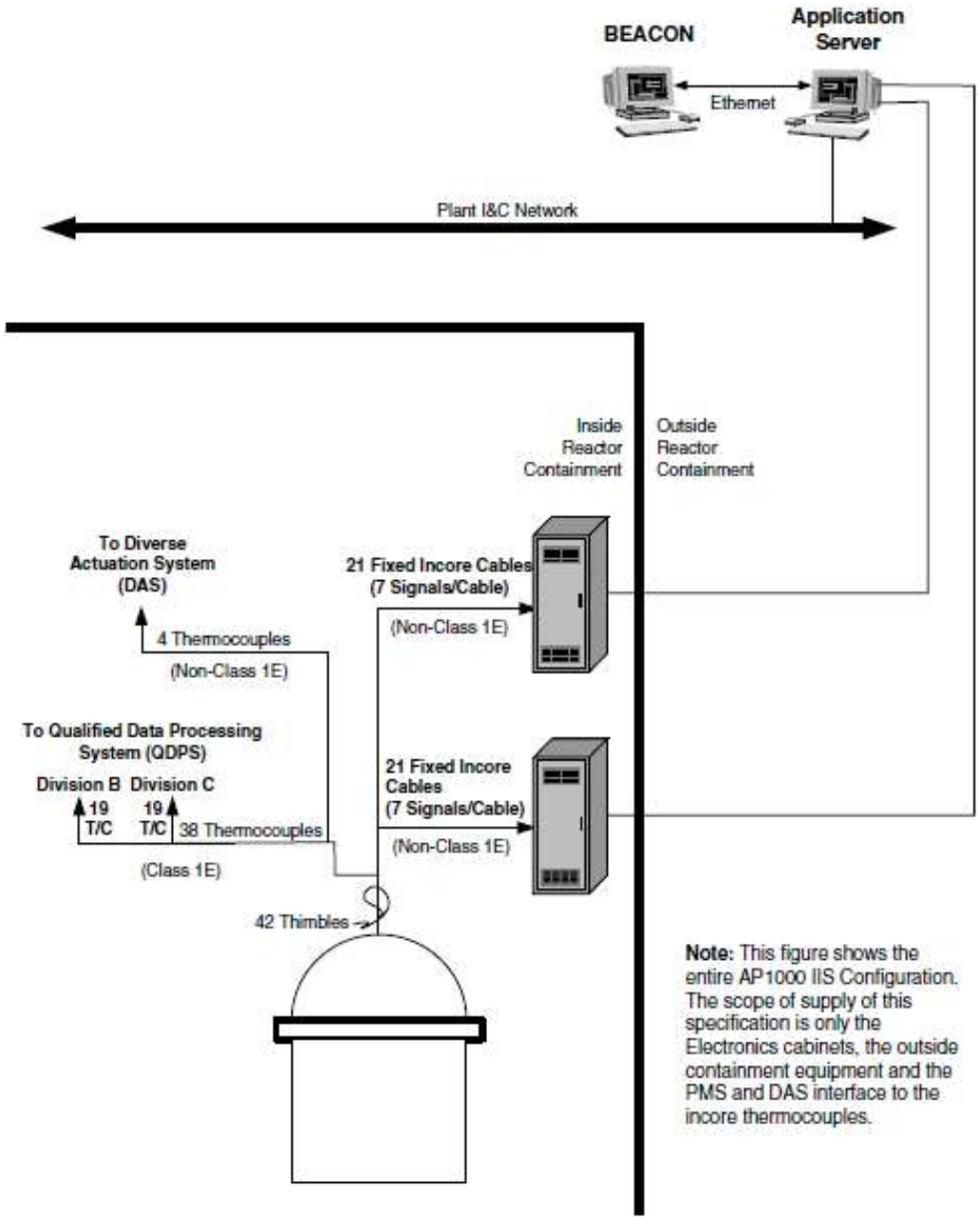


Figure 19-6. AP1000 Plant IIS Configuration

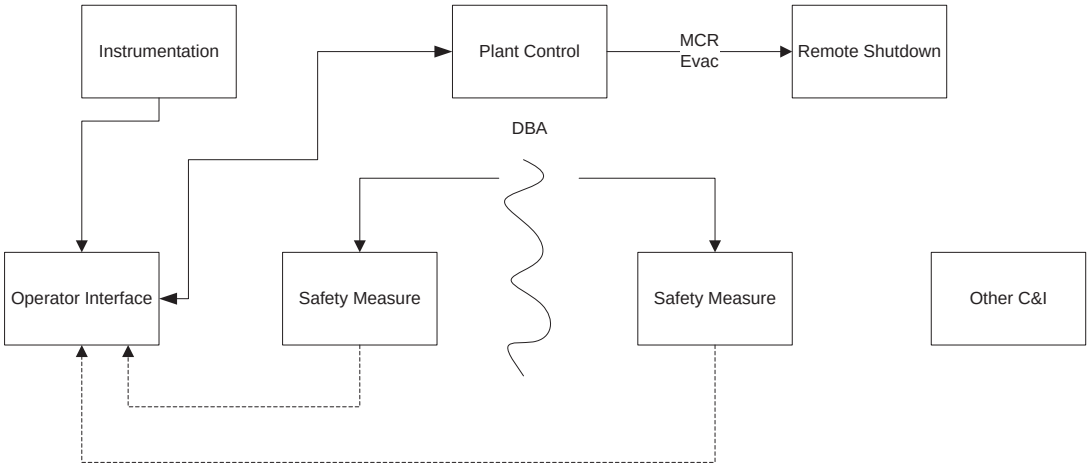


Figure 19-7 Schematic of fundamental safety case driven C&I architecture

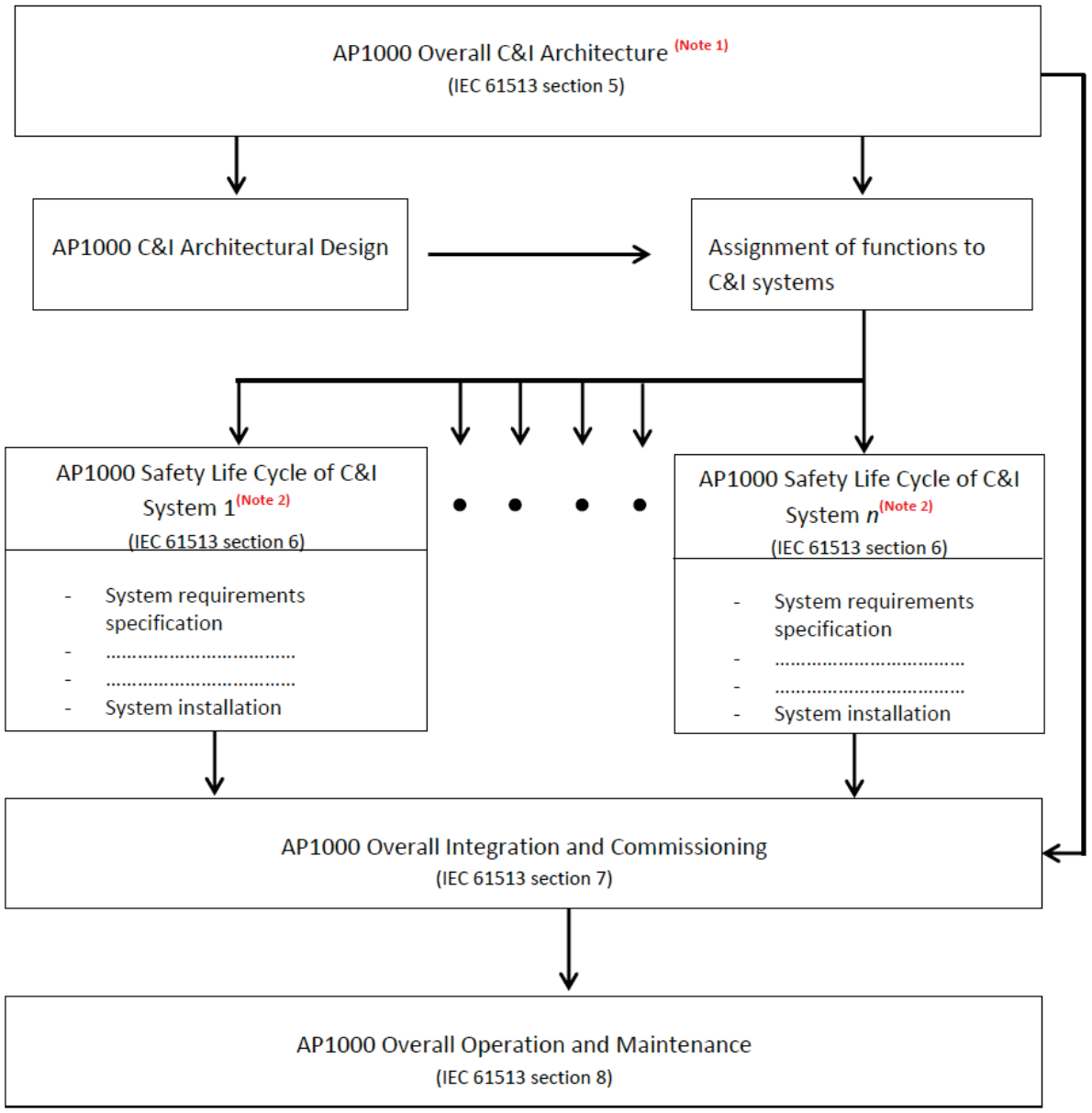


Figure 19-8. Definition of scope boundary for coverage between the PCSR and System BSCs

Note 1: PCSR Chapter 19 will provide justification and substantiation of the overall C&I architecture and shall provide demonstration of a safety life cycle based on IEC 61513, Sections 5, 7 and 8 (Reference 19.16).

Note 2: The BSCs will provide a detailed descriptions and substantiation of the individual systems and will include demonstration of a safety life cycle based on IEC 61513, Sections 6, 7 and 8 (Reference 19.16).

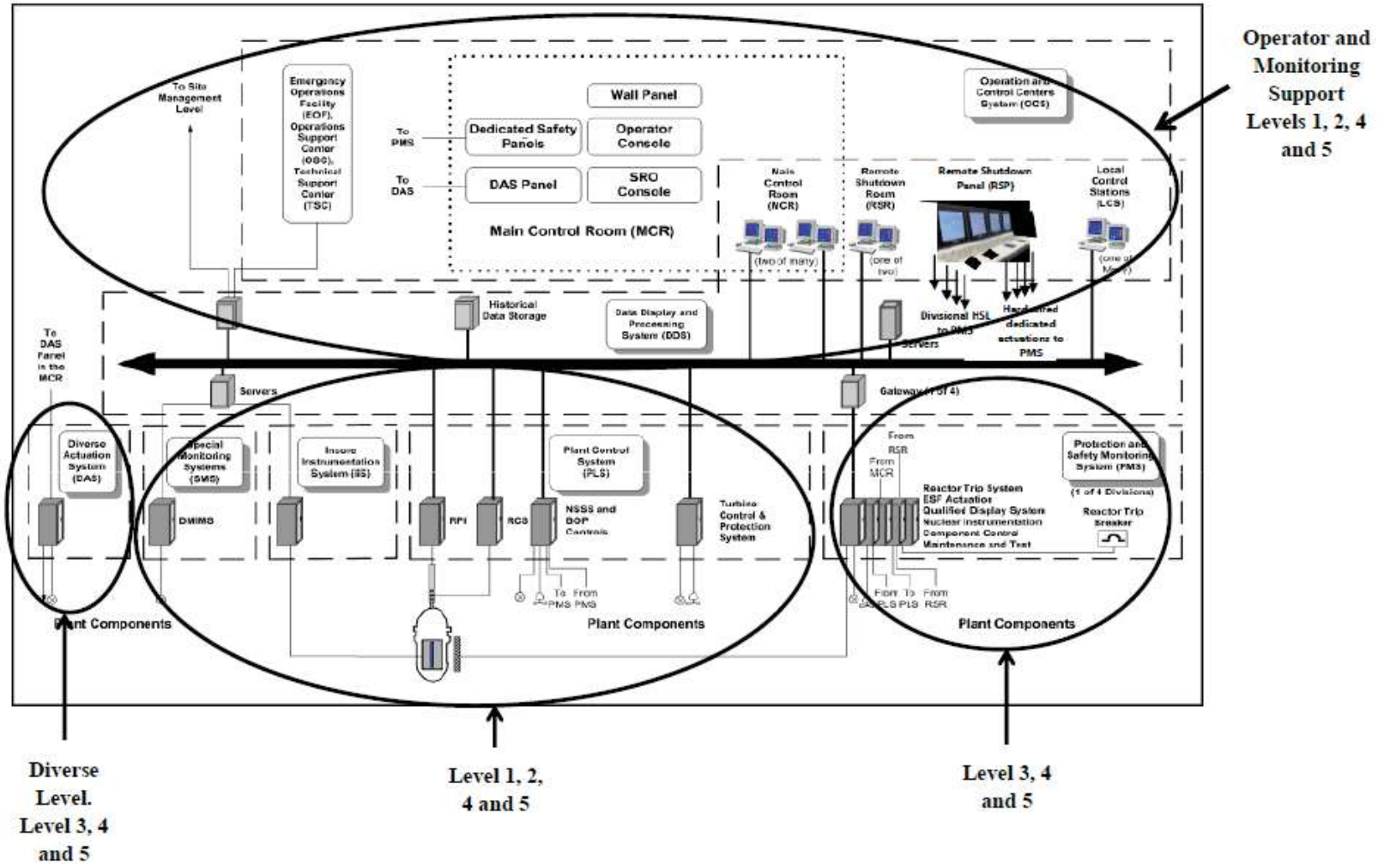


Figure 19-9: Levels of DiD mapped to the C&I architecture

TABLE OF CONTENTS

TABLE OF CONTENTS (cont.)

LIST OF TABLES

LIST OF FIGURES

None.

LIST OF ABBREVIATIONS AND ACRONYMS

ADS	automatic depressurisation system
ALARP	as low as reasonably practicable
ASME	American Society of Mechanical Engineers
BEZ	break exclusion zone
C&I	control and instrumentation
CFR	Code of Federal Requirements
CMT	core makeup tank
CSR	Component Safety Report
CV	containment vessel
D-RAP	design reliability assurance program
DEGB	double-ended guillotine break
DN	diametre nominel
DNB	departure from nucleate boiling
DSM	defect size margin
DVI	direct vessel injection
ELLDS	end of life limiting defect size
EMIT	examination, maintenance, inspection, and testing
ENIQ	European Network for Inspection and Qualification
GDA	generic design assessment
HI	high integrity
HSS	highest safety significance
IITA	in-core instrument thimble assembly
IoF	incredibility of failure
IRWST	in-containment refuelling water storage tank
ISI	in-service inspection
LFCG	lifetime fatigue crack growth
LOCA	loss-of-coolant accident
MCR	main control room
MSIV	main steam isolation valve
MSL	main steam line
MSLB	main steam line break
NDT	nondestructive testing
NPS	nominal pipe size
O-RAP	operability reliability assurance program
PRHR HX	passive residual heat removal heat exchanger
PSA	probabilistic safety assessment
PXS	passive core cooling system
QEDS	qualified examination defect size
RCCA	rod cluster control assembly
RCL	reactor coolant loop
RCP	reactor coolant pump
RCPB	reactor coolant pressure boundary
RCS	reactor coolant system
RNS	normal residual heat removal system
RV	reactor vessel
RVI	reactor vessel internals
SFR	safety functional requirement

LIST OF ABBREVIATIONS AND ACRONYMS (CONT.)

SG	steam generator
SoL	start of life
SSC	system, structure, or component
TAGSI	Technical Advisory Group on Structural Integrity
UK	United Kingdom

20 STRUCTURAL INTEGRITY

20.1 INTRODUCTION

This chapter presents safety arguments to demonstrate how the structural integrity of the AP1000 plant United Kingdom (UK) Class 1 systems, structures, and components (SSCs) can be assured over the 60-year design life of the plant to a level of structural reliability and a degree of rigour commensurate with the consequences of gross failure.

To achieve this, a classification methodology has been developed based on an evaluation of the direct and indirect consequences of postulated gross failure. Based on this classification, structured arguments are presented for each major component and are tailored to support the structural reliability claimed for that component. They are presented as a series of individual Component Safety Reports (CSRs), which are included as appendices to this chapter.

For components for which the consequences of gross failure are intolerable, and hence for which the claim is that the probability of gross failure is so low as to be discounted, a multi-legged safety argument has been presented as described in Section 20.6.4. For such components, the arguments include supplemental requirements for defect tolerance and the use of qualified manufacturing inspections to provide a robust demonstration that the component will enter service free from defects that could be of concern through life. For components for which the postulated consequences are less severe, the safety arguments are based on design in accordance with recognised standards.

The safety arguments for each component are presented in the form of a series of claims, arguments, and evidence. Further support is provided by a suite of referenced documentary evidence that provides specific details of the design and functional specifications, code design assessments, manufacturing specifications, material specifications, and inspectability assessments applicable to each component. This documentary envelope is presented as a Technical Index within each individual CSR.

20.2 SCOPE

The broad scope of this chapter is to substantiate the structural integrity of a number of plant SSCs for all conditions within the design basis. A series of individual CSRs are included as appendices to this chapter, which establish safety arguments to support structural integrity claims for the following SSCs:

- Reactor vessel (RV) — Appendix 20A
- Pressuriser — Appendix 20B
- Steam generators (SGs) — Appendix 20C
- Main steam lines (MSLs)[1] — Appendix 20D
- Reactor coolant loop (RCL) piping — Appendix 20E
- Reactor coolant pump (RCP) — Appendix 20F
- Passive residual heat removal heat exchanger (PRHR HX) — Appendix 20G
- Core makeup tank (CMT) — Appendix 20H
- Accumulator — Appendix 20I
- RV internals and core support structures — Appendix 20J
- Containment vessel (CV) — Appendix 20K

1. The main steam line assessment in Appendix 20D includes the MSL inside containment and outside containment, up to the main steam isolation valve located at compartment wall 11.

The rationale for the selection of SSCs included for detailed evaluation within is summarised in Section 20.5.1. The SSCs addressed in these appendices include the major components that constitute the primary and secondary system pressure boundaries within containment. Each appendix listed above includes definition of a detailed scope that is specifically applicable to that CSR. Concrete structures and fluid systems are not included within the scope of this chapter. These are covered in Chapters 16 and 17, respectively.

20.3 OBJECTIVES

At a high level, the objective of each CSR is to support the claim established in Chapter 14 that the AP1000 plant risk remains both tolerable and as low as reasonably practicable (ALARP) for the design lifetime. Satisfying the safety design bases for each SSC and the associated structural integrity safety functional requirements (SFRs) provides support to this claim. The SFRs correspond to the functions that need to be maintained to provide assurance of nuclear and radiological safety; the basis for the derivation of these SFRs is described in Section 20.4. Several components addressed in this chapter feature design enhancements adopted as ALARP measures to minimise frequency of failure, and these are identified in the relevant appendices.

20.4 DERIVATION OF SAFETY FUNCTIONAL REQUIREMENTS

Each SFR of any particular SSC establishes a specific role required to maintain nuclear and radiological safety under normal operating and fault conditions. SFRs are identified for each AP1000 plant component addressed in Appendices 20A to 20K, to specify the required safety functional performance in each case.

Performance and safety design bases provide the basis for identifying the SFRs. The performance and safety design bases of the reactor coolant system (RCS) and its major components are interrelated, and are applicable to the derivation of SFRs for the RCS pressure boundary components addressed in the appendices to this chapter. The performance and safety design bases for the RCS are identified in Reference 20.1.

For the structural integrity CSRs appended to this chapter, SFRs have been identified by a review of the performance and safety design bases relevant to a particular component to establish where, and to what extent, structural integrity must be justified to maintain the required safety functional performance. Table 20-1 lists the SFRs allocated to each AP1000 plant component addressed in Appendices 20A to 20K. The range of operating conditions included within the design basis for each component are detailed in the relevant CSR and include all those associated with normal operations and planned tests; a range of upset, emergency, and faulted conditions are also included. Each CSR specifies a deterministic assessment to substantiate the structural integrity of the AP1000 plant components for all conditions within the design basis. The capability of the AP1000 plant to maintain nuclear safety in response to design basis internal hazards is addressed in Chapter 11, and to external hazards in Chapter 12.

Postulated failure modes, which result in a loss of SFRs, lead to the identification of a structural classification that is commensurate with the consequences of gross failure, as determined through the process of component classification described in Section 20.5. The CSRs are provided to substantiate that the structural reliability will be commensurate with the consequences of gross failure. The basis for the safety case presented in the CSRs is established according to the classification allocated to a particular component.

20.5 STRUCTURAL INTEGRITY CLASSIFICATION

Key to the AP1000 plant component structural integrity is the understanding of the radiological consequences of any postulated failure mode. Based on this, a structured and systematic basis has been developed for establishing the level of rigour applied during the design assessment, material procurement, fabrication, in-manufacture inspection, testing, in-service testing, maintenance, and inspection of the components. This level of rigour is based on the component structural integrity classification scheme, as presented in the AP1000 UK Structural Integrity Classification (Reference 20.2).

For a component with a high degree of redundancy or with diverse means of protection, a minimum level of structural reliability based on the demonstration of good design, manufacture, and inspection in accordance with relevant design code requirements, may be appropriate. However, for those components for which no redundancy or diverse means of protection can be provided, it must be shown the likelihood of gross failure is so low that it can be discounted. For such components it is necessary for a higher degree of structural reliability to be sought and substantiated. This requires measures to be implemented over and above design code requirements, with a particular emphasis on demonstrating that a structure is free of structurally significant manufacturing defects and is tolerant to in-service degradation. That is, an acceptable margin must be shown to exist between a qualified examination defect size (QEDS) and the maximum allowable start of life (SoL) defect size.

The structural integrity classification scheme has been developed to be consistent with the overall AP1000 plant safety categorisation and classification scheme as described in Chapter 5. The categorisation process for the AP1000 plant is performed by identifying the high-level safety functions that a specific SSC delivers or supports. These safety functions are categorised A to C, based on the nuclear safety significance of delivery failure. Once a safety function category has been assigned to a specific SSC in line with the safety function it delivers (or supports the delivery of), the SSC is assigned a Safety Class between 1 and 3. This safety class takes the safety category into account, and considers the extent to which the SSC supports the associated safety function.

In practice, the AP1000 plant safety categorisation and classification methodology is too coarse to determine component structural integrity requirements, since Class 1 covers a very broad range of initiating event frequencies and consequences and hence, a commensurately broad range of structural reliability targets.

Consistent with accepted UK practice, an alternative classification methodology for determining structural integrity requirements for passive structures has been established, which subdivides Class 1 SSCs according to the consequences of postulated gross failure. The details of this classification methodology and the conclusions from the application of the methodology are presented in Reference 20.2.

20.5.1 Structural Integrity Classification Process

The starting point in the process was to use the safety classification and categorisation methodology described in Section 5.2 to identify each Class 1 SSC. A high-level review was then undertaken to identify a short list of SSCs for which postulated gross failure could conceivably lead to intolerable consequences, through direct or indirect means, and hence, meriting a more detailed evaluation.

All valves were excluded from the structural integrity classification process on the basis that their consequences of gross failure would be bounded by the assessment of a selection of piping systems. Similarly, civil structures and cranes, included within the scope of Class 1 components, were also excluded as these are covered in Chapters 16 and 17. The CV was not included in the initial assessment since the primary reliability claim against the CV is under faulted plant conditions and this does not lend itself to consideration using the established method. Nonetheless, the CV is included within the scope of this chapter, and the basis for determining the structural integrity requirements for the CV are detailed in Appendix 20K.

For the selected components, a thorough review of the radiological consequences of gross failure was performed. An important element of the process was the assumption of gross failure, which was assumed irrespective of any anticipated material properties and crack development behaviour. Hence, supplemental design practices were not considered as part of the classification process. These practices do, however, feature as a defence in depth element in certain CSRs.

The consequences were considered in a broad sense and included the direct effects on plant safety, for example, a loss of coolant inventory or reactivity excursions; and the indirect effects from, for instance, missiles, blast, pipe whip, flooding, and water/steam jets. This also considered any longer-term effects on the availability of essential safety systems and instrumentation required to maintain plant safety in the faulted condition. The first step in the process was to hold an expert review meeting with relevant specialist input. The AP1000 design 3-D model was used to establish the proximity of adjacent essential systems and enabled secondary consequences to be robustly evaluated. The approach ensures that the final classification has been reached following extensive engagement with the appropriate AP1000 design technical experts.

20.5.2 Component Structural Integrity Classifications

The structural integrity classification scheme for the AP1000 plant is summarised in Table 20.2. The following classes are identified:

- Highest safety significance (HSS)
- High integrity (HI)
- Standard Class 1
- Standard Class 2 or 3

Highest Safety Significance

HSS is assigned to failure modes for which there is no protection, failure is intolerable, and where it is not reasonably practicable to provide protection. In practice, this applies to fault sequences where the assessed consequences include both severe core damage and potential large uncontrolled releases. The Demonstration of Incredibility of Failure in Structural Integrity Safety Cases (Reference 20.5), prepared in response to a question asked of the UK Technical Advisory Group on Structural Integrity (TAGSI), provides an authoritative view on when an incredibility of failure (IoF) case is required and how such cases should be presented. In the context of the methodology described here, IoF and HSS are considered equivalent. The basis and format of the safety case arguments for HSS components are summarised in section 20.6.4.

High Integrity

The failure of HI components can lead to severe core damage but, in general terms, it can be shown that effective containment will limit the offsite consequences. HI is assigned where the component can be described as single-failure intolerant, i.e., where there is a single line of protection, but no redundancy. In this case, it is therefore possible to make a consequence argument, but this is deemed not to provide the same degree of confidence from a fully qualified line of protection with redundancy. Thus, partial protection may be available and this is reflected in the degree of substantiation required. The basis and format of the safety case arguments for HI components are summarised in section 20.6.3.

Standard Class 1 Systems, Structures, and Components

It is required to demonstrate that only limited core damage can result in the event of failure of a component classified as Standard Class 1. The basis and format of the safety case arguments for Standard Class 1 components are summarised in section 20.6.2.

Standard Class 2 or 3 Systems, Structures, and Components

Failure of components classified as Standard Class 2 or 3 SSCs should not result in any core damage although contamination can lead to worker exposure in excess of annual statutory limits. The basis and format of the safety case arguments for Standard Class 2 or 3 SSCs are summarised in section 20.6.1.

20.5.3 Results of Structural Integrity Classification

Reference 20.2 describes the application of the classification methodology at a component level. It should be noted that where a component has been categorised as HSS, this highest level of classification does not necessarily apply to all regions of the component. To address this, a more detailed assessment of individual locations has been carried out. Specifically, this includes the identification of HSS weld locations where additional measures will be applied in terms of the assessment of defect tolerance and the application of qualified inspection to detect defects of structural significance.

The results of the assessment are presented in Reference 20.2. A summary of the basis for structural integrity classification of each component assessed is reproduced in Table 20-3 to Table 20-21.

The following components have been assessed as HSS:

- RV
- Pressuriser
- SG channel head, tube sheet, and secondary shell

The main coolant loop piping hot leg and cold leg to RV nozzle safe end welds have been classified as HI. The remaining components have been classified as Standard Class 1.

20.6 BASIS OF THE COMPONENT SAFETY CASES

Each CSR presents a safety argument to establish that the structural reliability of the component is commensurate with the consequences of gross failure. A system of structural integrity classification that establishes appropriate structural integrity requirements has been described for the AP1000 plant components addressed in Appendices 20A to 20K.

The structural integrity design of the piping and pressure vessels considered in these appendices is substantiated by demonstrating sound engineering practice. This is argued to provide a high level of confidence in the ability of a component to deliver its required safety functions throughout its life. A qualitative approach to demonstrate defence in depth for nuclear plant components, such as those addressed in Appendices 20A to 20K, is commonly adopted within the nuclear industry worldwide because of a general lack of sufficiently reliable data to support quantitative substantiation of the low frequencies of failure typically claimed. Various elements of sound engineering practice are identified in each CSR that confirm quality of design, construction, inspection, and testing in accordance with relevant nuclear codes. In combination, this evidence establishes robust defence in depth against failure of structural integrity without resort to quantitative statistical or modelling approaches.

20.6.1 Standard Class 2 or 3 Components

For Standard Class 2 or 3 components, reliance can be placed on the application of the appropriate design codes (Reference 20.2). This, in combination with either redundancy or diversity in the plant protection leads to structural integrity cases and the inspection requirements for component failures in this class being based on the compliance with design code requirements. Standard inspection techniques in accordance with code requirements are used to underpin integrity claims. Specific measure may be required where known degradation mechanisms exist. Specification and procurement of materials in accordance with the requirements of the applicable design codes, including the application of operating experience (OE) to provide further evidence, ensures that appropriate materials, relative to the importance of the component, are used.

Table 15A-1 presents, among other details, the UK safety class associated with each mechanical SSC. As noted in Reference 20.2, all UK Safety Class 2 or 3 SSCs have a corresponding structural integrity classification of Standard Class 2 or 3, respectively. Table 15A-1 identifies the principal design code used for each Class 2 or 3 SSC. Note that for the design AP1000 plant UK Class 2 SSCs, with their limited safety significance, non-nuclear codes and standards, and additional regulatory oversight proposed (enhanced quality programmes, design / operational reliability assurance program (D-RAP / O-RAP), and availability control programs), provide the evidence to support the arguments for the claim that it is proper to design UK Class 2 SSCs to non-nuclear codes and standards (Reference 20.22).

20.6.2 Standard Class 1 Components

As noted in Reference 20.2, the failure statistics for industrial pressure vessels and piping built according to the good practice embodied in modern codes and standards supports the inference of a failure rate that is in accordance with the structural integrity requirements for Standard Class 1 components. Substantiation of the structural reliability of the Standard Class 1 components in Appendices 20D to 20K is accordingly based on demonstrating a high quality of design and build by compliance with relevant aspects of the American Society of Mechanical Engineers (ASME) Boiler & Pressure Vessel Code (Code) as a minimum.

The ASME Code prescribes rules governing the design, fabrication, and inspection of boilers and pressure vessels that are internationally recognised to be well established for application in the nuclear industry. The following sections of the ASME Code establish requirements that address key aspects of component design for the AP1000 plant:

- Section II Materials

- Section III Rules for the construction of nuclear facility components
- Section V Nondestructive examination
- Section IX Welding and brazing qualifications
- Section XI Rules for in-service inspection of nuclear power plant components

The safety arguments for the Standard Class 1 components are structured according to a series of claims to demonstrate compliance with relevant requirements of the ASME Code. The key topics addressed in each Standard Class 1 CSR are summarised below.

Each safety argument presented in Appendices 20D to 20K identifies applicable codes and standards, including relevant sections of the ASME Code, as one element of the evidence presented to demonstrate good design. The codes, standards, and regulations specified to control quality of design and manufacture embody extensive operating experience relevant to the AP1000 plant components. This ensures a structurally robust design and provides a means to prevent, minimise, and control component degradation at the design stage. Compliance with the codes, standards, and regulations, therefore, provides a foundation for assuring that structural integrity of the AP1000 plant components will be maintained for the design lifetime. The revision or edition of codes and standard applicable to the AP1000 plant vary by component. For example, the reactor vessel has been designed in accordance with the ASME Code Section III, 1998 Edition with addenda up to and including 2000. The Licensee will need to review newer editions of the ASME Code, and possibly other codes and standards, to determine what changes might be required to comply with newer editions, and either make those changes or justify why the changes are not practical.

Evidence is provided in the Standard Class 1 safety arguments to demonstrate good choice of materials. Specification and procurement of materials in accordance with the requirements of the ASME Code, Section II ensures that well-proven materials are chosen, and that the materials have good resistance to fracture and are of suitable chemical composition to limit the effect of through-life degradation mechanisms. OE provides further evidence to support the material choice.

The rules prescribed in ASME Code, Section III provide control of a diverse range of aspects of nuclear component construction. The applicable criteria and requirements of Section III are identified on the basis of the definition of various classes of SSCs for nuclear power plants. The ASME class applicable to components or subcomponents is identified in the safety arguments presented in Appendices 20D to 20K where it is necessary to define the applicable requirements of the ASME Code.

The ASME Code, Section III includes a requirement to conduct structural analyses to support the design for all conditions within the design basis. This supports the claim that the AP1000 components can fulfil their SFRs over the required period of service. Assessments are specified in each CSR to deterministically justify the structural integrity of AP1000 components against stress and fatigue limits established in the ASME Code, Section III. These assessments are based, in part, on a common set of RCS design transients. A summary of the RCS design transients and associated frequency of occurrence is presented in Table 20-22, as specified in Reference 20.3.

Other design aspects controlled by the requirements of ASME Code, Section III include mechanical testing to confirm material properties, manufacturing inspections to confirm the achievement of quality, and functional testing to confirm pressure boundary integrity. Welding procedures, testing of weld materials, and welder qualification are controlled by rules prescribed in ASME Code, Sections III and IX. The full range of design aspects

controlled by Section III of the Code is described in detail in the CSRs in a manner specifically applicable to the particular component.

The aspects of compliance with the ASME Code as summarised above provide a high level of confidence that the AP1000 plant components categorised as Standard Class 1 will enter service sufficiently free of defects so that their safety functions are not compromised. Assurance that the structural integrity of the Standard Class 1 components will be maintained throughout the design lifetime is provided by the in-service inspection (ISI) requirements prescribed in the ASME Code, Section XI. Like ASME Code, Section III, ISI requirements for the Standard Class 1 components are established in accordance with ASME classification. The planned programme of ISI for each Standard Class 1 component is identified in the CSRs on the basis of the requirements of the ASME Code Section XI, supplemented by requirements specified in the United States Code of Federal Requirements (CFR) 10 CFR 50.55a, as applicable. ISI constitutes the preferred means of providing forewarning of in-service failure for Standard Class 1 components, and this is supplemented by leak-monitoring and detection arrangements.

In the case of the MSLs and the RCL piping, supplemental mechanistic design requirements have been applied to improve reliability. The measures are applied where an improvement in reliability has an appreciable beneficial impact on plant safety, radiation exposure, and plant examination, maintenance, inspection, and testing (EMIT) obligations. These supplementary mechanistic design requirements, which are discussed in Reference 20.23, are included in the relevant CSRs as evidence of supplementary defence in depth, in addition to the robust demonstration of structural integrity provided by compliance with the ASME Code.

20.6.3 High Integrity Components

It is necessary for the structural integrity of the HI welds to be substantiated to a higher degree of rigour than that required for the Standard Class 1 components. When applicable, this is provided by a claim with evidence to demonstrate that these welds will be subject to appropriately qualified manufacturing inspections, supported by an elastic-plastic fracture assessment to demonstrate tolerance to all defects smaller than a QEDS by a size margin of two. In addition to the structural reliability justified by compliance with the ASME Code, these additional measures are claimed to support a degree of structural reliability commensurate with an HI classification. The role of defect tolerance assessments, in combination with qualified inspections, to support claims of a high degree of structural reliability are also important in the justification of HSS components, and described further in section 20.6.4.

20.6.4 Highest Safety Significance Components

Appendices 20A to 20C, respectively, provide justification of the structural reliability claimed for the following HSS components:

- RV
- Pressuriser
- SG secondary shell, tube sheet and channel head

The safety argument for each HSS component is presented according to a four-legged format well established in the UK for the safety justification of nuclear plant components that share similar structural reliability targets. The format of the safety argument follows that recommended by TAGSI (Reference 20.5). As noted previously, the approach for these passive mechanical components has been to substantiate structural integrity claims by

demonstrating sound engineering practice; in each of the four legs, diverse defence in depth measures are identified that, in combination, substantiate the structural reliability claimed for the HSS components. The four legs of the HSS arguments are as follows:

- Leg 1: Interpolation/extrapolation of experience – good design and manufacture
- Leg 2: Functional testing
- Leg 3: Failure analysis
- Leg 4: Forewarning of failure

In Appendices 20A to 20C, it is claimed that the four-legged safety arguments identify a suitable and sufficient diversity of evidence to demonstrate that their safety functions will not be compromised over the component lifetime. This is achieved through demonstration that the component will enter service free from defects of concern, that any manufacturing defect smaller than a QEDS will remain tolerable over the lifetime of the component, and the existence of defects that could compromise their safety function can be established through their life cycle. This is judged to substantiate the structural reliability claimed for the HSS components.

20.6.4.1 Good Design and Manufacture and Functional Testing

The first two legs of the safety argument provide evidence of high quality achieved through good design and manufacture, supplemented by functional testing to demonstrate fitness for purpose at the start of life. This forms a keystone for demonstrating high reliability and benefits from design code requirements and plant operating experience to achieve a high quality of build and the avoidance of defects. The basis for these claims is established, as a minimum, through compliance with relevant sections of the ASME Code. As such, legs 1 and 2 share many common features with the justification of Standard Class 1 components described in section 20.6.2.

Since the ASME requirements are identified as a minimum standard for all aspects of the design and construction of HSS components, additional measures are specified within these legs that exceed the requirements prescribed in the ASME Code. These supplementary requirements cover aspects such as chemical composition, mechanical testing of materials and heat treatment of components, and are specified in the relevant CSRs. Each HSS CSR specifies that manufacturing inspections for the HSS locations will be qualified in accordance with the European Network for Inspection Qualification (ENIQ) methodology (Reference 20.6). These qualified manufacturing inspections are specified in support of defect tolerance claims for the HSS locations. A procedure has been outlined (Reference 20.7) for the qualification of manufacturing nondestructive testing (NDT) for application to UK AP1000 manufacturing inspections. It establishes the qualification strategy (procedures, equipment, personnel), defines the link to defect tolerance analyses, and specifies the requirement for an independent qualification body. This procedure will also be applied to HI components in situations where small tolerable manufacturing defects need to be defended using targeted qualified NDT inspections (see section 20.6.3).

20.6.4.2 Failure Analysis

Leg 3 of the safety argument substantiates a claim that the HSS components are tolerant to through-life degradation over the design life of the plant. The demonstration of defect tolerance is an especially important element of a structural integrity safety case for components requiring the demonstration of high reliability (i.e., HSS and HI locations) because it is defect tolerance combined with effective manufacturing inspections that explicitly supports the argument that such components enter service free of structurally significant defects.

For Class 1 locations, design, manufacture and inspection in accordance with established codes and standards is considered sufficient. For Class 1 locations, defect tolerance is demonstrated by an assessment of through-life crack growth to show that such mechanisms will not threaten integrity over a specific interval. This assessment is based on the linear elastic fracture mechanics approach to the demonstration of non-ductile failure prescribed in Appendix G of ASME Code, Section III.

The assessment performed for Class 1 locations is performed as the base level of defect tolerance for HSS and HI locations. For HSS and HI locations, the demonstration of defect tolerance goes beyond ASME Code requirements to provide a further demonstration of integrity by acknowledging that flaws (smaller than a QEDS) may be present and demonstrating tolerance to them. This additional assessment is performed in accordance with the elastic-plastic fracture mechanics procedures specified in R6, Revision 4 (Reference 20.18). The R6 methodology is an accepted best practice within the UK nuclear industry. The R6 methodology differs from established US practice; and provides a complimentary demonstration of both defect avoidance and defect tolerance.

Where the defect tolerance is shown to be high, such that there is a large margin between the allowable SoL defect size and the QEDS, the requirements for inspection qualification may be straightforward to demonstrate. However, where this margin is small, robust qualification measures, as discussed in Section 20.6.4.1, will be applied in accordance with the ENIQ methodology to provide the necessary confidence regarding the absence of such defects.

In combination with the use of rigorous manufacturing controls and inspection qualification, the defect tolerance assessment provides the necessary understanding to support the claim, to an appropriate degree of confidence, that the specified component will enter service free from defects that could be of concern throughout the component's designed life. These measures, which exceed the requirements of ASME, provide the key argument that supports the claim that the gross failure of the specified component can be discounted during its operational life.

There are two important aspects to the defect tolerance assessment. Firstly, from the determination of the limiting defect size in a particular orientation and location, it is possible to apply reverse fatigue crack growth laws to determine the maximum allowable SoL defect size. This value is necessary to inform the NDT designers and qualification body of the required maximum QEDS. In many circumstances, depending upon the examination geometry and materials, it will be possible to support a smaller QEDS, thus representing margin in the defect tolerance assessment. Therefore, once the QEDS has been established, the second step is to evaluate the margin against the allowable SoL defect size. As has been stated in Reference 20.19, the regulatory expectation is that a defect size margin (DSM) of 2 will be achieved.

Reference 20.8 provides details of the assessment methodology and specifies input parameters to be used in the R6 analysis. The calculation steps are summarised as follows:

- Using transient stress data, calculate the lifetime fatigue crack growth (LFCG), considering an initial crack size equal to an assumed QEDS.

- Calculate the end of life limiting defect size (ELLDS) using the R6 methodology. The R6 approach includes consideration of both brittle and ductile failure as well as limit load failure of the net cross section.

- Verify the criterion in Equation (1), shown below, for a DSM of 2 and adjust the target QEDS if required.

$$QEDS + LFCG \leq \frac{ELLDS}{DSM}$$

Equation (1)

Reference 20.8 also provides the materials data required for the analyses (including tensile properties, fracture toughness data and fatigue crack growth rates for the applicable materials) as well as the required inputs in terms of postulated flaws, crack sizes for which detection is highly reliable, stress intensity factor solutions, plastic limit load solutions, treatment of weld residual stresses and the selection of the limiting loading combination for the ELLDS calculation. The LFCG and ELLDS calculations are initially performed using the aspect ratios (crack length to depth ratio) as determined from assumed detectable crack sizes given in Reference 20.8. In cases where this initially assumed QEDS gives rise to a DSM of less than 2, a new (smaller) target QEDS is defined as an output of the damage tolerance assessment such that a DSM greater than or equal to 2 is obtained.

A final definition of QEDS is thus established and adopted as a performance requirement for inspection qualification. The results of the defect tolerance assessments and the technical justification for qualification of inspection capability are discussed in the relevant appendices to demonstrate that a DSM of at least 2 can be justified for all of the assessed HSS and HI welds.

Supplementary testing detailed in Reference 20.24, which is above and beyond that which is prescribed by ASME, will be performed to underpin the fracture toughness values used as input to the defect tolerance assessments.

The full implementation of the R6 methodology to all identified HSS and HI locations within the plant requires extensive analysis. Completion of this work was precluded by timescales for the production of the safety case documents to support the generic design assessment (GDA) submissions. Therefore a phased implementation was agreed with the UK Regulator, whereby, at the end of GDA, sufficient information has been made available to provide confidence that there are no HSS or HI locations where either low defect tolerance or low NDT inspectability would preclude the component from being able to satisfy regulatory expectations and support the safety case claims for the UK AP1000 plant.

The GDA evaluation focused on weld regions (and the associated heat affected zones) since it is at these locations where it is most likely a structurally significant defect may be present. In the longer term, vulnerable locations in the parent material, such as nozzle crotch corners, will be included in the R6 assessment. Their exclusion at this stage is on the basis that they are bounded by the weld locations, which have an increased propensity for manufacturing defects to be introduced and hence have more onerous inspection requirements. In the interim, design and manufacture in accordance with established standards provides assurance high quality is achieved through the forging process.

The phases of implementation to support the GDA are as follows:

Phase 1: Weld Defect Tolerance and NDT Ranking

To evaluate those locations with the greatest risk of entering service with a defect of structural significance, either as a result of small allowable SoL defect sizes or a large QEDS, a ranking exercise was undertaken. The weld ranking involved screening and review of analyses produced per the ASME Code to establish a ranking of the welds based on their defect tolerance (e.g. primary stresses, fracture stress intensities and fatigue usage factors). The combination of this ranking with the NDT inspectability ranking (Reference 20.20) determined the final ranking of the weld locations. The details of this evaluation and the rationale behind the selection of the limiting locations are reported Reference 20.21.

Phase 2: Assessment of Bounding Locations

Of the welds identified in Phase 1, a limited number of locations were selected for more detailed demonstration of defect tolerance to support the GDA. For each of the selected locations, the R6 defect assessment methodology was used to determine the limiting SoL defect size. This work provides evidence that established NDT techniques are capable of screening out defects of structural significance. Quantitative arguments are presented in each HSS component CSR to show that de-selected regions are bounded by the locations selected for detailed assessment.

Phase 3: Assessment of Remaining Locations

The full defect tolerance assessment of the remaining HSS locations, including the selected locations in the parent material, will be carried out in due course. Once completed, the R6 assessment work will provide assurance that the QEDS is based on a robust assessment of the maximum allowable SoL defect size with appropriate consideration of materials ageing and degradation and through life crack growth.

The results for each of these phases of the defect tolerance evaluation performed to support the GDA are discussed in the relevant CSRs.

20.6.4.3 Forewarning of Failure

The fourth leg of the HSS safety argument establishes that effective systems are in place to provide forewarning of failure. These systems confirm the absence of unanticipated degradation mechanisms and also that known degradation mechanisms do not significantly compromise structural integrity. This provides a means of safely controlling anticipated component degradation and a contingency arrangement against the unexpected. ISI represents the preferred method for providing forewarning of failure, and ISI of the HSS locations is specified to be qualified in accordance with the ENIQ methodology. Surveillance, leak detection, and periodic leak testing are secondary, defence in depth measures to provide diversity in the arrangements that forewarn of structural failure.

20.6.4.3.1 Qualified In-Service Inspection of HSS Components

Implementation of a qualified ISI programme is the primary defence against failures in high energy systems. The inspection programmes for HSS components are qualified in line with the ENIQ methodology. The role of an effective ISI programme is to confirm the absence of any unknown degradation mechanisms and to confirm the known degradation mechanisms are not significant to integrity or will have limited consequences. ISI is used to confirm the absence of defects that could eventually lead to failure when the maximum tolerable defect

size (as determined using fracture mechanics as described in Section 20.6.4.2) is combined with a conservative assessment of in-service defect growth throughout the inspection interval.

In order to be effective, ISI requirements are identified according to established good practice and are determined relevant to the characteristics of each component and each inspection location. For the HSS locations on each of the components identified in section 20.6.4, the associated CSR (Appendices 20A, 20B and 20C) details the qualified ISI for the HSS locations relative to that component.

20.6.4.3.2 Leak Detection

The reactor coolant pressure boundary (RCPB) is monitored for leaks from the reactor coolant and associated systems by a variety of components located in multiple systems. The leak detection systems provide information that will prompt plant operators to take corrective action if any detected leakage exceeds the limits and conditions of the technical specifications. The leak detection system design incorporates good practice outlined in US NRC Regulatory Guide 1.45 (Reference 20.13). The system provides a means to detect and, to a limited extent, identify the source of the RCPB leakage.

Diverse measures including level, flow, and radioactivity measurements are provided to detect and monitor leakage from the RCPB. Per the UK categorisation and classification methodology detailed in section 5.2, the leakage detection is a Category C safety function in that leakage detection components monitor for the occurrence of, and alert personnel to take mitigating action following, an internal hazard event (RCPB break or leak). However, the safety classification for each of the systems and components used for leak detection is generally determined by the highest level requirements and functions of the system in which it is located. Section 9.2.1.7 of Reference 20.1 provides detailed information on the leakage detection measures.

Limits which satisfy position 9 of Regulatory Guide 1.45 for identified and unidentified reactor coolant leakage are identified in the generic technical specifications (Reference 20.14). Limiting conditions of operation are established to address RCS leakage (LCO 3.4.7), main steam line leakage (LCO 3.7.8), and leak detection instrumentation availability (LCO 3.4.9). If these limits are exceeded the plant is required to promptly shutdown to prevent propagation of the leak.

20.7 CONCLUSIONS

CSRs for AP1000 plant components are presented in Appendices 20A to 20K. These provide safety arguments to establish that the structural reliability of each component is commensurate with the consequences of gross failure. The AP1000 plant components addressed in this chapter are identified in Section 20.2.

SFRs have been identified for the components. These are to be maintained to ensure plant nuclear and radiological safety. Assurance that the SFRs will be maintained over the lifetime of the component is provided by substantiating structural integrity against qualitative reliability targets. These targets are based on a procedure of structural integrity classification, as described in Section 20.5. The components addressed have been variously ascribed structural integrity classifications of HSS, HI, and Standard Class 1. The safety arguments presented in each appendix are structured according to the structural integrity classification, as described in Section 20.6. The format applied to each level of classification ensures that the safety argument presented is robust and appropriate for justification of structural reliability commensurate with the consequences of gross failure of a particular component.

In Appendices 20A to 20K, it is concluded that the safety arguments presented identify a suitable and sufficient diversity of evidence to substantiate the structural integrity claimed for the AP1000 components addressed. Detailed substantiation of these claims is provided in the individual CSRs.

20.8 REFERENCES

20.1 Westinghouse Report APP-RCS-M3-001, Rev. 8, "Reactor Coolant System, System Specification Document," June 2015.

20.2 Westinghouse Report UKP-GW-GLR-004, Rev. 3, "UK AP1000 Structural Integrity Classification," January 2017.

20.3 Westinghouse Report APP-RCS-M1-001, Rev. 4, "Reactor Coolant System Design Transients, February 2013.

20.4 Not used.

20.5 Bullough, R., et. al, "The Demonstration of Incredibility of Failure in Structural Integrity Safety Cases," in *International Journal of Pressure Vessels and Piping 78*, pp 539–552, 2001.

20.6 ENIQ Report 31, "European Methodology for Qualification of Nondestructive Testing," Third Issue, European Network for Inspection and Qualification, August 2007.

20.7 Westinghouse Report WDI-PJF-2405360-TCR-002, Rev. 0, "Draft Procedure for the Manufacturing NDT Qualification Process Related to UK-Build AP1000 Plant," October 2010.

20.8 Westinghouse Report UKP-MV01-Z0R-101, Rev. 2, "Methodology and Input Data for the Application of the R6 Flaw Evaluation Procedure and Fatigue Crack Growth Analysis to the UK AP1000 Components," December 2016.

20.9 Westinghouse Report EPS-MP01-M2-001, Rev. C, "Design Specification for Wet Winding Reactor Coolant Pumps for System:RCS," February 2012.

20.10 "Reactor Coolant Pump Type *RUV* for Westinghouse Reactor AP1000," Rev. 0, KSB, November 2008.

20.11 Westinghouse Report UKP-GW-GL-022, Rev. 1, "AP1000 Probabilistic Risk Assessment," June 2016.

20.12 Not used.

20.13 Regulatory Guide 1.45, Rev. 0, "Reactor Coolant Pressure Boundary Leakage Detection Systems," US Nuclear Regulatory Commission.

20.14 Westinghouse Report UKP-GW-GL-501, Rev. 0, "AP1000® UK Generic Technical Specifications," January 2016.

20.15 Not used.

20.16 Not used.

20.17 WRCB 175 (Welding Research Council Bulletin 175), "PVRC Recommendations on Toughness Requirements for Ferritic Materials," August 1972.

20.18 R6, Rev. 4, "Assessment of the Integrity of Structures Containing Defects," British Energy Generation Ltd., 2007.

20.19 Report No. AR 09/013-P, "Nuclear Directorate Generic Design Assessment – New Civil Reactor Build, Step 3 Structural Integrity Assessment of the AP1000," Division 6 Assessment.

20.20 Westinghouse Report WDI-PJF-2405360-TCR-001, Rev. 1, "Results of the weld ranking process for the AP1000 Reactor Vessel, Steam Generator and Pressurizer – NDT Inspectability," (in response to GDA Step 4 Regulatory Observation R0-AP1000-19.A3), June 2010.

20.21 Westinghouse Report UKP-MV01-Z0R-100, Rev. 3, "Results of Weld Ranking Process for Reactor Vessel, Steam Generator, Pressurizer, Main Steam Line and Main Coolant Loop Piping," December 2015.

20.22 Westinghouse Report UKP-GW-GL-105, Rev. 1, "AP1000® Plant Review of UK Class 2 Structures, Systems and Components (SSCs)," August 2016.

20.23 Westinghouse Report UKP-GW-GLR-114, Rev. 1, "UK AP1000® Plant Internal Hazards Topic Report – Pressure Part Failure," January 2017.

20.24 Westinghouse Report UKP-GW-M0R-001, Rev. 0, "Additional Fracture Toughness Testing for the UK AP1000 Plant," January 2017.

20.25 Westinghouse Report UKP-GW-GLR-035, Rev. 0, "UK AP1000® Fuel Tolerability of Depressurisation of the Primary Circuit Assessment," August 2016.

20.26 Westinghouse Report UKP-GW-GL-107, Rev. 1, "AP1000® Plant Assessment of Impact from Reactor Coolant Pump Failure on Steam Generator Column Report," December 2016.

20.27 Westinghouse Report UKP-GW-GLR-108, Rev. 1, "UK AP1000 Internal Hazards Topic Report – Internal Missiles," January 2017.

Table 20-1. Component Integrity Safety Functional Requirements

Component	SFR	Description
Reactor vessel	20.1.1	The RV is required to provide the highest reliability pressure boundary to contain the primary coolant, heat-generating reactor core, and fuel fission products during normal and faulted design basis conditions for the design life of the plant.
	20.1.2	The RV is required to provide support for the reactor internals and core to ensure that the core remains in a coolable configuration.
	20.1.3	The RV is required to direct main coolant flow through the core by close interface with the reactor internals and flow skirt.
	20.1.4	The RV is required to provide for core internals location and alignment.
	20.1.5	The RV is required to provide support and alignment for the control rod drive mechanisms and in-core instrumentation assemblies.
	20.1.6	The RV is required to provide support and alignment for the integrated head assembly.
	20.1.7	The RV is required to provide an effective seal between the refuelling cavity and sump during refuelling operations.
	20.1.8	The RV is required to support and locate the main coolant loop piping.
	20.1.9	The RV is required to provide support for safety injection flow paths.
	20.1.10	The RV is required to serve as a heat exchanger during core meltdown scenario with water on the outside surface of the vessel.
Pressuriser	20.2.1	The pressuriser is required to maintain the integrity of the primary coolant pressure boundary during standby, normal operation, and under design basis faulted conditions for the design life of the plant.
	20.2.2	The pressuriser is required to provide the point in the RCS where system pressure is controlled during steady-state operations and transients, to ensure that minimum pressure requirements associated with core coolant boiling and departure from nucleate boiling (DNB) limits are maintained.
	20.2.3	The pressuriser is required to provide the controlled volume from which the level of reactor coolant can be measured.
	20.2.4	The pressuriser is required to contain the water volume used to maintain RCS volume in the event of a minor system leak for a reasonable time without replenishment.

Table 20-1. Component Integrity Safety Functional Requirements (cont.)

Component	SFR	Description
Steam generator	20.3.1	The SG pressure boundary is required to maintain the integrity of the primary and secondary coolant boundaries during standby, normal operation, and under design basis faulted conditions for the design life of the plant.
	20.3.2	The SG secondary side is required to provide a heat sink for the RCS during power operations and anticipated transients and under natural circulation conditions in accordance with component performance requirements (not required to provide safe shutdown of the plant).
Primary pipework	20.4.1	The pipework is required to maintain the integrity of the RCP during standby, normal operation, and under design basis faulted conditions for the design life of the plant.
	20.4.2	The pipework is required to exhibit leak behaviour in the event of a through-wall defect developing (defence in depth).
MSL	20.5.1	The MSL is required to maintain the integrity of the secondary coolant pressure boundary during standby, normal operation, and under design basis faulted conditions for the design life of the plant.
	20.5.2	MSLs are required to exhibit leak behaviour in the event of a through-wall defect developing (defence in depth).
	20.5.3	The pipework in the vicinity of the containment penetrations is required to maintain the integrity of the secondary coolant pressure boundary during standby, normal operation, and under design basis faulted conditions for the design life of the plant.
	20.5.4	The pipework in the vicinity of the containment penetrations above DN 50 is required to exhibit leak behaviour in the event of a through-wall defect developing (defence in depth).
PRHR HX	20.6.1	The PRHR HX is required to maintain the integrity of the primary coolant pressure boundary during standby, normal operation, and under design basis faulted conditions for the design life of the plant.
	20.6.2	The PRHR HX is required to remove core decay heat in accordance with the component performance requirements.
CMT	20.7.1	The CMT pressure boundary must remain intact during standby, normal operation, and under design basis faulted conditions for the design life of the plant.
	20.7.2	The CMT is required to store borated water under reactor coolant system pressure for high-pressure reactor coolant makeup in accordance with the component performance requirements.
	20.7.3	The CMT is required to deliver borated water to the RCS in the event of a loss-of-coolant accident (LOCA) or non-LOCA when the normal makeup system is unavailable or insufficient.

Table 20-1. Component Integrity Safety Functional Requirements (cont.)

Component	SFR	Description
Accumulator	20.8.1	The accumulator tanks' pressure boundary must remain intact during standby, normal operation, and under design basis faulted conditions for the design life of the plant.
	20.8.2	The two accumulators are required to store borated water and a compressed nitrogen cover gas to provide rapid injection of borated makeup water to the RCS in the event of a large LOCA.
	20.8.3	The accumulator tanks are required to deliver a large volume of borated water to the RV at a high flow rate in the event of a LOCA in accordance with the component performance requirements.
CV	20.9.1	The CV is required to provide a leaktight barrier against the uncontrolled release of radioactivity to the environment under postulated accident conditions for the design life of the plant to assure that the containment design conditions important to safety are not exceeded for as long as postulated accident conditions require and to retain coolant inventory in the event of a LOCA.
	20.9.2	The CV is required, along with the shield building, to provide shielding for the reactor core and the reactor coolant system during normal operations.
	20.9.3	The CV is required to provide core residual heat removal during postulated accidents when active cooling is not available.
	20.9.4	The CV is required to act as a support for the polar crane at all times, including normal and faulted conditions, including seismic events.
RV internals	20.10.1	The RV internals are required to support, orient, and guide the core components, namely the in-core instrument thimble assembly (IITA), fuel assemblies, and rod cluster control assemblies (RCCAs) during standby, normal operation, and under design basis faulted conditions for the design life of the plant.
	20.10.2	The RV internals are required to direct the main coolant flow to and from the fuel assemblies and convey cooling water to the core for a postulated LOCA.
	20.10.3	The RV Internals are required to absorb control rod dynamic loads, fuel assembly loads, and other loads, and transmit these loads to the RV.
	20.10.4	The RV internals are required to provide protection for the RV against excessive irradiation exposure from the core.
	20.10.5	The RV internals are required to position and support RV irradiation capsule assemblies.
RCP casing	20.11.1	The RCP casing is required to maintain the integrity of the primary coolant pressure boundary during standby, normal operation, and under design basis faulted conditions for the design life of the plant.
	20.11.2	The RCP casing is required to retain missile fragments arising from a disruptive failure of the RCP flywheel without gross failure of the RCS pressure boundary.

Table 20-2. Component Structural Integrity Classification

Classification	Available Mitigation	Consequence
HSS	No protection	Severe damage to reactor core and large offsite release of radioactivity.
HI	At least one line of protection, without redundancy.	Severe damage to reactor core. Some protection against large offsite release. Limited release of radioactive material.
Standard Class 1 SSCs	At least one line of protection, with redundancy.	Localised fuel melt or damage to fuel. Minor release of radioactive material offsite. Release of significant quantities of radioactive material within nuclear island.
Standard Class 2 or 3 SSCs	At least two lines of protection, with diversity.	No core damage. Fault within capability of protection systems. Contamination within nuclear island.

Table 20-3. Detailed Assessment for Classification of the Reactor Vessel and Closure Head

Postulated Failure Modes	Disruptive failure of the RV, fragmentation of the pressure boundary, generation of missiles.

Introduction

The scope of the RV review included the assessment of the consequences arising from the failure of the RV body, including the nozzles and nozzle safe-ends, closure head, up to the CRDM penetration housing tubes and the bolting arrangements. Postulated failure modes were conservatively assumed to be disruptive, i.e., no credit has been given to the inherent ductility of the materials used in the manufacture of the RV and closure head. The review considered the direct consequences arising from gross failure of the RV pressure boundary, as well as the indirect effects, such as the effect of missiles on the operability of essential safety systems in the RV compartment, in adjacent compartments and within the CV.

Unmitigated Direct Failure Consequences

Gross failure of the RV has the potential to result in the most severe consequences, that is, severe core damage arising from disruption to core assembly, loss of coolant inventory, and loss of coolable core geometry. Other possible consequences include loss of core support or control rod alignment, or control rod withdrawal leading to potential reactivity addition.

Indirect Failure Consequences

The large energy release due to catastrophic RV failure could result in RV cavity structural damage and containment over-pressurisation.

The rupture of passive core cooling injection piping, delayed floodup and cooling of core would lead to increased core damage.

Missiles can cause consequential damage to:

i) RV sensors and core flux sensors.

ii) Possible containment damage and possible large offsite dose release.

Lines of Protection

There is no claimed protection against gross failure of the RV. Partial protection is provided by:

i) RV compartment and biological shield structure provides some protection against most missile damage.

ii) RV cavity is still flooded by coolant loss, and passive core cooling system (PXS) operation can restore core cooling even with failed lower RV.

iii) RV closure head bolts evaluated to show that single bolt failure does not cause RV/head separation.

Discussion

The direct consequences arising from a postulated gross failure of the RV are, in the worst case, assumed not to be protectable; it is, therefore, assumed that core damage would occur. The effects of postulated missiles and the overpressurisation of the CV introduce the possibility of large offsite release. In accordance with the methodology, an HSS classification has been assigned to gross failure of the RV.

While the RV compartment structure may withstand RV failure, promote long-term cooling of fuel, and protect against significant offsite release, this has not been analysed and consequently no credit has been claimed.

Table 20-4. Detailed Assessment for Classification of the SG Secondary Shell

Postulated Failure Modes	Disruptive failure of the SG secondary shell. Fragmentation of the pressure boundary, generation of missiles.
Introduction In applying the classification methodology to the SG, the secondary shell, channel head, and tube sheet were considered separately because of differences in the consequences of failure. The scope of the secondary shell review included the assessment of the consequences arising from the postulated failure of the secondary shell, including the steam and feedwater nozzles, up to but not including the pipe welds, and the manway. Postulated failure modes were conservatively assumed to be disruptive, i.e., no credit has been given to the inherent ductility of the materials used in the manufacture of the SG shell. The review considered the direct consequences arising from gross failure of the pressure boundary, as well as the indirect effects, such as the effect of missiles on the operability of essential safety systems in the SG compartment, in adjacent compartments and the CV.	
Unmitigated Direct Failure Consequences The gross failure of the SG secondary shell is a severe transient that is beyond the analysed main steam line break (MSLB) assumed within the design basis, and takes credit from the flow restrictor in the main steam nozzle. It is, therefore, assumed that the direct consequences could lead to violation of core thermal limits (core damage) and pressurisation of the containment above its design pressure.	
Indirect Failure Consequences Disruptive failure of the secondary shell could lead to consequential damage to tube bundle and so result in a large unisolable primary LOCA. The LOCA would be bounded by a double-ended guillotine break (DEGB) of the primary loop, which is protectable, but a simultaneous secondary and primary break in the containment is beyond the design basis and is, therefore, assumed to be unprotectable. The high-energy release rate or generation of high-energy missiles from shell fragments introduces the possibility for a loss of containment integrity, resulting in a release of activity outside containment. Damage to containment would not prevent the passive protection systems from core cooling but the release rate from loss of containment integrity would be increased.	
Lines of Protection Large LOCA protection is provided by passive protection systems. SG compartment provides significant protection against missiles generated within the SG compartment, although it is recognised that this barrier does not extend to the full height of the SG steam drum. It is conservatively assumed that no mitigation exists.	
Discussion A gross failure of the SG shell is outside the AP1000 design basis and so has conservatively been assumed not to be protectable. The high-energy release rate and associated containment demand and direct pathway for missiles to impact the CV means that containment integrity cannot be ensured, introducing the possibility of large offsite release. In accordance with the methodology, gross failure of the SG secondary shell has been classified as HSS.	

Table 20-5. Detailed Assessment for Classification of the SG Channel Head

Postulated Failure Modes	Disruptive failure of the SG channel head. Fragmentation of the pressure boundary, generation of missiles.
Introduction The scope of the SG channel head review included the assessment of the consequences arising from the postulated failure of the channel head pressure boundary, including the inlet and outlet nozzles (including safe ends/buttering). The inlet nozzle safe end to pipe weld was outside the scope of the assessment, but the outlet nozzle to RCP weld was considered as part of this review. Postulated failure modes were conservatively assumed to be disruptive, i.e., no credit has been given to the inherent ductility of the materials used in the manufacture of the SG channel head. The review considered the direct consequences arising from gross failure of the pressure boundary, as well as the indirect effects, such as the effect of missiles on the operability of essential safety systems in the SG compartment, in adjacent compartments and the CV.	
Unmitigated Direct Failure Consequences Gross failure of the channel head would result in a large unisolable LOCA. This would be bounded by a DEGB of the primary loop, included within the large break LOCA safety analysis (section 9.6.4), which includes a range of LOCAs up to and including a break equivalent in size to the double-ended rupture of the largest pipe in the RCS. The failure described here would, therefore, be protectable without violating the acceptance criteria on core thermal limits in section 9.6.4.1.	

Table 20-5. Detailed Assessment for Classification of the SG Channel Head (cont.)

Indirect Failure Consequences

Loss of SG Support

A disruptive failure of the channel head could cause the SG support to fail, leading to collapse of the SG onto the RCPs. This event has not been analysed and so has conservatively been assumed to lead to a simultaneous steam line break with possible pressurisation of the containment above its design pressure.

Missiles

The postulated initiating event assumes that the channel head will fail in a disruptive manner, leading to the generation of energetic missiles. The channel head is located at the lower end of the SG, down low in the SG compartment. These compartments are constructed of thick steel/concrete/steel modules. Although the resulting missiles would be more energetic than those analysed in the AP1000 design basis (section 16.7.5.3), judgementally, it is considered that the module walls would act as a barrier, preventing energetic missiles from escaping outside the boundary of the compartment and so threatening containment integrity. It is recognised that the SG compartment is open to the containment volume at its upper end; however, given the location of the channel head, the potential for an energetic fragment to travel up the space between the SG secondary shell and the SG compartment wall was considered so low as to be discounted.

Blast/Jet Loading/Compartment and Containment Pressurisation

A disruptive failure of the channel head would result in jet loading from blowdown of the RCS and internal pressurisation of the SG compartment. A disruptive failure of the channel head would be beyond the design basis in terms of jet loading and compartment pressurisation. Nonetheless, on a best-estimate basis, it is judged that this failure would not lead to the most severe offsite consequences. The containment integrity analysis considers, as its design basis, the complete double-ended severance of the largest RCS pipe (Section 9D) and hence containment integrity would not be challenged by this postulated break.

Pipe Whip

Disruptive failure of the channel head would result in a loss of support to the hot leg and RCP in the casualty loop. An evaluation of the dynamic effects of a guillotine break in this location has not yet been performed. Best-estimate judgment is that the shield wall between the RV and SG compartments would provide support for the cold leg and that, due to the short distance between the wall and the SG, pipe whip is unlikely. In the absence of a deterministic assessment to support this, the effects of pipe whip hinging at the compartment wall were evaluated using the 3-D model. Based on this, it was concluded that further escalation of the consequences as a result of pipe whip would not occur.

Flooding/Spray

Flooding of the SG compartment is within the design basis.

Lines of Protection

Large LOCA protection is provided by passive protection systems.

SG compartment provides significant protection against missiles generated within the SG compartment.

Table 20-5. Detailed Assessment for Classification of the SG Channel Head (cont.)

Discussion
The direct consequences arising from a gross failure of the SG channel head is within the AP1000 plant design basis and would, therefore, be considered protectable. Furthermore, the indirect consequences arising from missiles or pipe whip have been assessed and discounted as not being credible. However, due to a lack of evidence to evaluate the effect of the postulated channel head failure on the integrity of the SG support column (attached to the channel head), it has conservatively been assumed that this would lead to intolerable consequences. In accordance with the methodology, gross failure of the SG channel head (including the SG-to-RCP weld) has been classified as HSS.

Table 20-6. Detailed Assessment for Classification of the SG Tube Sheet

Postulated Failure Modes	Disruptive failure of the SG tube sheet. Fragmentation of the primary to secondary pressure boundary, generation of missiles.

Introduction

As the boundary between the primary and secondary systems, the consequences arising from a postulated gross failure of the tube sheet are specific to this failure mode. As a result, the tube sheet was assessed separately. Postulated failure modes were conservatively assumed to be disruptive, i.e., no credit has been given to the inherent ductility of the materials used in the manufacture of the tube sheet. The review considered the direct consequences arising from gross failure of the pressure boundary, as well as the indirect effects, such as the effect of overpressurisation of the secondary shell or the effects of resulting missiles on the operability of essential safety systems in the SG compartment, in adjacent compartments and the CV.

Unmitigated Direct Failure Consequences

The direct consequences arising from gross failure of the tube sheet would lead to a large primary to secondary LOCA, the direct consequences of which would be bounded by a DEGB of the primary loop, included in the large-break LOCA safety analysis for the AP1000 plant (section 9.6.4). This includes a range of LOCAs up to and including a break equivalent in size to the double-ended rupture of the largest pipe in the RCS. The LOCA analyses consider the limiting single failure. The direct consequences of the primary to secondary LOCA would, therefore, be protectable without violating the acceptance criteria on core thermal limits in section 9.6.4.1.

Indirect Failure Consequences

The review of the indirect consequences identified that the tube sheet failure and associated primary to secondary leak would open and may lead to a stuck-open SG safety valve(s) and result in direct release of primary coolant into the containment. Furthermore, a large tube sheet failure could damage or fail the secondary side pressure boundary, resulting in a simultaneous primary and secondary break, an unanalysed and beyond design basis transient. In the absence of a more detailed analysis, it has been conservatively assumed that the resulting containment overpressurisation and/or high-energy missile generation from failure of the SG shell could result in damage or loss of containment boundary. Damage to containment would not prevent the passive safety systems from providing core cooling but the rate of release of radioactivity due to loss of containment integrity would be increased.

Lines of Protection

Large primary to secondary LOCA protection is provided by passive protection systems.

SG compartment provides significant protection against missiles. Missile protection is provided for lower portion of the secondary shell only.

Discussion

The direct consequences arising from a gross failure of the SG tube sheet is within the AP1000 design basis and is, therefore, protectable; however, a large primary to secondary LOCA could fail the secondary side pressure boundary leading to a simultaneous primary and secondary break, an unanalysed transient, conservatively assumed to lead to core damage and overpressurisation of the containment with possible offsite release. In accordance with the methodology, a HSS classification has therefore been assigned to gross failure of the SG tube sheet.

Table 20-7. Detailed Assessment for Classification of the Pressuriser

Postulated Failure Modes	Disruptive failure of the pressuriser. Fragmentation of the pressure boundary, generation of missiles.
Introduction The scope of the pressuriser review included the assessment of the consequences arising from the postulated failure of the pressuriser shell and nozzles, up to but not including the safe end to pipe welds. Postulated failure modes were conservatively assumed to be disruptive, i.e., no credit has been given to the inherent ductility of the materials used in the manufacture of the pressuriser. The review considered the direct consequences arising from gross failure of the pressure boundary, as well as the indirect effects, such as the effect of missiles on the operability of essential safety systems in the pressuriser compartment, in adjacent compartments and the CV.	
Unmitigated Direct Failure Consequences A postulated gross failure of the pressuriser would result in an unisolable large LOCA. The leak rate would be limited by surge line diameter, and is included within the large-break LOCA safety analysis (section 9.6.4), which includes a range of LOCAs up to and including a break equivalent in size to the double-ended rupture of the largest pipe in the RCS. The analysis includes consideration of the limiting single failure. The direct consequences of the pressuriser failure would, therefore, be protectable without violating the acceptance criteria on core thermal limits in section 9.6.4.1.	

Table 20-7. Detailed Assessment for Classification of the Pressuriser (cont.)

Indirect Failure Consequences

Missiles

It is conservatively assumed that the pressuriser shell fails in a disruptive manner, leading to the generation of energetic missiles. The pressuriser is located in the pressuriser upper and lower compartments, constructed of thick steel/concrete/steel modules. Although the resulting missiles would be more energetic than those analysed within the AP1000 design basis (section 16.7.5.3), judgementally it is considered that the module walls would act as a barrier, preventing energetic missiles from escaping outside the boundary of the compartment and so threatening containment integrity or the operability of essential safety systems in adjacent compartments. It is recognised, however, that the pressuriser compartment is open at the top and so high-energy missile generation could impact and damage the containment shell. Damage to containment would not prevent the passive safety systems from core cooling but the release rate due to loss of containment integrity would be increased.

Blast/Jet Loading/Compartment & Containment Pressurisation

A disruptive failure of the pressuriser would result in jet loading and internal pressurisation of the pressuriser upper and lower compartments. Failure of the pressuriser within the scope of pressure part failure is not deemed credible because the pressuriser is fitted with safety valves (Reference 20.23). A disruptive failure of the pressuriser would, therefore, be beyond the design basis in terms of jet loading and compartment pressurisation. Nonetheless, on a best-estimate basis, it is judged that this indirect failure mode would not lead to the most severe offsite consequences. The containment integrity analysis considers the complete double-ended severance of the largest RCS pipe (Section 9D) and hence containment integrity would not be challenged by this postulated break.

Pipe Whip

Disruptive failure of the pressuriser would result in a loss of support to the surge line. The pipe whip effects of a surge line failure were judged in Table 17 of Reference 20.23 to be consistent with those of a reactor coolant loop pipe impacting the module wall. Pipe whip resulting from a reactor coolant line break has been determined to not result in unacceptable consequences. As such, it is concluded that further escalation of the consequences as a result of a surge line pipe whip would not occur.

Flooding/Spray

Flooding of the pressuriser compartment is within the design basis.

Lines of Protection

Direct consequences of a pressuriser LOCA are mitigated by passive protection systems.

The pressuriser is mostly located within its own structural compartment, which would absorb a significant proportion of the energy and missiles that could affect other systems.

Discussion

The direct consequences arising from a gross failure of the pressuriser is within the AP1000 design basis and is therefore protectable. Although the pressuriser is mostly located within its own structural compartment, which would absorb a significant proportion of the energy and missiles that could affect other safety systems, the pressuriser compartment is open at the top and hence a postulated circumferential failure of the shell could result in ejection of the pressuriser fragments from the compartment, which could challenge containment. Under such circumstances, it has been conservatively assumed that the effectiveness of core cooling could be degraded, leading to core damage and offsite release. In accordance with the methodology, gross failure of the pressuriser has been classified as HSS.

Table 20-8. Detailed Assessment for Classification of the RCP

Postulated Failure Modes	Disruptive failure of the RCP casing pressure boundary resulting in fragmentation of the casing. Disruptive failure of the flywheel leading to the generation of high-energy missile fragments.
Introduction The scope of the RCP review includes the failure of the RCP pressure boundary and the rotating parts of the RCP internals, including the flywheel. Failure modes were conservatively assumed to be disruptive, i.e., no credit has been given to the inherent ductility of the materials used in the manufacture of the RCP casing and flywheel. The welds connecting the RCP to the loop pipework and the RCP to SG channel head welds were not considered as part of this review as they are considered part of the pipework and SG assessment respectively. The review considered the direct consequences arising from gross failure of the RCP casing pressure boundary, and the effect of missiles on the operability of essential safety systems in the SG compartment and in adjacent compartments.	
Unmitigated Direct Failure Consequences The direct consequences arising from gross failure of the RCP casing will be bounded by a DEGB of the cold leg and is included within the large-break LOCA safety analysis (section 9.6.4) for the AP1000 plant, which includes a range of LOCAs up to and including a break equivalent in size to the double-ended rupture of the largest pipe in the RCS. The analysis has been performed using the WCOBRA/TRAC code, a best-estimate thermal-hydraulic computer code used to calculate realistic fluid conditions in the PWR during blowdown and reflood of postulated large-break LOCAs. The direct consequences of the RCP failure would, therefore, be protectable without violating the acceptance criteria on core thermal limits in section 9.6.4.1. The design specification for the RCP (Reference 20.9, Section 3.2.4.2) requires demonstration that the pump casing can contain fragments arising from disintegration of the RCP flywheel. A scoping assessment to substantiate this claim is presented in Reference 20.10. Appendix 20F presents the structured argument supporting the integrity of the RCP and cites the relevant evidentiary documentation.	

Table 20-8. Detailed Assessment for Classification of the RCP (cont.)

Indirect Failure Consequences

Missiles

The postulated initiating event assumes that the pump casing will fail in a disruptive manner, leading to the generation of energetic missiles. In reviewing the indirect consequences of this failure mode, the potential for indirect effects to lead to more severe consequences were considered, in this case, leading to intolerable offsite consequences (i.e., resulting in a possible HSS classification). RCPs are located directly beneath the SGs within the SG compartments. These compartments are constructed of thick steel/concrete/steel modules. Although the resulting missiles would be more energetic that those analysed within the AP1000 design basis (section 16.7.5.3), judgementally it is considered that the module walls would act as a barrier, preventing energetic missiles from escaping outside the boundary of the compartment and so threatening containment integrity. It is recognised that the SG compartment is open to the containment volume at its upper level; however, given the location of the pumps, the potential for an energetic fragment to travel up the space between the SG compartment and the SG was considered so low as to be discounted. Consideration was given to the potential for missile fragments from the RCP casing to lead to a disruptive failure of the SG channel head or secondary shell, which would in itself attract a HSS classification. Although no impact analysis has been presented relating to the impact on the channel head, the consequences of this would be bounded by the guillotine break of the loop. A missile penetrating the tube sheet (784 mm / 30.9 in) was discounted as incredible. The assumption of two consecutive disruptive failures, the second of which is postulated to breach the containment boundary, is considered out with the methodology and hence was dismissed.

Consideration was also given to the possibility that a missile from the RCP casing would lead to failure of the SG support. Analysis has been performed which demonstrates that core cooling would be maintained in the unlikely event that the vertical support should fail (Reference 20.26).

Blast/Jet Loading/Compartment and Containment Pressurisation

A disruptive failure of the RCP would result in jet loading from blowdown of the RCS and internal pressurisation of the SG compartment. Failure of the RCP within the scope of pressure part failure is not deemed credible because the pressuriser is fitted with safety valves (Reference 20.23). A disruptive failure of the RCP would, therefore, be beyond the design basis in terms of jet loading and compartment pressurisation. Nonetheless, on a best-estimate basis, it is judged that this failure would not undermine the operability of the passive protection systems so meriting a higher classification. The containment integrity analysis considers, as its design basis, the complete double-ended severance of the largest RCS pipe (Section 9D), and hence containment integrity would not be challenged by this postulated break.

Pipe Whip

Disruptive failure of the RCP casing would result in a loss of support to the cold leg in the casualty loop. Reference 20.23 concludes that pipe whip of the cold leg does not propagate a failure to other systems, does not result in unacceptable loading conditions on claimed barrier and does not adversely affect the required safety functions for mitigation of the postulated failure. Based on this, it was concluded that further escalation of the consequences as a result of pipe whip would not occur.

Flooding/Spray

Flooding of the SG compartment is within the design basis.

Core Depressurization Forces

The core depressurization forces resulting from a gross failure of the RCP case would be less limiting those resulting from a gross failure of a cold leg. A detailed evaluation of the gross failure of a cold leg (Reference 20.25) has demonstrated that grid crush may occur in low power peripheral assemblies, however, the core geometry would remain coolable. As a result, significant core damage is not expected.

Table 20-8. Detailed Assessment for Classification of the RCP (cont.)

Lines of Protection i) The RCP casing provides protection against missiles arising from RCP internals. ii) The SG compartment structure will prevent missiles damaging the containment. iii) The containment structure will remain intact and prevent large offsite release.
Discussion The direct consequences arising from a postulated gross failure of the RCP would be bounded by a DEGB break of the cold leg. This postulated fault is within the design basis and it has, therefore, been concluded that this would not lead to severe core damage. Consideration of indirect consequences concludes that there were no effects that could escalate the consequences leading to core damage or offsite release. According to the methodology, a Standard Class 1 classification has been assigned to the RCP casing. Failure of the flywheel is also within the design basis and so has also been assigned a Standard Class 1 classification.

Table 20-9. Detailed Assessment for Classification of the Reactor Coolant Loop Hot and Cold Legs (RV Safe End to Loop Welds)

Postulated Failure Modes	Guillotine break of a primary loop hot or cold leg to RV safe end weld.

Introduction

The review considered a postulated guillotine break occurring at the weld between the RV nozzle safe ends and the attached hot and cold leg primary loop pipework. The assessment assumes a DEGB of the pipe and also considers the risk from pipe whip, flooding, and pressurisation of the RV compartment.

Unmitigated Direct Failure Consequences

Guillotine failure of the primary loop pipework is included within the AP1000 design basis and can be protected by the passive safety systems without significant fuel damage or containment overpressurisation. The failure would result in a large unisolable LOCA. The large-break LOCA safety analysis for the AP1000 plant (section 9.6.4) includes a range of LOCAs up to and including a break equivalent in size to the double-ended rupture of the largest pipe in the RCS. The analysis has been performed using the WCOBRA/TRAC code, a best-estimate thermal-hydraulic computer code used to calculate realistic fluid conditions in the PWR during blowdown and reflood of a postulated large-break LOCA. This analysis includes the effects of a rapid depressurisation of the primary loop. The postulated failure described here would, therefore, be protectable without violating the acceptance criteria on core thermal limits in section 9.6.4.1.

Indirect Failure Consequences

The indirect failure consequences associated with RCS coolant loop failure in the RPV nozzle area is the subject of Case 1 presented in Section C.5 of Reference 20.23. Below is a summary of the conclusions presented relative to pipe whip, jet impingement, asymmetric pressurisation and subcompartment pressurisation.

Therein it is determined that pipe whip of the cold leg does not propagate a failure to other systems, does not result in unacceptable loading conditions on claimed barrier and does not adversely affect the required safety functions for mitigation of the postulated failure. The effects of asymmetric pressurisation were included in the evaluation of the loading conditions.

With respect to jet impingement, the RV supports are expected to exceed minimum elastic stress allowable limits but remain functional as a result of the failure; i.e., minor deformation will likely occur. Additionally, the RV and the remainder of the RCS are adequately restrained and remain intact. The direct vessel injection (DVI) lines are susceptible to high stresses outside of Room 11205; however, their injection ability is not compromised using conservative linear modelling techniques. Therefore, it was concluded that jet impingement following a failure of the RCS cold leg will not adversely affect the plant safety case as the post-failure RCS conditions and Class 1 injection capability is retained.

The gross failure of a RCS cold leg will result in significant pressurisation of Room 11205 which is expected to challenge the availability and operation of Class 1 SSCs; however, the consequential failure of these SSCs is consistent with the plant safety case and the analysis of the direct effects of a large break LOCA event.

The containment integrity analysis considers the complete double-ended severance of the largest RCS pipe (Section 9D), and hence containment integrity would not be challenged by this postulated break.

Depressurisation of the reactor vessel coupled with thrust from the pipe break and asymmetric reactor cavity pressurisation hold the potential to damage the fuel. A detailed evaluation of the scenario (Reference 20.25) has demonstrated that grid crush may occur in low power peripheral assemblies, however, the core geometry would remain coolable. As a result, significant core damage is not expected.

Table 20-9. Detailed Assessment for Classification of the Reactor Coolant Loop Hot and Cold Legs (RV Safe End to Loop Welds) (cont.)

Lines of Protection i) Passive core and containment cooling systems. ii) Biological shield wall offering restraint against pipe whip. iii) Minimisation of number of welds.
Discussion A guillotine failure of the primary loop piping is included within the design basis and can be protected by the passive safety systems. A deterministic evaluation of this transient has been undertaken to substantiate this. In relation to the indirect consequences such as pipe whip, missile, blast, and compartment, a deterministic evaluation of the dynamic effects arising from a guillotine break of the large bore pipework has also been undertaken. Based on consideration of the anticipated effects of a postulated pipe break, it has been concluded that significant core damage is not anticipated. In accordance with the methodology, the welds joining the RV safe ends to the primary loop have been classified as **Standard Class 1**.

Table 20-10. Detailed Assessment for Classification of the Reactor Coolant Loop Hot and Cold Legs (Loop to SG/RCP Welds)

Postulated Failure Modes	Guillotine break of a primary loop hot leg to SG channel head or cold leg to RCP weld.

Introduction

The review considered a postulated guillotine break occurring at the weld between the SG channel head nozzle safe ends and the attached primary loop hot leg pipe work and the RCP to primary loop cold leg welds. The assessment assumes a DEGB of the pipe and also considers the risk from pipe whip, flooding, and pressurisation of the SG compartment.

Unmitigated Direct Failure Consequences

Guillotine failure of the primary loop pipework is included within the AP1000 design basis and can be protected by the passive safety systems without significant fuel damage or containment overpressurisation. The failure would result in a large unisolable LOCA. The large-break LOCA safety analysis for the AP1000 plant (section 9.6.4) includes a range of LOCAs up to and including a break equivalent in size to the double-ended rupture of the largest pipe in the RCS. The analysis has been performed using the WCOBRA/TRAC code, a best-estimate thermal-hydraulic computer code used to calculate realistic fluid conditions in the PWR during blowdown and reflood of postulated large-break LOCAs. This analysis includes the effects of a rapid depressurisation of the primary loop. The postulated failure described here would, therefore, be protectable without violating the acceptance criteria on core thermal limits in section 9.6.4.1.

Indirect Failure Consequences

The indirect failure consequences associated with RCS coolant loop failure at the SG/RCP are enveloped by the consequences associated with a failure occurring at the RPV nozzles as indicated in Table 17 of Reference 20.23. Additionally, based on the expert review undertaken in support of SI classification the following conclusions were reached.

The potential for pipe whip to occur from a failure at the SG/RCP side of the hot and cold legs is considered low, limited by the relatively short lengths of pipe available to whip due to the small distances between the RV compartment outer wall and the SG. In the absence of a deterministic pipe whip assessment, however, pipe whip was conservatively assumed to occur with a hinge occurring at the penetration through the RV compartment wall. The consequences were assessed using the AP1000 plant 3-D model. The steel/concrete/steel construct of the module wall was considered to provide protection from dynamic effects to essential systems outside the compartment. The only aspect of the PXS in the SG compartment was identified as the PXS sump screens in the east compartment. A more detailed evaluation of this concluded that downward whip of east hot leg would be limited by interference between the bottom-mounted RCS to normal residual heat removal system (RNS) suction nozzle and pipe (DN 500 (nominal pipe size (NPS)) 20) and the RV compartment wall. This is judged to prevent impact damage to the PXS sump screens.

Whip impingement on the SG support column was not considered credible because of its position relative to the RCPs.

The core depressurization forces resulting from a gross failure of a hot or cold leg at the SG/RCP would be less limiting than those resulting from a gross failure of a cold leg at the reactor vessel. A detailed evaluation of the gross failure of a cold leg (Reference 20.25) has demonstrated that grid crush may occur in low power peripheral assemblies, however, the core geometry would remain coolable. As a result, significant core damage is not expected.

Table 20-10. Detailed Assessment for Classification of the Reactor Coolant Loop Hot and Cold Legs (Loop to SG/RCP Welds) (cont.)

Lines of Protection i) Passive core and containment cooling systems. ii) Biological shield wall offering restraint against pipe whip. iii) Minimisation of number of welds.
Discussion A guillotine failure of the primary loop piping is included within the design basis and can be protected by the passive safety systems. A deterministic evaluation of this transient has been undertaken to substantiate this. In relation to the indirect consequences such as pipe whip, missile, blast, and compartment, an equivalent deterministic evaluation of the dynamic effects arising from a guillotine break of the large bore pipework has not been undertaken since the consequences are anticipated to be enveloped by those of a failure of a reactor coolant line at the RPV. Based on consideration of the anticipated effects of a postulated pipe break, it was concluded that pipe whip, although unlikely, cannot be dismissed. Considering the effects of whip in more detail using the 3-D model, however, it was concluded that whip would not compromise the effectiveness of passive protection systems and hence core damage would be mitigated. Best judgment was that the thick module walls would prevent consequential effects outside the casualty SG compartment. In accordance with the methodology, the welds joining the primary loop hot and cold legs to the RCP and SG channel head have been evaluated as Standard Class 1.

Table 20-11. Detailed Assessment for Classification of the CMT

Postulated Failure Modes	Disruptive failure of the CMT. Fragmentation of the pressure boundary, generation of missiles.

Introduction

The scope of the CMT review included the assessment of the consequences arising from the postulated gross failure of the CMT pressure boundary, including the inlet and outlet nozzles. Postulated failure modes were conservatively assumed to be disruptive, i.e., no credit has been given to the inherent ductility of the materials used in the manufacture of the CMT. The review considered the direct consequences arising from gross failure of the pressure boundary, as well as the indirect effects, such as the effect of missiles on the operability of essential safety systems adjacent to the CMTs and the CV.

Unmitigated Direct Failure Consequences

The CMT is not isolated during normal operation and is at loop pressure but ambient temperature. The LOCA caused by a gross failure of a CMT is limited by the cold leg balance line. This LOCA is analysed and shown not to lead to core damage and is within the design basis. Loss of a CMT is bounded by the postulated failure of either of the DVI lines, which is included within the AP1000 design basis and can be protected by the passive safety systems. Section 9.6.5 describes the small-break LOCA analyses, including the DVI line break. The small-break LOCA analyses show that the performance of the AP1000 plant design in small-break LOCA scenarios is excellent and that the passive safeguards systems in the AP1000 design are sufficient to mitigate LOCAs. The analyses demonstrate that cladding temperatures will remain near the coolant saturation temperature, well below the peak cladding temperature acceptance criterion in section 9.6.5.0.

The isolation for a failed CMT does not have single-failure protection and so the LOCA is assumed to be unisolable but the break is small enough to prevent the core from becoming uncovered.

Indirect Failure Consequences

Missiles/Blast

Failure of the CMT within the scope of pressure part failure is not deemed credible because the pressuriser is fitted with safety valves (Reference 20.23). It is conservatively assumed that the CMT shell fails in a disruptive manner, leading to the generation of missiles. Such a failure is outside the AP1000 design basis and so the consequences of missile damage have not been analysed using deterministic approaches. The best judgment is that the energy of these missiles will be limited by the low temperature of the makeup tank inventory. Nonetheless, because of the proximity of the CMTs to the CV, along with their size and operating pressure, it is conservatively assumed that damage to the containment could occur. On the basis of best-estimate analyses performed in support of the probabilistic safety assessment (PSA) (Reference 20.11, Chapter 4), damage to containment (i.e., failure to achieve containment isolation) would not prevent the passive protection systems from maintaining core cooling but release rate due to loss of containment integrity would be increased.

The potential for missile damage to Category 1 control and instrumentation (C&I) cables was also identified; however, it was concluded that this damage would not prevent the redundant train of affected safety system equipment from operating properly.

Table 20-11. Detailed Assessment for Classification of the CMT (cont.)

Lines of Protection The LOCA caused by gross failure of the PXS CMT is bounded by the more limiting DVI line failure, which has been analysed and shown not to lead to core damage. Containment cooling with damaged containment has been analysed and results show that CV pressure is reduced to and maintained near atmospheric pressure. Also, CMT failure cannot impact the containment below elevation 102.1 m (107 ft), thus, the mass loss from CV does not deplete the water inventory inside containment quickly.
Discussion A disruptive failure of the CMT would result in a LOCA limited in diameter to the DN 200 (NPS 8) cold leg balance line. This failure is bounded by the DVI line break and so can be protected by the passive safety systems. A deterministic evaluation of this transient has been undertaken to substantiate this. A disruptive failure of a CMT is not considered as part of the AP1000 design approach and hence there has been no deterministic evaluation of the effects of missiles. Because of the proximity of the CMT to the CV, it has been conservatively assumed that damage to the containment could occur. On the basis of best-estimate analyses performed in support of the PSA (Reference 20.11, Chapter 4), damage to containment would not prevent the passive protection systems from maintaining core cooling. In accordance with the methodology, the CMT has been evaluated as Standard Class 1.

Table 20-12. Detailed Assessment for Classification of the Accumulator

Postulated Failure Modes	Disruptive failure of the Accumulator. Fragmentation of the pressure boundary, generation of missiles.

Introduction

The accumulators contain cold borated water with a 4.83 MPa (700 psig) nitrogen overpressure injected into the RV through the DVI nozzles in the event of falling loop pressure. The scope of the accumulator review included the assessment of the consequences arising from the postulated gross failure of the accumulator pressure boundary. Postulated failure modes were conservatively assumed to be disruptive, i.e., no credit has been given to the inherent ductility of the materials used in the manufacture of the accumulator. The review considered the direct consequences arising from gross failure of the pressure boundary, as well as the indirect effects, such as the effect of missiles on the operability of essential safety systems within the accumulator compartments and in adjacent compartments.

Unmitigated Direct Failure Consequences

Gross failure of the accumulator will not lead to LOCA due to the check valves on injection line. Isolation is achieved through two tilt disk-type check valves that will close quickly in the event of reverse flow. Nonetheless, if these valves failed to shut or were damaged by the accumulator failure, the LOCA would be bounded by the postulated failure of either of the DVI lines, which is included within the AP1000 design basis and can be protected by the passive safety systems. Section 9.6.5 describes the small-break LOCA analyses, including the DVI line break. The small-break LOCA analyses show that the performance of the AP1000 plant design to small-break LOCA scenarios is excellent and that the passive safeguards systems in the AP1000 plant are sufficient to mitigate LOCAs. The analyses demonstrate that cladding temperatures will remain near the coolant saturation temperature, well below the peak cladding temperature acceptance criterion in section 9.6.5.0.

Indirect Failure Consequences

Missiles/Blast

Failure of the accumulator within the scope of pressure part failure is not deemed credible because the pressuriser is fitted with safety valves (Reference 20.23). It is conservatively assumed that the accumulator shell fails in a disruptive manner, leading to the generation of missiles. Such a failure is outside the AP1000 design basis and so the consequences of missile damage have not been analysed using deterministic approaches. The best judgment is that the resulting energy of these missiles will be restricted by the low temperature of the makeup inventory (ambient) and comparably low overpressure of 4.38 MPa (700 psig). On the basis of expert judgment, it is considered that the steel/concrete/steel structures of the accumulator compartment (wall thickness between 76 and 137 cm (30 and 54 inches) and floor thickness of 61 cm (24 inches)) would prevent missile and blast damage to essential safety systems in adjacent compartments. This judgement is based on a deterministic evaluation of the missile withstand for the nuclear island structures. The compartment walls surrounding the accumulator are structurally similar in design to the nuclear island for which deterministic impact analysis is completed. Failure may lead to damage of other passive core cooling components within the accumulator compartment but will not affect the redundant train of the PXS.

A review of 3-D models confirms that failure of the accumulator would not lead to missile damage to the hot leg to RNS suction line and isolation valves in the adjacent area.

Table 20-12. Detailed Assessment for Classification of the Accumulator (cont.)

Lines of Protection The accumulators are isolated from the RCS by two series check valves. The accumulators are situated within protected compartments that would contain this energy and would not lead to consequential damage to the containment, RCS components, or redundant train PXS components. Failure is within the plant design basis.
Discussion The LOCA resulting from a failure of an accumulator would be expected to be isolated by virtue of the two flap-type check valves. In the event that these are made ineffective by the initiating failure, the resulting LOCA would be bounded by the DVI line break and so be protected by the passive safety systems. A deterministic evaluation of the DVI line break substantiated the claim such breaks would be protected by the passive safety systems (section 9.6.5). A disruptive failure of an accumulator is not considered as part of the AP1000 design approach and hence there has been no deterministic evaluation of the effects of missiles; however, the accumulators are located within their own compartments and judgmentally, it is believed that the steel/concrete/steel module walls would prevent secondary damage to essential systems in adjacent compartments and to the CV. A review of the 3-D model were undertaken to identify potentially vulnerable systems and none were identified. In accordance with the methodology, the accumulator has been evaluated as Standard Class 1.

Table 20-13. Detailed Assessment for Classification of the PRHR HX

Postulated Failure Modes	Gross failure of the headers or tube assembly.
Introduction The PRHR HX provides core residual heat removal during postulated non-LOCA events where SG heat removal is not available or is insufficient. The component consists of an HX and inlet and outlet lines connected to the RCS. The systems is normally pressurised at loop pressure. The scope of the PRHR HX review included the assessment of the consequences arising from the postulated gross failure of the pressure boundary, including the inlet and outlet channel headers and the tube assembly. Postulated failure modes were conservatively assumed to be disruptive, i.e., no credit has been given to the inherent ductility of the materials used in the manufacture of the PRHR HX tubes or headers. The review considered the direct consequences arising from gross failure of the pressure boundary, as well as the indirect effects, such as the effect of missiles on the operability of essential safety systems within the in-containment refuelling water storage tank (IRWST) and in adjacent spaces.	
Unmitigated Direct Failure Consequences The direct consequences of failure of the PRHR HX will be equivalent to the guillotine failure of one of the PRHR HX lines. This is included within the AP1000 design basis and can be protected by the passive safety systems. Although the failure would be isolable, it is assumed that isolation cannot be achieved since there is no single-failure protection. This LOCA would be bounded by a DEGB of the primary loop, included within the AP1000 large-break LOCA safety analysis (section 9.6.4), which includes a range of LOCAs up to and including a break equivalent in size to the double-ended rupture of the largest pipe in the RCS. The failure described here would, therefore, be protectable without violating the acceptance criteria on core thermal limits in section 9.6.4.1. It should be noted that the loss of the decay heat removal function is not a concern in the case of the large LOCA where rejection of heat is achieved through the LOCA itself rather than via the PRHR HX.	
Indirect Failure Consequences Failure of the PRHR HX within the scope of pressure part failure is not deemed credible because the pressuriser is fitted with safety valves (Reference 20.23). Additionally, risk of consequential damage due to a failure of the PRHR HX tubing is considered to be small because of the location of the HX in the IRWST. As discussed in Table 20-21, an evaluation of indirect consequences resulting from the failure of a PRHR return line has concluded that failure of the PRHR HX outlet plenum is not anticipated. This event is discussed further in Section 20G.3.2.	
Lines of Protection i) PXS and PCS ii) The passive safety injection system would not be damaged as a result of a PRHR failure.	
Discussion A gross failure of the PRHR HX is included within the design basis and can be protected by the passive safety systems. Indirect consequences have been evaluated and it is considered that these would not be significant because of the submerged position of the HX. In accordance with the methodology, the PRHR HX has been evaluated as Standard Class 1.	

Table 20-14. Detailed Assessment for Classification of the RV Lower Internals Core Barrel and Lower Core Support Plate (Core Support Structure)

Postulated Failure Modes	Circumferential failure of a core barrel weld.

Introduction

The RV internals (RVI) provide the appropriate guidance, protection, alignment, and support for the core and control rods to enable safe and reliable reactor operation. Although the RVI do not have a pressure boundary function, the review considered the potential effects arising from failure of any of the major welds, in this case on the core barrel or barrel flange, and the potential for vertical displacement of the RVI and the subsequent implications in terms of control of reactivity or maintaining core cooling.

Unmitigated Direct Failure Consequences

Failure of core barrel weld would result in the downward displacement of the core and core support plate. Through the radial clevis supports and the secondary core support structure (designed to mitigate a postulated core drop event), however, this vertical displacement would be limited and as such would not lead to an intolerable increase in reactivity or loss of coolant flow. A hypothetical core drop accident has been analysed to ensure that engagement of the fuel alignment pins and control rods is maintained, and impact load to the RV is minimised. Details of this analysis are provided in Appendix 20A. The criteria for the postulated core drop accident are based on analyses that determine the total downward displacement of the internal structures, following a hypothetical core drop resulting from loss of the normal core barrel supports. The initial clearance between the secondary core support structures and the RV lower head in the hot condition is approximately 1.27 cm (0.5 inch).
An additional displacement of approximately 1.52 cm (0.6 inch) would occur from the strain of the energy-absorbing devices of the secondary core support. Therefore, the total drop distance is about 2.79 cm (1.1 inches). That distance is less than the distance that permits the tips of the RCCA to come out of the guide thimble in the fuel assemblies. The secondary core support is only required to function during an accident involving the hypothetical catastrophic failure of core support (such as core barrel or barrel flange). There are four supports in each reactor. This structure limits the fall of the core and absorbs much of the energy of the fall, which otherwise would be imparted to the vessel.

Indirect Failure Consequences

Since the RVI are not part of the pressure-retaining boundary, indirect consequences as described in this methodology are not directly applicable because there is little stored energy to lead to secondary effects such as missiles or blast. The effects on reactivity and flow conditions are considered as direct effects.

Lines of Protection

Secondary core support structure limits downward movement of the core such that control rod insertion capability is maintained as follows:

- RCCAs do not disengage from guide tubes in the fuel assemblies.
- Fuel assembly upper guide pins do not disengage from the upper core support plate.
- Radial keys in the RV bottom head maintain alignment of the lower core support plate with the RV axial centreline.
- Limited downward movement ensures that adequate core flow (cooling) is maintained.

Discussion

Failure of a core barrel circumferential weld will only result in an allowable vertical displacement of the lower RVI and the core on account of the secondary core support structure and radial clevis supports. Consequently, coolant flow and control rod insertion will be retained. On this basis, the RVI have been categorised as Standard Class 1 components.

Table 20-15. Detailed Assessment for Classification of the RV Upper Internals

Postulated Failure Modes	Gross failure of weld in upper internals.
Introduction The RVI provide the appropriate guidance, protection, alignment, and support for the core and control rods to enable safe and reliable reactor operation. Although the RVI do not have a pressure boundary function, the review considered the potential effects arising from failure of any of the major welds, specifically the potential for vertical displacement of the RVI and the subsequent implications in terms of control of reactivity or maintaining core cooling.	
Unmitigated Direct Failure Consequences There is a potential for disruption to internal flow, leading to fuel damage or inability to insert control rods. Consequences are limited because of the design of the upper internal structures.	
Indirect Failure Consequences Since the RVI are not part of the pressure-retaining boundary, indirect consequences as described in this methodology are not directly applicable because there is little stored energy to lead to secondary effects such as missiles or blast. The effects on reactivity and flow conditions are considered as direct effects.	
Lines of Protection Upper internals are supported by a flanged barrel that is independent of the core barrel. Upper internals' supporting structure is sandwiched between fuel assemblies (springs) and RV head closure flange such that weld failure will not result in movement. Stuck RCCA assumption in safety analyses covers any local failures of RCCA guides.	
Discussion The review concluded that the direct consequences of gross failure of the upper RVI would be the potential for either disruption to internal flow leading to fuel damage or an inability to insert control rods. As the upper RVI are supported by an independent flange to the core barrel and have their supporting structure sandwiched between the (spring-loaded) upper core plate and the RV closure head, however, there will be no significant displacement as a result of a failure of an upper support assembly circumferential weld. In addition, evaluation demonstrates that even with the highest-worth control rod assembly stuck in the fully withdrawn position, the necessary shutdown margin (with combined use of chemical shimming) is maintained during long-term xenon decay and plant cooldown, thus accounting for any local failures of the RCCA guides. On the basis, the RVI have been categorised as Standard Class 1 components.	

Table 20-16. Detailed Assessment for Classification of the MSLs Inside Containment

Postulated Failure Modes	Guillotine break of the MSL inside containment.
Introduction The review considered a DEGB of an MSL inside containment. Consideration was given to the direct consequences in terms of the effect of the transient on the thermal-hydraulic conditions and reactivity control. The review also considered the indirect consequences arising from pipe whip, jet spray and flooding. Flow restrictors are installed in the SG outlet nozzle as an integral part of the SG. The effective throat area of the nozzles is 0.13 m^2 (1.4 ft^2), which is considerably less than the main steam pipe area; thus, the flow restrictors serve to limit the maximum steam flow for a break at any location.	
Unmitigated Direct Failure Consequences With respect to maintaining specified, acceptable fuel design limits and radiological consequences, a DEGB of the MSL inside containment is bounded by a DEGB outside containment. A failure of the MSL (MSLB) outside the containment vessel is analysed at hot zero power (section 9.1.5) and at full power (section 9.1.6) to demonstrate the event can be mitigated without core damage. The limiting break size is dependent on the transient conditions as detailed in each section. Both core analyses conservatively model the hypothetical core configuration (that is, stuck RCCA, nonuniform inlet temperatures, pressure, flow, and boron concentration) and directly evaluate the total reactivity feedback including power, boron, and density redistribution in an integral fashion. The effect of void formation is also included. The MSLB analyses show no DNB occurs for the MSL rupture assuming the most reactive RCCA is stuck in its fully withdrawn position. With respect to containment integrity, an analysis of the peak containment pressure incurred due to a MSLB inside containment is provided in Section 9D.3. The results are summarised in Table 9D.1-1. The containment pressure response is shown in Figure 9D.1-1. These analyses take consideration of a single failure of one of the three valves available for delivery of passive containment cooling water flow as well as failure of the main steam isolation valve (MSIV) in the faulted loop. The availability of ac power is assumed to maximise the mass and energy releases to containment. The containment pressure is maintained within acceptable limits following a DEGB of the MSL inside containment.	

Table 20-16. Detailed Assessment for Classification of the MSLs Inside Containment (cont.)

Indirect Failure Consequences As indicated in Reference 20.23, the main steam line is piping with supplemental mechanistic design requirements but was not selected as a supplemental gross failure scenario for GDA. There is, therefore, a potential for pipe whip since the pipe supports are not designed to prevent it. Based on the expert review undertaken in support of SI classification, the following conclusions were reached: The review, based on detailed interrogation of a 3-D model, indicates that damage to containment as a result of pipe whip is not credible if the main steam line retains its curvature. Any straightening out of the steam line is likely to result in impact with the containment and potential jet spray damage; therefore, a breach of containment could not be ruled out. Damage to containment would not prevent the passive protection systems from core cooling; but the release rate from loss of containment integrity would be increased. There exists the potential for the loss of one group (half) of the automatic depressurisation system (ADS) Stages 1, 2, and 3 valves as a result of pipe whip affecting safety-related conduit. However, as described in section 9.1.5.2.3, the ADS is not actuated during a MSLB event. Additionally, best estimate probabilistic safety analysis (Chapter 6, Reference 20.11) further demonstrates a loss of one group of ADS Stages 1, 2, 3 is acceptable in this scenario. Steam generator movement as a result of pipe whip could not be ruled out. There may be some twisting and bending, but significant failure (SG falling off vertical support, for example) is not expected. It is not considered feasible that the casualty line could rupture the non-casualty MSL, leading to a double MSLB, as the geometry does not allow for this. The valves included in these lines have been designed to prevent missiles as discussed in Reference 20.27.
Lines of Protection The following functions provide the protection for a steam line rupture that is within design basis and is protectable: i) CMT actuation. ii) The overpower reactor trips (neutron flux and DT) and the reactor trip occurring in conjunction with receipt of the “S” signal. iii) Redundant isolation of the main feedwater lines. iv) Redundant isolation of the startup feedwater system. v) Fast-acting MSL isolation valves. vii) Flow restrictors in the SG outlet nozzle.
Discussion The consideration of a guillotine failure is considered to be a very conservative assessment. The direct consequences arising from a guillotine break of the MSL are within the AP1000 design basis and are therefore protectable. In relation to the indirect consequences, however, an equivalent deterministic evaluation of the dynamic effects arising from a guillotine break of the MSL has not been undertaken. Based on consideration of the anticipated effects of a postulated pipe break, it was concluded that pipe whip, although unlikely, cannot be dismissed because pipe whip restraints are not included in the design. The review concluded that pipe whip impinging on the containment could not be ruled out and hence it has conservatively been assumed that a breach of the containment boundary could occur. However, no core damage is anticipated to occur. In accordance with the methodology, a Standard Class 1 classification has been assigned to a DEGB of an MSL inside containment.

Table 20-17. Detailed Assessment for Classification of the MSL and Main Feedwater Line in MSIV Compartment

Postulated Failure Modes	Guillotine break of the MSL or main feedwater line in the main steam isolation valve (MSIV) compartment.

Introduction

The review considered a DEGB of main steam and feedwater lines outside containment within the MSIV compartment and upstream of the MSIV. Consideration was given to the direct consequences in terms of the effect of the transient on the thermal-hydraulic conditions and reactivity control. The review also considered the direct and indirect consequences arising from compartment pressurisation, pipe whip, and flooding. Flow restrictors are installed in the SG outlet nozzle as an integral part of the SG. The effective throat area of the nozzles is 0.13 m^2 (1.4 ft^2), which is considerably less than the main steam pipe area; thus, the flow restrictors serve to limit the maximum steam flow for a break at any location. The main steam and feedwater lines inside the MSIV compartment are described as break exclusion zone piping, primarily because of their proximity to the main control room (MCR) and the potential for leakage outside containment, resulting in the application of standards that exceed ASME requirements for Class 3 pipework.

Unmitigated Direct Failure Consequences

As with the MSLs inside containment, a guillotine break of the MSL is analysed within the design basis and is protectable without core damage. The MSLB is analysed at hot zero power (section 9.1.5) and at full power (section 9.1.6) to demonstrate the event can be mitigated without core damage. The limiting break size is dependent on the transient conditions as detailed in each section.

Both core analyses conservatively model the hypothetical core configuration (that is, stuck RCCA, nonuniform inlet temperatures, pressure, flow, and boron concentration) and directly evaluate the total reactivity feedback including power, boron, and density redistribution in an integral fashion. The effect of void formation is also included.

The analyses show that no DNB occurs for the MSL rupture assuming the most reactive RCCA is stuck in its fully withdrawn position.

Indirect Failure Consequences

Supplemental analysis Case 3 of Reference 20.23 reflects the gross failure of a main steam or main feedwater line in the main steam isolation valve B compartment. The space was selected by the expert panel based on the magnitude of the mass and energy release rate and the close proximity of the compartment to vital areas of the plant including the MCR and the Class 1 C&I spaces. The MSIV A Compartment is larger and does not have the same layout constraints as those identified for the MSIV B Compartment. The following is a summary of the indirect failure consequences determined for Case 3 of Reference 20.23:

A review concluded that the main steam lines do not pose a pipe whip concern and the reaction of the main feedwater line poses a risk of structural impact to the floor and east wall of the respective MSIV compartment. The initial plant response to the postulated main feedwater pipe whip was considered unacceptable and remedial actions were applied. After applying these measures it was concluded that the effects of pipe whip within the MSIV B compartment resulting from the gross failure of a main steam or main feedwater line do not result in unacceptable loading conditions on claimed barriers, and do not adversely affect the required safety functions for mitigation of the associated plant-level event.

With respect to jet impingement, it has been concluded that the failure of either the main steam or main feedwater line in the MSIV B compartment will not adversely affect the plant safety case as the pipes are adequately restrained or experience limited displacement such that the resulting jet effects are reduced.

The MSIV compartments do not contain SSCs that are sufficiently large such that the time required for the pressure wave to travel from the break point to the opposite side of the SSC could result in significant differential pressures; therefore, asymmetric pressurisation is not a concern.

The gross failure of a main steam or main feedwater line in the MSIV B compartment will result in significant pressurisation of the compartment but will not affect the barriers claimed for protection of the operators and Class 1 C&I equipment. Therefore, the plant response to these postulated failures are consistent with the plant safety case.

The valves included in these lines have been designed to prevent missiles as discussed in Reference 20.27.

Lines of Protection

The following functions provide the protection for a steam line rupture that is within design as is and is protectable:

i) CMT actuation.

ii) The overpower reactor trips (neutron flux and temperature differential) and the reactor trip occurring in conjunction with receipt of the “S” signal.

iii) Redundant isolation of the main feedwater lines.

iv) Redundant isolation of the startup feedwater system.

v) Fast-acting MSL isolation valves.

vi) Flow restrictors in the SG outlet nozzle.

Further mitigation is provided by the following:

i) Whip restraints and jet barriers in the MSIV B compartment.

Discussion

A guillotine failure of a MSL outside containment is included within the design basis and can be protected by the passive safety systems. Indirect consequences have been reviewed and shown not to escalate the consequences of failure. In accordance with the methodology, the MSLs outside containment have been evaluated as Standard Class 1.

The evaluation of the main feedwater line is bounded by the MSL.

Table 20-18. Detailed Assessment for Classification of the DVI Line

Postulated Failure Modes	Guillotine break of a DVI line, including failure of the RV DVI nozzle safe end to pipe weld.

Introduction

The review considered a DEGB of one of the DVI lines that inject makeup water directly into the core in the event of a LOCA, so maintaining core cooling. The review considered the direct consequences in terms of the degraded core cooling as well as the indirect consequences arising from pipe whip, jet spray, and flooding.

Unmitigated Direct Failure Consequences

Guillotine failure of either of the DVI lines is included within the AP1000 design basis and can be protected by the passive safety systems. Section 9.6.5 describes the small-break LOCA, including the DVI line break. The small-break LOCA analyses described in the referenced section show that the performance of the AP1000 plant design to small-break LOCA scenarios is excellent and that the passive safeguards systems in the AP1000 design are sufficient to mitigate LOCAs.

The DVI line break analyses evaluate the ability of the plant to recover from a moderately sized break with only half of the total emergency core cooling system capacity available. The vessel side of the break of the DVI line break is DN 100 (NPS 4). The double-ended nature of this break means that in effect, two breaks are modelled as follows:

- Downcomer to containment. The DVI nozzle includes a venturi, which limits the available break area.
- DVI line into containment from the cold leg balance line and the broken-loop CMT.

A sensitivity case was also performed to assess the effect of higher than expected entrainment in the upper plenum and hot legs on the overall system response and core cooling.

The analyses demonstrate that cladding temperatures will remain near the coolant saturation temperature, well below the peak cladding temperature acceptance criterion in section 9.6.5.0.

Indirect Failure Consequences

The gross failure of a DVI line in the PXS A compartment was evaluated as Case 2 of Reference 20.23. The PXS A Room was chosen as it is a smaller compartment volumetrically and therefore is anticipated to yield a greater magnitude of subcompartment pressurisation. Furthermore, the complement of Class 1 SSCs between the PXS rooms differs only by the RNS isolation valves, which are located in an adjoining room to the PXS B room, and do not have an active response to the postulated event of full pressure DVI line rupture. The consequences presented in Reference 20.23 are summarized as follows.

The analysis of the piping response to the reaction loads caused by the gross failure of the DVI A line will cause a pipe whip. Pipe impact with the IRWST injection squib valve (PXS-V125A) will occur which is assumed to incapacitate the Class 1 SSC. The consequential loss of the IRWST injection or containment recirculation squib valve function in the PXS compartment is acceptable in the supplemental case and consistent with the plant safety case. A secondary hinge was formed by the impact of the DVI line against the IRWST injection discharge line, however, the propagation criteria do not result in a gross failure of the IRWST injection discharge line. The specific failure analyzed did not result in an impact to a structure; however, based on the assessment performed to support Case 1 of Reference 20.23, the pipe whip load potential of a DN 200 (NPS 8) pipe is well within the loads applied to containment internal structures by a 55.88 cm (22 in) diameter coolant line and therefore there is sufficient confidence to conclude that PXS compartment barriers are adequate for the spectrum of DVI line failures that can be postulated.

As the upstream piping does not form a plastic hinge, the direction of the jet flow is unaffected by pipe movement. Also, as the upstream side is a non-expanding liquid jet, the resulting zone of influence is effectively reduced to line of sight. The potential targets for this jet are the low pressure IRWST injection and containment recirculation piping. These forces should be considered in the pipe analysis; however, based on the fluid velocity and range it was been concluded that other design effects are more limiting for Class 1 piping analysis; i.e., safe shutdown seismic load combinations. The downstream side piping is subject to dynamic motion and will result in an expanding jet with an unrestrained zone of influence opposed to the thrust vector on the free end of the pipe. Affected components include the Accumulator and various instrumentation lines. Since the initiating event is a loss of injection capability into the reactor vessel, the function of the Accumulator and its associated piping is not accounted for in the safety analysis. Additionally, the incidental instrument lines were considered in the discussion of failure propagation and were not considered to be a risk to the performance of the Class 1 SSCs required to respond to a DVI line break in the PXS A room. Therefore, it was concluded that the jet impingement effects resulting from the failure of the DVI A line in the PXS A room would not adversely affect the plant safety case as the required Class 1 injection capability is retained in this case.

Components within the PXS rooms are not considered for asymmetric pressurisation due to their size and the resulting pressurisation rate of the volume; i.e., transient pressurisation of the compartment does not occur fast enough compared to the velocity of the pressure wave to create an appreciable differential pressure.

The gross failure of DVI A line will result in pressurisation of PXS A compartment; however, the communication between PXS A compartment and the Containment has been shown to be adequate to limit the dynamic differential pressure across structural barriers to a reasonable value. Therefore, the integrity of the room and the claimed barriers is consistent with the plant safety case and the analysis of the direct effects of a DVI line break event.

The valves included in these lines have been designed to prevent missiles as discussed in Reference 20.27.

The core depressurization forces resulting from a gross failure of a DVI line would be less limiting than those resulting from a gross failure of a cold leg. A detailed evaluation of the gross failure of a cold leg (Reference 20.25) has demonstrated that grid crush may occur in low power peripheral assemblies, however, the core geometry would remain coolable. As a result, significant core damage is not expected.

Table 20-18. Detailed Assessment for Classification of the DVI Line (cont.)

Lines of Protection PXS. Containment.
Discussion A guillotine failure of a DVI line is included within the design basis and can be protected by the passive safety systems. Indirect consequences have been shown not to escalate the consequences of failure. In accordance with the methodology, the DVI lines have been evaluated as Standard Class 1.

Table 20-19. Detailed Assessment for Classification of the Pressuriser Surge Line

Postulated Failure Modes	Guillotine break of the surge line.
Introduction The review considered a guillotine break of pressuriser surge line. The assessment assumes a DEGB of the pipe and also considers the risk from pipe whip, flooding, and pressurisation of the lower pressuriser compartment and SG compartment 01.	
Unmitigated Direct Failure Consequences Guillotine failure of the pressuriser surge line is included within the AP1000 design basis and can be protected by the passive safety systems without significant fuel damage or containment overpressurisation. The failure would result in a large unisolable LOCA. The AP1000 large-break LOCA safety analysis (section 9.6.4) includes a range of LOCAs up to and including a break equivalent in size to the double-ended rupture of the largest pipe in the RCS. The analysis has been performed using the WCOBRA/TRAC code, a best-estimate thermal-hydraulic computer code used to calculate realistic fluid conditions in the PWR during blowdown and reflood of postulated large-break LOCAs. This analysis includes the effects of a rapid depressurisation of the primary loop. The postulated failure described here would, therefore, be protectable without violating the acceptance criteria on core thermal limits in section 9.6.4.1.	
Indirect Failure Consequences As indicated in Reference 20.23, the surge line is piping with supplemental mechanistic design requirements but was not selected as a supplemental gross failure scenario for GDA. Based on the expert review undertaken in support of SI classification, it was concluded that in the unlikely event of a DEGB of the pressuriser surge line, the resulting dynamic effects would not compromise the integrity of the passive safety systems or containment; damage would be contained within the thick steel/concrete/steel module walls of the lower pressuriser compartment and SG compartment 1. It is judged that the DEGB failure of the surge line cannot create a large missile out of the pressuriser.	
Lines of Protection Passive safety systems. Containment.	
Discussion A guillotine failure of the pressuriser surge line is included within the design basis and can be protected by the passive safety systems. Indirect consequences have been evaluated and it is considered that these would not lead to escalated consequences of failure. In accordance with the methodology, the pressuriser surge line has been evaluated as Standard Class 1.	

Table 20-20. Detailed Assessment for Classification of the ADS Piping and Safety Valve Piping

Postulated Failure Modes	Guillotine break of one of the automatic depressurisation system (ADS) pipes.
Introduction Failure of one of the ADS lines is included within the small-break LOCA safety design approach for the AP1000 plant. The approach is to provide for a controlled depressurisation of the primary system if the break cannot be terminated. The controlled depressurisation is required to ensure that the passive protection systems initiate. The assessment assumes a DEGB of one of the lines and also considers the risk from pipe whip and flooding.	
Unmitigated Direct Failure Consequences Guillotine failure of the any of the ADS lines is included within the AP1000 design basis and can be protected by the passive safety systems. Section 9.6.5 describes the small-break LOCA, including the more limiting inadvertent actuation of the ADS. The small-break LOCA analyses described in the referenced section show that the performance of the AP1000 plant design to small-break LOCA scenarios is excellent and that the passive safeguards systems in the AP1000 are sufficient to mitigate LOCAs. A break within the ADS does not, therefore, impair its function to depressurise the RCS.	
Indirect Failure Consequences As indicated in Reference 20.23, the ADS piping is piping with supplemental mechanistic design requirements but was not selected as a supplemental gross failure scenario for GDA Based on the expert review performed in support of SI classification, it was concluded that in the unlikely event of a DEGB of one of the larger-diameter lines not protected by pipe whip restraints, the resulting dynamic effects would not compromise the ability of the passive protection systems to protect the core by virtue of the plant layout and the physical separation of the different sides of the PXS. Pipe whip arising from failure of ADS pipework would therefore not compromise integrity of passive safety systems. The review identified that, in light of the exposed location of the upper ADS valve area, there was the remote potential for a missile impact that damages containment and would result in larger release rates. But the containment cooling with damaged containment has been analysed and shown to effectively reduce the CV pressure to near atmospheric pressure without compromising its effectiveness. The potential for flooding to prevent correct operation of the passive protection systems was considered and discounted. Section 11.3 describes how the AP1000 plant is designed to withstand internal flooding events due to pipe breaks. The valves included in these lines have been designed to prevent missiles as discussed in Reference 20.27.	
Lines of Protection Passive safety systems. Containment	
Discussion A guillotine failure of an ADS line is included within the design basis and can be protected by the passive safety systems. Indirect consequences have been shown not to escalate the consequences of failure. In accordance with the methodology, the ADS pipework has been evaluated as Standard Class 1.	

Table 20-21. Detailed Assessment for Classification of the PRHR HX Inlet and Return Lines

Postulated Failure Modes	Guillotine break of either inlet or return lines
Introduction The PRHR HX inlet and return lines form part of the PXS, which removes decay heat in the event of a loss of normal residual heat removal. The review considered a guillotine break of either of the pipes during normal operation or standby. The assessment assumes a DEGB of one of the lines and also considers the risk from pipe whip and flooding.	
Unmitigated Direct Failure Consequences Guillotine failure of the any of the PRHR HX lines is included within the AP1000 design basis and can be protected by the passive safety systems. The failure would result in a large unisolable LOCA. This would be bounded by a DEGB of the primary loop, included within the AP1000 large-break LOCA safety analysis (section 9.6.4), which includes a range of LOCAs up to and including a break equivalent in size to the double-ended rupture of the largest pipe in the RCS. The failure described here would therefore be protectable without violating the acceptance criteria on core thermal limits in section 9.6.4.1. It should be noted that the loss of the decay heat removal function is not a concern in the case of the large LOCA where rejection of heat is achieved through the LOCA itself rather than via the PRHR HX.	

Table 20-21. Detailed Assessment for Classification of the PRHR HX Inlet and Return Lines (cont.)

Indirect Failure Consequences The containment integrity analysis considers, as its design basis, the complete double-ended severance of the largest RCS pipe (Section 9D) and hence containment integrity would not be challenged by this postulated break. In addition to pressurisation of the containment, a DEGB of the PRHR HX return lines would result in internal pressurisation of SG compartment 1. The PRHR return line is a line with supplemental mechanistic design controls which was not selected for further assessment during GDA (Reference 20.23). Nonetheless, on a best-estimate basis, it is judged that this failure would not lead to offsite consequences because any failure would not compromise integrity of the redundant train of the PXS. A DEGB of the PRHR HX inlet and return lines would result in pipe whip in the maintenance floor/ mezzanine areas and in SG compartment 1. The PXS DN 350 (NPS 14) piping has not yet been assessed deterministically (Reference 20.23). In the absence of a deterministic assessment to support the SI classification review, the effects of pipe whip hinging at the compartment wall were evaluated using the 3-D model. Based on this, it was concluded that pipe whip arising from failure of the PRHR HX system pipework would not compromise integrity of the redundant train of the PXS. Additionally, a DEGB of the PRHR HX inlet and return lines has the potential to cause pipe whip resulting in the failure of conduit for one group (half) of the ADS Stages 1, 2, and 3 valves. Probabilistic safety analysis (Reference 20.11, Chapter 6) has shown a loss of one group of ADS Stages 1, 2, and 3 valves is acceptable in this scenario. The pipe whip resulting from a DEGB of the PRHR HX return line has the potential to affect the IRWST wall at the PRHR outlet. If the IRWST wall were to be damaged, there is potential the IRWST could be drained to a low level by the break. As a result, there exists the potential for insufficient driving head for passive PXS injection to occur when it is needed. However, the IRWST is constructed of thick steel/concrete/steel composite walls. As such, local deformation of the inside liner of the IRWST and global plastic strain of the structural walls have been concluded to not occur as a result of the impact force resulting from a DEGB of a PRHR HX return line. Furthermore, the mounting ring and base metal associated with the PRHR HX outlet plenum have been shown to remain functional. The pipe whip resulting from a DEGB of the PRHR HX return line has the potential to affect the RCPs or the RCP cooling heat exchanger, which would prevent the RCPs from functioning properly. This is of little consequence, as the RCPs are not needed or credited in a large-break LOCA scenario. The valves included in these lines have been designed to prevent missiles as discussed in Reference 20.27. Flooding of the SG compartment is within the design basis.
Lines of Protection PXS and PCS. Containment.
Discussion A guillotine failure of PRHR HX inlet and return lines is included within the design basis and can be protected by the passive safety systems. Indirect consequences have been evaluated and it is considered that they would not lead to escalated consequences of failure. In accordance with the methodology, the PRHR HX inlet and return lines have been evaluated as Standard Class 1.

Table 20-22. Summary of RCS Design Transients

Design Transient	Number of Occurrences
ASME III Service Level A Transients	
Reactor Coolant Pump Startup/Shutdown	
Case A … Pump Startup	3,000
Case B … Pump Shutdown	3,000
Full Plant Heatup …….. (120°F - 557°F) (49°C - 292°C)	200
Partial Plant Heatup …….. (120°F - 350°F) (49°C - 176°C)	200
Partial Plant Heatup …….. (350°F - 557°F) (176°C - 292°C)	200
Full Plant Cooldown ……. (557°F - 120°F) (292°C - 49°C)	200
Partial Plant Cooldown …. (557°F - 350°F) (292°C - 176°C)	200
Partial Plant Cooldown …. (350°F - 120°F) (176°C - 49°C)	200
Unit Loading (Between 0-15% Power)	500
Unit Unloading (Between 15-0% Power)	500
Unit Loading (15-100% @ 5% per minute)	2,000
Unit Unloading (100-15% @ 5% per minute)	2,000
Reduced Temperature Return to Power	(See Note 1)
Step Load Increase (+10% Power)	3,000
Step Load Decrease (-10% Power)	3,000
Large Step Load Decrease (w/Steam Dump)	200
Tie Line Thermal Backup	(See Note 2)
Steady-State Fluctuations	
Case A … Initial	$\leq 1.5 \times 10^5$
Case B … Random	$\leq 4.6 \times 10^6$
Load Regulation	750,000
Boron Concentration Equalization	2,900
Feedwater Cycling	
Mode 1 … Slug flow every 2 hours	3,000
Mode 2 … Slug flow every 24 minutes	15,000
Core Lifetime Extension	40
Feedwater Heaters Out of Service	180

Table 20-22. Summary of RCS Design Transients (cont.)

Design Transient	Number of Occurrences
ASME III Service Level A Transients (cont.)	
Reactor Coolant Pump Out of Service	(See Note 1)
Refueling	40
Turbine Roll Test	20
Primary Leakage Test	200
Secondary Leakage Test	80
Core Makeup Tank Recirculation and Heated Draindown Test	5
Passive Residual Heat Removal Test	5
Reactor Coolant System Makeup	5,640
Daily Load Follow Operations	17,800
Automatic Depressurisation System Stage 1, 2, and 3 Test	3
ASME III Service Level B Transients	
Loss of Load	30
Loss of Offsite Power	30
Reactor Trip (from Reduced Power)	180
Reactor Trip (from Full Power)	
Case A … w/o Inadvertent Cooldown	50
Case B … w/ Cooldown, w/o Safeguards	50
Case C … w/ Cooldown, w/ PRHR actuation	20
Inadvertent Startup of an Inactive Pump	(See Note 1)
Control Rod Drop	
Case A … w/ Reactor trip, w/o Safeguards	30
Case B … w/ Reactor trip, w/ Safeguards	20
Case C … w/o Reactor trip, w/o Safeguards	30
Inadvertent Safeguards Actuation	10
Cold Overpressure	15
Partial Loss of Primary Flow	60
Inadvertent RCS Depressurization	
Case 1 - Spurious Single PZR Safety Valve Actuation	20(3)
Case 2 - Inadvertent PZR Main, Auxiliary Spray Actuation	15

Table 20-22. Summary of RCS Design Transients (cont.)

Design Transient	Number of Occurrences
ASME III Service Level B Transients (cont.)	
Excessive Feedwater Flow	30
Loss of Power w/Natural Circulation Cooldown	
Case A … w/ On-Site AC Power	20
Case B … w/o On-Site AC Power	10
ASME III Service Level C Transients	
Small Loss of Coolant Accident	5
Small Steam Line Break	5
Complete Loss of Primary Flowrate	(See Note 2)
Small Feedwater Line Break	5
Steam Generator Tube Rupture	5
Inadvertent Pressurizer Auxiliary Spray	(See Note 2)
Inadvertent Opening of the ADS Valves	15
ASME III Service Level D Transients	
Reactor Coolant Pipe Break (Large LOCA)	1
Large Steam Line Break	1
Large Feedwater Line Break	1
Reactor Coolant Pump Locked Rotor	1
Control Rod Ejection	1
Simultaneous Steam Line/Feedwater Line Break	(See Note 1)
ASME III Test Transients	
Primary Hydrostatic Test	10
Secondary Hydrostatic Test	10
Steam Generator Tube Leakage Test	800

Notes:

1. Not an AP1000 design basis event.
2. This event is bounded by another event.
3. Evaluated at bounding power level on a per component basis except for the steam generators, which are evaluated at specified power levels as detailed in design transients document.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS AND ACRONYMS

ADS	automatic depressurisation system
ALARP	as low as reasonably practicable
ANI	authorised nuclear inspector
ANS	American Nuclear Society
ASME	American Society of Mechanical Engineers
BPVC	Boiler & Pressure Vessel Code
CFR	Code of Federal Regulations
CH	closure head
CMTR	certified material test report
CRDM	control rod drive mechanism
CSR	Component Safety Report
CT	compact tension
CVS	chemical and volume control system
DN	deviation notice
DSM	defect size margin
DVI	direct vessel injection
ELLDS	end of life limiting defect size
ENIQ	European Network for Inspection and Qualification
EoL	End-of-life
FCG	fatigue crack growth
FE	finite element
FUF	fatigue usage factor
GDA	generic design assessment
HSS	highest safety significance
HVAC	heating, ventilation, air conditioning
ICI	in-core instrumentation
IHP	integrated head package
IITA	in-core instrumentation thimble assembly
ISI	in-service inspection
IVC	inspection validation centre
LCO	limiting conditions for operation
LEFM	linear elastic fracture mechanics
LFCG	lifetime fatigue crack growth
LOCA	loss-of-coolant accident
LTOP	low temperature overpressure protection
NDE	nondestructive examination
NDT	nondestructive testing
NDTT	nil ductility transition temperature
NPP	nuclear power plant
NRC	Nuclear Regulatory Commission
OD	outside diameter
P/T	pressure/temperature
PC	plant condition
PRHR	passive residual heat removal
PSI	pre-service inspection
PWD	primary working direction
PWHT	post-weld heat treatment
PWR	pressurised water reactor
PWSCC	primary water stress corrosion cracking

LIST OF ABBREVIATIONS AND ACRONYMS (cont.)

PXS	passive core cooling system
QEDS	qualified examination defect size
QMS	Quality Management System
RCPB	reactor coolant pressure boundary
RCS	reactor coolant system
RT_{NDT}	nil ductility transition temperature
RV	reactor vessel
RXS	reactor system
SAP	safety assessment principle
SFR	safety functional requirement
SoL	start of life
SSC	system, structure, or component
SSE	safe shutdown earthquake
STP	standard temperature and pressure
T_{NDT}	temperature for nil ductility transition
UK	United Kingdom
US	United States
UT	ultrasonic testing

APPENDIX 20A
REACTOR VESSEL COMPONENT SAFETY REPORT

20A.1 INTRODUCTION

This is the component safety report (CSR) for the reactor vessel (RV). As introduced in Section 20.2, the safety argument herein substantiates the structural integrity of the RV to a degree of rigour commensurate with the consequences of gross structural failure. The safety argument is supported by a suite of documentary evidence outlined in Section 20A.6 regarding the quality of design, manufacture, installation and operation of the RV.

20A.1.1 Scope

This report supports the claim that the nuclear and radiological risk potentially arising from gross structural failure of the RV remains tolerably low for the 60 year design lifetime. Conventional hazards to personnel safety are outside the scope of this Appendix 20A.

This CSR demonstrates that the structural reliability for the RV is commensurate with the consequences of failure; which, in the case of the RV, necessitates a demonstration that the probability of gross failure of the RV is so low that it can be discounted for the required period of operation.

The RV is a component of the reactor coolant system (RCS). The scope of the assessment is limited to the RV only and does not include any other components of the RCS or any other systems. The physical boundaries of the RV are identified in Section 20A.1.7.

This CSR is restricted to consideration of those pressure, temperature, and mechanical loadings within the design basis. The design basis includes normal operating conditions, anticipated transients, and postulated accident conditions. Design parameters and transient definitions for the required period of operation are identified in Section 20A.2.1. Severe accident transients, including the ability of the RV to retain molten core debris, are outside the scope of this appendix; but are described in Section 10.3.

20A.1.2 Objectives

This CSR supports the claim the AP1000 plant risk remains both tolerable and as low as reasonably practicable (ALARP) for the design lifetime. These claims are substantiated by satisfying structural integrity safety design bases for all safety-significant AP1000 systems, structures, or components (SSCs). The safety design bases, applied across the operational, process and lifecycle scope of the safety case, embody the technical scope of the safety case: if these can be maintained at all times, the plant will be acceptably safe. Specific safety functional requirements (SFRs) for each particular component are developed from the structural integrity safety design bases, and correspond to the functions that need to be maintained to provide assurance of nuclear and radiological safety. The SFRs applicable to the RV are identified in Section 20A.1.9.

20A.1.3 Strategy

The SFRs of the RV provide a basis for the criteria against which the acceptability of the safety argument is to be judged. The RV SFRs are substantiated by means of a structured safety argument which is consistent with United Kingdom (UK) regulatory expectation and in accordance with the relevant safety assessment principles (SAPs). The structure and philosophy of the safety argument are established in Section 20A.1.8.

20A.1.4 Interface with other Safety Case Documents

The safety argument presented in this report is supported by a dossier of technical data and analyses. These are listed in the technical index (Section 20A.6) and each is specifically identified in the relevant section of the structured safety argument.

20A.1.5 Description

20A.1.5.1 Overview

The RV consists of a cylindrical main section with a transition ring, hemispherical bottom head, and a removable flanged hemispherical upper head (Figure 20A-1). Key dimensions are shown in Figure 20A-2 and Figure 20A-3. The RV, including closure head (CH), is approximately 12.208 m (40 ft) long and has an inner diameter at the core region of approximately 4038.6 mm (13.25 ft). The total weight of the vessel including the CH is approximately 352 tonnes. Surfaces, including the upper shell top surface, which can become wetted during operation and refuelling are clad to a nominal 5.6 mm (0.22 in) of thickness with austenitic stainless steel welded overlay. The RV's design objective is to withstand the design environment of 17.24 MPa (2500 psia) and 343.3°C (650°F) for 60 years.

The cylindrical section consists of two shells, the upper shell and the lower shell. The upper and lower shells and the lower hemispherical head are fabricated from low alloy steel (ASME SA-508, Grade 3, Class 1) and clad with austenitic stainless steel. The upper shell forging is welded to the lower shell forging, and the lower shell is welded to the transition ring, which is welded to the hemispherical bottom head. The removable flanged hemispherical upper head consists of a single forging, which includes the CH flange and the CH dome. The CH is fabricated from a low alloy steel forging and clad with austenitic stainless steel. The base, clad and weld materials used in the construction of the RV are identified in Section 20A.2.1. The removable flanged hemispherical CH is attached to the vessel (consisting of the upper shell-lower shell-bottom hemispherical head) by a ring of 45 studs. Two metal o-rings are used for sealing the two assemblies. Inner and outer monitor tubes are provided through the upper shell to collect any leakage past the o-rings. Material specification for all RV components is provided within the safety argument in Section 20A.2.1.4.2.

There are no penetrations below the top of the core. This reduces the frequency of a loss-of-coolant accident (LOCA) from these penetrations that could allow the core to be uncovered. The core is positioned as low as possible in the vessel to limit re-flood time in the event of an accident. During the beyond-design-basis severe accident core meltdown, the RV bottom head retains the molten core and is cooled by floodup of water on the exterior surfaces of the RV.

20A.1.5.2 Lower Head and Lower Shell

The lower head has an approximate 2 m (6.6 ft) inner spherical radius to the cladding surface. The thickness of the lower head is about 158 mm (6.2 inches). The lower radial supports are located on the head at the elevation of the lower internals lower core support plate. The transition ring is welded to the lower shell course with the weld located outside the high fluence active core region. The lower shell is a ring forging about 213.4 mm (8.4 inches) thick with an inner diameter of approximately 4.038m (159 inches). The length of the shell is greater than 4.267 m (168 inches) to place the upper shell weld outside of the active fuel region. A surveillance programme is used to monitor the radiation damage to the vessel material in the belt line region.

20A.1.5.3 Upper Shell and Nozzles

The upper shell is a large ring forging. Included in this forging are four 558.8 mm (22-inch) inner diameter inlet nozzles, two 787.4 mm (31-inch) inner diameter outlet nozzles and two (DN 200 (NPS 8) schedule 160 pipe connections) direct vessel injection (DVI) nozzles. These nozzles are made from the same material as the RV body and are fabricated by "set in" construction. The inlet and outlet nozzles are offset axially in different planes, which allows pump maintenance without discharging the core. The injection nozzles are approximately 2540 mm (100 inches) below the main flange. The outlet nozzles are approximately 2032 mm (80 inches) and the inlet nozzles are approximately 1587.5 mm (62.5 inches) below the mating surface. A stainless steel safe end is shop welded to each of the four inlet, two outlet and two DVI nozzles to facilitate field welding without heat treatment to the stainless steel reactor coolant piping system. The primary coolant nozzles support one end of the primary coolant system. Reaction loads are transferred into the nozzles and eventually into the support pads.

The top of the upper shell contains a ring of 45 threaded stud holes and has the sealing surface for the CH. Inner and outer monitor tubes are provided through the shell to collect any leakage past the closure region o-rings. Attached to the top surface and along the outer periphery of the upper shell is a seal ledge. During field assembly the seal ledge is welded to the refuelling cavity seal liner. This ring provides an effective water seal between the refuelling cavity and sump during refuelling operations.

20A.1.5.4 Closure Head, Bolting and Closure Head Penetrations

The CH is manufactured from a single forging and has an integral flange. The CH is manufactured from an SA508 Grade 3 Class 1 low alloy steel forgings to minimise size. It has an approximately 1968.5 mm (77.5-inch) inner spherical radius to the cladding surface and an approximately 4775.2 mm (188.0-inch) outside diameter (OD) outer flange. Cladding is extended across the bottom of the flange for refuelling purposes. Studs attach the head to the lower vessel and two metal o-rings are used for sealing. The upper head has sixty-nine 101.6mm (4-inch) outer diameter penetrations for the control rod drive mechanism (CRDM) housings and eight nozzles for the in-core instrumentation (ICI). Each CRDM is positioned in its opening and welded to the CH using a J-prep weld against the inside spherical radius of the head. Lugs are welded to the outside surface of the CH along the outer periphery of the dome section. The lugs provide support and alignment for the integrated head package (IHP).

20A.1.5.5 Vessel Supports

Four vessel supports are located beneath the inlet nozzles and the internals support ledge is machined into the top of the upper shell. The support pad is integral to each of the four inlet nozzles. The pads are simply supported on steel base pads atop a support structure, which is attached to the concrete foundation wall; justification of the support structure is beyond the scope of this document. Thermal expansion and contraction of the vessel are accommodated by sliding surfaces between the support pads and the base plates. Side stops on these plates keep the vessel centred and resist lateral loads.

20A.1.5.6 Reactor Vessel Internals

The RV supports the internals. An internal ledge is machined into the top of the upper shell section. The core barrel flange rests on the ledge. A large circumferential spring is positioned on the top surface of the core barrel flange. The upper support plate rests on the top surface of the spring. The spring is compressed by installation of the RV CH and the upper and lower core support assemblies are restrained from any axial movements.

Four core support blocks are located on the bottom hemispherical head just below the transition ring-to-lower shell circumferential weld. The core support blocks function as a clevis. At assembly, as the lower internals are lowered into the vessel, the keys at the bottom of the lower internals engage the clevis in the axial direction. With this design, the internals are provided with a lateral support at the furthest extremity and may be viewed as a beam supported at the top and bottom.

The interfaces between the RV and the lower internals core barrel are such that the main coolant flow enters through the inlet nozzle and is directed down through the annulus between the RV and core barrel and through the flow skirt and flows up through the core. The annulus is designed such that the core remains in a coolable configuration for all design conditions.

Prior to installation of the internals into the RV, guide studs are assembled into the upper shell. Dimensional relationships are established between the guide studs and the core support blocks such that when the lower internals lifting rig engages the guide studs, the keys at the bottom of the lower internals are in relative circumferential position to enter the core support blocks.

20A.1.5.7 Guide Studs

The guide studs position and align the CH when the head is lowered by the crane onto the vessel, to facilitate drive rod insertion into the CRDMs and head-to-vessel alignment pin engagement in the CH keyways. The guide stud locations are outside the vessel flange area so that the guide studs do not normally have to be removed for outage activities and reactor operation. Therefore, the guide studs are designed with consideration in regard to materials and features to be permanently installed during all operational and outage conditions. The design permits the guide studs to be removed from their positions in a relatively easy and timely manner, if removal becomes necessary.

20A.1.6 Function

The RV is the high-pressure containment boundary used to support and enclose the reactor core. It provides flow direction with the reactor internals through the core and maintains a volume of coolant around the core. The vessel interfaces with the reactor internals, primary loop piping, safety injection piping, head vent piping, insulation, head lifting rig, cavity seal, digital metal impact monitoring system, and steel structures from the IHP and is supported by RV supports on the containment building concrete structure.

Inlet and outlet nozzles are provided to accommodate the flow of reactor coolant that circulates through the core to remove heat and transfer it to the steam generators. DVI nozzles are provided for the passive core cooling system (PXS), which provides flow for a variety of accident conditions. To minimise the potential for draining the RV and exposing the core, all nozzles are located above the core.

In addition to providing access to the inside of the vessel for refuelling and maintenance, the removable CH also serves as the attachment point for the CRDMs, the QuickLoc connections for the ICI, the head vent system penetrations, and the digital metal impact monitoring system. In order to support the IHP and accommodate lifting, supports and lift lugs are attached to the CH.

The vessel flange contains the threaded holes for the closure stud and its top surface provides the mating sealing surface for the CH. Inner and outer monitor tubes are provided through the vessel flange to collect any leakage past the closure gaskets.

To support the reactor internals and core, a support ledge is provided near the top of the vessel flange and core supports are located at the bottom of the core. The lower head supports the reactor core during the postulated core drop accident.

Vessel support pads are provided on the primary inlet nozzles to act as an interface between the vessel and the vessel supports. The pads must limit circumferential motion of the vessel and allow radial thermal growth. The vessel supports provide no restraint to vessel motion in the vertical upward direction.

To provide a means of support and sealing for the cavity seal, a seal ledge is provided near the top of the vessel. The seal ledge also acts as a support for the CH flange insulation.

20A.1.7 Boundaries

The physical boundaries for safety case assessment of the RV, as defined in Reference 20A.2, are shown in Figure 20A-4 and identified below:

- The interface with the RV supports and the containment internal structures is at the integral vessel support pads located under the inlet nozzles.
- The interface between the RV and the main loop piping or the safety injection piping occurs at the nozzle safe-end prep.
- The interface with each CRDM assembly occurs at the bi-metallic weld between the bottom of the one-piece latch housing and the penetration.
- The interface between the QuickLoc pressure boundary and the ICI thimble assemblies (IITA) occurs at the Swagelok fitting on top of the QuickLoc stalk.
- The interface with the head lifting rig is the CH lifting lug pins.
- The interfaces with the reactor internals occurs at the internals support ledge, the outlet and DVI nozzle internal projections and the core support blocks for the internals radial support keys.
- The interface with the head vent system occurs at the first circumferential pipe weld beyond the head junction weld.
- The interface with the IHP occurs at the IHP supports.
- The two interfaces with the closure gasket leak monitor system are at the first circumferential tube welds beyond the two monitor tube-to- vessel junction welds.

- The interface with the cavity seal is the outer edge of the vessel flange seal ledge.
- The interface with the flow skirt is the flow skirt attachment weld.
- The interface with the digital metal impact monitoring system is the mounting bosses/pads

20A.1.8 **Safety Case Requirements**

This report substantiates the claim that the structural reliability of the RV is commensurate with the consequences of gross failure by means of a structured safety argument, supported by suitable and sufficient evidence. The safety argument is presented according to an established four legged structure (Reference 20A.3), to demonstrate an appropriate level of defence in depth by identifying evidence to satisfy safety claims and objectives identified within each leg of the argument, as follows:

Leg 1	**Interpolation/Extrapolation of Experience – 'Good' Design and Manufacture**
Objective:	Provides evidence of good design and manufacture based on a proven track record. It provides a keystone for a demonstration of high reliability and embodies the code and plant operating experience with objective of achieving quality of build, high integrity and the avoidance of defects.
Claim:	High quality is achieved through good design and manufacture.
Leg 2:	**Functional Testing**
Objective:	Incorporates the build experience as embodied in design codes and provides some diversity and redundancy to the pre-service inspection (PSI).
Claim:	Components are shown to be fit for purpose through effective functional testing.
Leg 3:	**Failure Analysis**
Objective:	Provides an assessment of through-life degradation mechanisms and shows that such mechanisms will not threaten integrity over a specific interval. Goes beyond design code requirements to provide a further demonstration of integrity. Recognises that flaws may be present and shows tolerance to them. Supplements the Leg 1 aim of avoidance of defects to provide a safety case with both defect avoidance and defect tolerance.
Claim:	Components are tolerant to through life degradation over the design life of the plant.
Leg 4	**Forewarning of Failure**
Objective:	Confirms the absence of a degradation mechanism or that a known degradation mechanism is not significant to integrity or will have limited consequences. Provides contingency for the unexpected.
Claim:	Effective systems are in place to provide forewarning of failure.

The four legged safety argument will substantiate specific SFRs for the RV. The RV SFRs are identified in Section 20A.1.9.

The safety argument is tailored according to the structural reliability claims derived from a process of component classification, with the purpose of demonstrating that component structural reliability is commensurate with the consequences of gross failure. Classification of the RV and its component parts is established in Section 20A.1.10.

The four legged safety argument is provided in Section 20A.2 and the strength of the argument is discussed in Section 20A.3.

20A.1.9 Safety Functional Requirements

The performance and safety design bases for AP1000 SSCs are identified in Section 20.4. These are requirements of plant systems, some duty, some accident response, which must be maintained at all times to provide assurance of plant nuclear and radiological safety. Identification of the SFRs for the RV follow from the performance and safety design bases, as follows:

SFR 20.1.1 The RV is required to provide the highest reliability pressure boundary to contain the primary coolant, heat generating reactor core, and fuel fission products during normal and faulted design basis conditions for the design life of the plant.

SFR 20.1.2 The RV is required to provide support for the reactor internals and core to ensure that the core remains in a coolable configuration.

SFR 20.1.3 The RV is required to direct main coolant flow through the core by close interface with the reactor internals and flow skirt.

SFR 20.1.4 The RV is required to provide for core internals location and alignment.

SFR 20.1.5 The RV is required to provide support and alignment for the CRDMs and ICI assemblies.

SFR 20.1.6 The RV is required to provide support and alignment for the integrated head assembly.

SFR 20.1.7 The RV is required to provide an effective seal between the refuelling cavity and sump during refuelling operations.

SFR 20.1.8 The RV is required to support and locate the main coolant loop piping.

SFR 20.1.9 The RV is required to provide support for safety injection flow paths.

SFR 20.1.10 The RV is required to serve as a heat exchanger during core meltdown scenario with water on the outside surface of the vessel.

Postulated failure modes which result in a loss of these SFRs lead to identification of structural reliability targets commensurate with the consequences of gross failure, as determined through the process of component classification as described in Section 20A.1.10. The safety argument in Section 20A.2 is provided to establish that structural integrity of the RV will be maintained for all conditions within the design basis and thus demonstrate that all of the above SFRs will be maintained at all times.

20A.1.10 Reactor Vessel Structural Integrity Classification

Key to the RV structural integrity safety case is the clear understanding of the potential radiological consequences of any postulated gross failure mode. Based on this understanding, a structured and systematic basis can be established for setting the level of rigour applied during the design assessment, material procurement, fabrication, in-manufacture inspection, testing and in-service testing, maintenance, inspection and safety case assessment of the component. Details of the approach for developing AP1000 component structural integrity safety cases are given in Reference 20A.4.

The approach to structural integrity classification is discussed in Section 20.5 and is consistent with the overall AP1000 safety classification scheme as detailed in Chapter 5. Reference 20A.4 details the approach taken whereby a detailed assessment of selected individual components is made to establish the consequences of gross failure, due to both direct consequences such as a LOCA, and indirect consequences, such as the effect of missiles, jet loading or pipe whip on essential safety systems. Based on this assessment, and in accordance with the scheme identified in Table 20-2, components are ascribed one of the five structural integrity classifications described in Section 20.5.2.

For the RV, the unmitigated direct consequences of gross failure have been assessed in Reference 20A.4 as having the potential for severe core damage arising from disruption to the core assembly, loss of coolant inventory and loss of coolable core geometry. Other postulated beyond design basis consequences include loss of core support or control rod ejection leading to a potential reactivity excursion. Failure of the RV could also lead to loss of in-vessel retention of core debris which is a defence in depth measure. Considering the indirect consequences, there exists the potential for secondary damage to essential safety systems or damage to the containment vessel as a result of high energy missile generation. Gross failure of the RV could therefore lead to the most severe offsite consequences against which there is no claimed protection. As such, the RV is classified as a highest safety significance (HSS) component and this safety report seeks to substantiate this claim.

The HSS classification does not however apply to each and every component of the RV or to every postulated failure mode and defect orientation, since certain failure modes will not lead to the most severe off site consequences. Since the identification of HSS locations is important to the safety case arguments at each individual location, as well as for establishing the inspection requirements for individual welds, it is important to consider each location in turn. This is presented in Table 20A-1. Where postulated gross failure could lead to severe core damage, but without threatening containment and so not leading to offsite release of activity, the HI classification has been applied. Where postulated gross failure would not lead to severe core damage, as a result of either direct or indirect means, Class 1 has been

assumed. For HI components, defect tolerance assessments will be carried out and the capability of ultrasonic testing (UT) inspections will be evaluated to establish that the inspection is capable of screening out defects of structural significance.

20A.2 Safety Argument

This section provides a structured safety argument to demonstrate that the RV is fit for purpose for the required component lifetime of 60 years. The safety argument is presented according to the four-legged structure described in 20A.1.8.

Consistency with the appropriate ASME rules for Class 1 components provides the basic demonstration of fitness-for-purpose and is generally inferred as providing substantiation for a component's reliability. In the case of the RV, it is necessary to substantiate a lower frequency of failure such that the probability of gross failure is so low that it can be discounted. This is achieved by identifying supplementary measures to ensure high quality and by demonstrating the tolerance to manufacturing defects above qualified detection limits. Additional qualitative arguments are presented in Section 20A.2.2 and Section 20A.2.4 to demonstrate evidence of defence in depth and to substantiate component reliability commensurate with the structural integrity classification of the RV.

20A.2.1 Leg 1: Interpolation/Extrapolation of Experience – Good Design and Manufacture

The objective of Leg 1 is to provide the evidence to support the conclusions that the design of the RV is based on the highest standards of engineering design, that the chosen materials have well understood characteristics with a proven track record in an RV environment and are subject to tight specification and procurement controls and that the manufacture is carried out using experienced fabricators with a proven track record using established high quality processes and subject to robust examination. A number of elements are built up to support this claim. These are:

- The Design is Well Founded, Designed in Accordance with Internationally Recognised Standards and Takes Into Account Operating Experience (Section 20A.2.1.1).
- Loading, Temperatures and Environment Have Been Well Defined (Section 20A.2.1.2).
- The AP1000 RV Design has Been Assessed Against Relevant Design Code Requirements (Section 20A.2.1.3).
- Components are Manufactured Using a Good Choice of Materials (Section 20A.2.1.4).
- Good Manufacturing (Section 20A.2.1.5).
- Manufacturing Inspection (Section 20A.2.1.6).
- Plant Operation and Maintenance (Section 20A.2.1.7).

Together these provide an important keystone for a demonstration that the vessel is well designed, will enter service free from structurally significant defects and that the effects of through-life degradation on material properties will not have a deleterious effect on the structural reliability of the vessel. The arguments and evidence associated with each of these claims are expanded in sections 20A.2.1.1 to 20A.2.1.7 below.

20A.2.1.1 **The Design is Well Founded, Designed in Accordance with Internationally Recognised Standards and Takes Into Account Operating Experience**

In order to demonstrate that the design is well founded, designed in accordance with internationally recognised standards and takes into account operating experience, evidence to substantiate the following arguments is provided.

- Westinghouse design of RVs is well founded and supported by an excellent safety record.
- The design of the RV takes account of in-service experience and known age related degradation mechanisms.
- Design and manufacture in accordance with established codes, standards and regulations provides assurance of high reliability based on experience.
- Novel features of the design are avoided or adequately justified.
- The use of forgings is maximised to limit the number of welds.
- The AP1000 RV arrangement optimises safety.

20A.2.1.1.1 Westinghouse Design of Reactor Vessels is Well Founded and Supported by an Excellent Safety Record

Westinghouse has designed, developed, and manufactured nuclear facilities since the 1950s, beginning with the world's first large central station nuclear plant (Shippingport), which produced power from 1957 until 1982. Westinghouse has since designed and delivered more than 100 commercial nuclear power plants (NPPs) worldwide, including the design of Sizewell B in the UK, with a combined electrical generating capacity in excess of 90,000 MW. The design of the AP1000 reactor pressure vessel is therefore supported by decades of successful plant operating experience which have accumulated many operating years without significant issue. Westinghouse has substantial proven experience, knowledge, and capability to design, manufacture and furnish technical assistance for the installation, start-up and service of NPPs.

The AP1000 RV is of similar design to that of the earlier Westinghouse designs, and also to typical pressurised water reactor (PWR) RV design which use similar proven materials and manufacturing processes. The design has been the subject of regulatory scrutiny overseas: the United States Nuclear Regulatory Commission approved the final design certification for the AP1000 in December 2005 following the earlier approval of AP600 design certification in 1999.

Whilst the substantial record of safe operating experience is insufficient to directly support reliability claims commensurate with a HSS component, it provides confidence that there is a thorough understanding of the in-service performance of these vessels, the management and mitigation of through-life degradation issues and in the avoidance of issues at the design and manufacturing stage that can affect the through life performance.

20A.2.1.1.2 The Design of the RV Takes Account of In-service Experience and Known Age Related Degradation Mechanisms

Historically RVs have encountered in-service issues that have resulted in unscheduled outages and prolonged plant down time. Most prominent among these failure events are RV head penetration and bottom instrumentation tube cracking, leakage from mechanical joints and stuck RV studs. The design of the AP1000 RV therefore takes benefit of lessons learned over the many years of operation and includes a number of design features aimed at mitigating against issues reported on other PWR plants. Reference 20A.6, presents a review of the susceptibility of the AP1000 RV design to known in-service degradation mechanisms. The main conclusions from this review of each of the major in-service issues are summarised below.

Head Penetration and Instrumentation Tube Cracking

Previous reactor designs used CRDM nozzles made of Alloy 600, which operating experience showed was susceptible to primary water stress corrosion cracking (PWSCC). The CRDM nozzles and head vent pipe in the AP1000 RV CH are all Ni-Cr-Fe Alloy 690 material. Alloy 690 has been shown by laboratory testing to be resistant to PWSCC. In addition, a narrow gap J-groove weld is specified for the CRDM penetrations in order to reduce the residual weld stresses that contributed to earlier PWSCC issues.

The AP1000 RV does not have bottom head penetrations, but the lesson learned regarding material selection has been applied to the QuickLoc instrument penetrations in the CH. The material of the pressure boundary parts of the QuickLoc are SA-182, SA-479, and UNS S21800. The AP1000 RV head penetrations are also designed with consideration for the inspections for PWSCC that are currently mandated by the United States (US) Nuclear Regulatory Commission (NRC) and the industry. The internal protrusions of the CRDM penetration nozzles have sufficient length such that there is approximately 50.8 mm (2 inches) of inspectable length below the lowest point on the toe of the J-groove weld in accordance with the current directives.

Leakage from Mechanical Joints

The major cause of RV closure gasket (O-ring) leakage over the years has been debris on the vessel flange seating surfaces that interferes with the sealing of the O-ring. To a large extent the offending debris has been rust particles that have washed or dropped onto the seating surfaces after the flange surface was cleaned and the head was set. The major source of the rust has been eliminated in the AP1000 RV design by applying stainless steel cladding to the RV flange bolting ring and seal ledge. However, prevention of RV closure gasket leakage will still depend heavily on careful cleaning and inspection of the seal surfaces prior to setting the head during refuelling outages. Other leakage from joints above the CH has been eliminated in the AP1000 design by eliminating the joints altogether. The instrumentation ports which have been subjected to conoseal joint leakage in years past are not included in the AP1000 design. In addition, the CRDM lower canopy seal weld is eliminated, and there are no spare penetrations with threaded and canopy seal-welded head adapter plug and capped latch housing joints.

Stuck Reactor Vessel Closure Studs

At several current plants RV closure studs have become bound in their stud holes due to thread galling. The stuck studs have resulted in studs having to be machined out of the stud holes, and in some cases the stud holes had to be sleeved due to thread damage. The galling has been contributed in part to the close thread clearances with the traditional 8N threads. The AP1000 RV closure studs and flange stud holes have 4UN threads. This design provides larger clearances between the stud and stud hole threads in addition to a more robust thread form.

Irradiation Embrittlement

The fracture toughness properties for the low alloy steel material in the core region of the RV are affected over time by fast neutron fluence (energy $\geq$ 1 MeV). In order to comply with the limits for these properties, such as RT_{NDT} and upper shelf energy, that have been established by the NRC, Reference 20A.2 puts restrictions on the core region material chemistry and initial properties with consideration of the end-of-life fast neutron fluence. In addition, the core region shell inside diameter is one inch further removed from the core compared to the standard 3-loop and AP600 reactor designs. This diameter change reduced the maximum fast neutron fluence at the AP1000 vessel inside surface to 9×10^{19} n/cm^2 for 56 EFPY in order to comply with the limits.

Fatigue Cracking

The AP1000 RV fatigue usage at the locations of maximum peak stress intensity range has been analysed in accordance with the ASME Code. As in the case with all of the previous Westinghouse RVs designed in accordance with ASME Code, Section III, the RV was found to be acceptable for cyclic operation for the plant lifetime accordant with the number of cycles of design transients and design mechanical loads specified in the RV Design Specification. To date there have been no fatigue failures in Westinghouse RVs due to conditions that could be anticipated in the design. As a result of the satisfactory ASME Code, Section III fatigue analysis for the AP1000 RV and the years of plant operating experience, no AP1000 RV fatigue failures are anticipated for the 60-year plant lifetime.

Stress Corrosion Cracking

Primary water stress corrosion cracking of Ni-Cr-Fe Alloy 600 materials has been eliminated for the AP1000 RV by eliminating the use of Alloy 600 base and weld materials for the RV design. As previously discussed, Ni-Cr-Fe Alloy 690 is applied in the AP1000 RV in all locations where Alloy 600 was previously used. Stress corrosion cracking of other RV materials is expected to be avoided by careful control of materials and chemicals that come in contact with RV materials as well as elimination of geometry susceptible to stress corrosion cracking, such as canopy seals.

Corrosion Wastage

The most destructive incidents of corrosion wastage on Westinghouse RVs have resulted from instrumentation port conoseal, CRDM lower canopy seal, and head adapter canopy seal leaks. Therefore, corrosion wastage failures have been addressed for the AP1000 RV by eliminating these features from the reactor design. In addition to the corrosion wastage resulting from leaks, the vessel flange outboard of the mating surface has been subject to corrosion during refuelling outages. The corrosion of the flange bolting ring and seal ledge complicated the sealing of the stud hole plugs and the refuelling cavity seal. For the AP1000 RV design, the top surfaces of flange bolting ring and the seal ledge are clad with austenitic

stainless steel, as previously discussed. In addition, the welded cavity seal eliminates the installation of the cavity seal ring during refuelling outages.

Wear and Mechanical Damage

Wear and mechanical damage have not been responsible for any significant failures related to the RV. However, the recent discovery of wear due to the flow excitation of CRDM thermal sleeves has affected both the thermal sleeves and the inside surface of the CRDM nozzles. This wear issue does not affect the AP1000 RV design because the thermal sleeves have been replaced by threaded-on and welded CRDM extensions and funnels. The only other locations in the RV that are subjected to relative motion that can result in wear and mechanical damage are the closure stud and stud hole threads, the flange mating surfaces, and the reactor internals interfaces. The closure studs are lubricated and have weight compensation when they are turned in and out of the stud holes. Furthermore, the frequency of stud installation and removal is not enough to create a wear issue. Reactor vessel and head flange mating surfaces have been damaged by foreign material that has been crushed between them, but these incidents have been extremely rare and could have been avoided by careful visual inspection and/or vessel water level control. Loose objects have also been crushed in the RV/reactor internals interfaces. However, these loose part incidents have not resulted in any significant downtime. Therefore, there are no additional wear and mechanical damage issues that can be addressed in the AP1000 RV design.

Reference 20A.8, issued in 2005, also presents a comprehensive review of the ageing effects in NPP components, including PWR RVs, as covered by generic ageing management programmes. In the context of Leg 1 of the UK AP1000 RV safety argument, these reports provide an up to date list of in-service issues that have previously affected RV integrity and against which it can be shown that the design takes account of worldwide in-service experience. Additional assurance is provided by a structured in-service inspection (ISI) regime as identified in Section 20A.2.4.1.1; for brevity ISI measures are generally not also reproduced in the AP1000 mitigation arguments below.

Recorded Generic In Service Issue (from Reference 20A.8).	AP1000 Mitigation
Stress corrosion cracking of stainless steel bottom-mounted guide tubes.	Bottom-mounted guide tubes are not a feature of the AP1000 design.
Stress corrosion cracking of CH stud assemblies	Specific controls are applied to the material properties of the CH studs, nuts and washers in accordance with NRC Regulatory Guide 1.65 (Reference 20A.9).
Wear of CH stud assemblies	Resolutions found in NUREG-1339 (Reference 20A.10) are incorporated into the design, material selection, fabrication, and maintenance of the AP1000 bolted connections. Because of the emphasis in the design on access for maintenance and inspection, the recommended maintenance practices can be implemented.
Cumulative fatigue damage of CH stud assemblies	AP1000 components are evaluated against a design life of 60 years and fatigue usage factors (FUFs) shown to be below unity for the life of each component.

Recorded Generic In Service Issue (from Reference 20A.8).	AP1000 Mitigation
Stress corrosion cracking of nickel alloy CRDM penetration nozzles, welds and pressure housings	The use of material susceptible to PWSCC is forbidden by the AP1000 RV Design Specification. CRDM penetrations will be manufactured from Alloy 690 tubes with an increased resistance to PWSCC. This is supplemented with additional inspection in accordance with ASME Code Case N-729-1.
Thermal ageing and embrittlement of cast austenitic stainless steel CDRM pressure housings.	CRDM penetrations will be manufactured from Alloy 690 which is not susceptible to the same thermal ageing issues as cast austenitic stainless steel.
Stress corrosion cracking of nickel alloy core support blocks and core guide lugs.	The use of material susceptible to PWSCC is forbidden by the RV Design Specification.
Boric acid corrosion of unprotected external steel surfaces when exposed to borated water leakage	Material selection to minimise component susceptibility to corrosion degradation. ISI of RV head to ASME CC N-729-1 and Code of Federal Regulations 10 CFR 50.55a requires inspection for indications of leakage and boric acid accumulation. Limiting conditions for operation (LCO) 3.4.7 defines RCS operational leakage limits. Leak monitoring confirms leakage within defined limits and provides warning of unidentified leakage. Hydrostatic tests prior to operation and periodically throughout plant life confirm integrity of the reactor coolant pressure boundary (RCPB).
Pitting or crevice corrosion of clad flanges, nozzles, penetrations, pressure housings, safe ends, vessel shells heads and welds.	Material selection, chemistry control and cladding of wetted surfaces minimises the risk of pitting. Features which result in crevice conditions are minimised in the design of the AP1000.
PWSCC of nozzle safe ends and welds with nickel alloy welds or buttering.	The use of material susceptible to PWSCC is forbidden by the RV Design Specification. Nozzle safe ends are manufactured from stainless steel and safe end buttering used Alloy 690 weld with a proven resistance to PWSCC.
Irradiation embrittlement of inlet, outlet and safety nozzles.	The AP1000 core is located low in the RV such that the nozzles are not considered to be susceptible to significant irradiation effects.
PWSCC of nickel alloy CH vent pipes and instrument tubes.	The use of material susceptible to PWSCC is forbidden by the RV Design Specification. CH vent pipes are manufactured from Seamless Alloy 690 pipe with a proven resistance to PWSCC.
PWSCC of nickel alloy instrument tubes in the bottom head.	The design of the AP1000 RV eliminates penetrations in the bottom head.

Recorded Generic In Service Issue (from Reference 20A.8).	AP1000 Mitigation
Fatigue of the RV support skirt and attachment welds.	AP1000 components are evaluated against a design life of 60 years and FUFs shown to be below unity for the life of each component.
Fatigue of RV components.	AP1000 components are evaluated against a design life of 60 years and FUFs shown to be below unity for the life of each component.

20A.2.1.1.3 Design and Manufacture in Accordance with Established Codes, Standards and Regulations Provides Assurance of High Reliability Based on Experience

The RV is designed, fabricated and installed in accordance with the codes, standards and regulations identified in the RV Design Specification (Reference 20A.2) as summarised below. Complying with such proven and established codes, standards and regulations minimises the level of design and manufacturing uncertainty in this respect. Compliance with the ASME Code provides assurance over a wide range of issues from material procurement, component design, selection of manufacturing consumables, qualification of welders, specification of heat treatment, manufacturing quality checks and nondestructive examination (NDE), nondestructive testing (NDT), installation, PSI and ISI requirements. The extensive body of experience that is embodied within the ASME Code and the successful operation of a significant number of pressure vessels (both nuclear and non-nuclear) mean that compliance with the code provides assurance that the vessel reliability will remain high for the design life of the component. However, in order to substantiate a reliability claim commensurate with a component classified as HSS, i.e. where gross failure can be discounted it is necessary to demonstrate that measures have been taken over and above the minimum requirements specified by ASME Code. This is discussed in Section 20A.3. Evidence of compliance with ASME Code requirements will come from the ASME certificate number for the RV.

ASME Boiler and Pressure Vessel Code

The RV is an ASME Code, Section III, Class 1 component. The applicable ASME Code is the 1998 edition up to and including the 2000 Addenda. Specifically,

- Section II Material Specifications
- Section III Rules for Construction of Nuclear Power Plant Components – The subsections of ASME Section III which are applicable to each component are identified in Table 20A-13.
- Section V Non-destructive Examination
- Section IX Welding Qualifications
- Section XI Rules for In-service Inspection of Nuclear Power Plant Components
- ASME Code Case 2142-2, F-Number Grouping for Ni-Cr-Fe Filler Metals Section IX (Applicable to all Sections, including Section III, Division 1, and Section XI)

- ASME Code Case N-729-1, Alternative Examination Requirements for PWR Reactor Vessel Upper Head With Nozzles Having Pressure-Retaining Partial-Penetration Welds, Section XI, Division 1

- ASME Code Case N-782, Use of Code Editions, Addenda, and Case, Section III, Division 1

ANSI/ASME Standards

- ASME NQA-1-1994 Quality Assurance Requirements for Nuclear Facility Applications (Basic Part I Requirements and Supplementary Requirements for Nuclear Facilities)

- ASME NQA-1-1994 Quality Assurance Requirements for Nuclear Facility Applications Part II (Quality Assurance Requirements for Nuclear Facility Applications)

- ANSI/ANS 51.1 Nuclear Safety Criteria for the Design of Stationary Pressurized Water Reactor Plants

- ANSI N18.2a Nuclear Safety Criteria for the Design of Stationary Pressurized Water Reactor Plants

US Code of Federal Regulations

- 10 CFR 21 Reporting of Defects and Non-compliance

- 10 CFR 50 General Design Criteria for Nuclear Power Plants Appendix A. General Design Criteria 1, 2, 4, 14, 30, 31, and 32 apply.

- 10 CFR 50 Quality Assurance Criteria for Nuclear Power Plants Appendix B and Fuel Reprocessing Plants

- 10 CFR 50 Fracture Toughness Requirements Appendix G

- 10 CFR 50 Reactor Vessel Material Surveillance Program Requirements Appendix H

- 10 CFR 50.55a Codes and Standards

US NRC Regulatory Guides

- 1.28 Rev. 3 Quality Assurance Program Requirements (Design and Construction)
- 1.29 Rev. 4 Seismic Design Classification
- 1.43 Rev. 0 Control of Stainless Steel Weld Cladding of Low-Alloy Steel Components
- 1.44 Rev. 0 Control of the Use of Sensitized Stainless Steel
- 1.50 Rev. 0 Control of Pre-heat Temperature for Welding of Low Alloy Steel
- 1.65 Rev. 0 Materials and Inspections for Reactor Vessel Closure Studs
- 1.99 Rev. 2 Radiation Embrittlement of Reactor Vessel Materials
- 1.147 In-service Inspection Code Case Acceptability ASME Section XI Division 1
- NUREG-0612 Control of Heavy Loads at Nuclear Power Plants, July 1980.
- 1.84 Design and Fabrication Code Case Applicability ASME Section III Division 1

20A.2.1.1.4 Novel Features of the Design are Avoided or Adequately Justified

AP1000 RV design is broadly similar to that typical of PWR RVs and is consistent with accepted industry practice. As such the RV design includes few novel features. AP1000 emergency core cooling is designed on passive means, where flow of coolant is by gravity and natural circulation. DVI nozzles located in the upper shell are provided as part of the RV design for the PXS, providing flow for core cooling under accident conditions. The PXS was introduced as a design measure to enhance plant safety by improving reliability of the emergency core cooling system as compared with earlier system designs. Incorporation of DVI nozzles to bypass the downcomer and inject coolant directly into the core region may be regarded as a novel feature. However, the DVI nozzle design detail benefits from considerable experience of PWR nozzle design, and justification for the DVI nozzle design is supported by extensive finite element (FE) analyses carried out to evaluate the response to thermal loading, the fatigue usage, and defect tolerance.

The use of QuickLoc assemblies as the pressure boundary interface to the IITA is also relatively novel. QuickLoc assemblies have been used on a number of other plants and hence there is some experience of their use dating back to the early 1990's.

20A.2.1.1.5 The Use of Forgings is Maximised to limit the Number of Welds and Avoid Welds in the Belt Line Region

To minimise welds and reduce ISI, the RPV cylindrical vessel sections will be forged shell courses, thereby eliminating the need for longitudinal seam welds. The beltline forged sections of the vessel are of a length such that the active core region is free of welds where the effects of irradiation embrittlement can be more severe due to the combined effects of the less well controlled composition of weld and the higher propensity for defect formation. The uppermost forged section will be an integral-type design in which the vessel flange and adjacent shell course are formed as a single reinforced ring forging. The shell of the RPV CH will also be a single forging encompassing both the bolting flange and dome geometry.

20A.2.1.1.6 The AP1000 Reactor Vessel Arrangement Optimises Safety

The general arrangement of the RV includes design measures to enhance the robustness of the design without affecting its operational performance. There are no penetrations in the RV below the core, eliminating the possibility for any pipe break or penetration failure to result in immediate core uncovery. The core is positioned as low as possible in the vessel to minimise re-flood time in accident conditions. Finally, in order to assist with the through-life assurance of integrity, the various nozzles are arranged to allow 360° internal and external inspection.

20A.2.1.1.7 Loading, Temperatures and Environment Have Been Well Defined

In order to demonstrate that the loading, temperature and environment have been well defined, evidence to substantiate the following arguments is provided.

- Design and operating parameters used in the design evaluation have been determined using established and conservative procedures and capture all normal and design basis conditions.

- Environment specification is clearly defined.

20A.2.1.1.8 Design and Operating Parameters used in the Design Evaluation have been Determined Using Established and Conservative Procedures and Capture all Normal and Design Basis Conditions

Evaluation of design and build against nuclear standards, as embodied in the ASME Boiler and Pressure Vessel Code, forms a key input to several of the safety-related claims made for the RV. The evaluation is based on valid, relevant and comprehensive data. To substantiate claims based on ASME Code compliance evidence is provided here to demonstrate that design and operating parameters used in the design evaluation have been determined using established and conservative procedures.

The Design and Operating parameters for the AP1000 plant are defined in Reference 20A.49 and are as shown below.

	Design Condition
Design pressure	17.24 MPa (2500 psia)
Normal operating pressure	15.51 MPa (2250 psia)
Design Temperature	343°C (650°F)
No load temperature	292°C (557°F)
Normal operating inlet water temperature	281°C (537.2°F)
Normal operating outlet water temperature	321°C (610°F)

The RV is designed and constructed to the requirements for Class 1 in ASME Code. Section III Subsection NB of the code requires that the design is evaluated against design, service, and test conditions and that the stresses within the vessel are shown to comply with specified allowable stress limits appropriate to the material of construction. The design conditions include those pressure, temperature, and mechanical loadings selected as the basis for the design. Service conditions cover those normal operating conditions, anticipated transients, and postulated accident conditions expected or postulated to occur during operation. The evaluation of the service and testing conditions includes an evaluation of fatigue due to cyclic stresses.

The following five categories of operating condition, as defined in ASME Code, Section III, have been evaluated as part of the design substantiation for the RV. These encompass all operating conditions within the design basis, as summarised in Table 20-22 along with the number of occurrences of each transient over the design life of the plant.

- Level A Service Conditions – Normal Conditions.
- Level B Service Conditions – Upset Conditions, Incidents of Moderate Frequency
- Level C Service Conditions – Emergency Conditions, Infrequent Incidents
- Level D Service Conditions – Faulted Conditions, Limiting Faults
- Testing Conditions – Include primary and secondary hydrostatic tests and steam generator tube leak tests specified.

Cyclic loads are introduced by normal power changes, reactor trips, and start-up and shutdown operations. These design base cycles are selected for fatigue evaluation and constitute a conservative design envelope for the design life. To provide a high degree of integrity for the equipment in the RCS, the transient conditions selected for equipment fatigue evaluation are based upon a conservative estimate of the magnitude and frequency of the temperature and pressure transients that may occur during plant operation.

The specific transients to be considered for equipment fatigue analyses are based upon PWR plant operating experience along with engineering judgment. The plant condition (PC) categorisation defined in ANS N51.1 (Reference 20A.12), which categorises transients on the basis of expected frequency, are also part of the process to define transients and which service condition applies for a given transient. The basis and derivation of the transients for each of these service conditions are specified in References 20A.2, 20A.13, and 20A.14.

Where thermal stratification during PXS operation and natural circulation cooldown is of concern, this is considered by performing a thermal/flow analysis using computational fluid dynamics techniques. This analysis includes thermally-induced fluid buoyancy, heat transfer between the coolant and the metal of the vessel and internals and uses thermal/flow boundary conditions based on an existing thermal/hydraulic transient analysis of the primary RCS. This analysis provides temperature maps that are used to evaluate thermal stresses.

The transients selected are a conservative representation of transients that, used as a basis for component fatigue evaluation, provide confidence that the component is appropriate for its application for the 60-year design objective. These transients are described by pertinent variations in pressure, fluid temperature, and fluid flow. The frequency of these transients in some cases is greater than the maximum frequency that defines the plant condition in American Nuclear Society (ANS) N51.1 (Reference 20A.12). The design transients and the number of events of each that are normally used for fatigue evaluations of components are summarised in Table 20-22 and further specified in the RV Design Specification (Reference 20A.2). Separate transients are defined for the DVI nozzle assessment, as outlined in Reference 20A.15.

Section 6.2.4 of Reference 20A.2 provides a description of the seismic loads and other mechanical loads and loading combinations evaluated. The seismic loading classification, as defined in Reference 20A.16, considers the safe shutdown earthquake (SSE) and low level seismic event. The latter is used only in the fatigue evaluation and considers 5 occurrences of 63 cycles per occurrence (315 cycles) having a magnitude of 1/3 SSE.

The peak ground acceleration of the SSE has been established as 0.30g for the AP1000 design. The vertical peak ground acceleration is conservatively assumed to equal the horizontal value of 0.30g. Both horizontal and vertical design response spectra are based on the Regulatory Guide 1.60 spectra augmented at the higher frequencies. A comparison of these spectra to the UK generic design basis PML spectra is made in Section 12.6.

During containment flood-up thermal transients, the RV is assumed to be immersed in water on the vessel OD up to the bottom of the outlet nozzles. Reference 20A.2 provides details of this transient.

20A.2.1.1.9 Environmental Specification is Clearly Defined

The materials selected for use in the RV are selected to be compatible with the full range of internal and external environmental conditions which may be encountered over the plant life. These environmental conditions include temperature humidity, radiation, chemistry of fluid or materials in contact, and other external conditions which may affect the suitability of a material. These have been determined based on extensive PWR operating experience. The normal limits for internal environment conditions of the primary coolant water are specified in Table 20A-3. The external environmental conditions are listed in Table 20A-4.

20A.2.1.1.10 The AP1000 Reactor Vessel Design has been Assessed Against Relevant Design Code Requirements

In order to demonstrate that the vessel design has been assessed against relevant design code requirements, evidence to substantiate the following arguments is provided:

- The RV design complies with the allowable stress limits and sizing limits as specified in ASME III for a Class 1 component.
- The end of life FUFs are below unity.

20A.2.1.1.11 The Reactor Vessel Design Complies with the Allowable Stress Limits and Sizing Limits as Specified in ASME III for a Class 1 Component

The RV is designed in accordance with relevant and recognised design codes, specifically the ASME Boiler and Pressure Vessel Code, Section III, Division 1 – 1998 Edition with addenda up through and including 2000 Addenda (Reference 20A.7). In order to demonstrate code compliance, the following key aspects are satisfied in the ASME Code Design Report for the RV (Reference 20A.17), which documents analyses substantiating the design against the ASME Code requirements.

- The tentative sizing of vessel wall thickness and head thickness.
- The nozzle openings and reinforcement requirements
- The CH studs are designed to ASME Code, Section III, Appendix E requirements.
- The minimum wall thickness requirements for nozzle ends and safe ends.
- The requirements for no leakage through the Seal O-ring.
- IHP support lugs and RV lift lugs are qualified per ASME Code Section III, Subsection NF. The RV lift lugs are also evaluated for the lift load meeting the NUREG-0612 (Reference 20A.20) criteria. The attachment welds of IHP support lugs and RV lift lugs to the CH are qualified to ASME Section III, Subsection NB criteria.
- The attachment for the nozzles with partial penetration welds for the CH penetrations (CRDM and vent pipe), including transferring the loading above the head.
- The primary stresses in the J-groove weld.
- The primary plus secondary stresses on CH penetrations.

- The ASME Code, Section III, Subsection NB criteria are used for the qualification of each pressure boundary component and studs.

The general FE code ANSYS (Reference 20A.24) was used to perform an analysis for each of the loading conditions and to evaluate the design against ASME III, Class 1 stress limits for design, operational, accident and testing conditions. It has been demonstrated that adequate margins exist in all cases.

Table 20A-11 contains the allowable ASME Code Stress Limits for the general primary membrane stress intensity (P_m) and primary local plus primary bending stress intensities (P_L+P_b) to which different regions of the RV have been assessed against.

Conservative approaches have been adapted to the stress analysis and the interpretation of ASME stress limits. Details of the methodology used in the assessment of individual locations and the associated FE models and the loadings used for the evaluation of each location are documented in each component analysis summarised in the ASME design report for the RV (Reference 20A.17). In the majority of cases, it has been demonstrated that adequate margins exist. In the small number of cases where this has not been achieved, further explanation is provided to support the basis for the design.

20A.2.1.1.12 The End of Life Fatigue Usage Factors are Below Unity

The RV is designed to meet the fatigue design criteria as defined in the ASME Code, Section III without compromising other aspects of the design. Critical RV design features are identified and analysed to demonstrate that the fatigue design criteria are met. The basis for the transient definition is discussed in Section 20A.2.1 of this safety argument.

The FUFs are determined as:

- Membrane plus bending component at each location (end points of each cut).
- A combination of the total components for all thermal cases, resulting in alternating stress intensity ranges in decreasing order until all usage cycles are exhausted.
- A partial usage factor is determined by computing the ratio of the number of cycles determined by the alternating stress range, divided by the allowable number of cycles for the same alternating stress range, as defined in the applicable ASME fatigue curve.
- A cumulative FUF is determined by summing the partial usage factors. The cumulative FUF must be less than 1.0.

The calculated FUFs have been derived in accordance with the design curves specified in the 2001 version of the ASME Boiler and Pressure Vessel Code. Based on the current approach, all assessed RV locations satisfy ASME acceptance criteria for fatigue usage for the full design life. Sensitivity to changes in conservatism in the fatigue assessment is mitigated by the other elements of the safety argument. The RV locations where predicted FUFs exceed 0.75 are specifically included within the ISI programme (Section 20A.2.4). The ISI is designed both to demonstrate freedom from significant defects and to provide timely forewarning of failure and supports the defect tolerance assessment described later in this Leg.

Using the FE based results, code compliance for ASME III Class 1 components has been assessed and the FUFs are reported in Reference 20A.17. Stress limits have been considered

pertaining to Design loadings, Level A service limits and FUFs, Level C design basis accident stress limits and test stress limits.

20A.2.1.2 Components Are Manufactured Using a Good Choice of Materials

In order to demonstrate that the AP1000 RV components are manufactured using a good choice of materials, evidence to substantiate the following arguments is provided.

- AP1000 RV materials have a proven service performance.
- Material specifications meet or exceed ASME specifications.
- Tight control on chemical composition is enforced to minimise the effects of irradiation embrittlement or thermal ageing and ensure that materials remain ductile when significantly stressed.
- Materials are compatible with each other and with the environment and are resistant to environmental degradation over the life of the plant. Degradation characteristics are known and understood.
- Materials testing is sufficient to demonstrate that the material properties are compliant with the relevant specifications.
- RV Surveillance Material.

20A.2.1.2.1 AP1000 Reactor Vessel Materials have a Proven Service Performance

The selection of the AP1000 RV materials reflects international experience in PWR design, manufacture and operation and the lessons learnt, for example in terms of refinement of chemical composition of belt line forgings to minimise the effects of through-life irradiation embrittlement. The vessel shell, lower head, nozzles and CH are manufactured from ASME SA-508 Grade 3 Class 1 which is recognised worldwide as the standard for PWR RV manufacture and its material properties and in-service performance are supported by an extensive body of evidence.

As is standard for PWR ferritic components which are in contact with primary coolant, wetted surfaces are clad with austenitic stainless steel or equivalent corrosion-resistant material; the AP1000 cladding is Type 308L/309L welded overlay. The use of nickel-chromium-iron alloys in pressure boundary components is limited to Alloy 690 or its associated weld metals. The use of Alloy 600 is prohibited which reflects the concerns relating to PWSCC of these nickel based alloys.

20A.2.1.2.2 Material Specifications Meet or Exceed ASME Specifications

The AP1000 RV materials comply with the corresponding material specification permitted by the ASME Code, Section III, Division 1. The material specifications used for the RV assembly are as identified in Table 20A-5. The material specifications detail requirements in terms of compliance with the following ASME Code requirements; limitations on manufacturing requirements and the use of weld repairs, supplementary requirements over and above ASME specifications, heat treatment requirements, chemical composition, mechanical testing, inspection and quality assurance requirements.

To support this argument, a quality assurance compliant certified material test report (CMTR) as per the ASME Code (Section III Div 1 Appendices Article P-1000) will be provided with shipment of the forgings. This will include the material test results and information on:

- Chemical analyses: heat and product
- Mechanical properties: tensile stress-strain, Charpy, drop weight, T_{NDT} and RT_{NDT}.
- Heat treatments
- Information on archive/weldment material
- Sketches or drawings with dimensions
- A statement certifying that no weld repairs had been made (where applicable)
- Start-of-life inspection results
- NDE Reports

For certain materials, Supplementary Requirements are specified within each of the material specifications which exceed the requirements specified in ASME II. The Supplementary Requirements, as detailed for the beltline forging in Reference 20A.25 include:

- S1 Simulated post-weld heat treatment (PWHT) of mechanical test samples
- S3 Charpy V-Notch Impact transition Curve
- S4 Additional Charpy Data
- S9 Additional restrictions on chemical composition
- S10 Alternative Fracture Toughness Requirements to establish a valid T0 fracture toughness Reference temperature.
- S13 Minimum Tempering Temperature
- S15 Product Analysis

Additional Supplementary Requirements are specified for RPV pressure boundary components which exceed the requirements specified in ASME Section II. The Additional Supplementary Requirements, as detailed in Reference 20A.41, are as follows:

- End-of-life Increased Irradiated Weld Metal Toughness for Reactor Vessel Beltline Welds
- Fracture Toughness for SA-182 316LN Material of RPV Nozzle Safe-Ends
- Minimum Yield Strength for Inconel 52/152 (N06690) Material of Dissimilar Metal Welds on RPV Inlet and Outlet Nozzles
- Minimum Yield Strength for SA-182 316LN Material of RPV Nozzle Safe-Ends

Supplementary fracture toughness testing will be performed to underpin the values assumed in the defect tolerance assessment as described in Reference 20A.57.

20A.2.1.2.3 Tight Control on Chemical Composition is Enforced to Minimise the Effects of Irradiation Embrittlement or Thermal Ageing

The RV base material and welding material chemistry will be controlled such that material susceptibility to neutron damage is as low as practicable. In the RV beltline region (i.e., upper shell, lower shell, transition ring, and the two girth welds at the top and bottom of the lower shell) a complete chemical analysis will be performed on the forgings, plates, and as deposited weld metal (excluding cladding) used.

The materials used for the beltline region will be restricted to the following maximum limits of nickel, copper, phosphorus, vanadium, and sulphur due to neutron fluence which is more than 1 x 10^{17} (n/cm^2).

As deposited weld metal:	Base metal:
copper – 0.06%	copper – 0.06%
phosphorus – 0.01%	phosphorus – 0.01%
vanadium – 0.05%	vanadium – 0.05%
sulphur – 0.01%	sulphur – 0.01%
nickel – 0.85%	nickel – 0.85%

20A.2.1.2.4 Materials are Compatible with Each Other and with the Environment and are Resistant to Environmental Degradation over the life of the plant. Degradation Characteristics are Known and Understood.

The materials selected for use in the RV will be compatible with the full range of internal and external environmental conditions which may be encountered over the plant life and are predicted not to degrade to an unacceptable degree in that time. These environmental conditions include temperature, humidity, radiation, chemistry of fluid or materials in contact, and other external conditions which may affect the suitability of a material.

To prevent corrosion of low alloy steel component in contact with primary coolant, all principal pressure-retaining components made from such materials, including the RV, have corrosion-resistant cladding on surfaces exposed to the reactor coolant. Clad surfaces will be "L" grade austenitic stainless steel and welds and buttering will be "L" grade austenitic stainless steel or Ni-Cr-Fe Alloy. The stainless steel cladding surfaces will meet all of the requirements of Westinghouse Material Specification for Austenitic Cladding (Reference 20A.26). For multiple layer stainless steel cladding, the stainless steel cladding will be Type 308L stainless steel weld metal with Type 309L stainless steel weld metal used for the first layer. The corrosion resistance of the cladding material is at least equivalent to the corrosion resistance of Types 304 and 316 austenitic stainless steel alloys or nickel-chromium-iron alloy, martensitic stainless steel, and precipitation-hardened stainless steel.

Austenitic stainless steel materials such as those used on the nozzle safe ends and nickel-chromium-iron alloy base materials such as those used on the CRDM penetrations (Alloy 690) are used in the solution-annealed or thermally treated conditions. These heat treatments are as required by the material specifications according to a laboratory-derived treatment process and are generally consistent with industry-accepted procedures. High margins against primary water stress corrosion cracking exist with the specification of thermally treated Alloy 690 over the range of anticipated operating environments. The use of materials with a low resistance to PWSCC is prohibited.

AP1000 design prohibits the use of sensitised stainless steel for safety related components. All austenitic stainless steels are solution annealed and are therefore not in a sensitised condition.

Compatibility with external insulation and environmental atmosphere is also an important consideration both during normal operation and during shutdown plant conditions. The reactor vessel insulation is reflective insulation similar to that in use in current pressurised water reactors. The reactor vessel insulation (including the insulation around the lower head) is mounted on a structural frame supported from the wall and floor of the reactor cavity; and is not in direct contact with the vessel. The insulation for the closure head flange is supported by the seal ledge. In the event of coolant leakage, the ferritic materials will show increased general corrosion rates. Ferritic materials exposed to coolant leakage can be readily observed as part of the in-service visual and/or non-destructive inspection programme to confirm the integrity of the component for subsequent service.

To guard against potential liquid metal embrittlement, all stainless steel and Ni-Cr-Fe Alloy will be free from deliberate addition of low melting point materials as alloying constituents such as lead, zinc, cadmium, tin, antimony, mercury, bismuth, sulphur and their compounds. If any of these impurities exist in the stainless steel and/or Ni-Cr-Fe Alloy, the data will be reviewed and approved by Westinghouse. These low melting-point elements, their alloys and compounds, are also restricted with regard to their use as construction materials, erection aids, cleaning agents and coatings for finished surfaces of the RPV that are in contact with RCS fluid. Lead or aluminium tipped prods may be used for magnetic particle examination of ferritic materials to which the stainless steel or Ni-Cr-Fe Alloy attaches. The use of copper prod tips is prohibited during magnetic particle examinations.

20A.2.1.2.5 Materials Testing Demonstrates that the Material Properties are Compliant with the Relevant Specifications

The mechanical testing requirements for each material are contained within the relevant material specifications as identified in the RV Design Specification and identified in Table 20A-5. For the RV main forgings the mechanical property tests will consist of Tensile Tests, Drop Weight Tests and Charpy V-Notch Impact Tests. These will be carried out in accordance with ASME III Section NB-2000.

Tensile Tests

Tensile tests will be carried out to confirm that the material properties satisfy the minimum tensile strength values given specified by ASME. Of specific note, in addition to the minimum tensile strength values given in SA-540, the closure studs, nuts and washers should not exceed the tensile strength limitations specified in NRC Regulatory Guide 1.65 (Reference 20A.9).

Impact Tests

The impact test specimens will be obtained after both the quenching and tempering operations and the forming operations, regardless of sequence. Each forging will have an equal number of impact test specimens taken at each of 2 locations 180° apart at the 1/4T x T test depth and will be oriented in a direction normal to the Primary Working Direction (PWD) (other than the thickness direction). Additionally all the forgings will have specimens, located as above, removed oriented in a direction parallel to the PWD.

Drop Weight Tests

Sufficient drop weight tests will be run to determine the actual nil-ductility transition temperature (NDTT) or nil-ductility temperature for each forging. The Design Specification requires that the NDTT will not be higher than minus -23.3°C (10°F). T_{NDT} as defined by ASME Code will be considered as the actual NDTT determined by drop weight tests.

Charpy V-Notch Impact Tests

Charpy V-notch impact tests will be performed for each location at a temperature not higher than the T_{NDT} temperature plus 33.3°C (T_{NDT} plus 60°F). For each test location, the RT_{NDT} temperature will not be higher than minus -23.3°C (10°F). The minimum upper shelf impact value will be 101.7 J (75 ft-lbs) for the upper shell, lower shell, and transition ring forging in both the longitudinal and transverse directions.

Fracture Toughness Tests

Fracture toughness tests will be performed on all ferritic base materials and weld metals used for the RV pressure boundary. Testing will be performed to establish the T_0 Reference temperature in accordance with ASTM E1921-05 (Reference 20A.51). Test specimen location and orientation will be in accordance with Code, Section, Section III subsection NB-2300. Except for the core beltline region, the RPV will be designed and fabricated such that the initial nil ductility transition temperature (RT_{NDT}) at the most limiting location is not greater than -12.2°C (10°F). The initial RT_{NDT} in the core belt region forgings will not exceed -23.3°C (-10°F) and the core belt region welds will not exceed -55.5°C (-68°F).

The calculated end-of-life (60 years of service) RT_{NDT} or RT_{PTS} caused by irradiation for core belt materials will not exceed 132.2°C (270°F) for forgings and 148.9°C (300°F) for welds as specified in Regulatory Guide 1.99 (Reference 20A.27) and indicated in Table 20A-6. End-of-Life RT_{PTS} (also equals RT_{NDT}) will be determined for as-built material. The preliminary RT_{PTS} for the beltline forging and beltline weld are 34.4°C (94°F) and 37.8°C (100°F) respectively.

Prior to fuel load, verification of plant-specific belt line material properties will be provided to confirm that assumptions used in the design assessment design assessment remain valid. This will form part of the site specific justification and will include a pressurised thermal shock evaluation based on as-procured RV material data and the projected neutron fluence for the plant design objective of 60 years. The related portions of the supplementary fracture toughness testing described in Reference 20A.57 will also be completed.

20A.2.1.2.6 Reactor Vessel Surveillance Material

To evaluate the effect of radiation damage on beltline fracture toughness properties, a number of surveillance samples will be installed within the RPV. The assessment is based on the comparison of the results from pre-irradiation testing of Charpy V-notch, 1/2-T compact tension (CT) fracture mechanics test specimens and tensile specimens and post-irradiation testing of Charpy V-notch, tensile, and 1/2-T CT specimens removed at different time through the plant lifetime. The programme is directed toward evaluation of the effect of radiation on the fracture toughness of RV steels based on the transition temperature approach and the fracture mechanics approach, and is in accordance with ASTM E185 (Reference 20A.28). Further details of this are included in Section 20A.2.4.3.1.

20A.2.1.3 **Good Manufacturing**

In order to demonstrate that the good manufacturing process will be used, evidence to substantiate the following arguments is provided.

- RV components will be manufactured by experienced suppliers with a track record for producing similar components.
- High confidence in RV manufacturing quality can be taken from compliance with ASME III and the experience embodied within the code.
- Approved welding procedures and qualified operators are used.
- Repairs and deviations from the design intent will be recorded.
- Manufacturing and procedural controls ensure quality of forging material.
- Manufacturing records and Procedures.
- Quality Assurance.

20A.2.1.3.1 Reactor Vessel Components will be Manufactured by Experienced Suppliers with a Track Record for Producing Similar Components Using Proven and Established Techniques

The supplier for the RV has not yet been selected. However, in selecting the manufacturer for the heavy pressure vessels, a detailed technical evaluation of the suppliers ability to comply with the Design Specification (Reference 20A.2) and quality assurance requirements will be undertaken, giving particular attention to the suppliers ability with regard to achievement of the material compositional requirements including minimum fracture toughness requirements, the methods for the qualification of weld procedures and the ability to carry out the required range of inspections during manufacture. The evidence to support this argument form part of a site specific justification.

The RV components will be joined by welding, using the single or multiple wire submerged arc and the shielded metal arc processes or other established techniques. Gas metal arc welding and plasma arc welding are acceptable methods of applying buttering for dissimilar metal welds. The use of severely sensitised stainless steel as a pressure boundary material is prohibited and is eliminated by either a select choice of material or by programming the method of assembly. At locations in the RV where stainless steel and nickel-chromium-iron alloy are joined, the final joining beads are nickel-chromium-iron alloy weld metal in order to prevent cracking. The location of full penetration weld seams in the upper CH and vessel bottom head are restricted to areas that permit accessibility during ISI. The stainless steel clad surfaces are sampled to demonstrate that composition requirements are met.

20A.2.1.3.2 High Confidence in Reactor Vessel Manufacturing Quality can be Taken from Compliance with ASME III and the Experience Embodied Within the Code

Design and fabrication of the RV is carried out in accordance with ASME Code, Section III, Class 1 requirements and manufactured using well established procedures. Details of manufacturing codes and standards are provided in Reference 20A.2 with certain more stringent requirements defined in Reference 20A.29. Compliance with the code and the experience embodied within the code provides a high degree of confidence that high quality

has been achieved and also that the vessel will be tolerant to minor variations in material properties and minor imperfections in fabrication. Measures, described in the following Section, are over and above minimum code requirements and provide additional confidence that the vessel will enter service free from defects of structural significance.

20A.2.1.3.3 Approved Welding Procedures and Qualified Operators are used to Minimise Defect Occurrence

As detailed in Reference 20A.2, welding of all materials will be done in accordance with welding procedures and using certified welders that have been qualified according to the rules of Sections III and IX of the ASME Code as well as the additional requirements identified in the RV Design Specification (Reference 20A.2) and the supplemental requirements detailed in Reference 20A.29. Control of welding variables (as well as examination and testing) during procedure qualification and production welding is performed according to ASME Code requirements. Specific details of welding processes, selection and control of welding consumables, welding procedure qualification, pre-heat, interpass temperatures and post heating requirements and specific control for cladding and buttering are provided in Reference 20A.29.

The penetration to head J-groove welding procedures will be qualified in accordance with the applicable requirements of Section IX of the ASME Code. Full-scale mock-up qualification tests will be performed. The tests will include metallography, measurement of residual stress and ultrasonic examinations to confirm ultrasonic inspectability.

20A.2.1.3.4 Repairs and Deviations from the Design Intent will be Recorded. Approval for Deviations from the Design Intent will be Appropriate with Justification where Necessary.

The requirement to record major/minor repairs and deviations for the design intent is stated within the RV Design Specification (Reference 20A.2). Deviation reports or deviation notices (DNs) will be prepared by the manufacturer for all conditions that do not meet requirements and cannot be corrected using previously approved repair procedures. Deviations/defects that are identified during processing/fabrication, which will not affect the final fit-up/function (e.g., weld defects) of the final component and which may be repaired by previously approved repair procedures, will not need to be submitted for Westinghouse approval as a DN. However, these will be recorded for future reference. The requirements placed on the manufacturer include the reporting criteria and the conditions under which formal review and approval by Westinghouse will be required. The following should be noted:

- All major repairs to base material and pressure boundary welds will be subjected to formal review by Westinghouse before approval to proceeding with the repair is granted.

- All arc strikes on pressure boundary and accessible non-pressure boundary materials will be removed and the areas ground to a smooth contour with a 4:1 taper. Any arc strike that exceeds a depth of 2.54 mm (0.10 inches) will be documented and reviewed by Westinghouse for approval.

- Repairs by welding will be cleared by the same NDE technique/procedure by which the indications were found.

- The location of these repairs will be identified on the as-built weld seam drawing for permanent record and may be required to be permanently marked on the vessel or head when so indicated in the deviation notice disposition.

- No repair welding is permitted to the J-groove welds without first performing full size mock-up qualification tests and measurement of residual stress to optimise the repair technique.

20A.2.1.3.5 Manufacturing and Procedural Controls Ensure Quality of Forging Material

The RV shell, lower head, nozzles and CH will be manufactured from high quality forgings supplied by an experienced forge master, working to approved procedures to meet relevant product specifications, which are compliant with ASME requirements. Individual material specifications for belt line and non beltline SA-508 Grade 3 Class 1 forgings and Stainless steel forgings are provided in the relevant material specifications as listed in the technical index. These provide specific details of controls on chemical composition, microstructures, heat treatment, materials testing, grain size evaluation and ultrasonic examination to ensure that the final product has the desired through thickness properties and is free from forging defects.

20A.2.1.3.6 Manufacturing Records and Procedures

To ensure that there is a high degree of control over the achievement of high quality during manufacture, the following controls on the manufacturing records and procedures are specified as part of the component design specification.

Weld Procedures

To ensure that weld procedures are acceptable, all procedures for weld and weld repair and base metal repair will be submitted to Westinghouse for approval prior to use in fabrication. Review and approval by Westinghouse of these documents is based on compliance with the applicable references, the RV specification and also on technical justification.

All welding procedure specifications to be used in the fabrication the RV will be prepared in accordance with a general welding procedure specification and the requirements of Sections III of the ASME Boiler and Pressure Vessel Code.

Heat Treatment

Heat treatment specifications will be approved prior to manufacture and will include the following (where applicable).

- Holding times for austenitising and tempering
- Rates of heating
- Temperature control
- Temperatures for the austenitising and tempering operations during heating/holding
- Time from the furnace to the quench tank
- Quenching medium
- Cooling method

Material Records

All material ordering specifications (including heat treatment and base metal repair procedures) will be submitted to Westinghouse for approval prior to material procurement. This includes all welding consumables. Each chemical analysis including both ladle and check, physical and mechanical mill test data sheets, supplier test data sheets, weld material certifications, and inspection reports for materials required by the Design Specification and

applicable references will also be provided. The Supplier will provide certified chemical and mechanical properties of the weld metal used for full penetration pressure boundary welds in the vessel and CH, any weld repairs to these welds, and all base metal weld repairs.

Manufacturing Inspections

Each NDE examination report will be submitted to the Westinghouse after the completion of each examination. Defects will be recorded and defect tolerance studies will be carried out by Westinghouse to ensure that recorded indications do not present a concern over the design life of the plant.

Dimensional Checks

The dimensional profile document will be used to record vessel and CH as-built dimensions. This information will be in accordance with the dimensions required by the Westinghouse as-built drawing format.

Cleaning and Contamination Protection Procedures

Materials used in the fabrication, installation, and testing of nuclear steam supply components and systems are handled, protected, stored, and cleaned according to recognised, accepted methods designed to minimise contamination that could lead to cracking.

20A.2.1.3.7 Quality Assurance

Activities affecting the quality of items and services for the AP1000 Project during design, procurement, fabrication, inspection, and/or testing are performed in accordance with the quality plan described in "Westinghouse Electric Company LLC Quality Management System (QMS)", Revision 7 (Reference 20A.30) to satisfy the requirements of 10 CFR 50 Appendix B. The following requirements are identified in Reference 20A.31.

For items designated as ASME Boiler & Pressure Vessel Code (BPVC) Section III, the Quality Assurance Programme applicable to the manufacture of the RV will meet the following requirements:

- 10 CFR 50 Appendix B – "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants"
- US Nuclear Regulatory Commission, Regulatory Guide 1.28, "Quality Assurance Program Requirements (Design and Construction)," Revision 3, August 1985
- ASME NQA-1-1994, "Quality Assurance Requirements for Nuclear Facility Applications"
- ASME B&PV Code, "Section III, Rules for Construction of Nuclear Power Plant Components," 1998 Edition through 2000 Addenda
- The RV Supplier will reference the ASME certificate number and expiration date on the applicable pages of the data package certification(s)

For items designated as Non-ASME B&PV Code, Safety-Related, the Quality Assurance Programme will meet the following requirements:

- 10 CFR 50 Appendix B – "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants"
- US Nuclear Regulatory Commission, Regulatory Guide 1.28, "Quality Assurance Program Requirements (Design and Construction)," Revision 3, August 1985
- ASME NQA-1-1994, "Quality Assurance Requirements for Nuclear Facility Applications"

20A.2.1.4 Manufacturing Inspection

Materials and fabrication processes are well designed in order to demonstrate that the AP1000 RV enters service free of significant defects, which will be confirmed by an effective manufacturing NDT inspection programme. Evidence to substantiate the following arguments required to meet the claimed objective is provided:

- Manufacturing inspections meet or exceed the requirements of ASME.
- Reliability of NDT is assured through a "Design for Inspection" philosophy.
- NDT performed at key stages of manufacture assures the high quality of the completed RV and its steel components.
- Qualified inspection performed on high safety significant components demonstrates a good safety margin.
- Qualified inspection of HSS components confirms the plant is free of defects meeting ASME Section XI criteria.
- The results of NDT performed at key stages of manufacture demonstrate a low frequency of significant defects in forgings and welds.
- The results of NDT performed confirm no degradation during key stages of manufacture.

20A.2.1.4.1 Manufacturing Inspections Meet or Exceed the Requirements of ASME

A diverse range of effective NDT methods and techniques are deployed at various manufacturing stages to ensure that steel forgings, plate, welds and cladding in the RV enter service free of significant manufacturing defects. The scope of the manufacturing NDT and the techniques applied either meet or exceed the requirements of ASME Section III and is summarised in Table 20A-7.

All repairs made as a result of NDT findings are subsequently inspected using the same NDT method(s) that originally detected the defect leading to the repair. For Class 1 welds, this compliance with ASME NDT requirements provides the adequate assurance regarding the achievement of manufacturing quality.

20A.2.1.4.2 Reliability of NDT is Assured through a "Design for Inspection" Philosophy

The AP1000 incorporates a "Design for Inspectability" philosophy (Reference 20A.32) in which the RV welds and surrounding areas are designed to facilitate NDT by:

- Ensuring a good surface finish for deploying the range of techniques.
- Enabling good access for NDT personnel and equipment.
- Providing sufficient access for deploying angle beam ultrasonic to give full volumetric coverage.
- Providing as many inspection surfaces/scanning directions as possible.

20A.2.1.4.3 NDT Performed at Key Stages of Manufacture Assures the High Quality of the Completed RV and its Steel Components

Sensitive volumetric and surface NDT methods are applied at points in the manufacturing programme that ensure any necessary repairs are undertaken at the earliest possible stage and that any degradation resulting from processes such as post-weld heat treatment is identified.

Supplemental inspections, additional to those specified by ASME Section III, are performed that match the pre-service inspection and in-service acceptance criteria of ASME Section XI. Here the objective is to reconcile the difference in acceptance standards between ASME III and ASME XI and ensures that the PSI does not report rejectable defects that were not identified as such during the standard manufacturing NDT (Reference 20A.2)

20A.2.1.4.4 Qualified Inspection Performed on Highest Safety Significant (HSS) Components Demonstrates a Good Safety Margin

Qualified ultrasonic volumetric inspections will be performed on HSS locations, identified in Table 20A-1, after the final post-weld heat treatment to provide a very high level of confidence that the RV enters service free of any defect that could threaten the structural integrity. A procedure for manufacturing NDT qualification of welds has been outlined. Target sizes for manufacturing defects for HSS welds have been derived from elastic-plastic fracture mechanics by calculating the end-of-life limiting defect sizes and fatigue crack growth in accordance with the R6 methodology. NDT performed with currently available tried and tested ultrasonic techniques provides a detect and reject capability that demonstrates a defect size margin (DSM) of 2 or greater. The basis for this is discussed in Section 20A.2.3.1. High reliability for these inspections will be demonstrated through qualifying the inspection system (procedure, equipment, and personnel) using the principles specified in the European Network for Inspection and Qualification (ENIQ) European methodology for qualification of non-destructive tests (Reference 20A.33). For selected HSS welds, a manufacturing inspection plan has been produced which provides the physical reasoning underpinning the claimed inspection capability; this is discussed in Section 20A.2.3.1.4. The manufacturing inspection plans were developed following a process (Reference 20A.56) which is based on the preparation of technical justifications described in ENIQ methodology. A process will be developed in due course to address parent material associated with HSS locations.

A rigorous approach to classification based on failure modes and consequences has identified the following pressure boundary welds as HSS (locations are further described in Table 20A-1):

1. RV shell circumferential welds (Locations 1.1, 1.2, 1.3)
2. RV primary circuit nozzle to shell welds (Location 2.1)
3. DVI Nozzle to shell welds (Location 3.1)
4. RV nozzle to safe end transition welds (Locations 2.2, 3.2)

The RV safe-end to inlet/outlet loop pipe welds have been assessed as HI. This is discussed in Section 20E.3.1.8.

20A.2.1.4.5 Qualified Inspection of HSS Components Confirms the Plant is Free of Defects Meeting ASME Section XI Criteria

The final stage of NDT for HSS welds is the application of qualified mechanised UT systems to confirm the welds are free of any defects that exceed the ASME Section XI criteria. These inspections have two purposes:

- They provide additional high reliability inspections at the end of all manufacturing stages.
- They generate a "finger-print" set of data against which future ISI results can be compared. By establishing that acceptable indications found during ISI were also present at PSI fabrication, potential unnecessary repairs are avoided.

20A.2.1.4.6 The Results of NDT Performed at Key Stages of Manufacture Demonstrate a Low Frequency of Significant Defects in Forgings and Welds

Experience shows that materials and manufacturing processes similar to those chosen for the AP1000 plant lead to a low frequency of defect occurrence. Nevertheless, sensitive volumetric and surface NDT methods are applied at points in the manufacturing programme to confirm that the materials and processes used for the forging and welds are well designed.

20A.2.1.4.7 The Results of NDT Performed Confirm no Degradation during Key Stages of Manufacture

Effective NDT inspections of HSS welds will be performed before and after post-weld heat treatment and hydrotest to confirm that no damage occurs as a result of these processes.

20A.2.1.5 Plant Operation and Maintenance

In order to demonstrate that the plant will be properly operated and maintained, evidence to substantiate the following arguments is provided.

- AP1000 Pressure/Temperature limits are clearly defined in accordance with recognised procedures and are suitably conservative.
- The AP1000 RCS chemistry specification is clearly defined and measures are in place to control corrosion of the reactor vessel.
- Records of operation and maintenance will be maintained to confirm compliance with procedural requirements.
- Incidents involving transgressions of set limits will be investigated.
- Procedures are in place to control maintenance activities.
- ISI will detect defects before they compromise structural integrity.

Westinghouse document UKP-GW-GL-501 (Reference 20A.50) presents the generic AP1000 technical specifications. The AP1000 technical specifications are consistent with the Standard

Technical Specifications – Westinghouse Plants, NUREG-1431, Reference 20A.52, to the maximum extent possible. The AP1000 technical specifications differ from those in NUREG-1431 only as necessary to reflect technical design differences between the "typical" Westinghouse design and the AP1000 design.

In order for the operators to safely operate and maintain the AP1000 plant, operating and maintenance manuals that are fully compliant with the technical specifications will be produced in due course. Regarding the RV, the following issues are considered the most pertinent at this stage in terms of providing assurances that the plant will be properly operated and maintained in such a way that minimises through-life degradation.

20A.2.1.6 AP1000 Pressure/Temperature Limits are Clearly Defined in Accordance with Recognised Procedures and are Suitably Conservative

Irradiation on the beltline regions of RV steels will lead to increasing embrittlement through life. The degree of embrittlement is sensitive to the material composition, most specifically in terms of percentage copper and nickel level, and also the cumulative dose and the flux rate. This embrittlement results in a degradation of the material's fracture toughness and increases the vulnerability to non-ductile failure. It is therefore necessary to demonstrate that the AP1000 reactor pressure vessel is designed with sufficient margin to assure that when stressed under operating, maintenance, testing, and postulated accident conditions that the boundary behaves in a non-brittle manner and that the probability of rapidly propagating fracture is minimised.

To guard against this, heatup and cooldown pressure/temperature (P/T) limit curves are provided to protect the RV during start-up and shut down and so minimise the possibility of brittle fracture. These curves take account of through life degradation effects such as irradiation embrittlement and other ageing effects. The assessment is undertaken using the methods outlined in Appendix G of Section III of the ASME Code. The approach specifies that the allowable stress intensity factors under limiting transients for specified defect sizes, typically T/4, do not exceed the ASME reference stress intensity factor for the metal temperature. Operating specifications include conservative margins for predicted changes in the material reference temperatures due to irradiation and a factor of safety on the primary load for normal and test conditions. Details of the derivation of the P/T limit curves are provided in Reference 20A.34, which has been carried out in accordance with the approach defined in Reference 20A.35.

The P/T limit curves are composite curves established by superimposing limits derived from stress analyses of those portions of the RV and head that are the most restrictive. At any specific pressure, temperature, and temperature rate of change, one location within the RV will dictate the most restrictive limit. Across the P/T span of the limit curves, different locations are more restrictive, and, thus, the curves are composites of the most restrictive regions. The heatup curve represents a different set of restrictions than the cooldown curve because the directions of the thermal gradients through the vessel wall are reversed. The thermal gradient reversal alters the location of the tensile stress between the outer and inner walls.

The through life degradation is measured in terms of the adjusted Reference nil ductility temperature. This includes a reference nil ductility temperature shift (ΔRT_{NDT}), initial RT_{NDT} and margin. Predicted ΔRT_{NDT} values are derived considering the effect of fluence and copper and nickel content for the RV steels exposed to 288°C (550°F) temperature. The approach defined in US NRC Regulatory Guide 1.99 (Reference 20A.27) has been used in calculating the adjusted Reference temperature. The P/T curves are developed considering the

irradiation embrittlement appropriate to 54 effective full power years consistent with the plant design objective of 60 years with 90 percent availability. Copper and nickel contents and initial RT_{NDT} for materials in the RV beltline region and the RV flange and the CH flange region are shown in Table 20A-8 and Table 20A-9, respectively.

The P/T curves are shown in Figure 20A-5 and Figure 20A-6. These are generic curves for AP1000 RV design, and they are the limiting curves based on copper and nickel material composition. However, for a specific AP1000 plant, these curves will be plotted based on measured percentage copper and nickel. The use of plant-specific curves also requires evaluation of the low temperature overpressure protection (LTOP) system. This includes an evaluation of the setpoint pressure for the normal residual heat removal system relief valve by the site licence holder to determine if the setpoint pressure needs to be changed based on the plant-specific pressure-temperature curves. The development of the plant-specific curves and evaluation of the setpoint pressure are required prior to fuel load.

The results of the material surveillance programme described in section 20A.2.4.2.1 will be used to verify the validity of ΔRT_{NDT} used in the calculation for the development of heatup and cooldown P/T limit curves. The projected fluence, copper, and nickel contents along with the RT_{NDT} calculation will be adjusted if necessary, from time to time using the surveillance capsule results. This may require the development of new P/T limit curves.

Due to the magnitude of irradiation embrittlement, the P/T limit curves developed for the beltline region are sufficiently bounding such that no unirradiated ferritic materials in other components of the RCS will be limiting in the analysis.

It is recognised that the imposition of more onerous P/T limits will provide higher safety margins for any single incident but it is likely to result in more unplanned reactor shutdowns throughout the reactor's operational life, each of which will introduce its own series of additional thermal and stress cycles.

20A.2.1.6.1 The AP1000 RCS Chemistry Specification is Clearly Defined and Measures are in Place to Control Corrosion of the Reactor Vessel

The RCS chemistry specifications, the control of chemistry and the compatibility of primary coolant boundary materials with the RCS chemistry are detailed in Sections 21.5.5 and 21.5.9. In summary, the RCS water chemistry is selected to minimise corrosion and routinely scheduled analyses of the coolant chemical composition are performed to verify that the reactor coolant chemistry continues to meet the specifications. Other additions, such as those to reduce activity transport and deposition, may be added to the system. The RCS chemistry specifications conform to the recommendation of US NRC Regulatory Guide 1.44 (Reference 20A.53).

The chemical and volume control system (CVS) provides a means for adding chemicals to the RCS. The chemicals perform the following functions:

- Control the pH of the coolant during pre-start-up testing and subsequent operation.
- Scavenge oxygen from the coolant during heatup.
- Control radiolysis reactions involving hydrogen, oxygen, and nitrogen during power operations following start-up.

The values presented in Table 20A-3 are bounding for chemistry operational control of primary fluids that are in contact with primary system materials and nuclear fuel. The operational chemistry programme may apply stricter limits as deemed appropriate.

20A.2.1.6.2 Records of Operation and Maintenance will be Maintained to Confirm Compliance with Procedural Requirements

Details of the quality assurance requirements during the operational phase are detailed in Sections 3.4.4 and 7.7. This will be considered as part of the Site Specific Justification.

20A.2.1.6.3 Incidents Involving Transgressions of Set Limits will be Investigated

The RV P/T limits, including heatup and cooldown rates will be contained in the pressure and temperature limits report. These pressure and temperature limits will be determined for each fluence period. Plant operation within these operating limits is specified within the technical specification. Limiting conditions for operation (LCOs) specify minimum requirements for ensuring safe operation of the unit. The following LCOs are relevant to the P/T limits.

- LCO 3.4.3, “RCS P/T Limits”
- LCO 3.4.14, “LTOP System”
- LCO 3.4.2, “RCS Minimum Temperature for Criticality”

The consequence of violating the LCO limits is that the RCS has been operated under conditions that can result in brittle failure of the RCPB, possibly leading to a non-isolable leak or LOCA. In the event that these limits are exceeded, an evaluation must be performed to determine the effect on the structural integrity of the RCPB components. ASME Code, Section XI, Appendix E (Reference 20A.7) provides a recommended methodology for evaluating an operating event that causes an excursion outside the limits.

20A.2.1.6.4 Procedures are in Place to Control Maintenance Activities

As specified in the Reactor Vessel Design Specification (Reference 20A.2), the Reactor Vessel Instruction Manual provided by Westinghouse will contain detailed instructions for the maintenance of the RV equipment. This will need to be developed further as part of the site specific safety case.

20A.2.2 Leg 2: Functional Testing

The objective of the functional testing leg of the safety case is to confirm the good standards applied in RV design, fabrication and installation identified in Section 20A.2.1 result in an installed component that is fit for purpose. Hydrostatic pressure tests are conducted to verify that the RV is proofed against its design pressure, and similar tests are periodically carried out to affirm that RCPB integrity will be maintained at the design pressure throughout component lifetime. Two elements are built up to support this claim. These are:

- The RV has been subject to proof testing
- Testing is carried out to confirm RV functionality

These provide evidence that functional testing of the RV will be conducted to ensure fitness for purpose at start of life (SoL) and continued integrity of the pressure boundary for the design life

20A.2.2.1 The Reactor Vessel has Been Subject to Proof Testing

In order to demonstrate that the RV will be subject to proof testing evidence to substantiate the following arguments is provided.

- The RV is subject to hydrostatic pressure testing to verify pressure boundary integrity at design pressure prior to operation.

20A.2.2.1.1 The RV is Subject to Hydrostatic Pressure Testing to Verify Pressure Boundary Integrity at Design Pressure Prior to Operation

The hydrostatic pressure test contributes to the safety case in a number of ways but principally it provides assurance regarding the basic strength of the assembled vessel, the absence of gross manufacturing defects and evidence of out of specification material properties. It is recognised that the hydrostatic pressure test provides less strength to the safety case at locations where defect tolerance may be dominated by thermal stresses. At such locations, assurance is provided by inspection to confirm the absence of structurally significant defects supported by defect tolerance justifications.

Details of the RV hydrostatic pressure testing requirements are specified in Section 8.4 of Reference 20A.2. The test will be conducted in accordance with the requirements of Article NB-6000 of the ASME Code; the hydrotests comply with IWA-5000 and IWB-5000 of the ASME Code, Section XI. Two tests will be carried out, the first a shop hydrotest and the second as part of the system hydrotest following installation.

The minimum hydrostatic pressure test temperature will be 33.3°C (60°F) above the highest RT_{NDT} established from materials testing. The procedure by which RT_{NDT} is established is described in Section 20A.2.1.4. The minimum hydrostatic test pressure will be equal to 1.25 times the design pressure which is 21.55 MPa (3125psi) as defined in Reference 20A.36. This will be held for at least 10 minutes and then reduced to the design pressure of 17.24 MPa (2500 psi) and examined for leaks. Reference 20A.36 describes the RV hydrotest procedure. The CRDM housing is similarly hydrotested to 125% of the system design pressure in the factory, after installation and as part of the assembled system.

No leakage during the hydrostatic pressure test is acceptable. The hydrostatic test will be witnessed by an Authorised Nuclear Inspector (ANI) and a Westinghouse representative. A

report will be provided to confirm that the results of the hydrostatic test of the RV conform to the requirements of the ASME Code Section III.

Section 8.3 of Reference 20A.2 describes a range of NDEs that are to be conducted following the hydrostatic pressure test of the RV. These include liquid penetrant and magnetic particle surface examinations, and repetition of ultrasonic examinations of pressure boundary welds to ensure that the Section XI pre-service examination acceptance criteria can be satisfied. Full details of the pre-service testing arrangements are given in Section 20A.2.1.6.

As shown in Table 20-22, the RCS is designed for 10 cycles of hydrostatic pressure tests through the design lifetime of 60 years if required. Each RCS hydrostatic test is assumed to be conducted at a water temperature compatible with reactor material ductility requirements and a test pressure of 1.25 times design pressure.

20A.2.2.2 Testing is Carried Out to Confirm Reactor Vessel Functionality

In order to support the claim that functional testing demonstrates RV fitness-for-purpose the following arguments are made.

20A.2.2.2.1 Functional Testing Has Been Specified

Section 7.5 describes an initial testing programme for AP1000 plant. The overall objective of the programme is to demonstrate that the plant has been constructed as designed, that systems perform consistent with the plant design, and that activities culminating in operation at full licensed power including initial fuel load, initial criticality, and power ascension are performed in a controlled and safe manner.

Pre-operational tests for all systems with safety related functions are specified to confirm that these functions will be maintained in operation. Pre-operational testing [1] of the RCS is specified in Section 7.5.6. Prerequisites to the pre-operational testing are identified; these include completion of the hydrostatic proof testing of the RV as described in Argument 2.1. Pre-operational testing of the RCS including the RV is conducted to verify that the as-installed RCS will fulfil the following safety-related functions:

- Provide RCS pressure boundary integrity.
- Provide core cooling and boration in conjunction with the PXS.
- Measure process parameters required for safety-related actuations and safe shutdown.
- Measure selected process parameters required for post-accident monitoring.
- Vent the RV head.

Pre-operational testing of the RCS is also performed to verify that the system fulfils the following defence in depth functions:

- Provide forced circulation cooling of the reactor core in conjunction with heat removal by the steam generator(s).

- Provide core cooling by natural circulation of coolant in conjunction with heat removal by the steam generator(s)

1. N.B. Pre-operational tests at elevated pressure and temperature are referred to as hot functional tests.

- In conjunction with the steam generator(s) and normal residual heat removal system, provide the capability to remove core decay heat and cool the reactor coolant to permit the reactor to be refuelled and started up in a controlled manner

- Provide pressuriser pressure control during normal operation

- Provide pressuriser level control in conjunction with the CVS

- Provide pressuriser spray

Pre-operational testing includes measures to confirm the integrity and leak tightness of the RCS and the high-pressure portions of associated systems. The RV is included within the scope of these tests. Structural integrity is verified by performing a cold hydrostatic pressure test in conformance with Section III of the ASME Code. Leakage monitoring during hot functional testing is conducted to confirm that any RCS leakage is within limits specified in the Technical Specifications.

A series of start-up test procedures is developed to confirm safe and controlled operation during activities culminating in operation at full licensed power. As is the case for pre-operational testing, these start-up tests are applicable to systems rather than individual components such as the RV.

20A.2.3 Leg 3: Failure Analysis

Leg 3 of the safety case provides an assessment of the effects of through-life degradation mechanisms on potential manufacturing defects to show that such mechanisms will not threaten vessel integrity over the plant design lifetime. This goes beyond design code requirements to provide a further demonstration of integrity, specifically by recognising that flaws may be present following manufacture and showing tolerance to them. The arguments supplement the Leg 1 aim of avoidance of defects to provide a safety case with both defect avoidance and defect tolerance.

20A.2.3.1 RV Components are Tolerant to Manufacturing Defects for the Design Life of the Plant

This section describes the scope of the analyses undertaken as part of the generic design assessment (GDA) process to demonstrate that the RV is tolerant to potential defects that could remain undetected after manufacturing inspection. In order to demonstrate that the AP1000 RV components are defect tolerant, evidence to substantiate the following key arguments to support the safety case will be provided in due course:

- Established methods are used to evaluate defect tolerance.

- Determination of crack growth rates and through-life crack sizes.

- Consideration of materials ageing and degradation.

- Demonstration of adequate margins between allowable SoL defect sizes and defect sizes based on suitably qualified inspections.

20A.2.3.1.1 Established Methods are used to Evaluate Defect Tolerance

As discussed in section 20.6.4.2, the following sections summarise the results of the R6 assessment for the RV and present a summary of the existing linear elastic fracture

mechanics (LEFM) assessment carried out in accordance with ASME Code, Section III, Appendix G.

Assessment using the R6 Methodology

In combination with the use of rigorous manufacturing controls and inspection qualification, the defect tolerance assessment provides the necessary understanding to support the claim, to an appropriate degree of confidence, that the vessel will enter service free from defects that could be of concern at the end of the RV's designed life. The approach to determination of the limiting defect size in a particular orientation and location and the maximum allowable SoL defect size is discussed in section 20.6.4.2. As has been stated in Reference 20A.38, the regulatory expectation is that a DSM of 2 will be achieved.

Phase 1: Weld Defect Tolerance and NDE Ranking

A detailed evaluation of selected, limiting weld locations has been made available to provide confidence that there are no regions of the RV where either low defect tolerance or low NDT inspectability would preclude the vessel design from being able to satisfy regulatory expectations and support the safety case claim for the RV. To evaluate those locations with the greatest risk of entering service with defect of structural significance, either as a result of small allowable SoL defect sizes or a large qualified examination defect size (QEDS), a ranking exercise was undertaken to consider, on a relative basis, the defect tolerance and the NDT inspectability at each of the AP1000 RV weld locations. The details of this evaluation are reported in Reference 20A.39. The selection of the locations for R6 assessment is summarised in Table 20A-15 of this report. The regions assessed are as follows:

a) Lower Shell to Upper Shell
b) DVI Nozzle to Upper Shell
c) Inlet Nozzle to Safe-End

Phase 2: Assessment of Bounding Locations

Table 20A-15 details the locations selected for detailed evaluation during the GDA. The scope of the locations that will either be directly assessed, or can be shown to be bounded by other locations is indicated in Table 20A-15. For each of the selected locations, the R6 methodology was used to determine the limiting SoL defect size. Details of the assessment methodology are provided in Reference 20A.41.

Assessments have been carried out for defects both parallel and transverse to the weld orientation, considering surface breaking defects on both the inside and outside surfaces of the vessel. Appropriate lower bound fracture toughness data were used to evaluate the margins; the supplementary testing described in Reference 20A.57 will be performed to underpin the values assumed. Material properties appropriate to the end of life conditions taking account of the effects of irradiation embrittlement, as determined using the end of life (EoL) RT_{NDT}, have been used. Fatigue crack growth has been evaluated using the ASME upper bound crack growth laws appropriate to the environment (wet or dry).

The results of the defect tolerance assessment have been used to inform an evaluation of the NDT capability at each of the highest ranked location. The results of this assessment are discussed in Section 20A.2.3.1.4.

Phase 3: Assessment of Remaining Locations

The full defect tolerance assessment of the remaining HSS/HI locations, including the selected locations in the parent material, will be carried out in due course. Once completed, the R6 assessment work for the RV will provide assurance that the QEDS is based on a robust assessment of the maximum allowable SoL defect size with appropriate consideration of materials ageing and degradation and through life crack growth.

ASME Code, Section III, Appendix G Linear-Elastic Fracture Mechanics Assessment

The ASME Code, Section III, Appendix G, "Protection against Non- ductile Failure", presents a method for obtaining the allowable loadings to protect against non-ductile failure for ferritic pressure-retaining materials in Class 1 components. Although this approach is not considered sufficient in a UK regulatory context, the results of the assessment nonetheless provide a conservative assessment of defect tolerance which is recognised internationally.

The assessment provides the basis on which the pressure-temperature limit curves described in Section 20A.2.1.6 of this report are derived. Full details of the assessment are presented in Reference 20A.42. A discussion of the methodology and the results is provided below.

This method is based on the principles of LEFM. At each evaluated location, a postulated defect is assumed. Typically, this is conservatively based on a quarter wall defect although at certain locations, ASME permits smaller defects to be used. At each location, the mode-I stress intensity factor, K_I, produced by each of the specified loadings is calculated. Then, the summation of the K_I values due to primary and secondary stresses resulting from mechanical and thermal loading during normal, upset, and test conditions is compared to a referenced stress intensity factor, K_{IR}. This Reference K_{IR} is the highest critical value of K_I allowed for the material and the temperature involved.

When interpreting the results, which are summarised in Table 20A-16, the following factors should be noted which differ significantly from the R6 methodology:

- The ASME Code, Section III, Appendix G assessment conservatively includes a factor of safety on the primary K_I of 1.5 for test conditions and 2.0 for all other conditions.
- The assessment locations are generally remote from weld locations.
- Residual stresses are not evaluated.
- The stress intensity factor is calculated based on the linearised stress distribution.
- Through life fatigue crack growth is not evaluated.
- Fracture toughness is based on the ASME K_{IR} arrest fracture toughness curve assuming an RT_{NDT} of -23.33°C (-10°F) in the beltline vessel course and -12.22°C (10°F) at other locations. Noting that the ASME Code, Section III Appendix G methodology only takes account of irradiation effects on toughness once the P/T limit curve has been derived.

The fracture mechanics evaluation was performed for several regions of the RV using the stresses and temperatures from the FEA derived stress analyses. The regions and corresponding analyses considered are:

1. Lower shell beltline core region and lower head shell region
2. CH flange and shell region

3. CH penetrations for CRDM, QuickLoc, and vent nozzles
4. Lower head core support block region
5. Inlet nozzle
6. Outlet nozzle
7. DVI nozzle

These results in Table 20A-16 compare the applied crack tip stress intensity factors with the allowable fracture toughness at the transient time and the crack tip metal temperature. The results indicate that the limiting locations are the Inlet, Outlet and DVI nozzle inside corner radius locations. The limiting locations are at the inner crotch corner locations and are remote from as-welded material. At the DVI nozzle to shell weld location, the assessment is based on a defect size of 6.36 mm (0.25 inches) and shows a limiting K_I/K_{IR} of ~0.3, indication that the defect tolerance at the weld location is significantly greater than at the corner radius. The defect tolerance of this weld and the associated inspectability has been confirmed by the R6 analysis and associated inspection qualification activities. The assumed flaw sizes used could be increased using more rigorous analyses to identify the conservatisms in the transient definitions and the use of crack initiation fracture toughness that has already been implemented in to the ASME Code, Section XI Appendix G.

20A.2.3.1.2 Determination of Crack Growth Rates and Through-Life Crack Sizes

As part of the R6 assessment the through life crack growth has been calculated in accordance with the procedures specified in the R6 procedure. This included the use of suitably conservative crack growth rates appropriate to the reactor coolant environment, based on the ASME upper bound FCG curves. As discussed in Reference 20A.41, these are considered to be conservative for modern steels with low sulphur content. The upper bound nature of these curves is supported by extensive testing worldwide.

20A.2.3.1.3 Consideration of Materials Ageing and Degradation

The material properties used in the R6 assessment will be based on lower bound properties as specified by ASME Code, Section II unless otherwise specified in Reference 20A.41. The through life shift in properties will be calculated in accordance with the procedures defined in US NRC Regulatory Guide 1.99 (Reference 20A.27) as discussed in Section 20A.2.1.6.

20A.2.3.1.4 Demonstration of Adequate Margins Between Allowable Start of Life Defect Sizes and Defect Sizes Based on Suitably Qualified Inspections

The results of the R6 defect tolerance assessments for the three RV welds identified in Section 20A.2.3.1.1 are reported in Reference 20A.46. A limiting QEDS, i.e. that leading to a DSM equal or larger than 2, has been calculated for one of two different defect aspect ratios according to flaw orientation. For flaws perpendicular to the weld axis, the QEDS is established for a defect aspect ratio of 2, since the potential length of flaws with that orientation is naturally limited by the weld width. For flaws oriented parallel to the weld axis it is recognised that flaws with higher aspect ratios may potentially occur, and a defect aspect ratio of 6 is additionally considered in determining QEDS.

Reference 20A.46 reports the limiting QEDS (i.e., leading to a DSM equal or larger than 2) for the RV welds as follows:

Weld	Limiting QEDS (mm)

RV Lower shell to upper shell weld	25
RV DVI nozzle to upper shell weld	25
RV inlet nozzle to safe end weld	6

Based on these QEDS values, Reference 20A.46 reports that the calculated values of end of life limiting defect size (ELLDS) and lifetime fatigue crack growth (LFCG) establish a DSM larger than 2 in all cases. Demonstrating the capability for qualified inspection of these RV welds is considered bounded by the inspection techniques defined and assessed for other AP1000 HSS welds as summarised below.

Reference 20A.47 including applicable amendments provides the technical basis for an array of inspection techniques applied on the RPV inner and outer surfaces to support detection and characterisation of both surface-breaking and near-surface breaking planar defects having a height of 25 mm in the RV lower shell to upper shell and DVI nozzle to upper shell welds. This basis included previous work associated with the Sizewell B manufacturing NDT inspections, the United Kingdom Atomic Energy Authority defect detection trials (DDT), qualified inspections used in Sweden and the USA, and common industry approaches. The technical basis of the inspection techniques described in Reference 20A.47 has been reviewed by an independent qualification body, the inspection validation centre (IVC), and the inspection techniques were deemed to be capable of formal qualification.

Reference 20A.48 including applicable amendments provides the technical basis for an array of inspection techniques applied on the RV inlet nozzle to safe end weld inner, outer, and end face surfaces to support detection and characterisation of both surface-breaking and near-surface breaking planar defects having a height of 6 mm. This basis included previous works associated with the Sizewell B manufacturing NDT inspections, qualified inspections used in Sweden and the US, and common industry approaches. The technical basis of the inspection techniques described in Reference 20A.48 has been reviewed by an independent qualification body, the IVC, and the inspection techniques were deemed to be capable of formal qualification.

This demonstrates that suitable systems are available for a subsequent inspection qualification against the limiting QEDS for the three RV welds included in the GDA programme of defect tolerance assessment, such that a satisfactory DSM (≥ 2) is justified.

20A.2.4 Leg 4: Forewarning of Failure

The objective of the forewarning of failure leg of the safety case is to confirm the absence of a degradation mechanism through plant inspection or that where a known degradation mechanism exists, uncertainty in the material behaviour is not significant to integrity or will have limited consequences. Three elements are built up to support this claim. These are:

- Appropriate ISI is carried out to provide forewarning of failure.
- Diverse systems are provided to detect, locate and monitor reactor coolant leakage from the RV.
- In service material surveillance provide forewarning of unanticipated damage behaviour.

The arguments presented provide contingency for the unexpected.

20A.2.4.1 **Appropriate In-Service Inspection is Carried out to Provide Forewarning of Failure**

In order to provide assurances that defects will be detected prior to becoming a threat to the structural integrity of the AP1000 RV, evidence to substantiate the following arguments is provided

- An extensive programme of ISI will identify any degradation long before failure.
- Qualified inspection of HSS welds provides high reliability ISI.
- ISI data enables judgement of in-service defect formation and growth by comparison with 'fingerprint' PSI data.
- A 'Design for Inspectability' philosophy facilitates effective ISI.

20A.2.4.1.1 An extensive Programme of ISI will Identify Any Degradation Long Before Failure

ISI is the preferred method of demonstrating forewarning of failure. The role of an effective ISI programme is to confirm the absence of any unknown degradation mechanisms and that known degradation mechanisms are not significant to integrity or will have limited consequences.

ISI is used to confirm the absence of defects that could eventually lead to failure when the maximum tolerable defect size, as determined from fracture mechanics in Section 20A.2.3, is combined with a conservative assessment of in-service defect growth throughout the inspection interval.

In order to be effective, ISI requirements should be identified according to established good practice relevant to the characteristics of each inspection location. Evidence to substantiate that this is the case for planned RV ISI is provided below.

ISI for the AP1000 RV and Vessel Head is planned in accordance with ASME Section XI, IWB-2500 and supplemented by 10 CFR 50.55a.

The planned ISI programme includes the RV components and welds of importance to nuclear safety. ISI requirements for the following welds and components of the RV are identified in Reference 20A.43[2]:

- Circumferential Shell Welds (lower shell to bottom head transition ring and lower shell to upper shell welds).
- The circumferential bottom head transition ring to bottom head welds.
- The nozzle to shell welds and nozzle inner radius regions.
- The vent nozzle and QuickLoc instrument nozzle full penetration welds
- Nozzle to safe end welds.

2. Reference 20A.42 does not constitute the Inspection Plan as required by 10 CFR 50.55a. The Inspection Plan remains to be issued at a later date, subsequent to regulatory Generic Design Acceptance.

- Studs, nuts and washers.
- IHP support lug welds.
- Core support lugs.
- The vessel interior.
- Removable core support structures.
- CRDM housing welds.

Reference 20A.43 identifies Code requirements for each of the above locations and takes into account the relevant code cases. Inspection methods and access arrangements are described to ensure effective ISI at each of the identified RV welds and components. For example, CH penetration welds are inspected from both the outer and inner surfaces by a combination of eddy-current and UT methods, and volumetric inspection, where demanded, is performed by sensitive UT methods.

20A.2.4.1.2 Qualified Inspection of HSS Welds Provides High Reliability ISI

Table 20A-1 identifies the Structural Integrity Classification for the RV components. For those components identified as HSS it is accepted good practice that qualified inspections are deployed as supporting evidence to demonstrate that there are no defects of concern in HSS components.

The reliability of the ISI for HSS welds in the RV is to be qualified by applying the principles of the ENIQ Methodology as contained in Reference 20A.33.

Adherence to the ENIQ Inspection Qualification methodology provides evidence of good practise for ISI of HSS locations. Reference 20A.32 identifies how inspection requirements and performance objectives are laid down in an inspection specification and provides a method for Inspection Qualification based on technical justification of the inspection method and practical trials on simplified or representative test pieces resembling the component to be inspected.

20A.2.4.1.3 ISI Provides Data to Judge In-service Defect Formation and Growth by Comparison with 'Finger-print' PSI Data

In Section 20A.2.1.6 qualified PSI of HSS components is described. The resulting data constitutes a "finger-print" against which ISI results can be compared. Comparison of ISI data with the PSI fingerprint is used to confirm the absence of significant degradation or that build defects are stable i.e. defects detected during ISI must have started life as no greater than the PSI validation defect size. PSI will be performed using the same equipment that is likely to be used for the periodic ISI.

20A.2.4.1.4 A 'Design for Inspectability' Philosophy Facilitates Effective ISI

For effective ISI, the RV design should accommodate requirements for inspection equipment and personnel access in accordance with current inspection technology and strategies. Reference 20A.32 describes how the RV design has been developed with the goal of maximising inspectability.

The AP1000 RV design accommodates current best-practice ISI techniques and, so far as is practicable, allows for newly emergent inspection technologies to be employed. Reference 20A.32 provides a summary of ISI requirements for each location of the RV and RV Head. Design for Inspectability is demonstrated by consideration of the following aspects:

- Access for personnel and equipment conducting either manual deployed or mechanically deployed techniques.
- Surface finish requirements.
- Access either side of the welds to facilitate UT of the full section, where necessary, with angle beams of up to 60°.

Reference 20A.32 establishes that provisions for inspectability are consistent with current best practice. An assessment is provided to demonstrate that design and access arrangements are provided to satisfy the requirements set out in NCA-3200 of the ASME Code Section III, IWA-1400 and IWA-1500 of the ASME Code Section XI and 10 CFR 50.55a(g)(3)(i) and 10 CFR 50.55a(g)(3)(ii).

An additional assessment of the RV Head penetrations is provided to ensure adequate design and access provisions to demonstrate compliance with ASME Code Section XI Code Case N-729-1, EPRI-MRP Letter 2003-013 (Reference 20A.54) and WesDyne Letter WDI-LTR-RVH-05-2 (Reference 20A.55). ISI of the RV head to ASME CC N-729-1 and 10 CFR 50.55a includes inspection for indications of leakage and boric acid accumulation.

20A.2.4.1.5 Diverse Systems are Provided to Detect, Locate and Monitor Reactor Coolant Leakage from the RV

In order to demonstrate that leaks from the RCPB will be detected before they result in a safety issue, the following arguments are presented.

20A.2.4.1.6 Leak Detection of the RCPB Provides Warning of Reactor Coolant Leakage from the RV

ISI is the preferred method of demonstrating forewarning of failure. The primary arguments for ISI are enumerated in this section. Whilst leak detection and monitoring provide forewarning of failure, this safety argument does not seek to establish a quantitative case for excluding the gross failure of the RV as a result of this forewarning. The leak detection measures described in this section are provided as qualitative evidence of defence in depth in support of this leg of the safety argument. Leak detection provides warning of unforeseen or unexpected loss of coolant from the RV, and monitoring provides a means to confirm that any leakage of the coolant is kept within the limits specified in the technical specifications (Reference 20A.50).

The RCPB is monitored for leaks by a variety of components located in multiple systems. The leak detection system provides information that will prompt plant operators to take corrective action if any detected leakage exceeds technical specifications.

Identified leakage from the RV is collected in the reactor coolant drain tank. The RV flange and head flange are sealed by two concentric seals. Seal leakage is detected by two leak-off connections: one between the inner and outer seal, and one outside the outer seal. These lines are combined in a header before being routed to the reactor coolant drain tank. An isolation

valve is installed in the common line. During normal plant operation, the leak-off valves are aligned so that leakage across the inner seal drains to the reactor coolant drain tank. A surface-mounted resistance temperature detector installed on the bottom of the common RV seal leak pipe provides an indication and high temperature alarm signal in the main control room indicating the possibility of an RV head seal leak. The temperature detector and drain line downstream of the isolation valve are part of the liquid radwaste system.

Diverse methods are provided to detect, quantify, and assist in locating unidentified leakage from the RV. It is possible for unidentified leakage to originate from the RV head or the RV head vent connections, which are flanged. During normal operation, variations in airborne radioactivity, containment pressure, temperature, or specific humidity above the normal level signify a possible increase in unidentified leakage rates and alert the plant operators that corrective action may be required. Similarly, increases in containment sump level signify an increase in unidentified leakage. Section 20.6.4.3.2 outlines the methods used to collect and monitor unidentified leakage.

Intersystem leakage through the RV is not possible, as no system interconnections exist within the jurisdictional boundaries of the RV.

20A.2.4.2 In Service Material Surveillance Provide Forewarning of Unanticipated Damage Behaviour

In-service materials surveillance programme will provide forewarning of unanticipated damage.

20A.2.4.2.1 Materials Surveillance Programme

The RV in-service materials surveillance programme provides plant specific data which confirms that irradiation shift predictions used in the RV defect tolerance assessment and in the derivation of P/T limits remain conservative for the current period of operation and also provides forewarning of unanticipated material behaviour which could lead to non-conservative shift predictions later in plant life. The evaluation of radiation damage is based on comparison of pre-irradiation testing of Charpy V-notch, 1/2-T CT and tensile specimens and post-irradiation testing of Charpy V-notch, tensile, and 1/2-T CT fracture mechanics test specimens.

The surveillance programme conforms to ASTM E185 (Reference 20A.28) and 10 CFR 50, Appendix H (Reference 20A.44). The RV surveillance programme incorporates eight specimen capsules. The capsules are located in guide baskets welded to the outside of the core barrel as shown in Figure 20A-7 and positioned directly opposite the centre portion of the core. The capsules can be removed when the vessel head is removed. In order to meet the guidelines of ASTM E185, the placement of the specimens should yield lead factors between 1.0 and 3.0 to facilitate closely mirroring the history of the RV. In order to meet this recommendation, the specimen guide baskets are located azimuthally near the lowest fluence locations at 135, 225, and 315 degrees. The 45 degree location is also a low fluence azimuthal location; however, there is a Roto-Lock insert for the internals lifting rig, which would prevent access for removal of the capsules from the baskets. Therefore, there are no guide baskets at the 45 degree location.

Eight specimen capsules are provided by including three guide baskets at the 135 and 315 degree azimuthal locations and two baskets at the 225 degree location. The capsules contain RV weld metal, base metal, and heat-affected zone metal specimens. The base metal specimens are oriented both parallel and normal (longitudinal and transverse) to the principal

rolling direction of the limiting base material located in the core region of the RV. The 8 capsules contain 72 tensile specimens, 480 Charpy V-notch specimens, and 196 CT specimens.

Dosimeters are placed in filler blocks drilled to contain them. The dosimeters permit evaluation of the flux seen by the specimens and the vessel wall. In addition, thermal monitors made of low melting point alloys are included to monitor the maximum temperature of the specimens. The specimens are enclosed in a tight-fitting stainless steel sheath to prevent corrosion and ensure good thermal conductivity. The complete capsule is helium leak tested. As part of the surveillance programme, a report of the residual elements in weight percent to the nearest 0.01 percent is made for surveillance material and as deposited weld metal.

The fast neutron exposure of the specimens occurs at a faster rate than that experienced by the vessel wall, with the specimens being located between the core and the vessel. Since these specimens experience accelerated exposure and are actual samples from the materials used in the vessel, the transition temperature shift measurements are representative of the vessel at a later time in life. The lead factors for the eight specimen capsule locations based on the Reference neutron flux distribution (flux distribution that results in the maximum fluence on the RV inner surface) vary between approximately 1.8 and 2.3. These lead factors will change over the life of the plant due to changes in core design and operating parameters. Data from CT fracture toughness specimens are expected to provide additional information for use in determining allowable stresses for irradiated material.

The recommended programme schedule for removal of the capsules for post-irradiation testing conforms to ASTM E185 for the first 4 removals, whilst the 5th removal is an additional recommendation. The following is the recommended withdrawal schedule.

Capsule Withdrawal Time

- 1st When the accumulated neutron fluence of the capsule is 5×10^{18} n/cm^2.
- 2nd When the accumulated neutron fluence of the capsule corresponds to the approximate end of life fluence at the RV 1/4T location.
- 3rd When the accumulated neutron fluence of the capsule corresponds to the approximate end of life fluence at the RV inner wall location.
- 4th When the accumulated neutron fluence of the capsule corresponds to a fluence not less than once or greater than twice the peak end of vessel life fluence.
- 5th End of plant design objective of 60 years (not required by ASTM E185).

Plant-Specific Calculations

The location, selection, and evaluation of neutron dosimetry and the associated radiometric monitors, as well as fast (E > 1.0 MeV) neutron fluence assessments of the AP1000 reactor pressure vessel, are conducted in accordance with the guidelines that are specified in Regulatory Guide 1.190 (Reference 20A.45). Specific details of the calculation procedures for evaluating the integrated flux and dosimetry procedures are presented in Reference 20A.18. These consider the effect of the differences between the plant material and surveillance capsule material conditions i.e. differences in the flux, temperature profile, power cycling, and knowledge of strain ageing, thermal ageing.

Material Archiving

Material will be archived and retained for delivery to the end customer for use as required to support future operation. The material will be traceable to the original source and have documentation of processing and heat treatment. The material will have had a similar thermal treatment and fabrication as the final material condition of the associated RV material. The material will include the following archive samples (where T is the nominal thickness) as detailed in the Design Specification (Reference 20A.2).

- Vessel Flange Shell: Nozzle cutout x 1 pc
- Outlet Nozzle: 89 mm (3.5 inches) x Tmm x 457 mm (18 inches) circ x 2 pcs
- Inlet Nozzle: 89 mm (3.5 inches) x Tmm x 457 mm (18 inches) circ x 4 pcs
- DVI Nozzle: 89 mm (3.5 inches) x Tmm x 152.4 mm (6 inches) circ x 2 pcs
- Outlet Nozzle Safe End: 89 mm (3.5 inches) x Tmm x 457 mm (18 inches) circ x 2 pcs
- Inlet Nozzle Safe End: 89 mm (3.5 inches) x Tmm x 457 mm (18 inches) circ x 4 pcs
- DVI Nozzle Safe End: 89 mm (3.5 inches) x Tmm x 152.4 mm (6 inches) circ x 2 pcs
- Lower Shell: 203 mm (8 inches) x 203 mm (8 inches) x 1,016 mm (40 inches) circ(1) x 1 pc
- Transition Ring: 203 mm (8 inches) x 203 mm (8 inches) x 1,016 mm (40 inches) circ x 1 pc
- Closure Head: 51 mm (2 inches) thk x 127 mm (5 inches) x 1,016 mm (40 inches) circ x 1 pc
- Bottom Head Dome: 152 mm (6 inches) thk x 127 mm (5") x 1,016 mm (40 inches) circ x 1 pc
- CRDM Penetration: 203 mm (8 inches) per heat of tube material
- Vent Tube: 203 mm (8 inches) x 1 pc
- QuickLoc Nozzle: 203 mm (8 inches) per heat of tube material

20A.3 Strength of the Safety Case

20A.3.1 Objective

SFRs for the RV are developed from the structural integrity safety design bases, as identified in Section 20A.1.9. This report provides a safety argument which identifies evidence to substantiate that the SFRs of the RV will be maintained for all conditions within the design basis.

The availability and reliability of the safety measures identified to deliver a component's SFRs should demonstrably be commensurate with the significance of the radiological hazards to be controlled. This is achieved by a process of component structural integrity classification

which, for the safety justification of each class of component, establishes the degree of rigour to be applied commensurate with the potential radiological consequences of any postulated gross failure mode.

The process of structural integrity classification is discussed in Section 20.5 and detailed in Reference 20A.4, where gross failure of the RV is assessed to potentially lead to the most severe and therefore intolerable offsite consequences against which there is no claimed protection. As identified in Section 20A.1.10, the RV is classified as a highest safety significance component[3]. HSS-classification necessitates substantiation of a tolerable failure frequency where the probability of gross structural failure of the RV is so low it can be discounted.

20A.3.2 **Evidence**

To substantiate the claim that gross structural failure of the RV can be discounted, a safety argument is presented in Section 20A.1.8. Various elements of sound engineering practice are identified which provide evidence that there is defence in depth against structural failure within the RV arrangement and design. A defence in depth justification usually involves the provision of multiple layers of protection and defence is provided through diversity, redundancy and segregation to provide a robust design. For single components without multiple protection layers, the defence in depth principle is retained by demonstrating that the likelihood of failure is so low that it can be considered as not credible. The safety argument comprises four conceptually different legs, within each of which multiple subordinate arguments are supported by diverse sources of substantiating evidence. Robustness is achieved by considering the combined contribution from the four legs, a philosophy generally known as conceptual defence in depth. In combination the four legs provide sufficient confidence that gross failure of the RV with unacceptable consequences will not occur during normal operation, during design basis transient or during fault conditions. The combined strength of the claims, arguments and evidence presented in Section 20A.2 is discussed in this section.

The safety argument is founded upon a high standard of manufacture sufficient to achieve an appropriately high level of structural integrity. Design and fabrication of the RV is to be in accordance with ASME Code, Section III, Class 1 requirements as a minimum. Supplemental requirements are identified that enhance the quality of RV design and fabrication beyond ASME Class 1 standards. These are detailed in Section 20A.2.1, where multiple arguments and supporting evidence to substantiate achievement of RV integrity are presented. Section 20A.2.1 includes claims, arguments and evidence to address the following aspects:

- The design is well founded and in accordance with internationally recognised standards. The design of PWR RVs is well established and Westinghouse has an established track record. The AP1000 RV benefits from this historical experience which is embodied in the codes and standards applied in design and fabrication.

- Procurement of materials is specified and controlled to ensure that well proven materials are chosen, that the materials have good resistance to fracture and are of suitable chemical composition to limit the effect of irradiation embrittlement and other through-life degradation mechanisms. AP1000 RV materials comply with the corresponding material specification permitted by the ASME Code, Section III,

3. The HSS classification does not apply to every component of the RV or to every postulated failure mode and defect orientation, since certain failure modes will not lead to the most severe off site consequences. Classification of each component of the RV is detailed in Section 20A.1.10.

Division 1. For certain RV materials, supplementary requirements are specified which exceed the requirements specified in ASME code. Materials testing is specified to confirm that material properties comply with the relevant specifications.

- Very high standards have been applied that control RV fabrication. RV components will be manufactured by experienced suppliers and evidence to confirm the suitability of the chosen manufacturer will form part of the Site Specific Justification. Compliance with ASME III and the experience embodied within the code provides high confidence in manufacturing quality. Supplemental requirements have been identified which enhance the standards applied in fabrication beyond ASME requirements. Approved welding procedures and qualified operators are used. Stringent Quality Assurance arrangements control manufacturing procedures and records are maintained to provide a clear auditable trail that will confirm this. There are procedural controls to limit deviations from the design intent and all repairs and deviations will be recorded to confirm acceptability.

- Manufacturing inspections and PSI with appropriate levels of redundancy and diversity confirm the absence of defects which have the potential for causing, or developing into a failure mode. This judgement is based on definition of allowable SoL defect sizes. Where appropriate the inspections are subject to independent validation and in the case of HSS components of the RV, a programme of qualified PSI is specified. In the unlikely event that defects are found, they will be repaired in accordance with accepted techniques.

The diverse evidence summarised above demonstrates that the RV will be designed and fabricated against well established and appropriate deterministic engineering rules, verified by application of rigorous PSI. The various elements identified establish defence in depth for preventing failure of RV structural integrity. Functional hydrostatic testing to demonstrate that the RV meets the design intent, as described in Section 20A.2.2, supplements the arguments to demonstrate achievement of RV integrity, ensuring that the RV enters service fit for purpose and free of safety-significant defects.

The measures established to ensure good design and construction are supplemented with additional claims and evidence to demonstrate continued structural integrity throughout the planned RV lifetime. Careful control of operating conditions enables the RV to fulfil its safety function for its projected lifetime. Plant Operation and Maintenance is clearly defined in accordance with recognised procedures as described in Section 20A.2.1. Design and operating parameters used in the design evaluation are robustly determined using established and conservative procedures, as detailed in Section 20A.2.1. The evidence provided to this effect ensures the validity of stress analysis and fracture analysis to substantiate claims based on ASME Code compliance.

Section 20A.2.3 and Section 20A.2.4 provide evidence to substantiate RV integrity under all design basis conditions by demonstrating that any defect which may have gone undetected during manufacture will not cause failure during the lifetime of the plant. The elements that substantiate this claim are as follows:

- Stress Analysis – The AP1000 RV is designed in accordance with the ASME Code, Section III, Division 1. Consideration of Levels A to D and Test conditions encompass the design basis for the purposes of the analysis. Stress analysis to the ASME code supports demonstrating fitness-for-purpose and also provides a basis for subsequent fracture analysis.

- Fracture Analysis – LEFM analysis, as prescribed in Appendix G of ASME Section III, has been supplemented by elastic-plastic fracture mechanics procedures specified in the R6 Defect Assessment code. These fracture analyses demonstrate that the sizes of defect which are of safety concern are large in relation to those which could remain undetected in the component following qualified inspection.

- In-Service Inspection – The RV is designed to facilitate effective ISI, which provides assurance that defects will be detected long before growing to a size that could threaten structural integrity of the RV. Qualified inspection of HSS locations establishes the sizes of defects that can be reliably detected and the associated sizing uncertainty. Qualification is to be achieved through a combination of Technical Justification of inspection procedures and equipment, supported by trials. ISI data enables judgement of in-service defect formation and growth by comparison with PSI data.

- Materials Surveillance – The RV in-service materials surveillance programme provides plant specific data which confirms that irradiation shift predictions used in the RV defect tolerance assessment and in the derivation of P/T limits remain conservative for the current period of operation and also provides forewarning of unanticipated material behaviour which could lead to non-conservative shift predictions later in plant life.

- Leakage Monitoring – Diverse systems are provided to detect, locate and monitor reactor coolant leakage from the RV. Alarm and indication of reactor coolant leakage from the RV in excess of specified limits provides diverse means to detect failure.

The summary and review of the safety argument in this section provides the basis for the conclusions of this report which are presented in Section 20A.5.

20A.4 Review of Open Issues

There are no open issues that affect the basis of the RV safety case arguments presented in support of GDA.

20A.5 Conclusions

This CSR for the UK AP1000 RV presents a safety argument to establish that the structural reliability of the RV is commensurate with the consequences of gross failure. SFRs have been identified for the RV, based on structural integrity safety design bases. These requirements are to be maintained for the lifetime of the plant to ensure plant nuclear and radiological safety. For the RV, assurance that these SFRs will be maintained is provided by substantiating structural integrity against appropriate reliability targets.

Structural reliability targets have been identified for the RV that are based on a procedure of structural integrity classification. Based on this, the RV has been classified as a HSS component. The structural reliability target associated with HSS classification is to substantiate a tolerable failure frequency that is so low that gross failure can be discounted.

The safety argument is presented in a four legged format that is well established in the UK for the safety justification of nuclear plant components similar to the RV that share similar structural reliability targets. The safety argument identifies diverse defence in depth measures to substantiate the structural reliability claimed for the RV:

- The intent and principles that govern the design, future manufacture and operation of the RV in the UK are identified to substantiate fitness for purpose within a pre-construction

safety case. The safety argument demonstrates how modern and well established good practice has been or will be implemented in RV design, manufacture, defect tolerance assessment, and in the provision for through-life inspection.

- The RV design benefits from the long operating history of PWR RVs and incorporates design measures to minimise frequency of failure based on that experience. To minimise the potential for a LOCA by leakage from the RV that would result in the core being uncovered, there are no penetrations in the RV below the core. In addition the core is positioned low in the RV to minimise re-flood time in accident conditions. The RV design facilitates effective inspection which supports a programme of qualified inspection to ensure timely forewarning of failure.

- Structural integrity of the RV is secured largely by passive means and is not significantly reliant on control systems, active safety systems or human intervention. As such, the diverse defence in depth measures identified focus on prevention of failure through conservative, robust design. Surveillance, inspection and leakage monitoring provide secondary defence in depth measures to detect and provide forewarning of failure.

- RV structural integrity is established based on extensive quality assurance measures in design, manufacture, materials, testing and qualified inspection. The strength of the safety case is based on achievement of integrity and the RV has been deterministically justified in accordance with ASME Code Class 1 requirements. Additional arguments provide robust evidence to demonstrate that the RV is defect tolerant and this is supported by qualified manufacturing inspection. Numerous other defence in depth measures are identified.

In combination these elements constitute a cogent argument to substantiate structural reliability commensurate with the HSS structural integrity classification of the RV.

20A.6 Index of Technical Reports

Table 20A-17 provides a list of technical references supporting the safety case and summarises the function of each document within the safety case.

20A.7 References

20A.1 Not used.

20A.2 Westinghouse Report APP-MV01-Z0-101, Rev. 14, “Design Specification for AP1000 Reactor Vessel for System: Reactor Coolant System (RCS),” July 2016.

20A.3 Bullough R. et al., “The Demonstration of Incredibility of Failure in Structural Integrity Safety Cases,” International Journal of Pressure Vessels and Piping 78 (2001), pages 539-552.

20A.4 Westinghouse Report UKP-GW-GLR-004, Rev. 3, “UK AP1000 Structural Integrity Classification,” January 2017.

20A.5 Not used.

20A.6 Westinghouse Letter LTR-MRCDA-07-201, “AP1000 Reactor Vessel Failure Modes and Effects Analysis (FMEA),” October 2007.

20A.7 ASME Boiler and Pressure Vessel Code, 1998 Edition with Addenda up through and including 2000 Addenda and applicable Code Cases, American Society of Mechanical Engineers.

20A.8 NUREG-1801, Vol. 1, Rev. 1, "General Ageing Lessons Learned (GALL) Report," US Nuclear Regulatory Commission, September 2005.

20A.9 Regulatory Guide 1.65, Rev. 0, "Materials and Inspections for Reactor Vessel Closure Studs," US Nuclear Regulatory Commission.

20A.10 NUREG-1339, "Resolution of Generic Safety Issue 29: Bolting Degradation or Failure in Nuclear Power Plants," US Nuclear Regulatory Commission.

20A.11 Not used.

20A.12 ANS/ANSI N51.1, "Nuclear Safety Criteria for the Design of Stationary Pressurized Water Reactors," American Nuclear Society / American National Standards Institute.

20A.13 Westinghouse Report APP-RCS-M1-001, Rev. 4 "Reactor Coolant System Design Transients," February 2013.

20A.14 Westinghouse Report APP-RCS-M1C-043, Rev. 0, "AP1000 Design Transient – Daily Load Following Operations," November 2007.

20A.15 Westinghouse Report APP-MV01-Z0C-040, Rev. 7, "Detailed Analysis of the Direct Vessel Injection (DVI) Nozzle for the AP1000 Reactor Vessel," August 2016.

20A.16 Regulatory Guide 1.29, Rev. 4, "Seismic Design Classification," Nuclear Regulatory Commission.

20A.17 Westinghouse Report APP-MV01-Z0R-101, Rev. 7, "AP1000 Reactor Vessel Design Report," August 2016.

20A.18 Westinghouse Report WCAP-15557, "Qualification of the Westinghouse Pressure Vessel Neutron Fluence Evaluation, August 2000.

20A.19 Not used.

20A.20 NUREG-0612, "Control of Heavy Loads at Nuclear Power Plants," US Nuclear Regulatory Commission, July 1980.

20A.21 Not Used.

20A.22 Not used.

20A.23 Not used.

20A.24 Westinghouse Letter LTR-SST-06-21, "Release of ANSYS 10 for XP, HPUX 11.0 and HPUX 11.23 and ANSYS Error Reports," July 2006.

20A.25 Westinghouse Report APP-VL51-Z0-004, Rev. 3, "AP1000 Reactor Vessel Material Specification for SA-508/SA-508M Grade 3 Class 1 for Core Region Forgings (Section III-NB)," August 2009.

20A.26 Westinghouse Process Specification APP-GW-Z0-608, Rev. 1, "Material Test Specification for Austenitic Stainless Steel Cladding," November 2010.

20A.27 Regulatory Guide 1.99, Rev. 2, "Radiation Embrittlement of Reactor Vessel Materials," US Nuclear Regulatory Commission.

20A.28 ASTM E185-82, "Surveillance Test for Light Water Cooled Nuclear Power Reactor Vessels," American Society for Testing and Materials.

20A.29 Westinghouse Report APP-GW-VLR-010, Rev. 2, "AP1000 Supplemental Fabrication and Inspection Requirements," January 2016.

20A.30 Westinghouse Document "Quality Management System (QMS)," Rev. 7, August 2013.

20A.31 Westinghouse Report APP-MV01-Z0-001, Rev. 4, "AP1000 Reactor Pressure Vessel Functional Specification," June 2013.

20A.32 Westinghouse Document APP-GW-VW-001, Rev. 1, "AP1000 Design for Inspectability Program. ISI Requirements for Class 1 Components," June 2014.

20A.33 "European Methodology for Qualification Of Non-Destructive Testing," European Network for Inspection Qualification Report 31, EUR 22906 EN, Issue 3, August 2007.

20A.34 Westinghouse Report APP-RXS-Z0R-001, Rev. 2, "AP1000 Generic Pressure Temperature Limits Report," October 2008.

20A.35 Westinghouse Report WCAP-14040-NP-A, Rev. 2, "Methodology Used to Develop Cold Overpressure Mitigating System Setpoints and RCS Heatup and Cooldown Limit Curves," January 1996.

20A.36 Westinghouse Report APP-MV01-Z0-332, Rev. 2, "AP1000 Reactor Vessel Requirements for Hydrotesting," February 2011.

20A.37 Not used.

20A.38 Report No. AR 09/013-P, "Nuclear Directorate Generic Design Assessment – New Civil Reactor Build, Step 3 Structural Integrity Assessment of the AP1000," Division 6 Assessment.

20A.39 Westinghouse Report UKP-MV01-Z0R-100, Rev. 3, "Results of Weld Ranking Process for Reactor Vessel, Steam Generator, Pressurizer, Main Steam Line and Main Coolant Loop Piping," December 2015.

20A.40 Not used.

20A.41 Westinghouse Report UKP-MV01-Z0R-101, Rev. 2 "Methodology and Input Data for the Application of the R6 Flaw Evaluation Procedure and Fatigue Crack Growth Analysis to the UK AP1000 Components," December 2016.

20A.42 Westinghouse Report APP-MV01-Z0C-010, Rev. 7, "AP1000 Reactor Vessel Fracture Mechanics Evaluation per ASME Section III Appendix G," August 2016.

20A.43 Westinghouse Report APP-MV01-VMR-001, Rev. A, "AP1000 Component ISI Inspectability Assessment: Reactor Pressure Vessel & Reactor Pressure Vessel Head," November 2008.

20A.44 10 CFR 50, Appendix H, US Nuclear Regulatory Commission.

20A.45 Regulatory Guide 1.190, Rev. 0, "Calculational and Dosimetry Methods for Determining Pressure Vessel Neutron Fluence," March 2001.

20A.46 Westinghouse Report UKP-MV01-Z0C-100, Rev. 2, "Flaw Evaluation of the UK AP1000 Reactor Pressure Vessel Welds," March 2016.

20A.47 Westinghouse Report WDI-TJ-1048, Rev. 1, "Manufacturing NDT Inspection Plan for the Lower Shell to Upper Shell and DVI Nozzle to Shell Welds of the AP1000 RPV in Response to Regulatory Observation Action RO-AP1000-19.A3," December 2010.

20A.48 Westinghouse Report WDI-TJ-1051, Rev. 1, "Manufacturing NDT Inspection Plan for the RPV Inlet Nozzle to Safe End Weld of the AP1000 RPV in Response to Regulatory Observation Action RO-AP1000-19.A3," December 2010.

20A.49 Westinghouse Report APP-RCS-M3-001, Rev. 8, "Reactor Coolant System, System Specification Document," June 2015.

20A.50 Westinghouse Report UKP-GW-GL-501, Rev. 0, "UK AP1000 Technical Specifications," January 2016.

20A.51 ASTM E1921-05, "Standard Test Method for Determination of Reference Temperature T_0, for Ferritic Steels in the Transition Range," American Society for Testing and Materials.

20A.52 NUREG-1431, Rev. 4, "Standard Technical Specifications – Westinghouse Plants," US Nuclear Regulatory Commission.

20A.53 Regulatory Guide 1.44, Rev. 0, "Control of the Use of Sensitized Stainless Steel," US Nuclear Regulatory Commission.

20A.54 "Pre-Service Inspection Guidance for New Reactor Pressure Vessel Heads," Letter from L. N. Hartz (Chair, MRP Senior Representatives; Dominion Generation) to MRP Utility Members, MRP 2003-013, dated June 26, 2003.

20A.55 Westinghouse Report WDI-LTR-RVH-05-2, Rev. 1, "Replacement Reactor Vessel Head Design Requirements Associated with PSI and ISI Requirements," Wesdyne International, March 2005.

20A.56 Westinghouse Report WDI-PJF-2405360-TCR-003, Rev. 2, "Westinghouse Process for the Development of AP1000 Related Manufacturing NDT Inspection Plans as Part of the GDA Process (UK)," Wesdyne International, February 2016.

20A.57 Westinghouse Report UKP-GW-M0R-001, Rev. 0, "Additional Fracture Toughness Testing for the UK AP1000 Plant," January 2017.

Table 20A-1. Structural Integrity Classification of Reactor Vessel Components

Location	Postulated Defect Orientation or Failure Mode	Classification	Supporting Comment
WELD REGIONS			
1. Main circumferential welds			
1.1 Lower head to transition ring circumferential weld	All	HSS	(1)
1.2 Transition ring to lower shell course circumferential weld	All	HSS	(1)
1.3 Lower shell course to upper shell course circumferential weld	All	HSS	(1)
2. Primary nozzle welds			
2.1 Primary nozzle to shell attachment welds	All	HSS	Failure of radial/circumferential weld postulated to run into shell forging hence HSS appropriate.
2.2 Primary nozzle to safe end transition weld	All	HSS	In absence of assessment of defect propagation along nozzle into RV shell, failure mode is conservatively assumed to be HSS.
3. DVI Nozzle welds			
3.1 DVI nozzle to shell attachment weld	All	HSS	Failure of radial/circumferential weld postulated to run into shell forging hence HSS appropriate.
3.2 DVI nozzle to safe end transition weld	All	HSS	In absence of assessment of defect propagation along nozzle into RV shell, failure mode is conservatively assumed to be HSS.
3.3 DVI nozzle safe end to DVI line attachment weld	All	Class 1	Defect originating in the pipe to safe end attachment weld will not extend through safe end and is bounded by double ended guillotine break of DVI line.

Table 20A-1. Structural Integrity Classification of Reactor Vessel Components (cont.)

Location	Postulated Defect Orientation or Failure Mode	Classification	Supporting Comment
4. CH penetration welds			
a) CH penetration J groove buttering and attachment welds (CRDM penetration, head vent pipe)	All	Class 1	Axial circumferential failure assessed as Class 1. Failure of weld would not result in tube ejection and would not result in CH failure.
b) CRDM latch housing to penetration bi-metallic weld	All	Class 1	Defect propagation from latch housing to CH forging not considered credible.
5. Welded support pads/blocks			
5.1 Vessel support pad attachment welds	All	Class 1	Support pads and lugs will be inspected in accordance with ASME III requirements and are assessed as Class 1.
5.2 Core support block attachment welds	All	Class 1	As above
5.3 IHP support lug	All	Class 1	As above
5.4 CH lift lugs	All	Class 1	As above
FORGING REGIONS			
6. Main forging regions			
6.1 Nozzle inner/outer crotch corners Inlet Nozzle, Outlet Nozzle, DVI Nozzle	All	HSS	(1)
6.2 Core support ledge radius	All	HSS	(1)
6.3 Main RV and CH forgings: CH, upper shell, lower shell, transition ring.	All	HSS	(1)
6.4 Seal Ledges	All	HSS	(1)
6.5 Clad/underclad defects in beltline region	All	HSS	(1)

Table 20A-1. Structural Integrity Classification of Reactor Vessel Components (cont.)

Location	Postulated Defect Orientation or Failure Mode	Classification	Supporting Comment
OTHER RV REGIONS			
7. RV Bolting			
7.1 Studs	All	Class 1	Failure of a single stud will not lead to loss of RV head. LOCA protectable and standard Class 1.
7.2 Nuts	All	Class 1	Bounded by bolt failure.
7.3 Washers	All	Class 1	Bounded by bolt failure.
8. RPV sealing arrangements			
8.1 Failure of Inner and Outer O ring seals	Leakage arising from seal failure	Class 1	Failure of a seal will not lead to loss of RV head. LOCA protectable and standard Class 1.
9. Latch Housings/CRDM extensions			
9.1 CRDM extension	R All	Class 1	Failure of CRDM extension tube would not affect pressure boundary integrity.
9.2 CRDM extension funnel	All	Class 1	Failure of CRDM extension funnel would not affect pressure boundary integrity.
9.3 Latch housing Assembly	All	Class 1	Defect propagation from latch housing to CH forging not considered credible.
10. Instrument Nozzles/Monitor Tubes			
QuickLoc Instrument Nozzle Flange Adaptor	All	Class 1	Leakage from instrument nozzles/monitor tubes is a protectable LOCA, hence Class 1.
QuickLoc Nozzle	All	Class 1	As above
Outer Monitor Tube	All	Class 1	As above
Inner Monitor Tube	All	Class 1	As above

Notes:

1. Individual failure modes assessed as HSS are bounded by the component level classification presented for the RV in Reference 20A.4.

Table 20A-2. Not Used

Table 20A-3. Reactor Coolant Water Chemistry Specifications

Electrical conductivity	Determined by the concentration of boric acid and alkali present. Expected range is <1 to 40 μmhos/cm at 25°C.
Solution pH	Determined by the concentration of boric acid and alkali present. Expected values range between 4.2 (high boric acid concentration) and 10.5 (low boric acid concentration) at 25°C. Values will be 5.0 or greater at normal operating temperatures.
Oxygen(1)	0.1 ppm, maximum
Chloride(2)	0.15 ppm, maximum
Fluoride(2)	0.15 ppm, maximum
Hydrogen(3)	25 to 50 cm^3 (STP)/kg H_2O
Suspended solids(4)	0.2 ppm, maximum
pH control agent (Li7OH)(5)	Lithium is coordinated with boron per fuel warranty contract.
Boric acid	Variable from 0 to 4000 ppm as boron
Silica(6)	1.0 ppm, maximum
Aluminium(6)	0.05 ppm, maximum
Calcium(6) + magnesium	0.05 ppm, maximum
Magnesium(6)	0.025 ppm, maximum
Zinc(7)	0.04 ppm, maximum

Notes:

1. Oxygen concentration must be controlled to less than 0.1 ppm in the reactor coolant by scavenging with hydrazine prior to plant operation above 93.33°C (200°F). During power operation with the specified hydrogen concentration maintained in the coolant, the residual oxygen concentration will not exceed 0.005 ppm.
2. Halogen concentrations must be maintained below the specified values regardless of system temperature.
3. Hydrogen must be maintained in the reactor coolant for plant operations with nuclear power above 1 MW. The normal operating range should be 25-35 cm^3 (STP) H2/kg H_2O.
4. Solids concentration determined by filtration through filter having 0.45-μm pore size.
5. The specified lithium concentrations must be established for start-up testing prior to heatup beyond 65.56°C (150°F). During cold hydrostatic testing and hot functional testing in the absence of boric acid, the reactor coolant limits for lithium hydroxide must be maintained to inhibit halogen stress corrosion cracking.
6. These limits are included in the table of reactor coolant specifications as recommended standards for monitoring coolant purity. Establishing coolant purity within the limits shown for these species is judged desirable with the current data base to minimise fuel clad crud deposition, which affects the corrosion resistance and heat transfer of the clad.
7. Specification is applicable during power operation when zinc is being injected. The zinc concentration is maintained at the lower of 0.04 ppm or that specified in the reload safety analyses.

Table 20A-4. Reactor Vessel External Environment

Environmental Parameter	Design Conditions		Abnormal Condition
	Max.	Min.	
Pressure, MPa (psig)	0.007 (1.0)	-0.01 (-0.2)	0[(1)] - 0.124 (18)[(2)]
Temperature, °C (°F) Vessel Closure Head	 57 (135) 49 (120)[(3)]	 10 (50)	 66 (150)[(1)] – 121 (250)[(2)]
Relative Humidity, (%)	100	1	100
Radiation Level, R-hr $^{-1}$	3.63 x 10^4	–	3.63 x 10^4

Notes:

1. Group 1: 66°C (150°F) Events
   Loss of nonsafety Heating Ventilation and Air Conditioning/Loss of a fan cooler
   Loss of all AC for up to 2 hours
   Pressuriser safety valve open/close during RCS transient
2. Group 2: 121°C (250°F) Events
   Spurious automatic depressurisation system (ADS) actuation
   Passive residual heat removal (PRHR) system use (long-term)
   RCS depressurisation via pressuriser safety valve
   Small LOCA
3. The maximum normal environmental operating temperature around the RV closure head (refuelling cavity) is 49°C (120°F).

Table 20A-5. Reactor Vessel Materials Specification

Part Name	Description	Material	Material Spec Ref
RV CH	Forging	SA-508, Grade 3, Class 1	APP-VL51-Z0-004
Upper Shell	Forging	SA-508, Grade 3, Class 1	APP-VL51-Z0-004
Lower Shell	Forging	SA-508, Grade 3, Class 1	APP-VL51-Z0-004
Transition Ring	Forging	SA-508, Grade 3, Class 1	APP-VL51-Z0-004
Lower Head	Forging	SA-508, Grade 3, Class 1	APP-VL51-Z0-003
Inlet Nozzle	Forging	SA-508, Grade 3, Class 1	APP-VL51-Z0-003
Outlet Nozzle	Forging	SA-508, Grade 3, Class 1	APP-VL51-Z0-003
DVI Nozzle	Forging	SA-508, Grade 3, Class 1	APP-VL51-Z0-003
IHP Support with Lift Lug	Forging	SA-508, Grade 3, Class 1	APP-VL51-Z0-003
Latch Housing Assembly (CRDM penetrations)	Assembly	SB-166, UNS N06690	APP-VL52-Z0-061
Outlet Nozzle Safe End	Forging	SA-182, F316LN	APP-VL51-Z0-012
Inlet Nozzle Safe End	Forging	SA-182, F316LN	APP-VL51-Z0-012
DVI Nozzle Safe End	Forging	SA-182, F316LN	APP-VL51-Z0-012
Monitor Tube (Inner & Outer)	Seamless Pipe, 1.00 SCH 160	SA-376, TP316 or SA-312 TP316	
Guide Stud Support Block	Forging	SA-508, Grade 3, Class 1	APP-VL51-Z0-003
Guide Stud Bracket	Plate	SA-533 or SA-508	APP-VL52-Z0-032 APP-VL51-Z0-003
Stud Bolt Assembly	7.000-4N-2A	SA-540	APP-VL52-Z0-006
Nut	7.000-4N-2A	SA-540	APP-VL52-Z0-006
Circular Washer	7.000-4N-2A	SA-540	APP-VL52-Z0-006
Guide Stud	Assembly	Chrome plated carbon steel	
IHP Support	Forging	SA-508, Grade 3, Class 1	APP-VL51-Z0-003
Seal Ledge	PL 3.00 STK	SA-533, Type B, Class 1 or SA-508, Grade 3, Class 1	APP-VL52-Z0-032 APP-VL51-Z0-003

Table 20A-5. Reactor Vessel Materials Specification (cont.)

Part Name	Description	Material	Material Spec Ref
Vessel Core Support Blocks		SB-166, UNS N06690	APP-VL52-Z0-061
Inner and Outer O-Rings	Assembly	UNS N07718 (silver plated)	APP-MV01-Z0-201
Vent Pipe	Seamless Pipe 1.00 SCH 160	SB-166, UNS N06690 or SB-167, UNS N06690	APP-VL52-Z0-061
Flow Skirt Support	Weld Build Up	Ni-Cr-Fe Weld Build Up	
Monitor Tube End (Inner and Outer)		SB-166, UNS N06690	APP-VL52-Z0-061
Vibration Monitor Pad		SA-533, Type B, Class 1 or SA-508, Grade 3, Class 1	APP-VL52-Z0-032 APP-VL51-Z0-003
QuickLoc Instrument Nozzle Flange Adapter		SA-479, Type 304, Type 316, S21800 or SA-182, F304 or F316	
QuickLoc Nozzle		P-3 Weld Build Up	
Cladding		Austenitic stainless steel or Ni-Cr-Fe Alloy	
Nozzle Buttering		Inconel 690 weld	

Table 20A-6. Projections for Upper Shelf Energy (USE) and RT_{NDT}(1) at End-of-Life (56 EFPY)

	1/4T	RT_{PTS}(1)
Beltline Forging	> 67.79 J (50 ft-lb)	< 132.2°C (270°F)

Notes:

1. End-of-Life RTPTS (Reference Temperature Pressurised Thermal Shock) and RT_{NDT} are equal.

Table 20A-7. Scope of Manufacturing Inspection for the RV Scope of Manufacturing Inspection for the RV

	RT(a)	UT(a)	PT(a)	MT(a)(b)
Forgings				
Flanges		Yes		Yes
Studs and nuts		Yes		Yes
CRDM latch housing nozzle		Yes	Yes	
Main nozzles		Yes		Yes
Nozzle safe ends		Yes	Yes	
Shell sections		Yes		Yes
Heads		Yes		Yes
Plates		Yes		Yes
Weldments				
Head and shell	Yes	Yes		Yes
CRDM latch housing nozzle to CH connection			Yes	
Main nozzle	Yes	Yes		Yes
Cladding		Yes	Yes	
Nozzle to safe ends	Yes	Yes	Yes	
All full-penetration ferritic pressure boundary welds accessible after hydrotest		Yes		Yes
Full-penetration non ferritic pressure boundary welds accessible after hydrotest a. Nozzle to safe ends		Yes	Yes	
Seal ledge				Yes
Head lift lugs				Yes
Core pad welds			Yes	
Flow skirt support lugs weld buildup		Yes	Yes	

(a) RT – Radiographic
UT – Ultrasonic
PT – Dye penetrant
MT – Magnetic particle

(b) Dye Penetrant (PT) examination may be used in lieu of Magnetic Particle (MT) examination in accordance with ASME Code Section III, NB-2541(a) when the inspection surface and surrounding geometry do not permit effective use of magnetic particle examination equipment.

Table 20A-8. Maximum Limits for Elements of the Reactor Vessel

Element	Beltline Forging (percent)	As Deposited Weld Metal (percent)
Copper	0.06	0.06
Phosphorus	0.01	0.01
Vanadium	0.05	0.05
Sulphur	0.01	0.01
Nickel	0.85	0.85

Table 20A-9. End-Of-Life RT_{NDT} and Upper Shelf Energy Projections

	Unirradiated		End-of-life (54 EFPY)	
	RT_{NDT} (°C / °F)	USE (J / ft-lb)	USE (J / ft-lb) 1/4T	RT_{PTS} (°C / °F)
Beltline Forging	-23.3 / -10	> 101.7 / 75[1]	> 67.79 / 50	< 132.2 / 270[2]
Head	10	N/A	N/A	N/A
Flange	10	N/A	N/A	N/A
Weld	10	N/A	N/A	N/A
Beltline Weld	-55.5 / -68	> 101.7 / 75	> 67.79 / 50	< 148.9 / 300[2]

Notes:

1. The minimum unirradiated upper shelf energy for beltline base metal is for the transverse direction.
2. End-of-Life RT_{PTS} requirements shown. End-of-Life RT_{PTS} (also equals RT_{NDT}) will be determined for as-built material. The preliminary RT_{PTS} for the AP1000 RV beltline forging and beltline weld are 34.4°C (94°F) and 37.8°C (100°F), respectively.

Table 20A-10. Not Used

Table 20A-11. ASME Code Stress Limits for Other than Bolts

Condition	Code Subsection	Criteria
Design	NB-3200	$P_m \leq S_m$
		$P_L \leq 1.5\ S_m$
		$P_L + P_b \leq 1.5\ S_m$
Normal (Level A)		$P_L + P_b + Q \leq 3\ S_m$
Upset (Level B)		$P_m \leq 1.1\ (S_m)$
		$P_L \leq 1.1\ (1.5\ S_m)$
		$P_L + P_b \leq 1.1\ (1.5\ S_m)$
		$P_L + P_b + Q \leq 3\ S_m$
Thermal Ratchet		Thermal Ratchet Ratio ≤ 1.0
Fatigue		FUF ≤ 1.0
Emergency (Level C)		$P_m \leq$ Greater of $1.2\ S_m$ or S_y
		$P_L \leq 1.5 \times P_m$ limit
		$P_L + P_b \leq 1.5 \times P_m$ limit
Faulted (Level D)	F	$P_m \leq$ Minimum $(2.4\ S_m, 0.7\ S_U)$, $0.7 S_U$ for ferritic
		$P_L \leq 1.5 \times P_m$ limit
		$P_L + P_b \leq 1.5 \times P_m$ limit
Test	NB-3200	$P_m \leq 0.9\ S_y$ at test temperature
		For $P_m \leq 0.67\ S_y$ $P_m + P_b \leq 1.35\ S_y$
		$P_m + P_b \leq (2.15\ Sy - 1.2\ P_m)$
Tri-Axial Stress		$\sigma 1 + \sigma 2 + \sigma 3 \leq 4.0\ S_m$

Table 20A-12. Not Used

Table 20A-13. ASME III Subsections

Component	ASME III Subsection
RV pressure boundary parts including vessel shell, closure and bottom heads, CRDM latch housing nozzles up to but not including bi-metallic welds, QuickLoc instrument nozzle and QuickLoc pressure boundary parts, and inlet, outlet, and DVI nozzles including safe-ends but excluding safe-end-to-piping welds:	ASME Section III, Subsection NB
Closure studs, nuts and washers:	ASME Section III, Subsection NB
IHP support and lift lugs:	Design, Level A/Level B analysis of lugs: ASME Section III, Subsection NF Design – lifting: ASME Section III, NUREG-0612 Design, Level A/Level B analysis of attachment weld: ASME Sect. III, Sub. NB Level D: ASME Section III, Appendix F
Vent pipe and monitoring tubes (sections supplied with RV):	ASME Section III, Subsection NB
Vessel support pads:	ASME Section III, Subsection NB
Core support blocks:	ASME Section III, Subsection NB
Seal ledge:	ASME Section III, Subsection NB
Guide stud support blocks and brackets:	ASME Section III, Subsection NB
Flow skirt supports (formed by weld build-up) and attachment weld to flow skirt:	ASME Section III, Subsection NB
CRDM extensions and funnels:	ASME Section III, Subsection NG
QuickLoc stalk assembly:	ASME Section III, Subsection NB

Table 20A-14. Not Used

Table 20A-15. Summary of Weld Defect Tolerance/NDT Ranking Assessment

HSS Location No.	Weld	Classification	Ranking (Defect Tolerance / NDT Ranking)	Selected for Defect Tolerance Assessment	Bounded by Other Location
1.1	Lower head to transition ring circumferential weld	HSS	2 / 1	NO	Bounded by Location 1.3
1.2	Transition ring to lower shell course circumferential weld	HSS	2 / 1	NO	Bounded by Location 1.3
1.3	Lower shell course to upper shell course circumferential weld	HSS	1 / 1	YES	
2.1	Primary nozzle to shell attachment welds	HSS	3 / 2 – Inlet 2 / 1 – Outlet	NO	Bounded by Location 3.1
2.2	Primary nozzle to safe end transition weld	HSS	1 / 1 – Inlet 3 / 1 – Outlet	NO	Bounded by location 3.2
2.3	Primary nozzle safe end to loop attachment weld	HI	Outside RV boundary	NO	Bounded by Location 3.1
3.1	DVI nozzle to shell attachment weld	HSS	1 / 2	YES	
3.2	DVI nozzle to safe end transition weld	HSS	2 / 2	YES	
3.3	DVI nozzle safe end to DVI line attachment weld	Class 1	Outside RV boundary	NO	Not Required
4.1	CH penetration J groove buttering and attachment welds	Class 1	Not Assessed	NO	Not Required
4.2	CRDM latch housing to penetration bi-metallic weld	Class 1	Not Assessed	NO	Not Required
5.1	Vessel support pad attachment welds	Class 1	Not Assessed	NO	Not Required
5.2	Core support block attachment welds	Class 1	Not Assessed	NO	Not Required
5.3	IHP support lug	Class 1	Not Assessed	NO	Not Required
5.4	CH lift lugs	Class 1	Not Assessed	NO	Not Required

Table 20A-16. Summary of ASME Appendix G Defect Tolerance Assessment (Ref. 20A.42)

Service Level	Region	Limiting Result				
		Flaw Type[1]	Flaw Size (mm)	a/T[3]	K_I/K_{IR}[3]	Temp (°C)
A/B	Lower Head and Shell Beltline	Circ – In			1.00	
	Closure Flange	Circ – Out			1.00	
	Closure Stud	See Note 2				
	CRDM and Vent Nozzle Penetrations	Ax – In			1.00	
	Quickloc Nozzle Penetrations	Circ – Out			1.00	
	Lift Lugs and IHP Lugs	Circ – Out			1.00	
	Core Support Block	Circ – In			1.00	
	Inlet Nozzle	Circ – In			1.00	
	Outlet Nozzle	Circ – In			1.00	
	DVI Nozzle	Ax – In			0.99	
C/D	Lower Head and Shell Beltline	Circ – In			1.00	
	Closure Flange	Circ – Out			1.00	
	Closure Stud	Circ – In			0.67	
	CRDM and Vent Nozzle Penetrations	Ax – In			1.00	
	Quickloc Nozzle Penetrations	Ax – In			1.00	
	Lift Lugs and IHP Lugs	Ax – In			1.00	
	Core Support Block	Circ – In			1.00	
	Inlet Nozzle	Circ – In			1.00	
	Outlet Nozzle	Circ – In			1.00	
	DVI Nozzle	Ax – In			0.99	
Test at 21.1°C[5]	Lower Head and Shell Beltline	Ax – In			1.00	
	Closure Flange	Circ – Out			1.00	
	Closure Stud	See Note 2				
	CRDM and Vent Nozzle Penetrations	Ax – Out			1.00	
	Quickloc Nozzle Penetrations	Circ – Out			1.00	
	Lift Lugs and IHP Lugs	Circ – Out			1.00	
	Core Support Block	Ax – In			1.00	
	Inlet Nozzle	Ax – In			1.00	
	Outlet Nozzle	Ax – In			0.98	
	DVI Nozzle	Ax – In			1.00	

Notes:

1. Flaw orientation: Circ = Circumferential, Ax = Axial/Meridional, In = ID flaw, Out = OD flaw.
2. Closure studs are not required to be evaluated to Level A/B or Test conditions as they require impact tests. See G-4000 of the ASME Code, Section III, Division 1, Appendix G, 1998 Edition through 2000 Addenda.
3. Per G-2120 of the ASME Code, Section III, Division 1, Appendix G, 1998 Edition through 2001 Addenda, flaw sizes smaller than 0.25T may be considered on an individual case basis if detection of the smaller flaw can be ensured. Thus, for flaw sizes smaller than0.25T that result in $K_I > K_{IR}$, a reduced, detectible flaw size was calculated assuming $K_I = K_{IR}$.
4. Per Section 7.C of the Welding Research Council Bulletin Number 175, for bolts over 3 inches in diameter, the recommended toughness requirement equates to a fracture toughness value of 142.8 MPa$\sqrt{}$m and is not dependent on temperature.
5. Per Paragraph 6.2.7 of the Reactor Vessel design specification, the minimum Hydrostatic Test temperature is 21.1°C. Larger flaw sizes can be determined if the Test temperature is raised to a more realistic value (i.e. 43.3°C).

Table 20A-17. Index of Technical Reports

Document Reference	Document Title	Description of Role in Safety Case
Specifications/Reports		
APP-MV01-Z0-001	AP1000 Reactor Pressure Vessel Functional Specification	This document defines the high level performance and operational requirements for the design of the reactor pressure vessel (RPV) that will be part of the reactor system (RXS) in the AP1000 plant. The requirements defined by this Functional Specification are to be used in the preparation of the RPV Design Specification. This Functional Specification serves as one of the documents against which the RPV design is formally reviewed during the design review process.
APP-MV01-Z0R-101	AP1000 Reactor Vessel Design Report	Substantiates the structural integrity of the AP1000 RV design with respect to the requirements of the Design Specification and Section III of the ASME Code. Consolidates the evidence from all pertinent structural analyses and relevant engineering drawings.
APP-MV01-Z0-101	Design Specification for AP1000 RV for System: Reactor Coolant System (RCS)	Provides details of the design specification, covering general design, fabrication, examination, testing documentation, cleaning, packaging and shipping of a RV, CH and associated equipment. The design specification also indicates the specific dimensions, design parameters, design details, design criteria, scope of supply and references.
APP-MV01-Z0-332	Requirements for Hydrostatic Testing	Provides details of the requirements for carrying out the hydrostatic testing of the RV.
APP-GW-VH-002	Packaging Nuclear Components and Spare Parts for Shipment and Storage	Provides details of the requirements for the packaging of nuclear components and spare parts when being shipped or placed in storage.
APP-GW-Z0-602	Cleaning and Cleanliness Requirements of Equipment for Use in Nuclear Steam Supply System and Associated Systems	Provides details of the cleaning and cleanliness requirements of equipment for use in the nuclear steam supply system along with associated systems.
UKP-MV01-Z0R-100	Results of Weld Ranking Process for Reactor Vessel, SG and Pressurizer – Defect Tolerance	Identifies welds to be included in the phased programme planned for defect tolerance assessments.

Table 20A-17. Index of Technical Reports (cont.)

Document Reference	Document Title	Description of Role in Safety Case
Specifications/Reports (cont.)		
APP-RCS-M1-001	Reactor Coolant System Design Transients	Defines the transients used to qualify the reactor coolant system to design requirement.
APP-GW-Z0-608	Material Test Specification for Austenitic Stainless Steel Cladding	Provides details of the test specification for materials testing of austenitic steel cladding.
APP-GW-Z0-609	Requirements for Evaluation of Low Alloy Steel Heat Affected Zone Cladding Overlap Areas	Provides details of the requirements for the evaluation of low alloy steel heat affected zone cladding overlap areas.
APP-GW-Z0-625	Chromium Plating	Provides details of the specification for chromium plating.
APP-GW-Z0-620	Requirements for Marking of Reactor Plant Components and Piping	Provides details of the requirements for the marking of reactor plant components and piping.
APP-GW-VLR-002	Technical Requirements of Stainless Steels, Nickel-Based Alloys, Carbon and Low Alloy Steels, and Welding Materials for AP1000	Contains technical requirements of stainless steels, nickel-base alloys, and carbon and low alloy steels used in the AP1000 design.
APP-VW20-Z0-038	P-NO 8 Clad or Buttering Weld Material Certification Testing	Provides details of the P-NO 8 Clad or Buttering Weld Material Certification Testing.
APP-VW30-Z0-043	P-NO 43 Clad, Buttering or Groove Weld Material Certification Testing	Provides details of the P-NO 8 clad or buttering weld or groove weld material certification testing.
APP-VW40-Z0-031	P-NO 1 Weld Material Certification Testing	Provide details of the P-NO 1 weld material certification testing.
APP-VW40-Z0-041	P-NO 3 Non Core Region Weld Material Certification Testing	Provides details of the P-NO 3 non-core region weld material certification testing.

Table 20A-17. Index of Technical Reports (cont.)

Document Reference	Document Title	Description of Role in Safety Case
APP-VW40-Z0-042	P-NO 3 Core Region Weld Material Certification Testing	Provides details of the P-NO 3 core region weld material certification testing.
Specifications/Reports (cont.)		
APP-MV01-Z0-900	Material Procurement Specification for the Grafoil Rings of the AP1000 QuickLoc Assemblies	Provides details of the specification of materials procurement for the Grafoil rings of the AP1000 QuickLoc assemblies.
APP-GW-VLR-010	AP1000 Supplemental Fabrication and Inspection Requirements	Provides details of the AP1000 supplemental fabrication and inspection requirements.
APP-GW-VW-001	AP1000 Design for Inspectability Program: ISI Requirements for Class 1 Components	Contains requirements and design guidance relative to ISI for ASME Class 1 components, specifically focused on the concept of design for inspectability, to ensure that adequate design and access provisions for meeting ASME Code, Section XI are considered in the overall plant design.
Materials Specification		
APP-VL51-Z0-012	AP1000 RV Material Specification for SA-182/SA-182M Grade F316LN Forgings (Section III-NB)	This specification covers SA-182, Grade F316LN forgings complying with the requirements of the ASME Boiler & Pressure Vessel Code, Section III, Division 1, Subsection NB for Code Class 1 components intended for pressure boundary applications.
APP-VL51-Z0-004	AP1000 RV Material Specification for SA-508/SA-508M Grade 3 Class 1 for Core Region Forgings (Section III-NB)	This specification covers SA-508 Grade 3 Class 1 quenched and tempered alloy steel forgings complying with the requirements of the ASME Boiler & Pressure Vessel Code, Section III, Division 1, Subsection NB for Code Class 1 components intended for core region RV pressure boundary applications.
APP-VL51-Z0-003	AP1000 RV Material Specification for SA-508/SA-508M Grade 3 Class 1 Non-Core Region Forgings (Section III-NB)	This specification covers SA-508 Grade 3 Class 1 quenched and tempered alloy steel forgings complying with the requirements of the ASME Boiler & Pressure Vessel Code, Section III, Division 1, Subsection NB for Code Class 1 components intended for non-core region RV pressure boundary applications.

Table 20A-17. Index of Technical Reports (cont.)

Document Reference	Document Title	Description of Role in Safety Case
Materials Specification (cont.)		
APP-VL52-Z0-032	AP1000 RV Material Specification for SA-533/SA-533M Type B Class 1 Plate (Section III – NB)	This specification covers SA-533 Type B Class 1 quenched and tempered alloy steel plate complying with the requirements of the ASME Boiler & Pressure Vessel Code, Section III, Division 1, Subsection NB for Code Class 1 non-core region structural attachments to the RV pressure boundary.
APP-MV01-Z0-201	AP1000 RV Specification for Alloy 718 Tubing Base Material and O-Ring Seal Fabrication (ASME Section III-NB)	This specification establishes the requirements for manufacturing O-Rings from seamless Alloy 718 tubing. The base material tubing requirements start from the Aerospace Material Specification AMS 5590 requirements with the material in the solution annealed and age hardened condition. The final O-Ring product is welded from one (1) or more formed segments of tubing. Silver plating is applied to the final surface.
APP-VL52-Z0-006	AP1000 RV Material Specification for SA-540/ SA-540M, Grade B23 Class 3 and Grade B24, Class 3 Bolting Material (Section III-NB)	This specification covers SA-540 Grade B23 Class 3 and Grade B24 Class 3 bolting material complying with the requirements of the ASME Boiler & Pressure Vessel Code, Section III, Division 1, Subsection NB for Code Class 1 components.
APP-VL52-Z0-061	AP1000 RV Material Specification for SB-166 UNS N06690 Rod and Bar (Section III-NB)	This specification covers the general manufacturing, inspection, testing, and quality assurance requirements for Nickel-Chromium-Iron Alloy 690 (UNS N06690) rod, bar, and wire meeting the chemical and mechanical property requirements as specified, and the requirements of SB-166 and Subsection NB of Section III of the ASME B&PV Code.
APP-VL53-Z0-013	AP1000 Reactor Vessel Material Specification for SB-167/SB-167M, UNS N06690 Seamless Pipe and Tube (Section III-NB)	This specification covers the general manufacturing, inspection, testing, and quality assurance requirements for Nickel-Chromium-Iron Alloy 690 (UNS N06690) seamless pipe and tubing meeting the chemical and mechanical property requirements as specified, and the requirements of SB-167 and Subsection NB of Section III of the ASME B&PV Code.

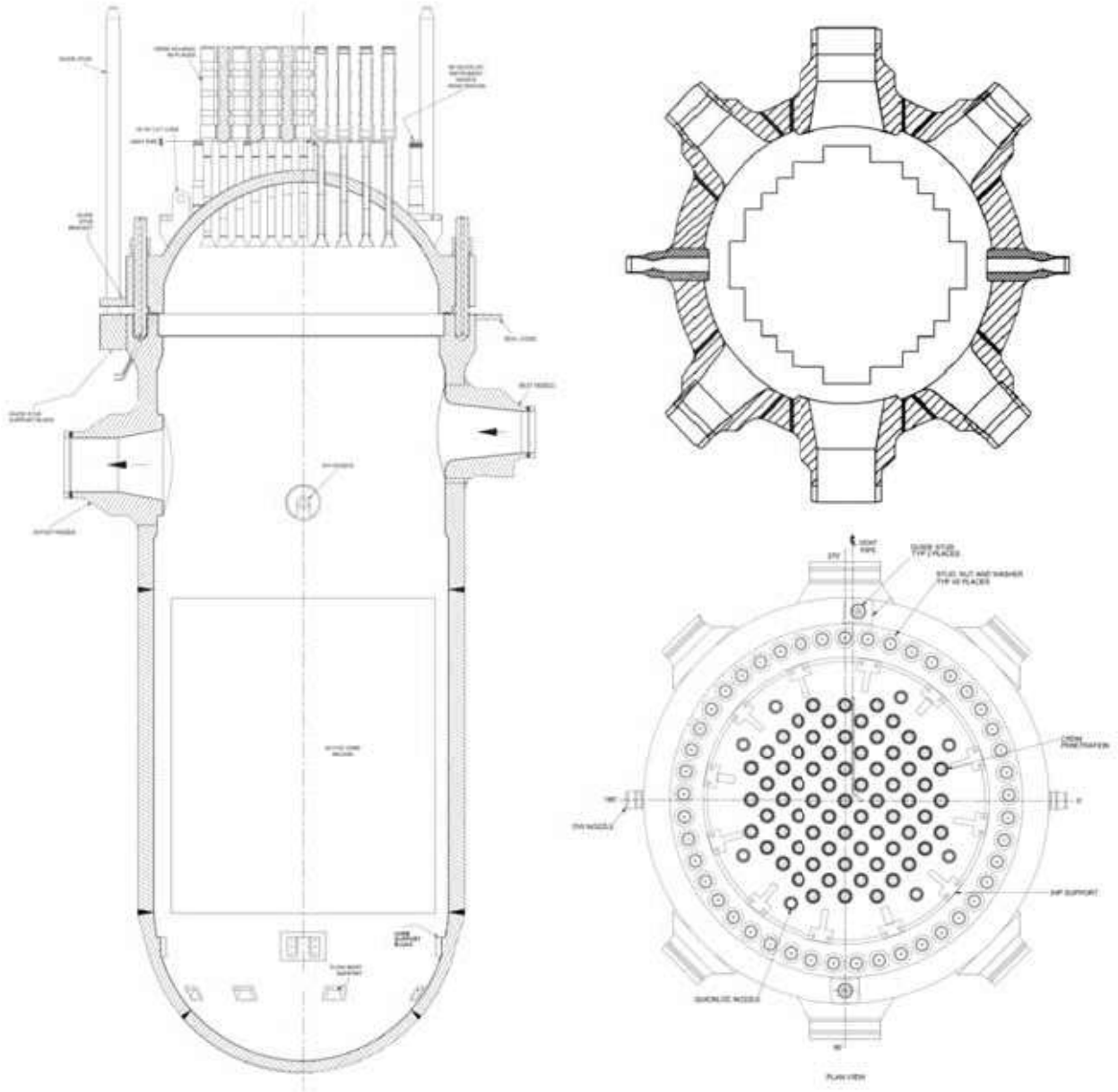


Figure 20A-1. Reactor Vessel

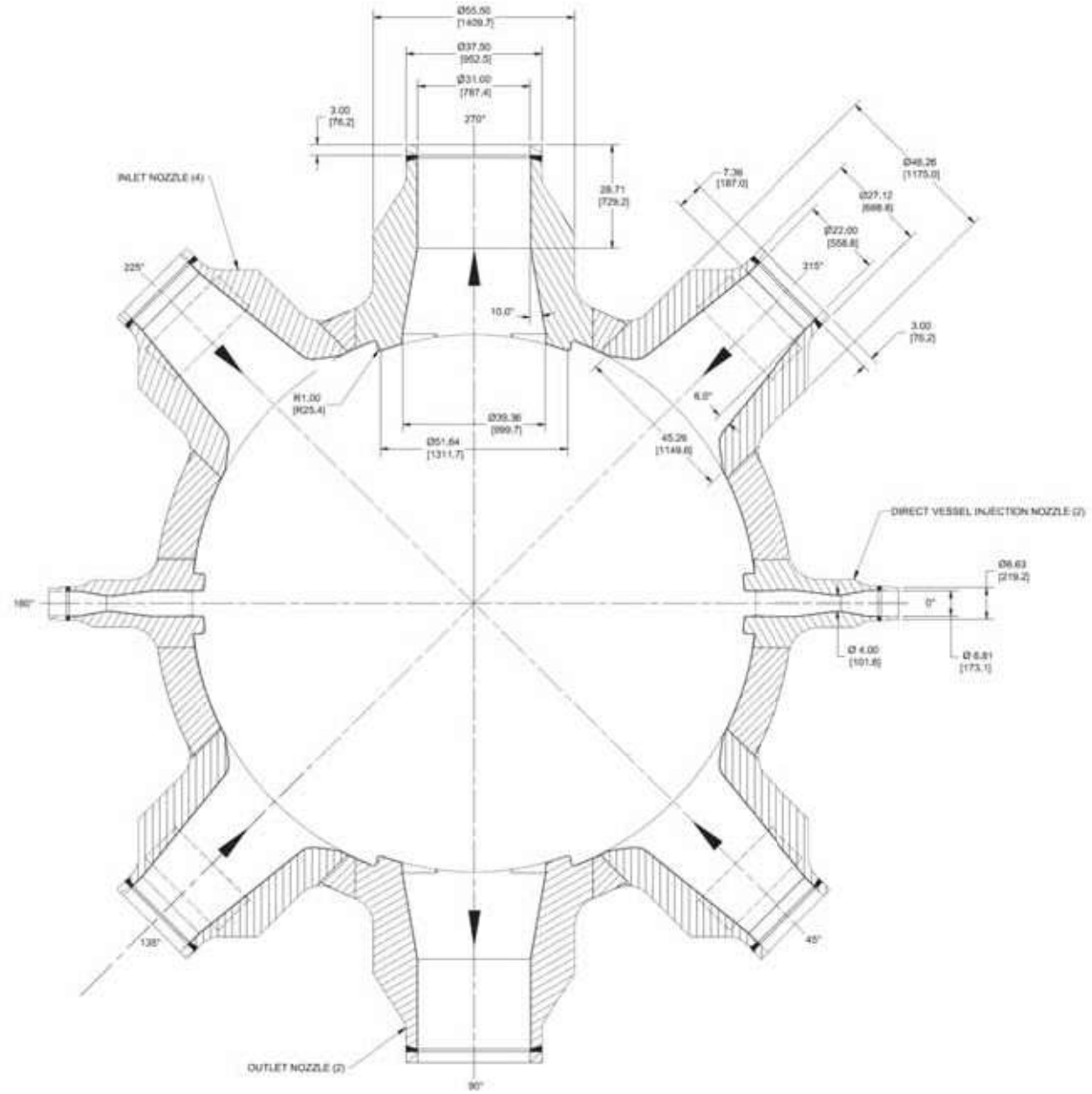


Figure 20A-2. Reactor Vessel Nominal Dimensions – Plan View

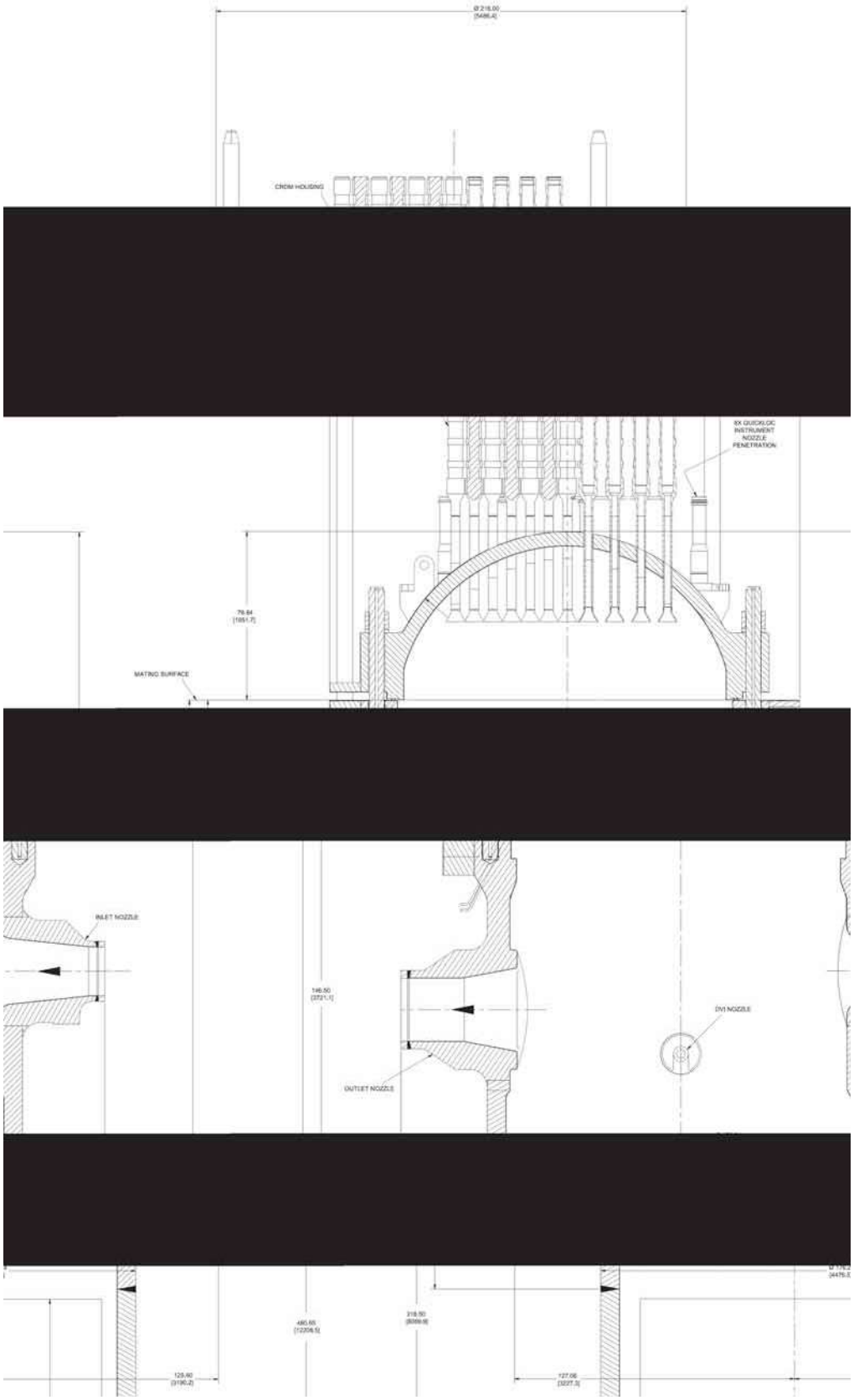


Figure 20A-3. Reactor Vessel Nominal Dimensions – Side View

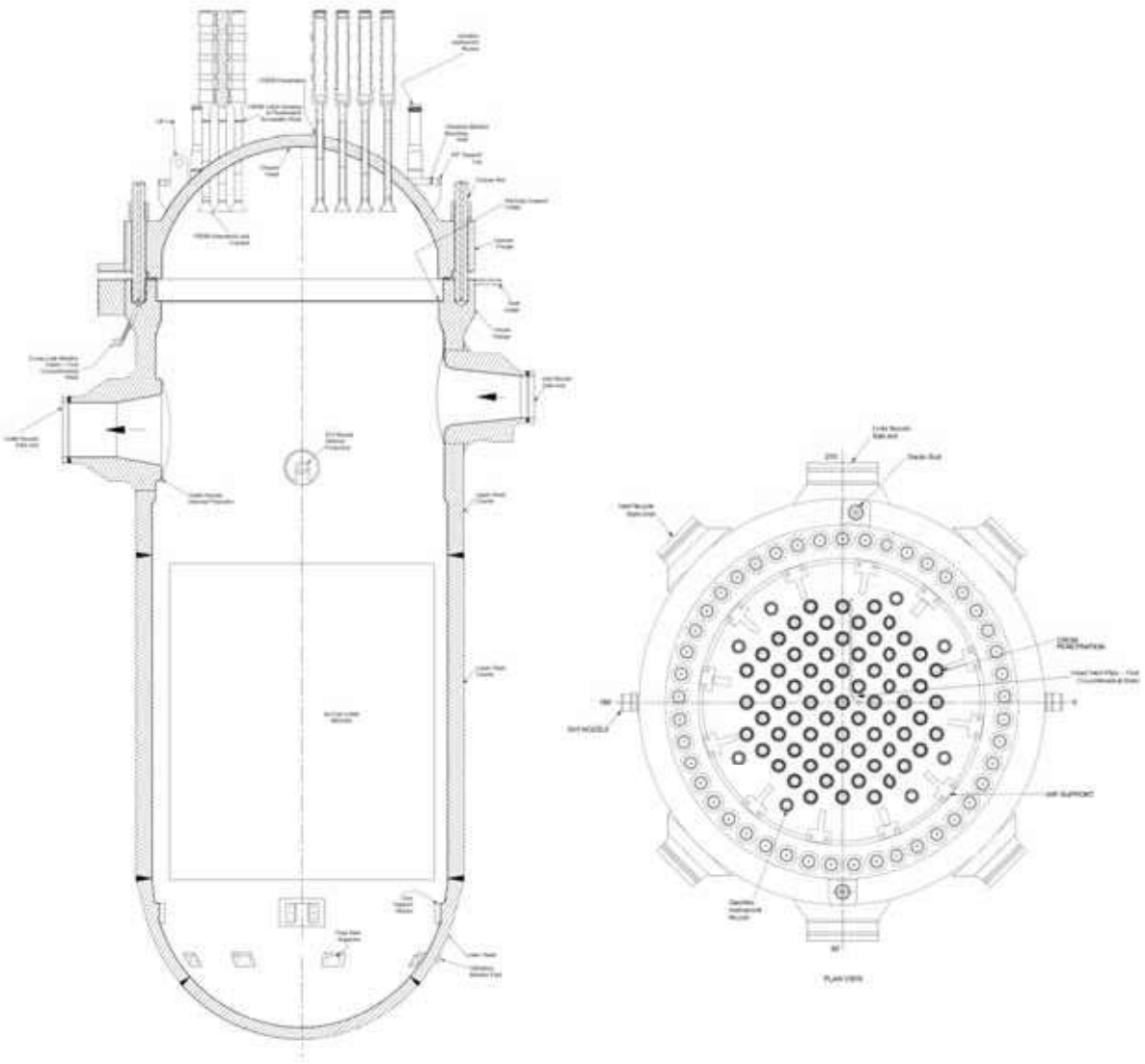


Figure 20A-4. Reactor Vessel Physical Boundaries

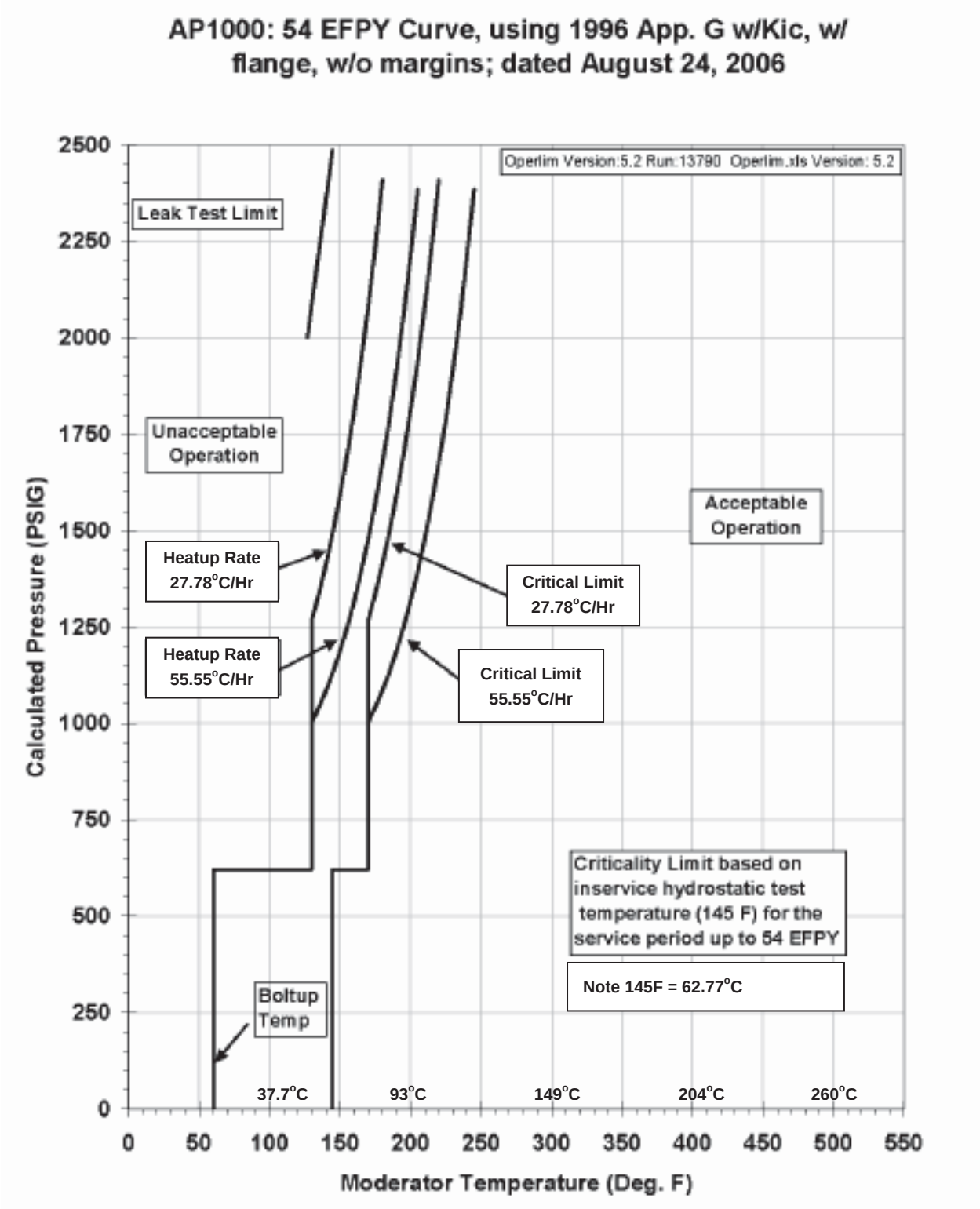


Figure 20A-5. AP1000 Reactor Coolant System Heatup Limitations (Heatup Rate Up to 27.7°C/hour (50°F/hour) and 55.5°C/hour (100°F/hour) Representative for the First 54 EFPY (Without Margins for Instrumentation Errors)

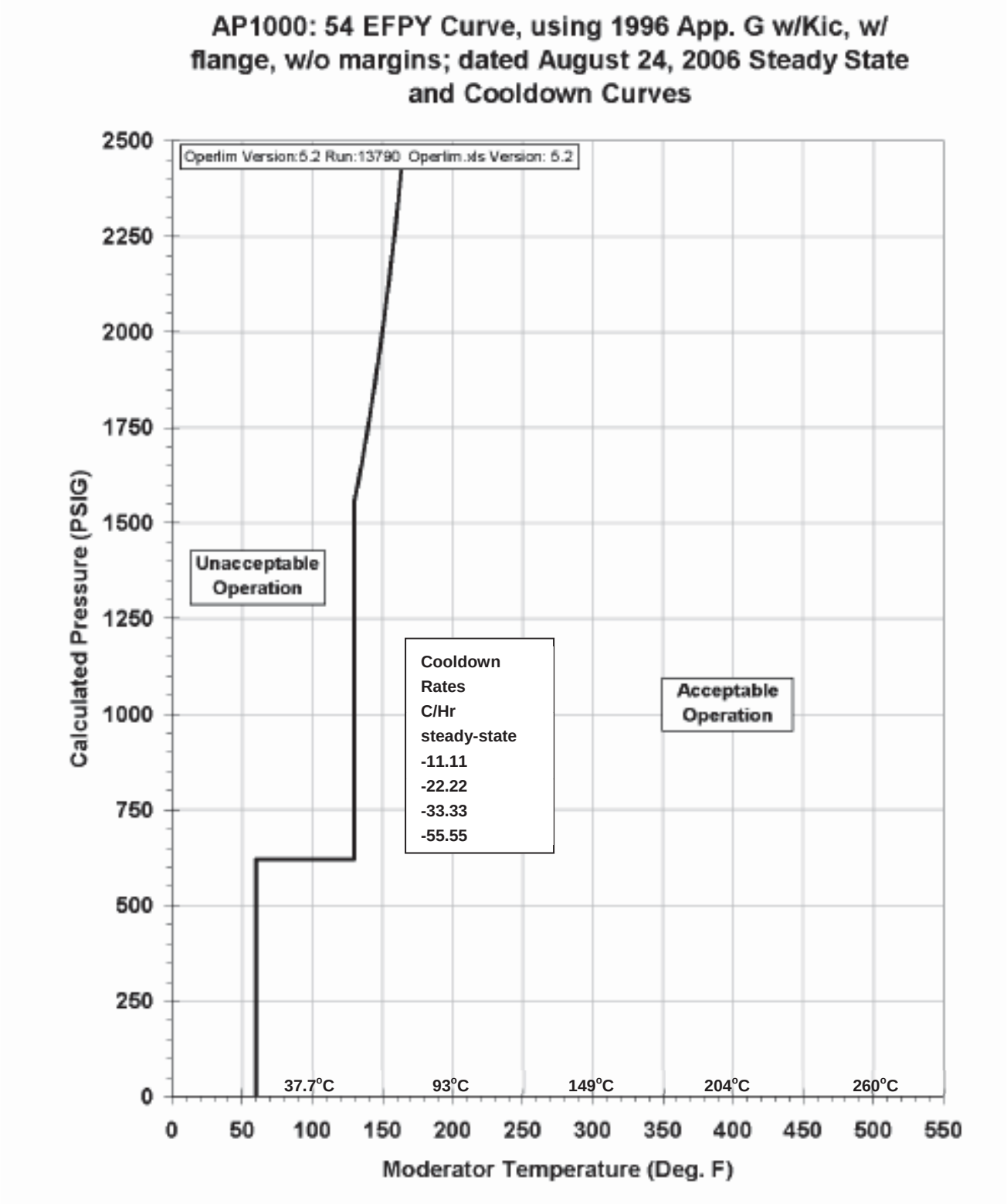


Figure 20A-6. AP1000 Reactor Coolant System Cooldown Limitations (Cooldown Rates up to 27.7°C/hour (50°F/hour) and 55.5°C/hour (100°F/hour) Representative for the First 54 EFPY (Without Margins for Instrumentation Errors)

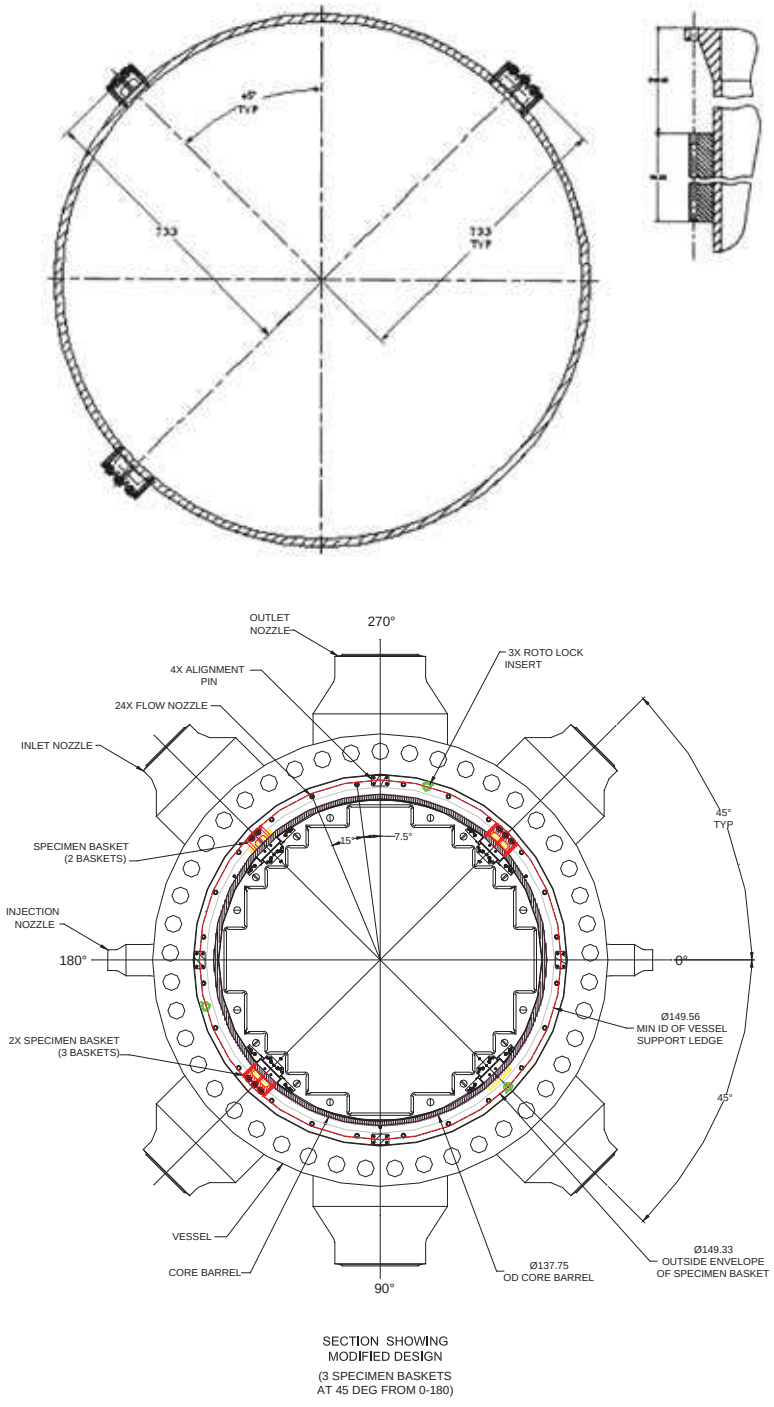


Figure 20A-7. AP1000 Reactor Vessel Surveillance Capsule Locations

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS AND ACRONYMS

ADS	automatic depressurisation system
ALARP	as low as reasonably practicable
ASME	American Society of Mechanical Engineers
CMT	core makeup tank
CSR	Component Safety Report
CVS	chemical and volume control system
DDT	defect detection trials
DSM	defect size margin
ELLDS	end of life limiting defect size
ENIQ	European Network for Inspection and Qualification
FCG	fatigue crack growth
FUF	fatigue usage factor
GDA	generic design assessment
HI	high integrity
HSS	highest safety significance
ISI	in-service inspection
IVC	inspection validation centre
LCO	limiting conditions for operation
LFCG	lifetime fatigue crack growth
LOCA	loss-of-coolant accident
LTOP	low temperature overpressure protection
MT	magnetic particle testing
NDE	nondestructive examination
NDT	nondestructive testing
NDTT	nil-ductility transition temperature
NPP	nuclear power plant
NRC	Nuclear Regulatory Commission
P/T	pressure/temperature
PSARV	pressuriser safety and relief valve
PSI	pre-service inspection
PSS	primary sampling system
PT	dye penetrant testing
PWHT	post weld heat treatment
PWR	pressurised water reactor
PWSCC	primary water stress corrosion cracking
PXS	passive core cooling system
PZR	pressuriser
QEDS	qualified examination defect size
RCPB	reactor coolant pressure boundary
RCS	reactor coolant system
RO	regulatory observation
RT	radiographic testing
RT_{NDT}	reference temperature for non-ductility transition
RV	reactor vessel
SAP	safety assessment principle
SFR	safety functional requirement

LIST OF ABBREVIATIONS AND ACRONYMS (cont.)

SG	steam generator
SoL	start of life
SSC	system, structure, or component
SSE	safe shutdown earthquake
T_{NDT}	temperature for non-ductility transition
UK	United Kingdom
US	United States
UT	ultrasonic testing

APPENDIX 20B
PRESSURISER COMPONENT SAFETY REPORT

20B.1 Introduction

This is the component safety report (CSR) for the pressuriser (PZR) as introduced in Section 20.2. The safety argument herein substantiates the structural integrity of the PZR to a degree of rigour commensurate with the consequences of gross structural failure. The safety argument is supported by a suite of documentary evidence outlined in Section 20B.7 regarding the quality of design, manufacture, installation and operation of the PZR.

20B.1.1 Scope

This CSR presents arguments to support the claim that the nuclear and radiological risks potentially arising from gross structural failure of the PZR are tolerably low for the lifetime objective of 60 years. Conventional hazards to personnel safety are outside the scope of this Appendix 20B.

20B.1.2 Objectives

This report supports the nuclear safety claim that the AP1000 plant risk remains both tolerable and as low as reasonably practicable (ALARP) for the design lifetime. This claim is substantiated by satisfying structural integrity safety design bases for all safety-significant AP1000 systems, structures, or components (SSCs). The safety design bases, applied across the operational, process and lifecycle scope of the safety case, embody the technical scope of the safety case: maintaining these at all times, the plant will be acceptably safe. Specific safety functional requirements (SFRs) for each particular component are developed from the structural integrity safety design bases, and correspond to the functions that need to be maintained to provide assurance of nuclear and radiological safety. The SFRs applicable to the PZR are identified in Section 20B.2.1.

20B.1.3 Interface with Other Safety Case Documents

The safety argument presented in this report is supported by a dossier of technical data and analyses. These are listed in the Technical Index (Section 20B.7) and each is specifically identified in the relevant section of the structured safety argument.

20B.1.4 Description

The PZR is a vertical, cylindrical vessel having hemispherical top and bottom heads constructed of low alloy steel. Internal surfaces exposed to the reactor coolant are clad using corrosion resistant materials. Material specifications for the PZR are provided in Table 20B-1.

The AP1000 PZR is approximately 13.78 m (542.4") long and has an inner diameter of approximately 2.54 m (100"). The nominal free internal volume for the PZR is 59.47 m^3 (2,100 cubic feet). The upper head of the vessel is penetrated by one (1) spray nozzle, two (2) safety relief nozzles, four (4) instrumentation nozzles and one (1) temperature nozzle. One (1) manway, four (4) instrumentation nozzles, one (1) sampling nozzle and one (1) temperature nozzle are located in the cylindrical shell. The lower head is penetrated by one (1) surge nozzle and seventy eight (78) heater assemblies, which are inserted from the bottom head through heater sleeve assemblies.

The general configuration of the PZR is shown in Figure 20B-1. The design data for the PZR are given in Table 20B-2 and Table 20B-4.

The PZR is designed to meet the requirements of the American Society of Mechanical Engineers (ASME) Boiler & Pressure Vessel Code (Code), Section III, subsection NB, 1998 Edition with Addenda up through and including 2000. Other applicable codes, standards and regulations are summarised in section 20B.3.1.1.3.

The surge nozzle design is such that it is integrally forged with the bottom head and the safety/relief nozzle and spray nozzle are both integrally forged with the upper head to limit the number of welds required. The surge nozzle safe-end will be spaced sufficiently below the lowest heater sleeve to facilitate field welding to the surge line. Thermal sleeves are included in the surge nozzle and the spray nozzle to limit thermal stresses during surge and spray transients. The spray line nozzles and the automatic depressurisation and safety valve connections are located in the top head of the PZR vessel.

The safety relief nozzle (DN 350, NPS 14), surge nozzle (DN 100, NPS 4) and temperature and instrumentation nozzles terminate in stainless steel material to facilitate compatibility with the interfacing material. The spray nozzle terminates in Alloy 690 material. The safe ends are of sufficient length to prevent damage to the transition weld on the nozzle during field welding. The surge, safety relief and ferritic nozzle weld end preparations are buttered prior to final post weld heat treatment (PWHT). After final PWHT, the safe ends are welded to the buttered nozzles. The internal upper head spray nozzle region, to which the spray nozzle nipple is welded, are first be buttered and then stress relieved prior to welding the spray nozzle nipple. The weld metal for buttering and the weld to join the safe end to the nozzle is detailed in section 20B.3.1.4.2. The compatibility of the materials is detailed in section 20B.3.1.4.4.

A retaining screen above the surge nozzle prevents passage of any foreign matter from the PZR to the reactor coolant system (RCS). Baffles in the lower section of the PZR prevent an in-surge of cold water from flowing directly to the steam/water interface. The baffles also assist in mixing the incoming water with the water in the PZR. The retaining screen and baffles also act as a diffuser and support the heaters to limit vibration.

Electric direct-immersion heaters are installed in vertically oriented heater wells penetrating the PZR bottom head. The heater sleeves are welded to the bottom head and form part of the pressure boundary. The heaters can be removed for maintenance or replacement. They are manufactured from austenitic stainless steel. Nickel-chromium-iron alloys are not used for the heaters.

The PZR is fitted with mirror-type insulation, which contains easy locking joints for quick removal and reinstallation. A manway in the upper shell provides access to the internal space of the PZR in order to inspect or maintain the spray nozzle. The manway closure is a gasketed cover held in place with threaded fasteners.

Brackets on the upper shell attach the structure (a ring girder) of the PZR safety and relief valve (PSARV) module. The PSARV module includes the safety valves and the first three stages of the automatic depressurisation system (ADS) valves. The support brackets on the PZR represent the primary vertical load path to the building structure. Sway struts between the ring girder and PZR compartment walls also provide lateral support to the upper portion of the PZR.

Support arrangement for the PZR is shown in Figure 20B-6. Four steel columns attach to pads on the lower head to provide vertical support for the vessel. Lateral support for the lower

portion of the vessel is provided by sway struts between the columns and compartment walls. As part of the lower support system, four support pads will be forged in the PZR lower head. The upper support system provides lateral/seismic support and consists of eight sway struts that attach to a ring girder which in turn attaches to eight pairs of support brackets on the shell. The other ends of the struts attach to the corners of the PZR compartment. The supports will be constructed in accordance with Subsection NF of the ASME Code. The support brackets are also used to support the ADS module that is located above the PZR. The support brackets will be constructed in accordance with Subsection NB of the ASME Code.

20B.1.5 Function

The PZR will perform the following functions:

- Provide a point in the RCS where liquid and vapour can be maintained in equilibrium under saturated conditions for pressure control purposes.
- Provide a barrier to the release of reactor coolant and other radioactive materials to the containment atmosphere.
- Provide a controlled volume from which level can be measured.
- Contain the water volume that is used as an initial source to maintain RCS volume in the event of a minor system leak.

The PZR is designed to accommodate positive and negative surges through the surge line connecting the bottom head to a hot leg. During normal transient events, the pressure increases caused by insurges are controlled/mitigated by the PZR spray, such that the high pressure reactor trip setpoint is not reached. During pressure decreases (outsurges), water-to-steam flashing and automatic heater operation keep the pressure above the low pressure reactor trip setpoint. The heaters are also energised on high water level during insurges to heat the sub-cooled surge water entering the PZR from the reactor coolant loop. A screen at the surge line nozzle, as well as baffles in the lower section of the PZR, prevent cold insurge water from flowing directly to the steam/water interface. The screen and baffles also assist in mixing. Because of the relatively low flow rate of the insurges and outsurges associated with normal PZR transients, the PZR may experience thermal stratification. This is taken account of in the design. During plant heat up and cool down, when the potential for thermal stratification is the greatest, the PZR may be operated with a continuous outflow of water to minimise the possibility of PZR thermal transients resulting from insurges (in addition to operation in Modes 1 and 2[1]).

The PZR volume and level setpoints are selected to prevent water relief through the safety valves following any normal or upset event (Condition I or II) without the benefit of the rod control and steam dump systems. Conservation of inventory during normal and upset events is a safety-related function. The RCS and PZR will perform this function in accordance with all of the applicable safety related criteria discussed in Section 20B.2.

1. Mode 1 – Feedwater Cycling, Slug Flow every 2 hours; Mode 2 – Feedwater Cycling, Slug Flow every 24 minutes.

On a best estimate basis, with normal plant conditions, the combination of the normal PZR liquid and vapour volumes is sufficient to support the following performance requirements:

- Maintain pressure response to programmed system volume changes within appropriate limits.
- Prevent uncovering of the heaters following a step load decrease.
- Accept a 100% load rejection without actuating a reactor trip in conjunction with automatic reactor control and steam dump to the condenser.
- Prevent letdown isolation on low PZR water level following a reactor trip.
- Avoid generation of a low PZR pressure safety injection signal (core makeup tank (CMT)/passive core cooling system (PXS) actuation) following reactor trip, assuming normal operation of control systems.
- Prevent safety valve actuation for any normal or upset event.

The PZR contains electrical heaters installed through the bottom head of the vessel. These heaters are removable for maintenance or replacement. The total heater capacity is selected to provide sufficient heat up of the PZR during start up operation to meet the RCS heat up requirements.

The heaters are configured into 5 groups. A control group is sized to accommodate steady state heat losses. The control group operates continuously during normal operation and is controlled by a proportional controller. Four backup groups of heaters are also installed. Two smaller backup groups can be manually loaded onto diesel generators. Backup heater capacity is based on producing the minimum heat required to maintain sub-cooled RCS pressure during standby operations to support natural circulation through the steam generators (SGs) (this assumes a loss of off-site power). The remaining heater capacity is arranged in two larger backup groups not normally loaded, but being capable of being loaded, onto the diesels. The backup heaters operate in a full on/full off mode, and are actuated during transient events to increase pressure in the RCS. A backup group(s) may be energised temporarily to promote mixing of the boron concentration between the RCS loop piping and the PZR. Energising a heater group(s) creates a demand for PZR spray and promotes mixing. The capacity of the control and backup groups is defined in Table 20B-3.

20B.1.6 Instrumentation

Instrument connections are provided in the PZR shell to measure important parameters. Eight (8) level taps are provided for four (4) channels of level measurement. Level taps are also used for connection to the pressure measurement instrumentation. Two (2) temperature taps monitor water/steam temperature. A sample tap connection is provided for connection to the sampling system to monitor coolant chemistry. The instrument and sample taps are constructed of austenitic stainless steel and designed for a socket weld of the connecting lines to the taps. The sample and instrument taps incorporate an integral flow restrictor to limit loss of coolant to within the capacity of the makeup system in the event of a failure.

All instrumentation nozzles are welded to the weld build up on the cladding on the inside wall of the vessel in accordance with the ASME Code, Section II, Subsection NB for partial penetration welds.

20B.1.7 Pressuriser Spray

Two separate, automatically controlled spray valves with remote manual overrides are used to initiate PZR spray.

In parallel with each spray valve is a manual throttle valve. The throttle permits a small, continuous flow through both spray lines to reduce thermal stresses and thermal shock when the spray valves open. Flow through this valve helps to maintain uniform water chemistry and temperature in the PZR. Temperature sensors with low temperature alarms are located in each spray line to alert the operator to insufficient bypass flow.

The layout of the common spray line piping routed to the PZR forms a water seal that prevents steam build up back to the control valves. The design spray rate is selected to prevent the PZR pressure from reaching the reactor trip setpoint during a step reduction in power level of 10% of full load.

The PZR spray lines and valves are large enough to provide the required spray flow rate under the driving force of the differential pressure between the surge line connection in the hot leg and the spray line connection in the cold leg. The spray line inlet connections extend into the cold leg piping in the form of a scoop in order to use the velocity head of the reactor coolant loop flow to add to the spray driving force. The spray line also assists in equalising the boron concentration between the reactor coolant loops and the PZR.

A flow path from the chemical and volume control system (CVS) to the PZR spray line is also provided. This path provides auxiliary spray to the vapour space of the PZR during cool down, hot standby, and hot shutdown when the reactor coolant pumps are not operating. The PZR spray connection and the spray piping can withstand the thermal stresses resulting from the introduction of cold spray water.

20B.1.8 Boundaries

The equipment boundary of ASME Code jurisdiction includes all components in Figure 20B-2 to Figure 20B-5. The welds at safe end/piping interface or nozzle/piping interface are considered as part of the RCS piping system. These figures show the end of the nozzle or safe end as the equipment boundary and also show the boundaries for the support interfaces.

The manway cover and attachment hardware are included within the equipment boundary.

20B.2 SAFETY CASE REQUIREMENTS

This CSR supports the substantiation of these claims by establishing that the structural integrity of the PZR is commensurate with the consequences of gross failure by means of a structured safety argument, supported by suitable and sufficient evidence. The safety argument is presented according to an established four legged structure as detailed in the Demonstration of Incredibility of Failure in Structural Integrity Safety Cases (Reference 20B.3), to demonstrate an appropriate level of defence in depth by identifying evidence to satisfy safety claims and objectives identified within each leg of the argument, as follows:

Leg 1	**Interpolation/Extrapolation of Experience – 'Good Design and Manufacture' (Section 20B.3.1)**
Objective	Provides evidence of good design and manufacture based upon a proven track record. It provides a keystone for a demonstration of high reliability and embodies the code and plant operating experience with the objectives of achieving good quality of build, high integrity (HI) and the avoidance of defects.
Claim	High quality is achieved through good design and manufacture.
Leg 2	**Functional Testing (Section 20B.3.2)**
Objective	Incorporates the build experience as embodied in design codes and provides some diversity and redundancy to the pre-service inspection.
Claim	Components are shown to be fit for purpose through effective functional testing.
Leg 3	**Failure Analysis (Section 20B.3.3)**
Objective	Provides an assessment of through-life degradation mechanisms and shows that such mechanisms will not threaten integrity over a specific interval. Goes beyond design code requirements to provide a further demonstration of integrity. Recognises that flaws may be present and shows tolerance to them. Supplements the Leg 1 aim of avoidance of defects to provide a safety case with both defect avoidance and tolerance.
Claim	Components are tolerant to through life degradation over the design life of the plant.
Leg 4	**Forewarning of Failure (Section 20B.3.4)**
Objective	Confirms the absence of a degradation mechanism or that a known degradation mechanism is not significant enough to threaten integrity or will have limited consequences. Provides contingency for the unexpected.
Claim	Effective systems are in place to provide forewarning of failure.

20B.2.1 Safety Functional Requirements

Chapter 20 identifies performance and safety design bases for the AP1000 SSCs. These are requirements of plant systems, some duty, some accident response, which must be maintained at all times to provide assurance of plant nuclear and radiological safety. Identification of the SFRs (also listed in Table 20-1) for the PZR follows from the performance and safety design bases as follows:

SFR	Description
20.2.1	The PZR is required to maintain the integrity of the primary coolant pressure boundary during standby, normal operation and under design basis faulted conditions for the design life of the plant.
20.2.2	The PZR is required to provide the point in the RCS where system pressure is controlled during steady state operations and transients, to ensure minimum pressure requirements associated with core coolant boiling and departure from nucleate boiling limits are maintained.

SFR	Description
20.2.3	The PZR is required to provide the controlled volume from which the level of reactor coolant can be measured.
20.2.4	The PZR is required to contain the water volume which is used to maintain RCS volume in the event of a minor system leak for a reasonable time without replenishment.

Postulated failure modes, which result in a loss of these SFRs lead to identification of structural reliability targets commensurate with the consequences of gross failure, as determined through the process of component classification as described in Section 20B.2.2. The safety argument in Section 20B.3 is provided to establish that structural integrity of the PZR will be maintained for all conditions within the design basis and thus demonstrate that all of the above SFRs will be maintained at all times.

20B.2.2 Pressuriser Structural Integrity Classification

Key to the PZR structural integrity safety case is the clear understanding of the potential radiological consequences of any postulated gross failure mode. Based upon this understanding, a structured and systematic basis can be established for setting the level of rigour applied during the design assessment, material procurement, fabrication, in-manufacture inspection, testing and in-service testing, maintenance, inspection and safety case assessment of the component. Details of the approach for developing the AP1000 component structural integrity safety cases are given in the United Kingdom (UK) AP1000 Structural Integrity Classification (Reference 20B.4).

The approach to structural integrity classification is discussed in Section 20.5 and is consistent with the overall AP1000 safety classification scheme as detailed in Chapter 5. Reference 20B.4 details the approach taken whereby a more detailed assessment of selected individual components is made to establish the consequences of gross failure, due to both direct consequences, such as a loss-of-coolant accident (LOCA), and indirect consequences, such as the effect of missiles, jet loading or pipe whip on essential safety systems. Based on this assessment, and in accordance with the scheme identified in Table 20-2, components are ascribed one of the five structural integrity classifications described in Section 20.5.2.

For the PZR, a detailed assessment of the failure consequences is documented in Reference 20B.4. The results of this assessment are tabulated in Table 20-7. This concludes that postulated gross failure of the PZR has the potential for the most severe off-site consequences and hence a Highest Safety Significance (HSS) Classification is appropriate.

The HSS classification does not, however, apply to each and every component of the PZR or to every postulated failure mode and defect orientation, since certain failure modes will not lead to the most severe consequences. Since the identification of HSS locations is most important to the safety case arguments at each individual location, as well as establishing the inspection and defect tolerance requirements for individual welds, it is important to consider each location in turn. This is presented in Table 20B-5.

20B.3 SAFETY ARGUMENT

This section provides a structured safety argument to demonstrate that the PZR is fit for purpose for the required component lifetime of 60 years. The safety argument is presented according to the four legged structure outlined in Section 20B.2.

Consistency with the appropriate ASME rules for design, manufacture and inspection forms the basis to substantiate fitness-for-purpose for PZR components with Standard Class 1 classification.

Compliance with the relevant rules of the ASME Code is generally inferred as providing substantiation for a component's reliability. In the case of the PZR, where gross failure is postulated to lead to severe off-site consequences, it is necessary to substantiate a lower frequency of failure such that the probability of gross failure is so low that it can be discounted. This is achieved by identifying supplementary measures to ensure high quality and by demonstrating tolerance to manufacturing defects above qualified detection limits. Additional qualitative arguments are presented in Section 20B.3.2 and Section 20B.3.4 to demonstrate evidence of defence in depth and substantiate component reliability commensurate with the structural classification of the PZR.

20B.3.1 Leg 1: Interpolation/Extrapolation of Experience – Good Design and Manufacture

The objective of Leg 1 is to provide evidence to support the claim that the quality of design and manufacture is commensurate with the classification of each component of the PZR. This supports the structural reliability targets associated with the classification of each PZR component.

Reference 20B.1 establishes the basis for the materials, design, operability, manufacture, inspection, and testing of the AP1000 PZRs. This provides the basis to demonstrate that the design and construction of the PZR conforms to the ASME Code, Section III, Rules for the Construction of nuclear power plant (NPP) components and the applicable Code Cases and Addenda for Class 1 and Class 2 vessels. The ASME Section III Rules embody extensive international industry-wide operating experience and compliance with these rules provides a keystone for a demonstration of high structural reliability. A number of elements are built up to support this claim.

- The design is well founded, designed in accordance with internationally recognised standards and takes into account operating experience (Section 20B.3.1.1).
- Loading, temperatures and environment have been well defined (Section 20B.3.1.2).
- The AP1000 PZR design has been assessed against relevant design code requirements (Section 20B.3.1.3).
- Components are manufactured using a good choice of materials (Section 20B.3.1.4).
- Good manufacturing (Section 20B.3.1.5).
- Manufacturing inspection (Section 20B.3.1.6).
- Plant operation and maintenance (Section 20B.3.1.7).

Together, these provide an important keystone for a demonstration that the PZR is well designed, will enter service free from structurally significant defects and that the effects of through-life degradation on material properties will not have a deleterious effect on the structural reliability of the PZR.

20B.3.1.1 The Pressuriser Design is Well Founded, Designed in Accordance with Internationally Recognised Standards and Takes into Account Operating Experience

In order to demonstrate that the design is well founded, designed in accordance with internationally recognised standards and takes into account historical experience, evidence to substantiate the following arguments is provided.

- The Westinghouse design of the PZRs is well founded and supported by an excellent safety record.
- The design of the PZR takes account of in-service experience and known age related degradation mechanisms.
- Design and manufacture in accordance with established codes, standards and regulations provides assurance of high reliability.
- Novel features of design are avoided or adequately justified.
- The use of forgings is maximised to limit the number of welds.

20B.3.1.1.1 Westinghouse Design of Pressurisers is Well Founded and Supported by an Excellent Safety Record

The design of the AP1000 PZR is supported by decades of successful plant operating experience which have accumulated many operating years without significant issue. Westinghouse has substantial proven experience, knowledge, and capability to design, manufacture and furnish technical assistance for the installation, start-up and service of NPPs.

The AP1000 PZR is of similar design to that of the earlier Westinghouse designs, and also to typical pressurised water reactor (PWR) PZR design, which use similar proven materials and manufacturing processes. The design has been the subject of regulatory scrutiny overseas: the United States (US) Nuclear Regulatory Commission (NRC) approved the final design certification for the AP1000 in December 2005 following the earlier approval of the AP600 design certification in 1999.

Whilst the substantial record of safe operating experience alone does not fully support reliability claims commensurate with a HSS component, it provides confidence that there is a thorough understanding of the in-service performance of these vessels, the management and mitigation of through-life degradation issues and in the avoidance of issues at the design and manufacturing stage that can affect the through-life performance.

20B.3.1.1.2 The Design of the Pressuriser Takes Account of In-service Experience and Known Age Related Degradation Mechanisms

NUREG-1801 (Reference 20B.6), issued in 2005, presents a comprehensive review of the ageing effects including PWR PZRs, as covered by generic ageing management programmes. During the design of the AP1000 PZR, consideration has been given to the susceptibility of the AP1000 PZR design to known in-service degradation mechanisms. The main conclusions from this review of each of the major in-service issues are summarised below.

Degradation Mechanism	Component	AP1000 Mitigation
Fatigue Cracking	• Reactor coolant pressure boundary components • Piping, piping components and piping elements • Flanges • Nozzles and safe-ends • Vessel shell, heads and welds • Heater sheaths and sleeves • Thermal sleeves • Penetrations • Integral support	Selection of materials. Good design & manufacture. AP1000 components are evaluated against a design life of 60 years and fatigue usage factors (FUFs) will be below unity for the life of each component. In-service inspection (ISI).
Stress corrosion cracking	• Spray head • Heater sheaths and sleeves • Heater bundle diaphragm plate • Instrumentation penetrations • Manways • Flanges	Selection of appropriate materials. The use of material susceptible to Primary Water Stress Corrosion Cracking (PWSCC) is forbidden by the PZR Design Specification. The concentration of chlorides, fluorides, sulphates, lithium, and dissolved oxygen and hydrogen are monitored and kept below the recommended levels. ISI.
Primary water stress corrosion cracking	• Spray head • Instrumentation penetrations • Heater sheaths and sleeves • Heater bundle diaphragm plate • Manways • Flanges • Surge and steam space nozzles • Welds	Selection of appropriate materials. The use of material susceptible to PWSCC is forbidden by the PZR Design Specification. The concentration of chlorides, fluorides, sulphates, lithium, and dissolved oxygen and hydrogen are monitored and kept below the recommended levels. ISI.

Recent UK PWR experience has highlighted concerns relating to the integrity of the PZR heater sheath material. Based on Westinghouse own knowledge of PZR design and worldwide operating experience, there are known issues associated with hardening and sensitisation of the heater sheath material as a result of coldworking during the fabrication process and the lack of a subsequent annealing heat treatment, which eventually lead to stress

corrosion cracking of the heater sheaths. In the AP1000 PZR design, an improved PZR heater sheath is produced in accordance with the ASME SA-213 material specification and with certain supplementary technical requirements, as detailed in Reference 20B.22. These include heat treatment and surface treatment procedures and supplementary material testing in accordance with ASTM A262 (Reference 20B.36).

Design and manufacture in accordance with established codes, standards and regulations provides assurance of high reliability.

The PZR is designed to meet all applicable regulations and standards defined in Reference 20B.1 as summarised below. Complying with such proven and established codes, standards and regulations minimises the level of design and manufacturing uncertainty. Compliance with the ASME Code provides assurance over a wide range of issues from material procurement, component design, selection of manufacturing consumables, qualification of welders, specification of heat treatment, manufacturing quality checks and nondestructive examination (NDE), testing, installation and pre-service inspection (PSI) and ISI requirements. The extensive body of experience that is embodied within the ASME Code and the successful operation of a significant number of pressure vessels (both nuclear and non-nuclear), mean that compliance with the code provides assurance that the vessel reliability will remain high for the design life of the component. However, in order to substantiate a reliability claim commensurate with a component classified (as per Reference 20B.4) as HSS, i.e., where gross failure can be discounted, or HI it is necessary to demonstrate that measures have been taken over and above the minimum requirements specified by ASME. This is discussed in Section 20B.4. Evidence of compliance with ASME requirements will come from the ASME certificate number for the PZR.

ASME Code, Section III, 1998 Edition through 2000 and Applicable Code Cases*

- Section II Materials
- Section III Nuclear Power Plant Components
- Section V Non-destructive Examination
- Section IX Welding and Brazing Qualifications
- Section XI Rules for In-service Inspection of Nuclear Power Plant Components
- N-782 Use of Code Editions, Addenda, and Code Section III Division 1

*Code Cases may be invoked if mutually agreed upon by the Owner

U.S Code of Federal Regulations

- 10 CFR 21 Reporting of Defects and Non-compliance
- 10 CFR 50 Appendix A General Design Criteria for Nuclear Power Plants Criteria 1, 2, 4, 14, 30, 31, and 32 apply
- 10 CFR 50 Appendix B Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants
- 10 CFR 50.55(a) Codes and Standards
- 10 CFR 50 Appendix G Fracture Toughness requirements

ANSI/ASME/ASTM Standards

Compliance with the NQA-1-1994 will be in accordance with the Westinghouse position as detailed in WCAP-12308, "ASME Quality Assurance Program Plan," as supplemented by the supplier's quality assurance programme plan.

- ASME NQA-1-1994, "Quality Assurance Program Requirements for Nuclear Facility Applications"
- ANSI N14.6-1993, "Special Lifting Devices for Shipping Containers Weighing 4,500 kg (10,000 Pounds) or More"
- ANSI B30.9-1996, "Slings"
- ANSI/ANS-51.1, "Nuclear Safety Criteria for the Design of Stationary Pressurized Water Reactor Plants"
- ASTM A262, "Standard Practices for Detecting Susceptibility to Intergranular Attack in Austenitic Stainless Steels" (Practice A and Practice E are required)
- ANSI N18.2a-75, "Nuclear Safety Criteria for the Design of Stationary Pressurized Water Reactor Plants.
- ASME B16.11, "Forged Fittings, Socket-Welding and Threaded"

US NRC Regulatory Guides

The following U.S. NRC Regulatory Guides are applicable to the PZR.

- 1.31 Rev. 3 Control of Ferrite Content in Stainless Steel Weld Material.
- 1.37 Rev. 0 Quality Assurance Requirements for cleaning of Fluid Systems and Associated Components of Water-Cooled Nuclear Power Plants.
- 1.38 Rev. 2 Quality Assurance Requirements for Packaging, Shipping, Receiving, Storage and Handling of Items for Water-Cooled Nuclear Power Plants.
- 1.44 Rev. 0 Control of the Use of Sensitized Stainless Steel.
- 1.50 Rev. 0 Control of Preheat Temperature for Welding of Low-Alloy Steel.
- 1.60 Rev.1 Design Response Spectra for Seismic Design of Nuclear Power Plants.
- 8.8 Rev. 3 Information Relevant to Ensuring that Occupational Radiation Exposure at Nuclear Power Stations will be as low as reasonably achievable.
- 1.26 Rev. 3 Quality Group Classification and Standards for Water, Steam and Radioactive Waste Components of Nuclear Power Plants.
- 1.29 Rev. 3 Seismic Design Classification.

- 1.28 Rev. 3 Quality Assurance Program Requirements (Design and Construction).
- 1.84 Rev. 31 Design and Fabrication Code Case Acceptability ASME Section III Division 1.
- 1.147 Rev. 15 In-Service Inspection Code Case Acceptability, ASME Section XI Division 1.
- 1.85 Rev. 31 Materials Code Case Acceptability – ASME Code Section III, Division 1.

20B.3.1.1.3 **Novel Features of Design are Avoided or Adequately Justified**

The PZR is sized to have sufficient volume to accomplish the functional requirements without power operated relief valves. The PZR has approximately 40% more volume than the PZRs for previous plants with similar power levels. This increased volume provides plant operating flexibility and minimises challenges to the safety relief valves.

In other regards, the AP1000 PZR design and materials selection is broadly similar to that typical of PWR PZRs and is consistent with accepted industry practice.

20B.3.1.1.4 **The Use of Forgings is Maximised to Limit the Number of Welds**

To minimise welds and reduce ISI, the PZR cylindrical sections (upper, middle and lower) will be forged shell sections, thereby eliminating the need for longitudinal seam welds. The safety relief nozzle and the spray nozzle of the upper head region and the support pads and the surge nozzle of the lower head region are integrally forged, again to minimise welds present at these regions.

20B.3.1.2 Loading, Temperatures and Environment have been Well Defined

In order to demonstrate that the loading, temperature and environment have been well defined, evidence to substantiate the following arguments is provided.

- Design and operating parameters used in the design evaluation have been determined using established and conservative procedures and capture all normal and design basis conditions.
- The PZR is designed to operate in the specified environmental conditions.

20B.3.1.2.1 **Design and Operating Parameters used in the Design Evaluation have been Determined using Established and Conservative Procedures and Capture all Normal and Design Basis Conditions**

The PZR is designed, fabricated, examined and tested in accordance with Reference 20B.1 and the ASME Code, Section III and all applicable Code Cases and Addenda for Class 1 Vessels. To substantiate claims based on ASME Code compliance, evidence is provided here to demonstrate that design and operating parameters used in the design evaluation have been determined using established conservative procedures. Section III Subsection NB of the code requires assessment against design, service and test conditions, and that the stresses within the vessel are shown to comply with specified allowable stress limits appropriate to the material of construction. The design conditions include those pressure, temperature and

mechanical loadings selected as the basis for the design. Service conditions cover those normal operating conditions, anticipated transients and accident conditions expected or postulated to occur during operation. The evaluation of service and testing conditions includes an evaluation of fatigue due to cyclic stresses.

The design and service conditions for the PZR are shown in Table 20B-2. The following five categories of operating condition, as defined in ASME Code, Section III, have been evaluated as part of the design substantiation for the PZR. These encompass all operating conditions within the design basis, as summarised in Table 20-22 along with the number of occurrences of each transient over the design life of the plant.

- Level A Service Conditions – Normal Conditions.
- Level B Service Conditions – Upset Conditions, Incidents of Moderate Frequency
- Level C Service Conditions – Emergency Conditions, Infrequent Incidents
- Level D Service Conditions – Faulted Conditions, Limiting Faults
- Testing Conditions – Include primary and secondary hydrostatic tests and SG tube leak tests specified.

The specific transients to be considered for equipment fatigue analyses are based upon PWR plant operating experience along with engineering judgment. The plant condition categorisation defined in ANS/ANSI N51.1 (Reference 20B.7), which categorises transients on the basis of expected frequency, are also part of the process to define transients and which service condition applies for a given transient. The transients for each of these service conditions are summarised in Table 20-22 and are further specified in Reference 20B.1.

The transients selected are a conservative representation of transients that, used as a basis for component fatigue evaluation, provide confidence that the component is appropriate for its application for the 60-year design objective. These transients are described by pertinent variations in pressure, fluid temperature, and fluid flow. The frequency of these transients, in some cases, is greater than the maximum frequency that defines the plant condition in Reference 20B.7. The design transients and the number of events of each that are normally used for fatigue evaluations of components are presented in Table 20-22, as specified in Reference 20.3.

Section 6.4.16 of Reference 20B.1 provides a description of the seismic requirements. The seismic loading is based upon that defined in the AP1000 Seismic Design Criteria (Reference 20B.11) and considers 20 safe shutdown earthquake (SSE) cycles (or alternatively 315 cycles of 1/3 SSE). The analysis also considers the hydraulic interaction between the coolant (gas or liquid) and the system structural elements. For dynamic analysis either equivalent static analysis or response spectrum analysis methods may be used.

The peak ground acceleration of the SSE has been established as 0.30 g for the AP1000 design. The vertical peak ground acceleration is conservatively assumed to equal the horizontal value of 0.30 g. Both horizontal and vertical design response spectra are based on the Regulatory Guide 1.60 (Reference 20B.34) spectra augmented at the higher frequencies. In Chapter 12, these spectra are compared to the UK generic design basis Principia Mechanica Limited spectra, which are based on a 0.25 g zero period acceleration event.

20B.3.1.2.2 **The Pressuriser is Designed to Operate in the Specified Environmental Conditions**

The PZR is designed to maintain performance and structural integrity when operating with specific environmental conditions. The interior of the PZR will be exposed to the primary coolant. Bounding conditions for operational chemistry control of primary fluids in contact with primary system materials and nuclear fuel are presented in Table 20A-3, which reflects well established EPRI guidelines for PWR primary chemistry (Reference 20B.12). The exterior will be exposed to the atmospheric conditions prevailing in the reactor containment defined in Table 20B-7. The internal and external environmental conditions are used in conjunction with the design transients of Table 20-22. The design accounts for the effects of the radiation fields in which the PZR operates. Applicable radiation environmental conditions are given in Reference 20B.1.

Table 20B-15 specifies the operating environment inside containment during group 1 and 2 abnormal events.

20B.3.1.3 The AP1000 Pressuriser Design has been Assessed Against Relevant Design Code Requirements

In order to demonstrate that the PZR design has been assessed against the relevant design code requirements, evidence to substantiate the following arguments is provided.

- The PZR design complies with the allowable stress limits and sizing limits as specified in ASME III for a Class 1 component.

- The end of life FUFs are below the 1.0 fatigue limit.

20B.3.1.3.1 **The Pressuriser Design Assessment Against Relevant Stress Limits and End of Life Fatigue Usage Factors are Below Unity**

The PZR is designed in accordance with the relevant and recognised design codes, discussed in Section 20B.3.1.1.3. The following regions of the PZR are included in the scope of the stress analysis:

- Upper Head and Shell
- Spray nozzle
- Surge Nozzle
- Safety Relief Nozzle
- Instrument Nozzle
- Manway
- Trunnion and Shell Build-up
- Bracket
- Lower Head/Support Pad
- Heater/Heater Support plate
- Heater/Heater Sleeve
- Heater Sheath

The PZR Design Report (Reference 20B.13) summarises results of detailed analyses to substantiate the design of the PZR. The scope of the analyses includes all locations identified above and all of the required loading conditions specified in Reference 20B.1.

The PZR is designed in accordance with the requirements of the ASME Boiler and Pressure Vessel Code, Section III, 1998 Edition with addenda up through and including 2000 as stated in the Design Specification (Reference 20B.1). The PZR Design Report (Reference 20B.13) consolidates the results of detailed analyses demonstrating the adequacy of the structural design to sustain and meet ASME Code requirements.

The components of the PZR forming part of the reactor coolant pressure boundary, including all openings in the vessel shell and upper and lower head, has been shown to meet the minimum thickness and reinforcement requirements for internal pressure in accordance with ASME Code, Section III. Detailed results for each component are presented in Reference 20B.13. Also reported in Reference 20B.13 are the calculated ratios of the stress intensities to the allowable stress limits and the calculated fatigue usage factors for each of the main locations on the PZR. The results demonstrate that all requirements of the Design Specification and of the ASME Code are met.

20B.3.1.4 Components are Manufactured Using Good Choice of Materials

In order to demonstrate that the AP1000 PZR components are manufactured using a good choice of materials, evidence to substantiate the following arguments is provided.

- AP1000 PZR materials have a proven service performance.
- Material specifications meet or exceed ASME specifications.
- Tight control on chemical composition is specified.
- Materials are compatible with each other and with the environment and are resistant to environmental degradation over the life of the plant. Degradation characteristics are known and understood.
- Nozzle and safe-end materials have been optimised for design and fabrication.
- Materials testing is sufficient to demonstrate that the material properties are compliant with the relevant specifications.

20B.3.1.4.1 AP1000 Pressuriser Materials have a Proven Service Performance

The selection of the AP1000 PZR materials reflects international experience in PWR design, manufacture and operation and the lessons learned. The upper, middle and lower shells, lower head, upper head and nozzles and support pads will be manufactured from ASME SA-508 Grade 3 Class 2 (same chemical composition as Grade 3 Class 1, used in the reactor vessel (RV), but has a higher specified strength of approximately 12%). There is extensive experience with this material in the nuclear industry.

Regulatory Observation, RO-AP1000-21, as detailed in the Step 3 Structural Integrity Assessment of the AP1000 (Reference 20B.14), was raised in regard to the choice of material for the pressuriser. UK precedent has been to use the UK modified specification of ASME SA-508 Class 3 (now Grade 3 Class 1) for the RV, PZR and SG (primary and secondary side) shells. A full response was provided to these concerns.

As is standard for PWR ferritic components, which are in contact with primary coolant, wetted surfaces are clad with austenitic stainless steel or equivalent corrosion-resistant material; the AP1000 cladding is Type 309L austenitic stainless steel followed by Type 308L weld material for weld overlay cladding. The use of Alloy 600 and associated weld metals is prohibited, which reflects lessons learned from the in-service issues relating to PWSCC of these nickel based alloys under PWR conditions.

20B.3.1.4.2 **Material Specifications Meet or Exceed ASME Specifications**

Materials comply with the applicable requirements of the design and construction codes and standards of the ASME Code, Section III. The approved materials used for the PZR assembly are as identified in Table 20B-1.

To support this argument, a QA compliant certified material test report as per the ASME Code will be provided with shipment of the forgings. This will include the material test results and information on:

- Chemical analyses: heat and product
- Mechanical properties: tensile stress-strain, Charpy V-Notch, drop weight, nil-ductility transition temperature (T_{NDT}) and reference nil-ductility transition temperature (RT_{NDT})
- Heat treatments
- Information on archive/weldment material
- Sketches or drawings with dimensions
- A statement certifying that no weld repairs had been made (where applicable)
- Start-of-life inspection results

The following Supplementary Requirements of SA-508 apply.

- S1 Simulated PWHT of Mechanical Test Samples
- S2 UT Reference Block Calibration
- S3 Charpy Impact Transition Curve
- S4 Additional Charpy Data
- S9 Restrictive Chemistry
- S10 Alternative Fracture Toughness Requirements
- S15 Product Analysis

The attachment of the safe ends to vessel nozzle ends for the PZR use buttering. The weld metal for this buttering and the weld to join the safe end to the nozzle is one or more of the following ASME Section II Part C specifications:

- SFA-5.11 ENiCrFe-7 (Alloy 152).
- SFA-5.14 ERNiCrFe-7 (Alloy 52).
- SFA-5.14 ERNiCrFe-7A (Alloy 54 – chemical specification as for Alloy 52, but with Cobalt (0.12%), Boron (0.005% max) and Zirconium (0.02% max).

20B.3.1.4.3 **Tight Control on Chemical Composition is Specified**

The chemical composition of the PZR shell forgings is specified in the Material Specification for SA-508/SA-508 M Grade 3 Class 2 Forgings (Reference 20B.15). A supplementary ASME Code Section II requirement for SA-508 Grade 3 Class 2 material (S9 – Restrictive Chemistry) includes additional restrictions on chemical composition. These are listed below.

- Phosphorus will be 0.015% maximum for heat analysis and 0.018% maximum for product analysis; sulphur will be 0.005% maximum for heat analysis and product analysis; copper will be 0.15% maximum for heat and product analysis.

- Chromium content for heat and product analyses will be greater than 0.10%.

Samples for product analysis will be taken from material adjacent to each tensile specimen, or may be taken from the ends of broken tensile specimens. The certified material test report will identify, by location, which product analysis corresponds to which reported tensile test results.

If the steel is vacuum-carbon deoxidised, the silicon content will be 0.10% maximum both by heat and product analyses. The test report will indicate that the steel was vacuum-carbon deoxidised.

20B.3.1.4.4 **Materials are Compatible with Each Other and with the Environment and are Resistant to Environmental Degradation over the Life of the Plant. Degradation Characteristics are Known and Understood**

The materials selected for use in the PZR will be compatible with the full range of internal and external environmental conditions, which may be encountered over the plant life and are predicted not to degrade in that time. These environmental conditions include temperature, humidity, radiation, chemistry of fluid or materials in contact, and other external conditions which may affect the suitability of a material.

To prevent corrosion of low alloy steel component in contact with primary coolant, all principal pressure-retaining components made from such materials, including the PZR, have corrosion-resistant cladding on surfaces exposed to the reactor coolant. Clad surfaces will be "L" grade austenitic stainless steel and welds and buttering will be "L" grade austenitic stainless steel or Ni-Cr-Fe Alloy. The stainless steel cladding surfaces will meet all of the requirements of the Material Test Specification for Austenitic Stainless Steel Cladding (Reference 20B.16). For multiple layer stainless steel cladding, the stainless steel cladding will be Type 308L austenitic stainless steel weld metal with Type 309L austenitic stainless steel weld metal used for the first layer. The corrosion resistance of the cladding material is at least equivalent to the corrosion resistance of Types 304 and 316 austenitic stainless steel alloys or nickel-chromium-iron alloy, martensitic stainless steel, and precipitation-hardened stainless steel.

20B.3.1.4.5 **Nozzle and Safe-end Materials have been Optimised for Design and Fabrication**

The safety relief, surge temperature and instrumentation nozzles will all terminate in Type 316LN austenitic stainless steel material for compatibility with the interfacing piping material, thus avoiding the requirement for field transition welds. The spray nozzle terminates in UNS N06690 (Alloy 690) material. The safe ends will be of sufficient length to prevent damage to the transition weld on the nozzle during field welding.

The surge, safety relief, and spray ferric nozzle weld end preparations will be buttered prior to final PWHT. After final PWHT, the safe ends will be welded to the buttered nozzles.

The internal upper head spray nozzle region to which the spray nozzle nipple is welded will be first buttered and then stress relieved prior to welding the spray nozzle nipple.

The instrument and temperature nozzle weld build up pads on the inside vessel wall will be first made with SFA 5.4 or SFA 5.9 Type 309L (first layer only) followed by Type 308L weld material and then be stress relieved prior to welding these nozzles.

The heater sleeve weld buildup pads on the inside vessel wall will be stress relieved prior to welding the nozzles.

The use of Nickel alloy weld and buttering consumables reduces the thermal mis-match stresses in the nozzles.

20B.3.1.4.6 **Materials Testing is Sufficient to Demonstrate that the Material Properties are Compliant with the Relevant Specifications**

The materials testing requirements for each material are contained within the relevant material specifications as identified in the PZR Design Specification. For the PZR main forgings the mechanical property tests will consist of Tensile Tests, Drop Weight Tests and Charpy V-Notch Impact Tests. Test methods, location and orientation of specimens will be in accordance with ASME Code, Section III, Subsection NB-2000.

Tests will be performed at the upper and lower head forgings, upper, middle and lower shell forgings, trunnions, manway pads and forgings exceeding 454 kg (1,000 lbs.) (prior to quenching and tempering treatment) and small forgings not exceeding 454 kg (1,000 lbs.) (prior to quench and tempering treatment).

Subsequent to quenching and tempering, mechanical property test specimens will be given a simulated PWHT as follows; place coupons in a furnace at not over 425°C (800°F), heat at no more than 56°C/hr. (100°F/hr.) to the range 595°C-621°C (1,100°F-1,150°F) and hold for 48 hours, then cool at not more than 56°C/hr. (100°F/hr.) to below 425°C (800°F).

Sufficient drop weight tests will be run to determine the actual nil-ductility transition temperature (NDTT) or nil-ductility temperature for each forging. Specimens from two locations on a given forging may be intermixed to determine the NDTT. However, one specimen from each of the two locations will show no-break at the lowest no-break temperature used to define the NDTT. The NDTT will not be higher than -12.2°C (10°F). T_{NDT} as defined by ASME Code will be considered as the actual NDTT determined by drop weight tests.

Charpy V-Notch tests and drop weight fracture toughness tests are required. Orientation of test specimens will be per the ASME Code, Section III, Subsection NB-2000. For each test location the RT_{NDT} will not be higher than -12.2°C (10°F). Charpy V-Notch tests (sets of three specimens) will be performed for each location at a temperature not higher than the T_{NDT} temperature plus 33°C (60°F). Three sets of data are required for weld material and heat-affected-zone (Reference 20B.15). Additional data, if necessary, will be obtained by testing of production material for the shell or head and incorporated into this specification. The supplier is responsible for providing these data.

Supplementary fracture toughness testing, which is described in Reference 20B.39, will be performed to underpin the values assumed in the Reference 20B.27 and 20B.38 defect tolerance assessments.

20B.3.1.5 Good Manufacturing

In order to demonstrate that good manufacturing processes will be used, evidence to substantiate the following arguments is provided.

- PZR components will be manufactured by experienced suppliers with a track record for producing similar components.
- High confidence in PZR manufacturing quality can be taken from compliance with ASME III and the experience embodied within the code.
- Approved welding procedures and qualified operators are used to minimise defect occurrence.
- Repairs and deviations from the design intent will be recorded. Approval for deviations from the design intent will be appropriate with justification where necessary.
- Manufacturing and procedural controls ensure quality of forging material.
- Manufacturing records and procedures.
- Quality Assurance.

20B.3.1.5.1 Pressuriser Components will be Manufactured by Experienced Suppliers with a Track Record for Producing Similar Components

In selecting the manufacturer for the heavy pressure vessels, a detailed technical evaluation of the suppliers ability to comply with Reference 20B.1 and quality assurance requirements will be undertaken, giving particular attention to the suppliers ability with regard to achievement of the material compositional requirements including minimum fracture toughness requirements, the methods for the qualification of weld procedures and the ability to carry out the required range of inspections during manufacture. The evidence to support this argument forms part of a site specific justification by the utility company.

The PZR components will be joined by welding, using the single or multiple wire submerged arc and the shielded metal arc processes or other established techniques. Gas metal arc welding and plasma arc welding are acceptable methods of applying buttering for dissimilar metal welds. The use of severely sensitised stainless steel as a pressure boundary material is prohibited and is eliminated by either a select choice of material or by programming the method of assembly. At locations in the PZR where austenitic stainless steel and

nickel-chromium-iron alloy are joined, the final joining beads are nickel-chromium-iron alloy weld metal in order to prevent cracking. The location of full penetration weld seams in the upper closure head and vessel bottom head are restricted to areas that permit accessibility during ISI. The austenitic stainless steel clad surfaces are sampled to demonstrate that composition requirements are met.

20B.3.1.5.2 **High Confidence in Pressuriser Manufacturing Quality can be Taken from Compliance with ASME III and the Experience Embodied within the Code**

Design and fabrication of the PZR is carried out in accordance with ASME Code, Section III, Class 1 requirements and manufactured using well established procedures. Details of manufacturing codes and standards are provided in Reference 20B.1 with certain more stringent requirements defined in the AP1000 Supplemental Fabrication and Inspection Requirements (Reference 20B.17). Compliance with the code and the experience embodied within the code provides a high degree of confidence that high quality has been achieved and also that the vessel will be tolerant to minor variations in material properties and minor imperfections in fabrication.

20B.3.1.5.3 **Approved Welding Procedures and Qualified Operators are used to Minimise Defect Occurrence**

As detailed in Reference 20B.1, welding of all materials will be done in accordance with welding procedures, using certified welders who have been qualified according to the rules of Sections III and IX of the ASME Code as well as the additional requirements identified in Reference 20B.1 and the supplemental requirements detailed in Reference 20B.17. Control of welding variables (as well as examination and testing) during procedure qualification and production welding is performed according to ASME Code requirements. Specific details of welding processes, selection and control of welding consumables, welding procedure qualification, pre-heat, interpass temperatures and post heating requirements and specific control for cladding and buttering are provided in Reference 20B.17.

20B.3.1.5.4 **Repairs and Deviations from the Design Intent will be Recorded. Approval for Deviations from the Design Intent will be Appropriate with Justification where Necessary**

The requirement to record major/minor repairs and deviations from the design intent is stated within Reference 20B.1. Deviation reports or deviation notices will be prepared by the manufacturer for all conditions that do not meet requirements of the Design Specification, the ASME Code or Westinghouse-approved Supplier procedures and drawings and cannot be corrected using previously approved repair procedures. Deviations/defects that are identified during processing/fabrication, which will not affect the final fit-up/function (e.g., weld defects) of the final component and which may be repaired by previously approved repair procedures, will not need to be submitted for Westinghouse approval as a deviation notice. However, these will be recorded for future reference. The requirements placed on the manufacturer include the reporting criteria and the conditions under which formal review and approval by Westinghouse will be required. The following should be noted:

- All major repairs to base material and pressure boundary welds will be subjected to formal review by Westinghouse before approval to proceeding with the repair is granted.

- All arc strikes on pressure boundary and accessible non-pressure boundary materials will be removed and the areas grounded to a smooth contour with a 4:1 taper. Any arc strike

that exceeds a depth of 2.54 mm (0.10 inches) will be documented and reviewed by Westinghouse for approval.

- Repairs by welding will be cleared by the same NDE technique/procedure by which the indications were found.

- The location of these repairs will be identified on the as-built weld seam drawing for permanent record and may be required to be permanently marked on the vessel or head when so indicated in the deviation notice disposition.

20B.3.1.5.5 **Manufacturing and Procedural Controls Ensure Quality of Forging Material**

The PZR upper, middle and lower shells, upper and lower heads and nozzles will be manufactured from high quality forgings supplied by an experienced forge master, working to approved procedures to meet relevant product specifications, which are compliant with ASME Code requirements. Individual material specifications for SA-508 Grade 3 Class 2 forgings and stainless steel forgings are provided in the relevant material specifications as listed in the technical index. These provide specific details of controls on chemical composition, microstructures, heat treatment, materials testing, grain size evaluation and ultrasonic examination to ensure that the final product has the desired through thickness properties and is free from unacceptable forging defects.

20B.3.1.5.6 **Manufacturing Records and Procedures**

To ensure that there is a high degree of control over the achievement of high quality during manufacture, the following controls on the manufacturing records and procedures are specified as part of the component design specification.

Weld Procedures

To ensure that weld procedures are acceptable, all procedures for weld and weld repair and base metal repair will be approved prior to use in fabrication.

All welding procedure specifications to be used in the fabrication of the PZR will be prepared in accordance with a general welding procedure specification and the requirements of Section III of the ASME Code.

Heat Treatment

Heat treatment specifications will be approved prior to manufacture and will include the following (where applicable).

- Holding times for austenitising and tempering
- Rates of heating
- Temperature control
- Temperatures for the austenitising and tempering operations during heating/holding
- Time from the furnace to the quench tank
- Quenching medium
- Cooling method

Material Records

All material ordering specifications (including heat treatment and base metal repair procedures) will be approved prior to material procurement. This includes all welding consumables. Each chemical analysis including both ladle and check, physical and mechanical mill test data sheets, supplier test data sheets, weld material certifications, and inspection reports for materials required by the Design Specification and applicable references will also be provided. The certified chemical and mechanical properties of the weld metal used for full penetration pressure boundary welds in the vessel will be provided, any weld repairs to these welds, and all base metal weld repairs.

Manufacturing Inspections

Each NDE examination report will be made available to Westinghouse for review after the completion of each examination. Defects will be recorded and defect tolerance studies will be carried out by Westinghouse to ensure that recorded indications do not present a concern over the design life of the plant.

Dimensional Checks

The dimensional profile document will be used to record vessel as-built dimensions to demonstrate that the as-built dimensions satisfy the design specification.

Cleaning and Contamination Protection Procedures

Materials used in the fabrication, installation, and testing of nuclear steam supply components and systems are handled, protected, stored, and cleaned according to recognised, accepted methods designed to minimise contamination that could lead to cracking.

20B.3.1.5.7 **Quality Assurance**

Activities affecting the quality of items and services for the AP1000 project during design, procurement, fabrication, inspection, and/or testing are performed in accordance with the quality plan described in the Westinghouse Electric Company Quality Management System, (Reference 20B.18) to satisfy the requirements of 10 CFR 50 Appendix B. The following requirements are identified in Reference 20B.1.

The reliability of the equipment identified in the design specification is dependent upon the design, together with the control of quality during fabrication of the equipment. The quality will be in accordance with the following requirements (Reference 20B.1):

- US Nuclear Regulatory Commission, Regulatory Guide 1.28, "Quality Assurance Program Requirements (Design and Construction)," Revision 3, August 1985.
- This item/service is nuclear safety-related; 10 CFR 21 "Reporting of Defects and Noncompliance" applies.
- 10 CFR 50 Appendix B – "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants."
- ASME NQA-1-1994, "Quality Assurance Requirements for Nuclear Facility Applications" applies.

- ASME Code, Section III, "Rules for Construction of Nuclear Power Plant Components," 1998 Edition with addenda up through and including 2000.

20B.3.1.6 Manufacturing Inspection

Materials and fabrication processes are well designed in order to demonstrate that the AP1000 PZR enters service free of significant defects, which will be confirmed by an effective manufacturing 20B-24 non-destructive testing (NDT) inspection programme. Evidence to substantiate the following arguments is provided.

- Manufacturing inspections meet or exceed the requirements of ASME.
- Reliability of NDT is assured through a "Design for Inspection" philosophy.
- NDT performed at key stages of manufacture assures the high quality of the completed PZR and its components.
- Qualified inspection performed on HSS components demonstrates a good safety margin.
- Qualified inspection of HSS components confirms the plant is free of defects meeting ASME Section XI criteria.

20B.3.1.6.1 Manufacturing Inspections Meet or Exceed the Requirements of ASME

A diverse range of effective NDT methods and techniques are deployed at various manufacturing stages to ensure that steel forgings, plate, welds and cladding in the PZR enter service free of significant manufacturing defects. The scope of the manufacturing NDT and the techniques applied either meet or exceed the requirements of ASME Section III, as summarised in Table 20B-17.

All repairs made as a result of NDT findings are subsequently inspected using the same NDT method(s) that originally detected the defect leading to the repair.

20B.3.1.6.2 Reliability of Nondestructive Testing is Assured through a "Design for Inspection" Philosophy

The AP1000 incorporates a "Design for Inspectability" philosophy, as detailed in the AP1000 Design for Inspectability Program: ISI Requirements for Class 1 Components (Reference 20B.19), in which the PZR welds and surrounding areas are designed to facilitate NDT by:

- Ensuring a good surface finish for deploying the range of techniques.
- Enabling good access for NDT personnel and equipment.
- Providing sufficient access for deploying angle beam ultrasonic testing to give full volumetric coverage.
- Providing as many inspection surfaces/scanning directions as possible.

20B.3.1.6.3 **Nondestructive Testing is Performed at Key Stages of Manufacture Assures the High Quality of the Completed Pressuriser and its Components**

Experience shows that materials and manufacturing processes similar to those chosen for the AP1000 lead to a low frequency of defect occurrence. However, sensitive volumetric and surface NDT methods are applied at points in the manufacturing programme that ensure any necessary repairs are undertaken at the earliest possible stage.

Inspections are carried out at various stages of manufacture, at increments during weld fill and following completion of major welds, to identify any degradation resulting from processes such as PWHT and hydrotest.

20B.3.1.6.4 **Qualified Inspection Performed on Highest Safety Significant Components Demonstrates a Good Safety Margin**

Qualified ultrasonic volumetric inspections are performed on HSS locations, identified in Section 20B.2.2, after the final post-weld heat treatment to provide a very high level of confidence that the PZR enters service free of any defect that could threaten the structural integrity. Target sizes for manufacturing defects for HSS welds have been established from elastic-plastic fracture mechanics by calculating the end-of-life limiting defect sizes and fatigue crack growth in accordance with the R6 methodology. Inspection of non-HSS welds in the PZR will be qualified in accordance with the requirements of ASME V. A procedure for the manufacturing NDT qualification process has been outlined and this will form the basis for the qualification procedure.

For HSS welds, NDT will be performed using currently available tried and tested ultrasonic techniques and will be shown to provide a detect and reject capability that demonstrates a defect size margin (DSM) of 2 or greater. The basis for this is discussed in Section 20B.3.3.1. High reliability for these inspections will be demonstrated through qualifying the inspection system (procedure, equipment, and personnel) using the principles specified in the European Network for Inspection and Qualification (ENIQ) document, European Methodology for Qualification of Non-Destructive Testing, (Reference 20B.20). For selected HSS welds, a manufacturing inspection plan has been produced which provides the physical reasoning underpinning the claimed inspection capability. Details of manufacturing inspection plans for the selected PZR welds are discussed in Section 20B.3.3.1.3. The manufacturing inspection plans were developed following a process (Reference 20B.37) which is based on the preparation of technical justifications described in ENIQ methodology. A process will be developed in due course to address parent material associated with HSS locations.

A rigorous approach to classification based on failure modes and consequences has identified the following pressure boundary welds as HSS (as identified in Table 20B-5).

1. PZR Vessel Shell Welds (Locations 1.1, 1.2, 1.3, 1.4, 1.5)
2. PZR Nozzle Welds (Locations 2.1, 2.2, 2.3, 2.4, 2.5)
3. PZR Vessel Shell Forgings (Locations 3.1, 3.2, 3.3)

20B.3.1.6.5 Qualified Inspection of Highest Safety Significant Components Confirms the Plant is Free of Defects Meeting ASME Section XI Criteria

The final stage of NDT for HSS welds is the application of qualified mechanised ultrasonic inspection systems to confirm the welds are free of any defects that exceed the specified acceptance criteria. These inspections have two purposes:

- They provide additional high reliability inspections at the end of all manufacturing stages.
- They generate a "fingerprint" set of data against which future ISI results can be compared. By establishing that acceptable indications found during ISI were also present at PSI fabrication, potential unnecessary repairs are avoided.

Supplemental inspections, additional to those specified by ASME Section III, are performed that match the PSI and ISI acceptance criteria of ASME Section XI. Here the objective is to reconcile the difference in acceptance standards between ASME III and ASME XI and ensure that the PSI does not report rejectable defects that were not identified as such during the standard manufacturing NDT (Reference 20B.1).

20B.3.1.7 Plant Operation and Maintenance

In order to demonstrate that the plant will be properly operated and maintained, evidence to support the following arguments is provided.

- The AP1000 RCS chemistry specification is clearly defined and measures are in place to control corrosion.
- Records of operation and maintenance will be maintained to confirm compliance with procedural requirements.
- Incidents involving transgressions of set limits will be investigated.
- Procedures are in place to control maintenance activities.
- ISI will detect defects before they compromise structural integrity.

In order for the operators to safely operate and maintain the AP1000, operating and maintenance manuals that are fully compliant with the technical specifications will be produced by the utility companies. Regarding the PZR, the following issues are considered the most pertinent at this stage in terms of providing assurances that the plant will be properly operated and maintained in such that through-life degradation is minimised.

20B.3.1.7.1 **The AP1000 Reactor Coolant System Chemistry Specification is Clearly Defined and Measures are in Place to Control Corrosion**

The RCS chemistry specifications, the control of chemistry, and the compatibility of primary coolant boundary materials with the RCS chemistry are detailed in section 21.5.5. In summary, the RCS water chemistry is selected to minimise corrosion and routinely scheduled analyses of the coolant chemical composition are performed to verify that the reactor coolant chemistry continues to meet the specifications. Other additions, such as those to reduce activity transport and deposition, may be added to the system. The RCS chemistry specifications conform to the recommendation of Regulatory Guide 1.44 (Reference 20B.35).

The CVS provides a means for adding chemicals to the RCS. The chemicals perform the following functions:

- Control the pH of the coolant during pre-start-up testing and subsequent operation.
- Scavenge oxygen from the coolant during heatup.
- Control radiolysis reactions involving hydrogen, oxygen, and nitrogen during power operations following start-up.

The values presented in Table 20A-3 are bounding for chemistry operational control of primary fluids that are in contact with primary system materials and nuclear fuel. The operational chemistry program may apply stricter limits as deemed appropriate.

20B.3.1.7.2 **Records of Operation and Maintenance will be Maintained to Confirm Compliance with Procedural Requirements**

Details of the quality assurance requirements during the operational phase are discussed in Section 3.4, and will be considered as part of the Site Specific Justification.

20B.3.1.7.3 **Incidents Involving Transgressions of Set Limits will be Investigated**

Operating limits for the UK AP1000 plant are specified within the generic technical specifications (Reference 20B.32). Limiting conditions for operation (LCOs) specify minimum requirements for ensuring safe operation of the plant. The following LCOs are relevant to the pressure/temperature (P/T) limits.

- LCO 3.4.3, “RCS pressure and temperature (P/T) Limits”
- LCO 3.4.14, “Low temperature overpressure protection (LTOP) System”
- LCO 3.4.2, “RCS Minimum Temperature for Criticality”

The consequence of violating the LCO limits is that the RCS has been operated under conditions that can result in brittle failure of the reactor coolant pressure boundary (RCPB), possibly leading to a non-isolable leak or LOCA. In the event these limits are exceeded, an evaluation must be performed to determine the effect on the structural integrity of the RCPB components. ASME Code, Section XI, Appendix E (Reference 20B.21) provides a recommended methodology for evaluating an operating event that causes an excursion outside the limits.

20B.3.1.7.4 **Procedures are in Place to Control Maintenance Activities**

As specified in Reference 20B.1, the PZR Instruction manual, provided by Westinghouse, will contain detailed instructions for the maintenance and repair of the PZR equipment. This will need to be developed further as part of the site specific safety case.

20B.3.2 **Leg 2: Functional Testing**

The objective of the functional testing leg of the safety case is to confirm that the good standards applied in PZR design, fabrication and installation identified in Section 20B.3.1 result in an installed component that is fit for purpose. Hydrostatic pressure tests are conducted to verify that the PZR is proofed against its design pressure, and similar tests are periodically carried out to affirm that reactor coolant pressure boundary integrity will be maintained at the design pressure throughout the component lifetime. Two elements are built up to support this claim. These are:

- The PZR is subject to Proof Testing.
- Testing is carried out to confirm PZR functionality.

These provide evidence that functional testing of the PZR will be conducted to ensure fitness for purpose at start of life (SoL) and continued integrity of the pressure boundary for the design life.

20B.3.2.1 The Pressuriser is Subject to Proof Testing

In order to demonstrate that the PZR will be subject to proof testing, evidence to support the following arguments is provided.

- The PZR is subject to hydrostatic pressure testing to verify pressure boundary integrity at design pressure prior to operation.

- Testing is carried out to confirm PZR functionality.

20B.3.2.1.1 **The Pressuriser is Subject to Hydrostatic Pressure Testing to Verify Pressure Boundary Integrity at Design Pressure Prior to Operation**

The hydrostatic pressure test contributes to the safety case in a number of ways but principally it provides assurance regarding the basic strength of the assembled vessel, the absence of gross manufacturing defects and evidence of out of specification material properties. It is recognised that the hydrostatic pressure test provides less strength to the safety case at locations where defect tolerance may be dominated by thermal stresses. At such locations, assurance is provided by inspection to confirm the absence of structurally significant defects supported by defect tolerance assessments.

Details of the PZR hydrostatic pressure testing requirements are specified in Section 7.1.1 of the AP1000 PZR Fabrication Specification (Reference 20B.22). The PZR will be hydrostatically tested in accordance with the ASME Code, Section III, Class 1 requirements.

A hydrostatic test will be performed at elevated pressure and a test temperature established by the Supplier. A hydrostatic test will be performed at a temperature not lower than RT_{NDT} plus 33°C (60°F), in accordance with ASME Section III, G-2400. The vessel will be capable of a subsequent field hydrostatic test as deemed necessary.

Reference 20B.22 describes NDEs which are required following the vessel hydrostatic test. These include magnetic particle testing (MT), visual and dimensional, liquid penetrant, ultrasonic and radiographic examinations.

As specified in Table 20-22, the RCS is conservatively designed for 10 cycles of hydrostatic pressure tests throughout the design lifetime of 60 years. Each RCS hydrostatic test is conducted at a water temperature compatible with reactor material ductility requirements.

20B.3.2.1.2 **Testing is Carried out to Confirm Pressuriser Functionality**

Section 7.5 describes a commissioning programme for AP1000 plant. The overall objective of the programme is to demonstrate that the plant has been constructed as designed, that systems perform consistent with the plant design, and that activities culminating in operation at full licensed power including initial fuel load, initial criticality, and power ascension are performed in a controlled and safe manner.

Pre-operational tests for all systems with safety related functions are specified to confirm that these functions will be maintained in operation. Pre-operational testing [2] of the RCS is specified in section 7.5.6. Prerequisites to the pre-operational testing are identified; these include completion of the hydrostatic proof testing of the PZR as described in section 20B.3.2.1.

Pre-operational testing of the RCS including the PZR is conducted to verify that the as-installed RCS will fulfil the following functions:

- Provide RCS pressure boundary integrity.
- Provide core cooling and boration in conjunction with the PXS.
- Measure process parameters required for safety-related actuations and safe shutdown.
- Measure selected process parameters required for post-accident monitoring.
- Vent the RV head.

Pre-operational testing of the RCS is also performed to verify that the system fulfils the following defence in depth functions:

- Provide forced circulation cooling of the reactor core in conjunction with heat removal by the SG(s).

- Provide core cooling by natural circulation of coolant in conjunction with heat removal by the SG(s).

- In conjunction with the SG(s) and the normal residual heat removal system, provide the capability to remove core decay heat and cool the reactor coolant to permit the reactor to be refuelled and started up in a controlled manner.

- Provide PZR pressure control during normal operation.

2. N.b. Pre-operational tests at elevated pressure and temperature are referred to as hot functional tests.

- Provide PZR level control in conjunction with the CVS.
- Provide PZR spray.

Pre-operational testing includes measures to confirm the integrity and leak tightness of the RCS and the high-pressure portions associated systems. The PZR is included within the scope of these tests. Structural integrity is verified by performing a cold hydrostatic pressure test in conformance with Section III of the ASME Code. Leakage monitoring during hot functional testing is conducted to confirm that any RCS leakage is within limits specified in the Technical Specifications.

A series of start-up test procedures are specified in Section 7.5. The start-up test procedures are to confirm safe and controlled operation during activities culminating in operation at full licensed power. As is the case for pre-operational testing, these start-up tests are applicable to systems rather than individual components such as the PZR.

20B.3.3 Leg 3: Failure Analysis

Leg 3 of the safety case provides an assessment of the effects of through-life degradation mechanisms on potential manufacturing defects to show that such mechanisms will not threaten vessel integrity over the plant design lifetime. This goes beyond design code requirements to provide a further demonstration of integrity, specifically by recognising that flaws may be present following manufacture and showing tolerance to them. The arguments supplement the Leg 1 aim of avoidance of defects to provide a safety case with both defect avoidance and defect tolerance.

20B.3.3.1 Pressuriser Components are Tolerant to Manufacturing Defects for the Design Life of the Plant

This section describes the scope of the analyses undertaken as part of the generic design assessment (GDA) process to demonstrate that the PZR is tolerant to potential defects that could remain undetected after manufacturing inspection. In order to demonstrate that the AP1000 PZR and its components are defect tolerant, evidence to support the following arguments is provided.

- Established methods are used to evaluate defect tolerance.
- The determination of crack growth rates and through-life crack sizes is conservative.
- Demonstration of adequate margins between allowable SoL defect sizes and defect sizes based on suitably qualified inspections.

20B.3.3.1.1 Established Methods are used to Evaluate Defect Tolerance

As discussed in section 20.6.4.2, the following sections describe the results of the R6 assessment for the PZR and present a summary of the existing LEFM assessment carried out in accordance with ASME Code, Section III, Appendix G.

Assessment using the R6 Methodology

In combination with the use of rigorous manufacturing controls and inspection qualification, the defect tolerance assessment provides the necessary understanding to support the claim, to an appropriate degree of confidence, that the vessel will enter service free from defects that

could be of concern at the throughout the PZR's designed life. The approach to determination of the limiting defect size in a particular orientation and location and the maximum allowable SoL defect size is discussed in section 20.6.4.2. As has been stated in Reference 20B.14 the regulatory expectation is that a defect size margin of 2 will be achieved.

Phase 1: Weld Defect Tolerance and NDE Ranking

A detailed evaluation of selected, limiting weld locations has been made available to provide confidence that there are no regions of the PZR where either low defect tolerance or low NDT inspectability would preclude the PZR design from being able to satisfy regulatory expectations and support the safety case claim for the PZR. To evaluate which locations present the greatest risk of entering service with a defect of structural significance, a ranking exercise was undertaken to consider, on a relative basis, the defect tolerance and the NDT inspectability at each of the PZR weld locations. The details of this evaluation and the rationale behind the selection of the limiting locations are reported in the results of weld ranking process (References 20B.24 and 20B.25). The final selection of the locations for R6 assessment are listed in Table 20B-19 of this report and summarised below.

a) Upper head to upper shell weld
b) Upper shell to middle shell weld
c) Manway to shell weld
d) Surge nozzle to safe end-weld

Phase 2: Assessment of Bounding Locations

Table 20B-19 details the locations selected for detailed evaluation during the GDA. The scope of the locations that were directly assessed, or have been shown to be bounded by other locations is indicated in Table 20B-19. For each of the selected locations, the R6 defect assessment methodology has been used to determine the limiting SoL defect size. Details of the assessment methodology are provided in Reference 20B.26. The results of this analysis for the pressuriser are presented in References 20B.27 and 20B.38 and are discussed in Section 20B3.3.1.1.

Phase 3: Assessment of Remaining Locations

The full defect tolerance assessment of the remaining HSS locations, including the selected locations in the parent material, will be carried out in due course. Once completed, the R6 assessment work for the PZR will provide assurance that the qualified examination defect size (QEDS) is based on a robust assessment of the maximum allowable SoL defect size with appropriate consideration of materials ageing and degradation and through life crack growth.

ASME Code, Section III, Appendix G Linear-Elastic Fracture Mechanics Assessment

The results of the ASME Code, Section III, Appendix G fracture assessment are described in Reference 20B.13. The procedure assumes a postulated defect having a depth of one-quarter of the section thickness (with a minimum value of 25.4 mm (1 in) and a length-to-depth ratio of 6.0. For the Service Level A and B and Test conditions, the calculated crack tip stress intensity must be less than the value of K_{IR}. K_{IR} is the reference stress intensity factor. For the Service Level C and D conditions, the calculated crack tip stress intensity must be less than the value of K_{IC}. K_{IC} is applied as an allowable fracture toughness and is the lower bound static initiation critical crack tip stress intensity. It is given in Section XI of the ASME Boiler and Pressure Vessel Code (Reference 20B.21). For limiting locations where the assumed quarter thickness flaw produces a stress intensity factor K_I greater than the reference or

allowable fracture toughness, the methods of WRCB-175 (Reference 20B.33) are used to determine the critical crack size.

20B.3.3.1.2 **The Determination of Crack Growth Rates and Through-life Crack Sizes is Conservative**

As part of the R6 assessment the through life crack growth has been calculated for selected locations in accordance with the R6 procedure. This includes the use of suitably conservative crack growth rates appropriate to the reactor coolant environment. As discussed in Reference 20B.26, these are based on the ASME upper bound FCG curves. These are considered to be conservative for modern steels with low sulphur content. The upper bound nature of these curves is supported by extensive testing worldwide.

20B.3.3.1.3 **Demonstration of Adequate Margins between Allowable Start of Life Defect Sizes and Defect Sizes Based on Suitably Qualified Inspections**

The results of the R6 defect tolerance assessments for three of the four PZR welds identified in Section 20B.3.3.1.1 are reported in Reference 20B.27. The results of the R6 defect tolerance assessment for the fourth PZR weld are reported in Reference 20B.38. A limiting QEDS, i.e., that leading to a DSM equal or larger than 2, has been calculated for one of two different defect aspect ratios according to flaw orientation. For flaws perpendicular to the weld axis, the QEDS is established for a defect aspect ratio of 2, since the potential length of flaws with that orientation is naturally limited by the weld width. For flaws oriented parallel to the weld axis, it is recognised that flaws with higher aspect ratios may potentially occur, and a defect aspect ratio of 6 is additionally considered in determining the QEDS. In addition to those used to calculate the limiting QEDS, an aspect ratio of 10 is also considered to demonstrate that “cliff-edge” effects do not occur.

Reference 20B.27 reports the calculated limiting QEDS (i.e., leading to a DSM equal or larger than 2) for select PZR welds as follows:

Weld	Limiting QEDS (mm)
Upper head to upper shell weld	11.5
Upper shell to middle shell weld	12.8
Manway to shell weld	10

Reference 20B.38 reports the calculated limiting QEDS (i.e., leading to a DSM equal or larger than 2) for the PZR surge nozzle to safe end weld as follows:

Weld	Limiting QEDS (mm)
Surge nozzle to safe end-weld	5

Based on these QEDS values, References 20B.27 and 20B.38 report that the calculated values of end of life limiting defect size (ELLDS) and lifetime fatigue crack growth (LFCG)

establish a DSM larger than 2 in all cases for the welds covered by each document. The demonstration of the capability for qualified inspection of these pressuriser welds is summarised below.

Reference 20B.30 provides the technical basis for an array of inspection techniques applied on the PZR outer surface at the upper head to upper shell weld, upper shell to middle shell weld and manway to shell weld to support detection and characterisation of surface-breaking and near-surface breaking planar defects having a height of 10 mm (0.39 in), and embedded planar defects of 20 mm (0.79 in). This basis included previous works associated with the Sizewell B qualified manufacturing NDT inspections, the United Kingdom Atomic Energy Authority defect detection trials (DDT), qualified inspections used in the US, and common industry approaches. This technical basis was reviewed by an independent qualification body (inspection validation centre (IVC)) and the inspection techniques were deemed to be capable of formal qualification.

Reference 20B.31 provides the technical basis for an array of inspection techniques applied on the surge nozzle/safe end inner diameter, outside diameter, and end face surfaces to support detection and characterisation of both surface-breaking and near-surface breaking planar defects having a height of 5 mm (0.20 in). This basis included previous works associated with the Sizewell B manufacturing NDT inspections, qualified inspections used in Sweden and the US, and common industry approaches. This technical basis was reviewed by an IVC and the inspection techniques were deemed to be capable of formal qualification.

Taken together with the QEDS discussed above, the results of the analyses provide assurance that there is a very low probability that the PZR will enter service containing defects that could challenge integrity over the lifetime of the component.

20B.3.4 Leg 4: Forewarning of Failure

The objective of the forewarning of failure leg of the safety case is to confirm the absence of a degradation mechanism through plant inspection or that, where a known degradation mechanism exists, uncertainty in the material behaviour is not significant to integrity or will have limited consequences. Three elements are built up to support this claim. These are:

- Appropriate ISI is carried out to provide forewarning of failure.
- Diverse systems are provided to detect, locate and monitor reactor coolant leakage from the PZR.
- In-service material surveillance provides forewarning of unanticipated degradation.
- The arguments presented provide contingency for the unexpected.

20B.3.4.1 Appropriate In-Service Inspection is Carried Out to Provide Forewarning of Failure

In order to provide assurances that defects will be detected prior to becoming a threat to the structural integrity of the AP1000 PZR, evidence to substantiate the following arguments is provided.

- An extensive programme of ISI identifies any degradation long before failure.
- Qualified inspection of HSS welds provides very high reliability ISI.

- ISI data enables judgment of in-service defect formation and growth by comparison with 'finger-print' PSI data.

- A 'Design for Inspectability' philosophy facilitates effective ISI.

20B.3.4.1.1 **An Extensive Programme of In-service Inspection Identifies any Degradation Long Before Failure**

ISI is the preferred method of demonstrating forewarning of failure. The role of an effective ISI programme is to confirm the absence of any unknown degradation mechanisms and that known degradation mechanisms are not significant to integrity.

ISI is used to confirm the absence of defects that could eventually lead to failure when the maximum tolerable defect size, as determined from fracture mechanics in Section 20B.3.3, is combined with a conservative assessment of in-service defect growth throughout the inspection interval.

In order to be effective, ISI requirements should be identified according to established good practice relevant to the characteristics of each inspection location. Evidence to substantiate this for planned PZR ISI is provided below, noting that the final ISI requirements are to be specified the operating utility company.

The anticipated ISI programme includes the PZR components and welds of importance to nuclear safety. ISI for the following welds and components of the PZR are identified in the AP1000 Component ISI Inspectability Assessment: Pressurizer (Reference 20B.28).

- Lower Shell to Lower Head Circumferential Weld
- Upper Shell to Upper Head Circumferential Weld
- Surge Nozzle Inside Radius Section
- Safety Relief Nozzle Inside Radius Section
- Spray Nozzle Inside Radius Section
- Surge Nozzle to Safe End Butt Weld
- Spray Nozzle to Safe End Butt Weld
- Safety/Relief Nozzle to Safe End Weld
- Studs and Nuts
- Welded Attachments (Support Bracket Pairs)
- Pressure Retaining Boundary

Reference 20B.28 identifies Code requirements for each of the above locations and takes into account the relevant code cases as approved by NRC. Inspection methods and access arrangements are described to ensure effective ISI at each of the identified PZR welds and components.

20B.3.4.1.2 **Qualified Inspection of Highest Safety Significant Welds Provides Very High Reliability In-service Inspection**

Section 20B.2.2 identifies the Structural Integrity Classification for the PZR components. For those components identified as HSS, it is accepted good practice that qualified inspections are deployed as supporting evidence to demonstrate that there are no defects of concern in HSS components.

The reliability of the ISI for HSS welds in the PZR is to be qualified by applying the principles of the ENIQ Methodology as contained in Reference 20B.20.

Adherence to the ENIQ Inspection Qualification methodology provides evidence of good practice for ISI of HSS locations. Reference 20B.20 identifies how inspection requirements and performance objectives are laid down in an inspection specification and provides a method for Inspection Qualification based on technical justification of the inspection method and practical trials on simplified or representative test pieces resembling the component to be inspected.

20B.3.4.1.3 **In-service Inspection Provides Data to Judge In-service Defect Formation and Growth by Comparison with 'Finger-print' Pre-service Inspection Data**

In Section 20B.3.1.6 qualified PSI of HSS components is described. The resulting data constitutes a "fingerprint" against which ISI results can be compared. Comparison of ISI data with the PSI finger-print is used to confirm the absence of significant degradation or that build defects are stable i.e., defects detected during ISI must have started life as no greater than the PSI validation defect size. PSI will be performed using the same equipment that is likely to be used for the periodic ISI.

20B.3.4.1.4 **A 'Design for Inspectability' Philosophy Facilitates Effective In-service Inspection**

For effective ISI, the PZR Design Specification includes the requirement to accommodate inspection equipment and personnel access in accordance with current inspection technology and strategies. Reference 20B.19 describes how the PZR design has been developed with the goal of maximising inspectability.

The AP1000 PZR design accommodates current best-practice ISI techniques and, so far as is practicable, allows for newly emergent inspection technologies to be employed. Reference 20B.19 provides a summary of ISI requirements for each location of the PZR. Design for Inspectability is demonstrated by consideration of the following aspects:

- Access for personnel and equipment conducting either manually deployed or mechanically deployed techniques.

- Surface finish requirements.

Reference 20B.19 establishes that provisions for inspectability are consistent with current best practice. An assessment is provided to demonstrate that design and access arrangements are provided to satisfy the requirements set out in NCA-3200 of the ASME Code, Section III, IWA-1400 and IWA-1500 of the ASME Code, Section XI and 10CFR50.55a. The following issues are identified in Reference 20B.19 that will be addressed to ensure that the AP1000 PZR satisfies the "Design for Inspectability" philosophy (Reference 20B.19) and the assessment defined in Reference 20B.28. These include:

- Recording as-built information
- Surface conditions and flatness specifications
- Nozzle blend radii
- Minimum safe-end length
- Qualification of PSI

20B.3.4.2 Diverse Systems are Provided to Detect, Locate and Monitor Reactor Coolant Leakage from the Pressuriser

In order to demonstrate that leaks from the reactor coolant pressure boundary will be detected before they result in a safety issue, evidence to substantiate the following argument is provided.

- Leak detection of the QEDS provides warning of reactor coolant leakage from the PZR.

20B.3.4.2.1 Leak Detection of the Reactor Coolant Pressure Boundary Provides Warning of Reactor Coolant Leakage from the Pressuriser

ISI represents the preferred method of demonstrating forewarning of failure and the primary element of Section 20B.3.4. Whilst leak detection and monitoring provide forewarning of failure, this safety argument does not seek to establish a quantitative case for excluding the gross failure of the PZR as a result of this forewarning. The leak detection measures described in section 20.6.4.3.2 are provided as qualitative evidence of defence in depth in support of this leg of the safety argument. Leak detection provides warning of unforeseen or unexpected loss of coolant from the PZR, and monitoring provides a means to confirm that any leakage of the coolant is kept within the limits specified in the generic technical specifications (Reference 20B.32).

Temperature is sensed downstream of each PZR safety relief valve and each ADS valve mounted on the PZR by a resistance temperature detector on the discharge piping just downstream of each globe valve. High temperature indications (alarms in the main control room) identify a reduction of coolant inventory as a result of seat leakage through one of the valves. These detectors are part of the RCS. This leakage is drained to the reactor coolant drain tank during normal plant operation and vented to containment atmosphere or the in-containment refuelling water storage tank during accident conditions. This identified leakage is measured by the change in level of the reactor coolant drain tank.

The primary sampling system takes suction from the PZR liquid space for chemistry control purposes. A flow restrictor is incorporated into the nozzle for this line, demarking the RCPB. A normally closed, fail closed isolation valve is provided in the primary sampling system (PSS) suction line inside containment in addition to the two normally closed containment isolation valves in series. Leakage from this connection would be measured by the change in level of the reactor coolant drain tank as unidentified leakage.

The connections on the PZR safety valves are flanged. During normal operation, variations in airborne radioactivity, containment pressure, temperature, or specific humidity above the normal level, or increases in containment sump level signify a possible increase in unidentified leakage and alert the plant operators that corrective action may be required. Unidentified leakage through the remaining jurisdictional boundaries of the PZR forming part of the RCPB is detected by the diverse methods described in section 20.6.4.3.2.

20B.4 Strength of the Safety Case

The availability and reliability of the safety measures identified to deliver a component's SFRs should demonstrably be commensurate with the significance of the radiological hazards to be controlled. This is achieved by a process of component structural integrity classification, which, for the safety justification of each class of component, establishes the degree of rigour to be applied commensurate with the potential radiological consequences of any postulated gross failure mode.

The process of structural integrity classification is detailed in Reference 20B.4, where gross failure of the PZR is assessed to potentially lead to the most severe and therefore intolerable offsite consequences against which there is no claimed protection. As identified in Section 20B.2.2, the PZR is classified as a HSS component[3]. HSS classification necessitates substantiation of a tolerable failure frequency where the probability of gross structural failure of the PZR is so low it can be discounted.

To substantiate the claim that gross structural failure of the PZR can be discounted, a safety argument is presented in Section 20B.2. Various elements of sound engineering practice are identified, which provide evidence that there is defence in depth against structural failure within the PZR arrangement and design. A defence in depth justification usually involves the provision of multiple layers of protection and defence is provided through diversity, redundancy and segregation to provide a robust design. For single components without multiple protection layers, the defence in depth principle is retained by demonstrating that the likelihood of failure is so low that it can be considered as not credible. The safety argument comprises four conceptually different legs, within each of which multiple subordinate arguments are supported by diverse sources of substantiating evidence. Robustness is achieved by considering the combined contribution from the four legs, a philosophy generally known as conceptual defence in depth. In combination the four legs provide sufficient confidence that gross failure of the PZR with unacceptable consequences will not occur during normal operation, during design basis transients or during fault conditions. The combined strength of the claims, arguments and evidence is discussed below.

The safety argument is founded upon a high standard of manufacture sufficient to achieve an appropriately high level of structural integrity. Design and fabrication of the PZR is to be in accordance with ASME Code, Section III, Class 1 requirements as a minimum. Supplemental requirements are identified that enhance the quality of PZR design and fabrication beyond ASME Class 1 standards. These are detailed in Section 20B.3.1, where multiple arguments and supporting evidence to substantiate achievement of PZR integrity are presented. Section 20B.3.1 includes claims, arguments and evidence to address the following aspects:

- The design is well founded and in accordance with internationally recognised standards. Design of PWR PZR vessels is long established and Westinghouse has an established track record. The AP1000 PZR benefits from this historical experience which is embodied in the codes and standards applied in design and fabrication.

- Procurement of materials is specified and controlled to ensure that well proven materials are chosen, that the materials have good resistance to fracture and other through-life degradation mechanisms. AP1000 PZR materials comply with the corresponding material specification permitted by the ASME Code, Section III, Division 1. For certain PZR materials, supplementary requirements are specified, which exceed the requirements specified in ASME code. Material testing is specified to confirm that material properties comply with the relevant specifications.

- Very high standards have been specified to control PZR fabrication. PZR components will be manufactured by experienced suppliers and evidence to confirm the suitability of the chosen manufacturer will form part of the Site Specific Justification. Compliance with ASME III and the experience embodied within the code provides high confidence in manufacturing quality. Supplemental requirements have been identified, which

3. The HSS classification does not apply to every component of the PZR or to every postulated failure mode and defect orientation, since certain failure modes will not lead to the most severe off site consequences. Classification of each component of the PZR is detailed in Section 20B.2.2.

enhance the standards applied in fabrication beyond ASME requirements. Approved welding procedures and qualified operators are used. Stringent Quality Assurance arrangements control manufacturing procedures and records are maintained to provide a clear auditable trail that will confirm this. There are procedural controls to limit deviations from the design intent and all repairs and deviations will be recorded to confirm acceptability.

- Manufacturing inspections and PSI with appropriate levels of redundancy and diversity confirm the absence of defects, which have the potential for causing, or developing into a failure mode. This judgement is based on definition of allowable SoL defect sizes. Where appropriate the inspections are subject to independent validation and in the case of HSS components of the PZR, a programme of qualified PSI is specified. In the unlikely event that defects are found, they will be repaired in accordance with accepted techniques.

The diverse evidence summarised above demonstrates that the PZR will be designed and fabricated against well established and appropriate deterministic engineering rules, verified by application of rigorous inspection. The various elements identified establish defence in depth for preventing failure of the PZR. Functional hydrostatic testing to demonstrate that the PZR meets the design intent, as described in Section 20B.3.2, supplements the arguments to demonstrate achievement of PZR integrity, ensuring that the PZR enters service fit for purpose and free of safety-significant defects.

The measures established to ensure good design and construction are supplemented with additional claims and evidence to demonstrate continued structural integrity throughout the planned PZR lifetime. Careful control of operating conditions enables the PZR to fulfil its safety function for its projected lifetime. Plant operation and maintenance will be defined in accordance with recognised procedures as described in Section 20B.3.1. Design and operating parameters used in the design evaluation are robustly determined using established and conservative procedures, as detailed in Section 20B.3.1. The evidence provided to this effect ensures the validity of stress analysis and fracture analysis to substantiate claims based on ASME Code compliance.

Section 20B.3.3 and Section 20B.3.4 provide evidence to substantiate PZR integrity under all design basis conditions by demonstrating that any defect, which may have gone undetected during manufacture, will not cause failure during the lifetime of the plant. The elements that substantiate this claim are as follows:

- Stress Analysis – The AP1000 PZR is designed in accordance with the ASME Code, Section III, Division 1. Consideration of Levels A to D and Test conditions encompass the design basis for the purposes of the analysis. Stress analysis to the ASME Code supports demonstrating fitness-for-purpose and also provides a basis for subsequent fracture analysis.

- Fracture Analysis – linear elastic fracture mechanics analysis, as prescribed in Appendix G of ASME Section III and XI, is to be supplemented by elastic-plastic fracture mechanics procedures specified in the R6 Defect Assessment code. The fracture analysis has demonstrated that the sizes of defect which are of safety concern are larger than those which could be present in the component following qualified manufacturing NDT. Qualified inspection of HSS locations establishes the sizes of defects that can be reliably detected and the associated sizing uncertainty. Qualification is to be achieved through a combination of Technical Justification of inspection procedures and equipment, supported by trials.

- ISI – The PZR is designed to facilitate effective ISI, which provides assurance that defects will be detected long before growing to a size that could threaten structural integrity of the PZR. ISI data enables judgment of in-service defect formation and growth by comparison with PSI data.

- Leakage Monitoring – Diverse systems are provided to detect, locate and monitor reactor coolant leakage from the PZR. Alarm and indication of reactor coolant leakage from the PZR in excess of specified limits provide diverse means to detect failure.

20B.5 Review of Open Issues

There are no open issues for the PZR that affect the basis of the safety case arguments.

20B.6 Conclusions

This CSR for the UK AP1000 PZR presents a safety argument to establish that the structural reliability of the PZR is commensurate with the consequences of gross failure. SFRs have been identified for the PZR, based on structural integrity safety design bases. These requirements are to be maintained to ensure plant nuclear and radiological safety. For the PZR, assurance that these SFRs will be maintained for the design life of the component is provided by substantiating structural integrity against appropriate reliability targets.

Structural reliability targets have been identified for the PZR that are based on a procedure of structural integrity classification (Reference 20B.4). Based on this, the PZR has been classified as a HSS component. The structural reliability target associated with HSS classification is to substantiate a failure frequency where the probability of gross structural failure of the PZR that is so low it can be discounted. The safety argument is presented in a four legged format that is well established in the UK for the safety justification of nuclear plant components similar to the PZR that share similar structural reliability targets. The safety argument identifies diverse defence in depth measures to substantiate the structural reliability claimed for the PZR:

- The intent and principles that govern the design, future manufacture and operation of the PZR in the UK are identified to substantiate fitness for purpose within a pre-construction safety case. The safety argument demonstrates how modern and well established good practice is to be implemented in PZR design, manufacture, defect tolerance assessment, and in the provision for through-life inspection.

- The PZR design benefits from the long operating history of PWR PZRs and incorporates design measures to minimise frequency of failure, which are based on this experience. The PZR design facilitates effective inspection, which supports a programme of qualified inspection to ensure timely forewarning of failure.

- Structural integrity of the PZR is secured largely by passive means and is not significantly reliant on control systems, active safety systems or human intervention. As such, the diverse defence in depth measures identified focus on prevention of failure through conservative, robust design. Surveillance, inspection and leakage monitoring provide secondary defence in depth measures to detect and provide forewarning of failure.

- PZR structural integrity is established based on extensive quality assurance measures in design, manufacture, materials, testing and qualified inspection. The strength of the safety case is based on achievement of integrity and the PZR has been deterministically justified in accordance with ASME Code Class 1 requirements. Additional arguments provide robust evidence to demonstrate that the PZR is defect tolerant and this is supported by qualified inspection. Numerous other defence in depth measures are identified.

In combination, these elements constitute a cogent argument to substantiate structural reliability commensurate with the HSS structural integrity classification of the PZR.

20B.7 Index of Technical Reports

Table 20B-20 provides a list of technical references supporting the safety case and summarises the function of each document within the safety case.

20B.8 References

20B.1 Westinghouse Report APP-MV20-Z0-100, Rev. 9, "Design Specification for AP1000 Pressurizer for RCS System," September 2016.

20B.2 Not used.

20B.3 Bullough, R. et al., "The Demonstration of Incredibility of Failure in Structural Integrity Safety Cases," International Journal of Pressure Vessels and Piping 78, 2001.

20B.4 Westinghouse Report UKP-GW-GLR-004, Rev. 3, "AP1000 UK Structural Integrity Classification," January 2017.

20B.5 Not Used.

20B.6 NUREG-1801, "General Ageing Lessons Learned (GALL) Report," Vol. 1, Rev. 1, US Nuclear Regulatory Commission, September 2005.

20B.7 ANS/ANSI N51.1 "Nuclear Safety Criteria for the Design of Stationary Pressurized Water Reactors," American Nuclear Society/American National Standards Institute.

20B.8 Not used.

20B.9 Not used.

20B.10 Not used.

20B.11 Westinghouse Report APP-GW-G1-003, Rev. 6, "AP1000 Seismic Design Criteria," August 2011.

20B.12 EPRI Document Number 1014986, "Pressurized Water Reactor Primary Water Chemistry Guidelines," Rev. 6, Electric Power Research Institute, September 2007.

20B.13 Westinghouse Report APP-MV20-Z0R-101, Rev. 4, "AP1000 Pressurizer Design Report," November 2016.

20B.14 "Nuclear Directorate Generic Design Assessment – New Civil Reactor Build, Step 3 Structural Integrity Assessment of the AP1000," Division 6 Assessment Report No. AR 09/013-P.

20B.15 Westinghouse Report APP-VL51-Z0-041, Rev. 0, "Material Specification for SA-508/SA-508 M Grade 3 Class 2 Forgings," April 2009.

20B.16 Westinghouse Report APP-GW-Z0-608, Rev. 1, "Material Test Specification for Austenitic Stainless Steel Cladding," November 2010.

20B.17 Westinghouse Report APP-GW-VLR-010, Rev. 2, "AP1000 Supplemental Fabrication and Inspection Requirements," January 2016.

20B.18 Westinghouse Electric Company "Quality Management System (QMS)," Rev. 7, October 2013.

20B.19 Westinghouse Report APP-GW-VW-001, Rev. 1, "AP1000® Design for Inspectability Program: ISI Requirements and Design Guidance for Class 1 Components," June 2014.

20B.20 "European Methodology For Qualification Of Non-Destructive Testing," European Network for Inspection Qualification (ENIQ) Report. 31, EUR 22906 EN Issue 3, August 2007.

20B.21 ASME Boiler and Pressure Vessel Code, 1998 Edition with addenda up through and including 2000 and Code Cases, American Society of Mechanical Engineers.

20B.22 Westinghouse Report APP-MV20-Z0-200, Rev. 2, "AP1000 Pressurizer Fabrication Specification," December 2012.

20B.23 Not used.

20B.24 Westinghouse Report UKP-MV01-Z0R-100, Rev. 3, "Results of Weld Ranking Process for Reactor Vessel, Steam Generator, Pressurizer, Main Steam Line and Main Coolant Loop Piping," December 2015.

20B.25 Westinghouse Report WDI-PJF-2405360-TCR-001, Rev. 1, "Results of the weld ranking process for the AP1000 Reactor Vessel, Steam Generator and Pressurizer – NDT Inspectability," (in response to GDA Step 4 Regulatory Observation R0-AP1000-19.A3), June 2010.

20B.26 Westinghouse Report UKP-MV01-Z0R-101, Rev. 2, "Methodology and Input Data for the Application of the R6 Flaw Evaluation Procedure and Fatigue Crack Growth Analysis to the UK AP1000 Components," December 2016.

20B.27 Westinghouse Report UKP-MV20-Z0C-100, Rev. 1, "Flaw Evaluation of the UK AP1000 Pressurizer Welds," December 2015.

20B.28 Westinghouse Report APP-MV20-VMR-001, Rev. 0, "AP1000 Component ISI Inspectability Assessment: Pressurizer," June 2011.

20B.29 Not used.

20B.30 Westinghouse Report WDI-TJ-1055, Rev. 1, "Manufacturing NDT Inspection Plan for the Upper Head to Upper Shell and Manway to Shell Welds of the AP1000 Pressurizer in Response to Regulatory Observation Action RO-AP1000-19.A3," February 2011.

20B.31 Westinghouse Report WDI-TJ-1054, Rev. 1, "Manufacturing NDT Inspection Plan for the Surge Nozzle to Safe End Weld of the AP1000 Pressurizer in Response to Regulatory Observation Action RO-AP1000-19.A3," January 2011.

20B.32 Westinghouse Report UKP-GW-GL-501, Rev. 0, "AP1000® UK Generic Technical Specifications," January 2016.

20B.33 WRCB-175 (Welding Research Council Bulletin 175), "PVRC Recommendations on Toughness Requirements for Ferritic Materials," August 1972.

20B.34 Regulatory Guide 1.60, Rev. 1, "Design Response Spectra for Seismic Design of Nuclear Power Plants," US Nuclear Regulatory Commission, December 1973.

20B.35 Regulatory Guide 1.44, Rev. 0, "Control of the Use of Sensitized Stainless Steel," May 1973.

20B.36 ASTM A262, "Standard Practices for Detecting Susceptibility to Intergranular Attack in Austenitic Stainless Steels," ASTM International.

20B.37 Westinghouse Report WDI-PJF-2405360-TCR-003, Rev. 2, "Westinghouse Process for the Development of AP1000 Related Manufacturing NDT Inspection Plans as Part of the GDA Process (UK)," Wesdyne International, February 2016.

20B.38 Westinghouse Report UKP-MV20-Z0C-103, Rev. 0, "Flaw Evaluation of the UK AP1000 Pressurizer Surge Nozzle to Safe-End Weld," February 2016.

20B.39 Westinghouse Report UKP-GW-M0R-001, Rev. 0, "Additional Fracture Toughness Testing for the UK AP1000 Plant," January 2017.

Table 20B-1. Pressuriser Material Specification (Reference 20B.1)

Component	Material	Class, Grade, or Type
Pressure Forgings	SA-508	GR 3, CL 2
Nozzle Safe Ends	SA-182 SA-336 SB163 or SB-564	F316, F316L, F316LN F316, F316L, F316LN N06690 N06690
Pressure Plates	SA-533	Type B, CL 1
Manway Studs	SA-193	GR B7
Manway Closure, Nuts, Washer Set	SA-194	GR 7
Heater Sleeves, Instrumentation, Sample, and Temperature Nozzles	Austenitic Stainless Steel	

Table 20B-2. Pressuriser Nominal Design Data

Design Pressure	17.13 MPa (2,485 psig)
Design Temperature	360°C (680°F)
Internal volume	59.47 m^3 (2,100 ft^3)
Design Life	60 years
Normal Operating Pressure	15.40 MPa (2,235 psig)
Normal Operating Temperature	345°C (653°F)

Table 20B-3. Pressuriser Heater Group Parameters

Voltage (Vac)	380
Frequency (Hz.)	50
Power Capacity (kW)	
Control Group	369
Backup Group A	246
Backup Group B	246
Backup Group C	369
Backup Group D	369

Table 20B-4 AP1000 Pressuriser Nozzle Mechanical Characteristics

Nozzle Description	Connecting NPS Pipe Size and Schedule	Connecting Pipe Material
Surge	18 (DN 450) x SCH 160	SA-312, TP316LN
Safety Relief	14 (DN 350) x SCH 160	SA-312, TP316LN
Spray	4 (DN 100) x SCH 120	SA-312, TP316LN
Instrumentation	1 (DN 25) x SCH 80	SA-312, TP304L
Temperature	1 (DN 25) Thermowell	N/A
Sample	1 (DN 25) x SCH 80	SA-312, TP304L

Table 20B-5. Structural Integrity Classification of Pressuriser Components

Location	Postulated Defect Orientation or Failure Mode	Classification	Supporting Comment
WELDS			
1. Vessel Shell			
1.1 Lower head to lower shell circumferential weld	All	HSS	Note 1
1.2 Lower shell to middle shell circumferential weld	All	HSS	Note 1
1.3 Middle shell to Upper shell circumferential weld	All	HSS	Note 1
1.4 Upper shell to upper head circumferential weld	All	HSS	Note 1
1.5 Manway to Upper Shell circumferential weld	All	HSS	Note 1
2. Nozzle Welds			
2.1 Safety/Relief nozzle to safe end weld	All	HSS	Note 1
2.2 Spray nozzle to safe end weld	All	HSS	Note 1
2.3 Surge nozzle to safe end weld	All	HSS	Note 1
FORGINGS			
3. Vessel Shell			
3.1 Crotch corner locations	All	HSS	Note 1
3.2 Clad/sub clad defects	All	HSS	Note 1
3.3 Shell materials	All	HSS	Note 1

Table 20B-5. Structural Integrity Classification of Pressuriser Components (cont.)

Location	Postulated Defect Orientation or Failure Mode	Classification	Supporting Comment
4. OTHER REGIONS			
4.1 Manway assembly in cylindrical shell	(i) Failure of cover plate (ii) Closure bolt failure	Class 1 Class 1	Failure of the cover plate would result in a LOCA. The effect would be bounded by the failure of the surge line which is within the design basis. Secondary effects are not considered to threaten passive protection systems.
4.2 Heaters	(i) Failure of heater sleeve seal welds (ii) Failure of heater sleeves (iii) Failure of heater support plate	Class 1 Class 1 Class 1	Failure of the heater assembly pressure boundary would result in a small LOCA.
4.3. Vessel Supports	Failure of support brackets.	Class 1	Failure of a vessel support leading to overload adjacent mounts and PZR pipework. Resulting LOCA is considered to be within design basis.

Note:
1. Basis for PZR HSS classification is presented in Table 20-7.

Table 20B-6. Not Used

Table 20B-7. Normal External Operating Conditions and Transients

Location/Parameter	Normal Range	Notes
Temperature	10 ~ 48.9°C (50 ~ 120°F)	
Pressure	-1.4 ~ +6.9 kPa (-0.2 ~ +1.0 psig)	
Humidity	1% to 100%	
Radiation, Dose Rate	3.3E+01 Rads-air/hr (3.3E-01 Gys-air/hr)	Room 11303
Radiation, 60 yr TID	1.7E+07 Rads-air/hr (1.7E+05 Gys-air/hr)	Room 11303
Chemistry	None	

Tables 20B-8. –20B-14. Not Used

Table 20B-15. Abnormal Operating Environment-Inside Containment

Conditions/Parameter	Abnormal Extreme	Duration	Notes
Group 1 (65.5°C (150°F))			
Temperature	65.6°C (150°F)	4 hours	Note 1
Pressure	13.7 kPa (2 psig)	4 hours	Note 1
Humidity	100%	4 hours	Note 1
Radiation	Same as normal		
Chemistry	None		
Submergence	None		
Group 2 (121.1°C (250°F))			
Temperature	121.1°C (250°F)	30 days	Note 1
Pressure	124.1 kPa (18 psig)	30 days	Note 1
Humidity	100%	30 days	Note 1
Radiation	Same as normal		
Chemistry	None		
Submergence	None		

Notes:
1. Parameter value is not maximum for full duration.

Table 20B-16. Not Used.

Table 20B-17. Scope of Manufacturing Inspection for the Pressuriser

	RT[(1)]	UT[(1)]	PT[(1)]	MT[(1)]
Heads				
Forged Head		Yes		
Cladding		Yes	Yes	
Shell				
Forgings		Yes		
Cladding		Yes	Yes	
Heaters				
Tubing		Yes[(2)]	Yes	
Centring of element	Yes			
Nozzle (Forgings)		Yes	Yes[(3)]	Yes[(3)]
Weldments				
Shell, circumferential	Yes			Yes
Nozzle to head (if fabricated)	Yes			Yes
Cladding		Yes	Yes	
Nozzle safe end	Yes		Yes	
Instrument nozzle			Yes	
Temporary attachments (after removal)				Yes
Boundary welds (after shop hydrostatic tests)		Yes		Yes
Support brackets				Yes

Notes:

1. RT – Radiographic testing, UT – Ultrasonic testing, PT – Dye penetrant testing, MT – Magnetic particle testing.
2. Eddy current testing can be used in lieu of UT.
3. MT or PT

Table 20B-18 Not Used

Table 20B-19. Summary of Defect Tolerance/NDT Ranking Assessment

Location No.	Weld	Classification	Ranking	Selected for Defect Tolerance Assessment	Bounded by other location
1.1	Lower head to lower shell circumferential weld	HSS	1	NO	Bounded by 1.4
1.2	Lower shell to middle shell circumferential weld	HSS	1	NO	Bounded by 1.3
1.3	Middle shell to upper shell circumferential weld	HSS	1	YES	
1.4	Upper shell to upper head circumferential weld	HSS	2	YES	
1.5	Manway to upper shell circumferential weld	HSS	1	YES	
2.1	Safety/Relief nozzle to safe end weld	HSS	1	NO	Bounded by 2.4
2.2	Spray nozzle to safe end weld	HSS	3	NO	Bounded by 2.4
2.3	Surge nozzle to safe end weld	HSS	1	YES	
3.1	Crotch corner locations	HSS	Not Assessed	NO	Non-Weld Region(1)
3.2	Clad/sub clad defects	HSS	Not Assessed	NO	Non-Weld Region(1)
3.3	Shell materials	HSS	Not Assessed	NO	Non-Weld Region(1)
4.1	Manway assembly in cylindrical shell	Class 1	Not Assessed	NO	Not Required
4.2	Heaters	Class 1	Not Assessed	NO	Not Required
4.3	Vessel Supports	Class 1	Not Assessed	NO	Not Required

Note:
1. See Section 20B.3.3.1.1

Table 20B-20. Index of Technical Reports

Document Reference	Document Title	Description of Role in Safety Case
Specifications/Reports		
APP-MV20-Z0-001	AP1000 Pressurizer Functional Specification	This document defines the performance and operational requirements for the PZR.
APP-MV20-Z0-100	AP1000 Pressurizer Design Specification for RCS System	Defines the requirements for the design, materials, performance, fabrication, examination, testing, cleaning, packaging, and shipping and handling of the PZR and associated equipment. Includes specific dimensional requirements, parameters, details, and criteria for the design and construction of the PZR.
APP-MV20-Z0-200	AP1000 Pressurizer Fabrication Specification	This document establishes the requirements for the fabrication. Material, examination, testing, cleaning, packaging, preparation for shipment, handling, storage, transportation, and quality assurance for the AP1000 PZR.
APP-GW-Z0-602	AP1000 Cleaning and Cleanliness Requirements of Equipment for use in Nuclear Steam Supply and Associated Systems	This document provides details of the cleaning and cleanliness requirements of equipment for use in the nuclear steam supply system along with associated systems. It provides inputs to the Design Specification.
APP-GW-VW-001	AP1000 Design for Inspectability Program: ISI Requirements for Class 1 Components	Contains requirements and design guidance relative to ISI for ASME Class 1 components, specifically focused on the concept of design for inspectability, to ensure that adequate design and access provisions for meeting ASME Code, Section XI are considered in the overall plant design.
APP-MV20-Z0R-101	AP1000 Pressurizer ASME Generic Design Report	Substantiates the structural integrity of the AP1000 PZR design with respect to the requirements of the Design Specification and Section III of the ASME Code. Consolidates the evidence from all pertinent structural analyses and relevant engineering drawings.
UKP-MV01-Z0R-100	Results of Weld Ranking Process for Reactor Vessel, SG and Pressurizer – Defect Tolerance	Identifies welds to be included in the phased programme planned for defect tolerance assessments.

Table 20B-20. Index of Technical Reports (cont.)

Document Reference	Document Title	Description of Role in Safety Case
APP-RCS-M1-001	Reactor Coolant System Design Transients	Defines the transients used to qualify the reactor coolant system to design requirement.
Materials Specification		
APP-VL51-Z0-041	Material Specification for SA-508/SA-508 M Grade 3 Class 2 Forgings	This document provides the material specification for SA-508SA-508 M Grade 3 Class 2 Forgings.
APP-VL51-Z0-121	Material Specification for SB-564	This document provides the material specification for SB-564.
APP-VL53-Z0-065	Material Specification for SB-167	This document provides the material specification for SB-167.
APP-VL52-Z0-122	Material Specification for SA-240 Type 304	This document provides the material specification for SA-240 Type 304.
APP-VL51-Z0-111	Material Specification for SA-336 Type 316LN	This document provides the material specification for SA-336 Type 316LN.
APP-VL51-Z0-112	Material Specification for SA-182 Type 316LN	This document provides the material specification for SA-182 Type 316LN.
APP-VL53-Z0-066	Material Specification for SA-376 Type 316LN	This document provides the material specification for SA-376 Type 316LN.
APP-VL52-Z0-131	Material Specification for SA-516 GR 70	This document provides the material specification for SA-516 GR 70.
APP-VL52-Z0-124	Material Specification for SA-240 Type 304L	This document provides the material specification for SA-240 Type 304L.

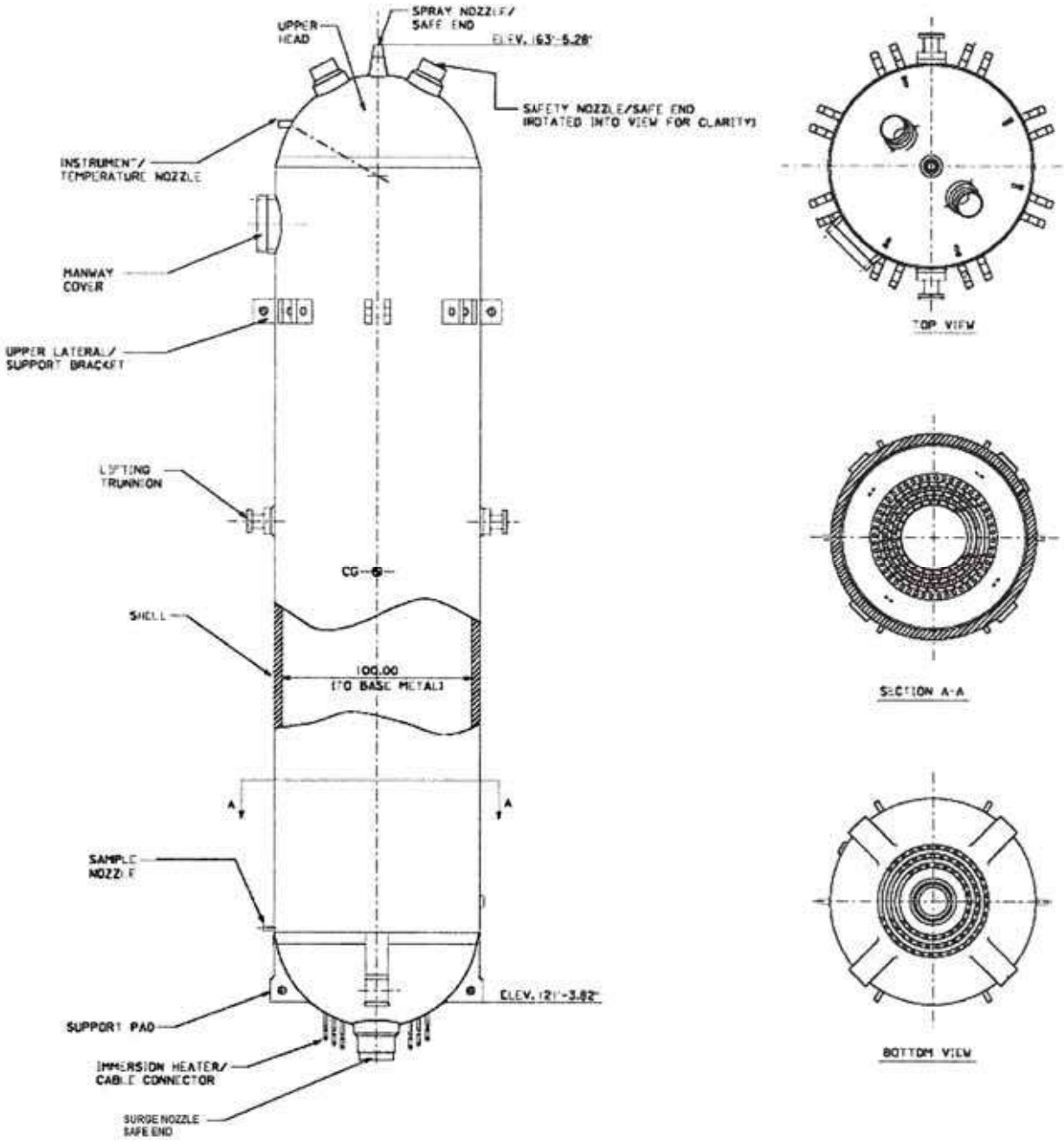


Figure 20B-1. Pressuriser[4]

[4] All dimensions and elevations are nominal. The manway cover is rotated into view for clarity.

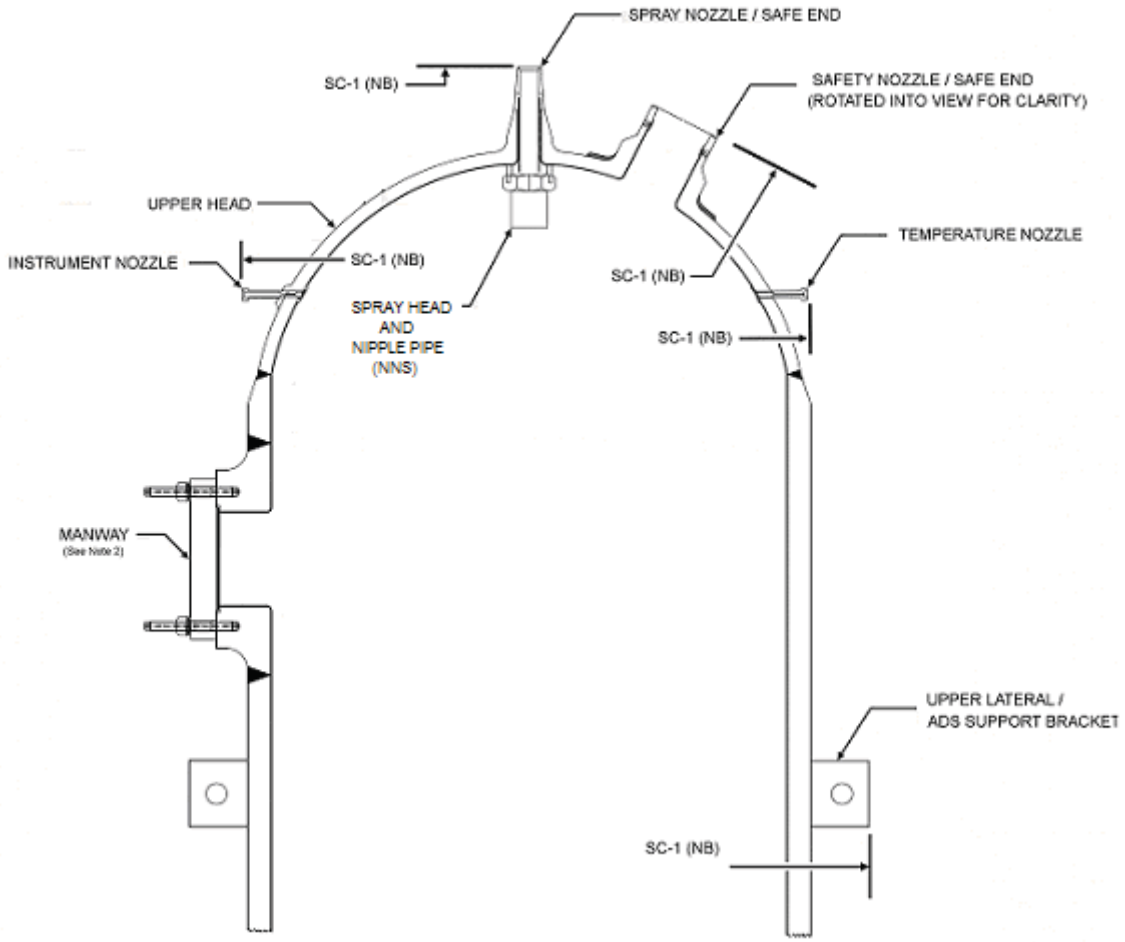


Figure 20B-2. AP1000 Pressuriser Jurisdictional Boundaries (Upper Section)

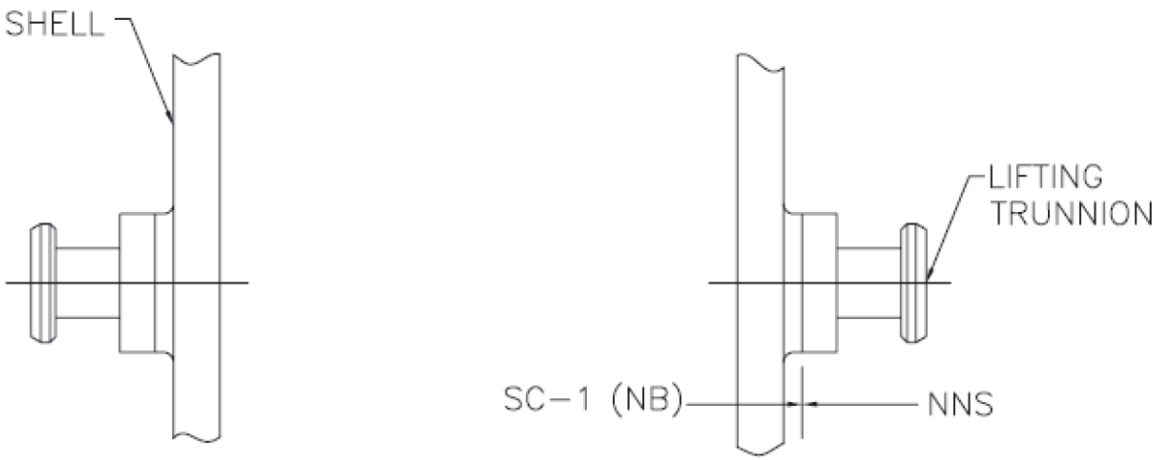


Figure 20B-3. AP1000 Pressuriser Jurisdictional Boundaries (Mid-Section)

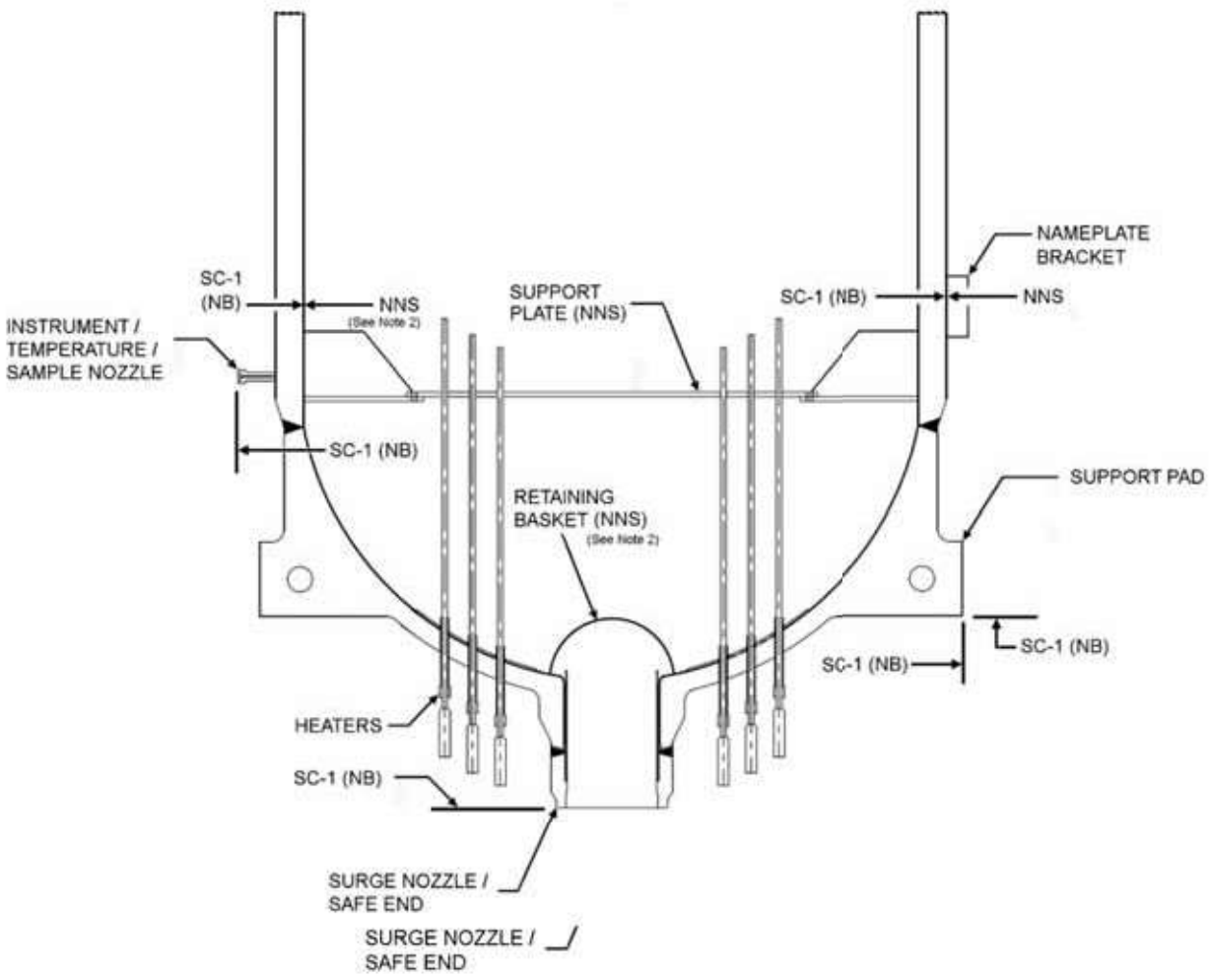


Figure 20B-4. AP1000 Pressuriser Jurisdictional Boundaries (Lower Section)

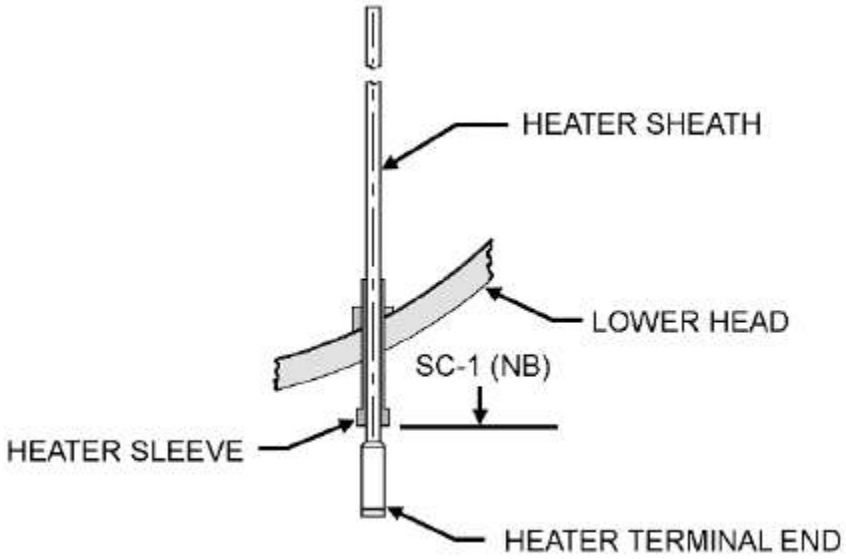


Figure 20B-5. AP1000 Pressuriser Jurisdictional Boundaries (Heaters)

Figure 20B-2 to Figure 20B-5 Notes:

1. The PZR assembly including nozzles and their safe ends, the ADS support lugs, lower head support lugs, and trunnion attachment pads are defined to be within the ASME Section III, Subsection NB jurisdictional boundary. The ADS lugs are considered structural attachments to the pressure boundary, and all attachments of internals to the pressure boundary are considered non-structural attachments.

2. Items outside of the ASME Section III NB Code jurisdiction are the heater support plate lug and attaching weld, heater support plates and attaching bolts, bolt-on trunnions and attaching bolts, surge line nozzle retaining screen and attachment weld, thermal sleeves, manway gasket, insert and seal plate, spray nipple pipe and attachment weld, spray nipple forging, and spray head.

3. The heaters are considered to be a part as they are welded into place prior to completion and stamping of the PZR. The attaching weld between the heater sleeve and the heater sheath will be evaluated in the PZR design report. The heater (including the heater connectors, seals and cables) jurisdictional boundary is defined in the heater design specification.

4. The connecting piping and its weld to the nozzles will be considered as part of the attached piping design.

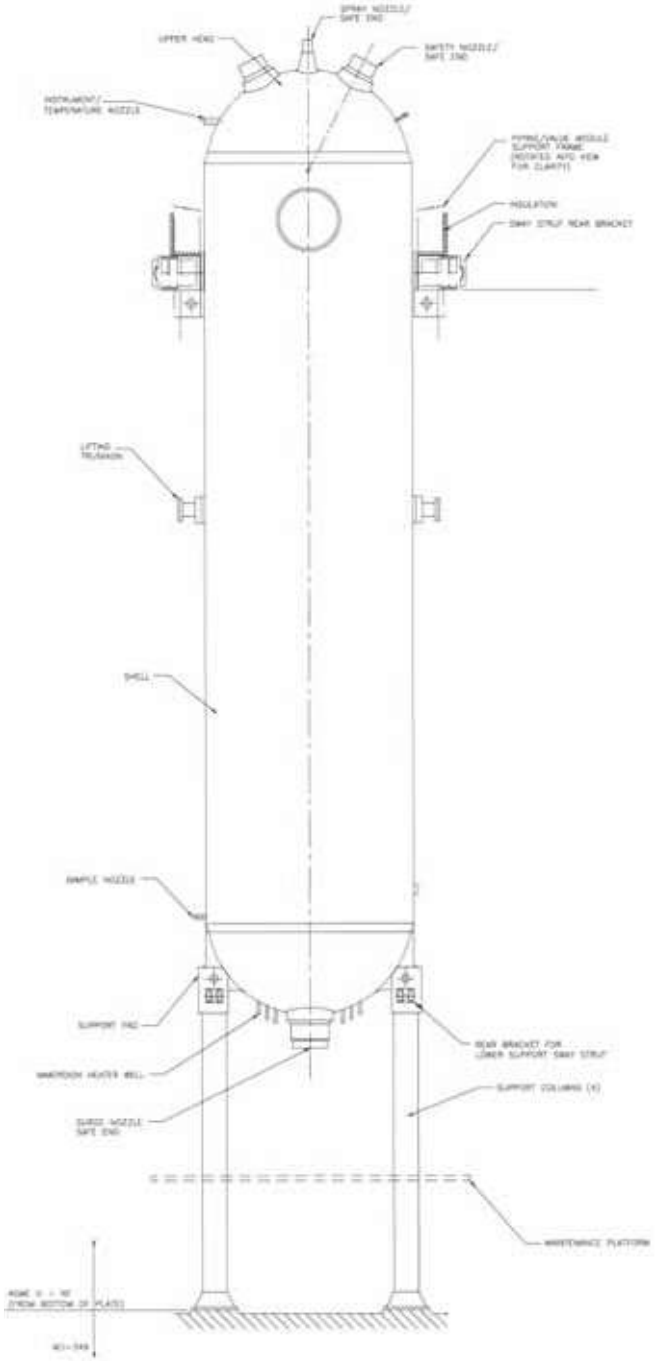


Figure 20B-6. Pressuriser Supports (Sheet 1 of 3)

Upper Supports

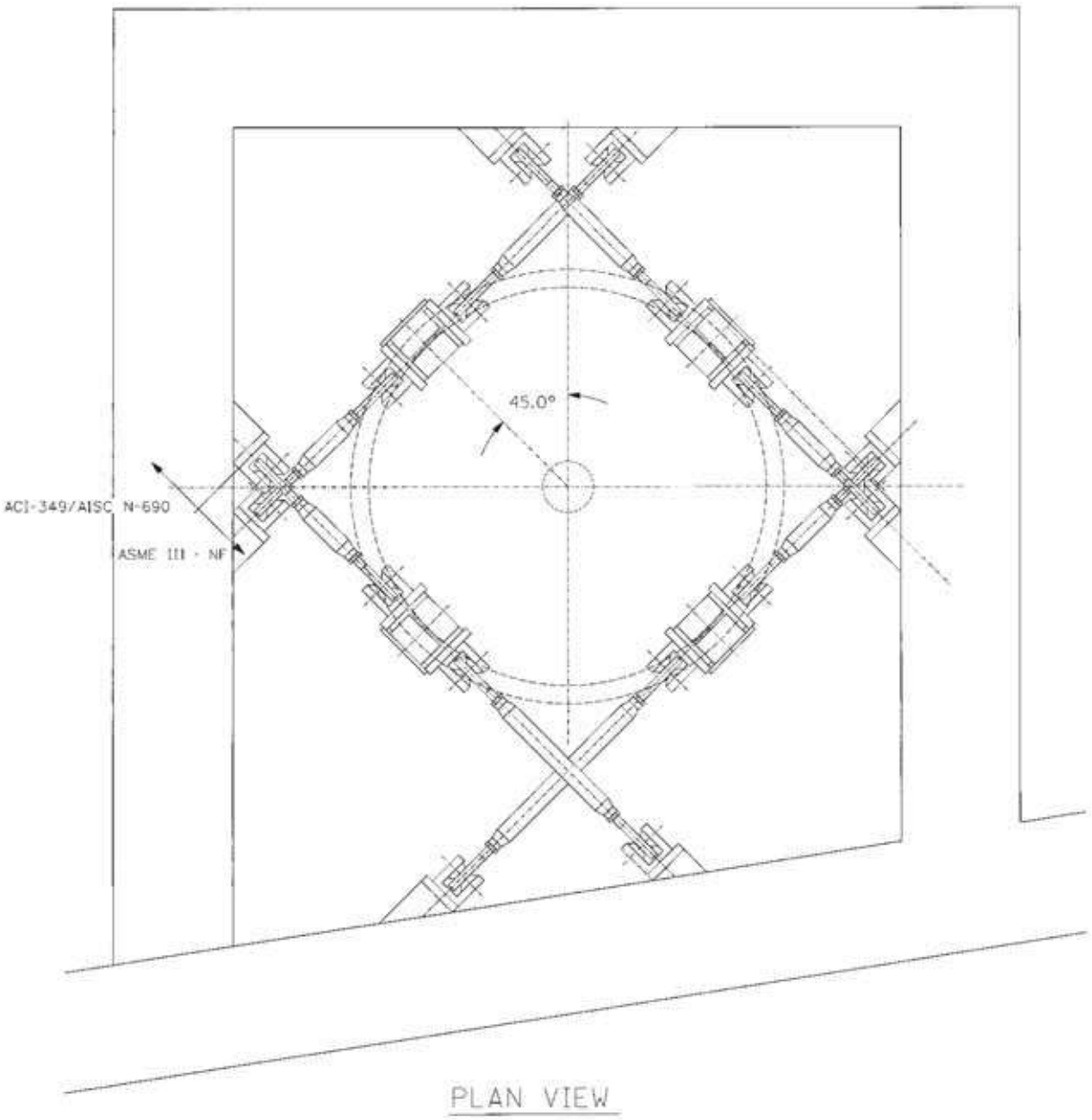


Figure 20B-6. Pressuriser Supports (Sheet 2 of 3)

Lower Lateral Supports

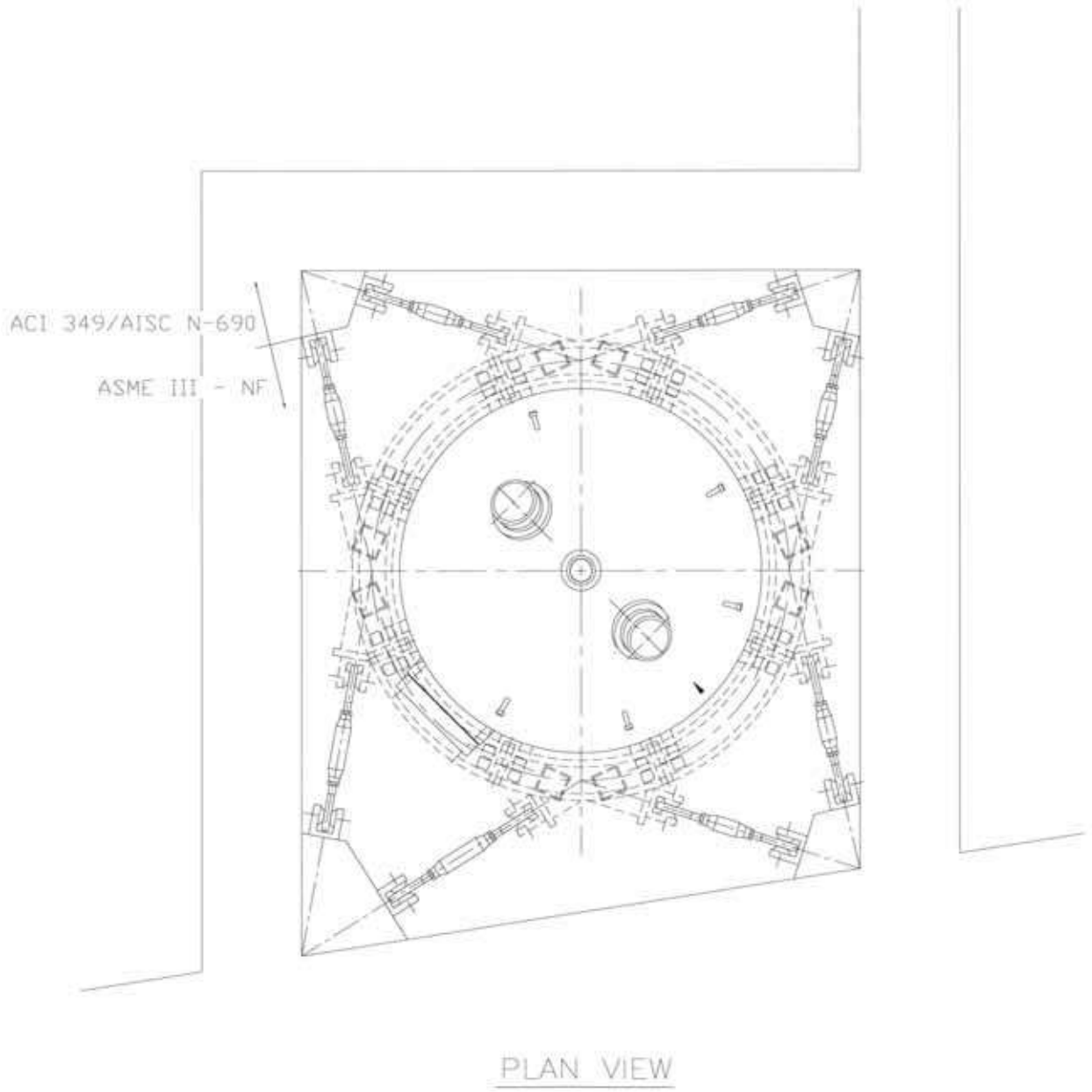


Figure 20B-6. Pressuriser Supports (Sheet 3 of 3)

Upper Supports

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS AND ACRONYMS

ALARP	as low as reasonably practicable
ANSI	American National Standards Institute
ASME	American Society of Mechanical Engineers
AVB	anti-vibration bar
CFR	Code of Federal Regulations
CMTR	certified material test report
CSR	Component Safety Report
CVS	chemical and volume control system
DDT	defect detection trials
DSM	defect size margin
ECT	eddy current testing
ELLDS	end-of-life limiting defect size
ENIQ	European Network for Inspection and Qualification
EPRI	Electric Power Research Institute
FUF	fatigue usage factor
GDA	generic design assessment
HI	high integrity
HSS	highest safety significance
ICD	interface control document
ID	inner diameter
ISI	in-service inspection
LCO	limiting conditions for operation
LEFM	linear elastic fracture mechanics
LFCG	lifetime fatigue crack growth
LOCA	loss-of-coolant accident
LTOP	low temperature overpressure protection
MT	magnetic particle testing
NCR	non-conformance report
NDE	nondestructive examination
NDT	nondestructive testing
NPP	nuclear power plant
NRC	Nuclear Regulatory Commission
OD	outside diameter
P/T	pressure / temperature
PML	Principia Mechanica Ltd
PRHR	passive residual heat removal
PSI	pre-service inspection
PWHT	post-weld heat treatment
PWR	pressurised water reactor
PWSCC	primary water stress corrosion cracking
PZR	pressuriser
QA	quality assurance
QEDS	qualified examination defect size
QMS	quality management system
RCP	reactor coolant pump
RCPB	reactor coolant pressure boundary
RCS	reactor coolant system
RO	regulatory observation
RPV	reactor pressure vessel
RT_{NDT}	reference temperature for nil ductility transition

LIST OF ABBREVIATIONS AND ACRONYMS (cont.)

SFR	safety functional requirement
SG	steam generator
SGS	steam generator system
SoL	start of life
SSC	system, structure, or component
SSE	safe shutdown earthquake
T_{NDT}	temperature for nil ductility transition
UK	United Kingdom
US	United States
UT	ultrasonic testing

APPENDIX 20C
STEAM GENERATOR COMPONENT SAFETY REPORT

20C.1 Introduction

This is the Component Safety Report (CSR) for the steam generator (SG) as introduced in Section 20.2. The safety argument herein substantiates the structural integrity of the SG to a degree of rigour commensurate with the consequences of gross structural failure. The safety argument is supported by a suite of documentary evidence outlined in Section 20C.7, including aspects of design assessment, material procurement, fabrication, manufacturing inspection, testing and in-service testing, maintenance and inspection.

20C.1.1 Scope

Arguments are presented herein to substantiate the claim that the nuclear and radiological hazards potentially arising from gross structural failure of the SG remain tolerably low for the design lifetime. Conventional hazards to personnel safety are outside the scope of this Appendix 20C.

Reliability targets are to be substantiated for the entire design lifetime objective of 60 years, as established in Section 6.1.1 of the Design Specification (Reference 20C.1). The 60 year design basis is used to determine corrosion allowance, for calculating cycle fatigue, and determining wear of components which are used to establish inspection and maintenance requirements needed to achieve the 60 year component lifetime.

This assessment considers all pressure, temperature, and mechanical loadings within the design basis. This includes normal operating conditions, anticipated transients, postulated accident conditions and test conditions. Design basis load parameters and transient definitions for the 60 year period of operation are described in Section 20C.3.1.2. Accident transients within the design basis are assessed in Chapter 9.

The AP1000 steam generator system (SGS) includes two SGs. The primary side components of the SGs form part of the reactor coolant system (RCS) pressure boundary. The scope of this assessment is limited to the structural reliability of the SGs only and does not include other components of the SGS, RCS or any other systems. A description of the SGs is provided in Section 20C.1.5 and the physical boundaries of the SGs are identified in Section 20C.1.6.

20C.1.2 Objectives

Safety functional requirements (SFRs) for a range of AP1000 components, including the SGs, are identified in Table 20-1. These correspond to the functions that need to be maintained to provide assurance of nuclear and radiological safety. Demonstrating that these SFRs will be maintained across the operational, process and lifecycle scope of the safety case supports the claim that the AP1000 plant risk remains both tolerable and as low as reasonably practicable (ALARP) for the design lifetime.

The SFRs applicable to the SGs are identified in Section 20C.2.1. This CSR demonstrates that the structural reliability of the SGs is commensurate with the consequences of failure; in the case of the SGs this necessitates a demonstration that the probability of gross failure of

certain components[1] of the SGs is so low that it can be discounted for the required 60 year period of operation. Establishing this level of structural reliability will demonstrate that the SGs maintain the capability to fulfil their SFRs in all design basis conditions.

20C.1.3 Strategy

Component classification forms the basis for identification of criteria against which the acceptability of the safety argument is to be judged. Substantiating structural reliability claims against these criteria provides an appropriate degree of assurance that the SFRs allocated to the SG will be maintained under all conditions within the design basis.

A safety argument is presented in Section 20C.3 according to a four-legged structure that is both consistent with established good practice in the United Kingdom (UK) nuclear industry and appropriate to SG component classification. For SG components with the highest level of component classification the safety argument will seek to demonstrate that the probability of gross failure of the SG is so low that it can be discounted for the required 60 year period of operation. For SG components that are allocated less onerous classifications, compliance with appropriate codes and standards forms the basis of the safety justification as identified within the appropriate elements of the safety argument.

The structure and philosophy of the safety argument are established in Section 20C.2. SFRs are identified in Section 20C.2.1 and SG component classification is established in Section 20C.2.2.

20C.1.4 Interface with other Safety Case Documents

The safety argument is supported by evidence to substantiate structural reliability claims, as identified in the relevant sections of the structured safety argument and tabulated in the technical index (Section 20C.7).

20C.1.5 Steam Generator Description

The AP1000 RCS consists of two heat transfer loops, each with a SG, two reactor coolant pumps, a single hot leg and two cold legs for circulating reactor coolant. All RCS equipment is located in the reactor containment. An isometric view of the AP1000 reactor coolant loops is shown in Figure 20F-2.

During normal plant operation, the reactor coolant pumps (RCPs) circulate pressurised reactor coolant through the reactor vessel then the SGs. The SGs serve as heat exchangers by converting secondary water into steam from heat produced in the reactor vessel. Reactor coolant flowing through tubes in the SG boils secondary water on the shell side to produce steam in the secondary loop that is delivered to the turbines. The steam is subsequently condensed via cooled water from the tertiary loop and returned to the SG to be heated once again. The reactor coolant is returned to the reactor vessel by the pumps to repeat the process.

The design specification (Reference 20C.1) gives a detailed description of the SGs, and provides the basis for demonstrating that the design and construction of the SGs conform to the rules set forth in the American Society of Mechanical Engineers (ASME) Boiler & Pressure Vessel Code (Code), Section III. Evidence to demonstrate accordance with established codes and standards provides evidence to substantiate claims regarding SG

1. These components are identified in Section 20C.2.2.

reliability by ensuring a high quality of design and manufacture. This evidence forms part of the safety argument in Section 20C.3 where a diverse range of relevant aspects is addressed.

The components of the steam generator forming part of the reactor coolant pressure boundary are AP1000 Equipment Class A components; and are designed to ASME Code, Section III, Class 1 requirements. The components of the steam generator forming the secondary side pressure boundary are AP1000 Equipment Class B components. Strict interpretation of the ASME Code requirements would dictate these components be designed to ASME Code, Section III, Class 2 requirements. However, for conservatism, all pressure retaining components on the secondary side of the steam generator are designed to ASME Code, Section III, Class 1 requirements.

Details regarding SG materials are given in Section 20C.3.1.4 and the controls to ensure quality of manufacture are identified in Section 20C.3.1.5. A simplified physical description of the SGs is provided in Section 20C.1.5.1 and a basic functional description is given in Section 20C.1.5.2.

20C.1.5.1 Physical Description

Two SGs are used in the AP1000 plant. The design of the SG is generally similar to earlier Westinghouse design SGs and also to typical pressurised water reactor (PWR) SG design. The design of PWR SGs has evolved over time and the SG for the AP1000 plant incorporates a number of safety-related design enhancements that are described in Section 20C.3.1.1.2.

The SG, shown in Figure 20C-2, is a vertical shell and U-tube evaporator with integral moisture separating equipment. Critical dimensions and volumes are identified in Table 20C-1 and the recommended materials of construction are identified in Table 20C-2.

The outer body of the SG is known as the shell, comprised of a primary (RCS) side and a secondary (feedwater) side containing moisture-separating internals, as described in the following sub-sections. SG interfaces, including supports, nozzles, access ports and instrumentation taps are described in the following sub-sections and listed in Table 20C-3.

20C.1.5.1.1 SG Shell

As illustrated in Figure 20C-3, the SG shell is comprised of a transition cone, shell barrels, Tubesheet, channel head, primary side inlet nozzle, primary side outlet nozzle, passive residual heat removal (PRHR) nozzle, main and start-up feedwater nozzles, trunnions, manways and elliptical head.

Nominal design parameters for the SG are provided in Table 20C-1. The SG measures approximately 22.5 m (73.8 ft) from steam outlet nozzle at its top to the flat, exterior portion of the channel head at its lower end. The inner diameter (ID) of the upper shell is approximately 5.33 m (17.5 ft), and that of the lower shell is approximately 4.19 m (13.7 ft). The maximum outside diameter (OD) of the SG is approximately 5.576 m (18.3 ft). All parts of the SG shell are low-alloy steel forgings. The ring forgings of the SG shell are connected by girth welds, and all welds on the surfaces of the shell, including nozzle attachments, are ground to remove discontinuities and stress risers as well as to facilitate examinations and inspections.

The Channel Head forms the lower part of the SG. A single primary inlet nozzle connects to the hot leg RCS pipe. The Channel Head is divided into inlet (hot leg) and outlet (cold leg) primary chambers by a vertical divider plate that extends from the centre of the channel head to the Tubesheet. The lower portion of these chambers is spherical and merges into a

cylindrical portion, which mates to the Tubesheet. Reactor coolant flow exits the SG through two pump suction nozzles in the Channel Head. Two RCP casings are directly connected to and supported by the SG Channel Head at the pump suction nozzles. This weld will be a nickel-chromium-iron (Alloy 690) weld made to nickel-chromium-iron alloy (Alloy 690) buttered ends of the SG channel head and RCP inlet nozzles. The buttering removes the need for field post-weld heat treatment (PWHT) of the closure weld. The interior surfaces of the Channel Head, primary nozzles, and primary manways are clad with weld deposited austenitic stainless steel with a finished nominal thickness of 5.9 mm (0.23 in).

A PRHR nozzle attaches near the bottom of the Channel Head of the loop 1 SG on the cold leg portion of the head. This nozzle provides recirculated flow from the PRHR heat exchanger to cool the primary side under certain accident conditions. A separate nozzle on the loop 1 SG Channel Head is connected to a line from the chemical and volume control system (CVS). This nozzle provides for purification flow and makeup flow from the chemical and volume control system to the RCS. The design of the loop 2 SG does not include these PRHR and CVS nozzles.

The Channel Head incorporates provisions to drain the head without operator action. To minimise deposits of radioactive corrosion products on the Channel Head surfaces and to enhance the decontamination of these surfaces, the Channel Head cladding is machined or electropolished for a smooth surface. Two primary manways in each Channel Head are provided for access to the primary chamber.

The upper surface of the Channel Head is connected to the Tubesheet. The Tubesheet has a base metal (low alloy steel) thickness of approximately 791 mm (31.1 in) and is clad with Alloy 690 of finished nominal clad thickness 6.60 mm (0.25 in). In order to achieve optimal secondary side crevice depths, the primary face of the Tubesheet is machine faced to a flatness of within 0.25 mm (0.01 in) on the primary side face and 0.13 mm (0.005 in) on the secondary side face. The secondary side face is parallel to the primary clad face to within 0.38 mm (0.015 in).

The upper surface of the Tubesheet is welded to the lower shell, which is comprised of three forged barrels. A blowdown nozzle is provided on the secondary side of the SG in the lower shell on the Tubesheet. Its function is to remove non-volatile, dissolved impurities and particulate matter from the secondary side water. Four hand-holes are provided to facilitate inspection and maintenance of the lower tube bundle assembly described in Section 20C.1.5.1.2. All secondary side handholes, inspection ports, and manways are gasketed closures using studs and nuts. These gaskets are of graphite wound construction or equivalent.

The lower shell connects to the larger diameter upper shell via a transition cone, which incorporates 2 U-bend inspection ports and a maintenance recirculation access port. The transition cone has a downstand on the small end and an upstand on the large end to locate the girth welds to lower stress regions.

A feedwater nozzle in the SG upper shell connects to the secondary feedwater pipework and a start-up feedwater nozzle is also located in the upper shell to supplement main feedwater during certain operating conditions and transient events. The start-up feedwater nozzle is located at approximately the same elevation as the feedwater nozzle, and is provided with an upward-sloping sparger assembly inside the upper shell. The feedwater and startup feedwater nozzles are clad on the inner surface.

To limit the motion of the end of the feedwater pipe under a postulated circumferential pipe break, a pipe whip restraint is provided and attached to the SG with two welded lugs located on the upper shell.

Secondary side access for repair and replacement of internal components such as moisture separator vanes is provided through two secondary manways, located in the upper shell of the SG. The SG upper shell also incorporates sludge collector piping (located internal to the SG close to a secondary manway).

The upper shell connects to the elliptical head knuckle and elliptical head. The elliptical head has an integral forged steam outlet nozzle. The steam outlet nozzle is NiCrFe clad around the ID on the exit of the nozzle by weld deposit. The steam outlet nozzle incorporates seven flow limiting venturi at the steam outlet nozzle interface. The flow-limiting venturi are designed to limit the pressure drop in the SG during steam line break so as not to exceed allowable loads on the internals and to limit the rate of mass and energy release into containment.

Instrument Taps

Four channels of narrow-range water level indication and four channels of wide-range water level indication are provided for each SG by the inclusion of level tap penetrations on the secondary side of the SG shell.

Both the wide-range and narrow-range taps are located circumferentially in the same horizontal plane on the SG shell to maximise separation between each channel and all other narrow-range channels. There are four DN 25 (NPS 1) tap connections in the lower shell for wide-range sensors, four DN 25 (NPS 1) tap connections in the transition cone for narrow-range sensors, and in the SG upper shell there are four DN 25 (NPS 1) tap connections that are shared for wide-range and narrow-range sensors. In addition there are three DN 25 (NPS 1) tap connections for steam flow differential pressure sensors.

Level tap locations on the upper shell of the SG are selected to prevent impulse line termination in high velocity flow areas. At any loading condition between 0 and 100 percent of full thermal load, the SG level is determined by measuring the differential pressure between the level taps.

SG Shell Supports

The SG shell is externally supported both vertically and laterally, as illustrated in Figure 20C-4. The vertical support consists of a single vertical column extending from the SG compartment floor to the bottom of each SG Channel Head. The column is constructed of a heavy wide flange section, and is pinned at both ends to permit thermal movement of each SG during plant heatup and cooldown. The column is located so that it allows full access to the SG for maintenance activities.

Lateral support is provided at lower, intermediate and upper levels. The lower lateral support is located at the bottom of the Channel Head. It consists of a tension/compression link bar and extension bar oriented approximately perpendicular to the hot leg. The link bar/extension bar is pinned at both the wall bracket and the SG Channel Head to permit movement of the SG during plant heatup and cooldown.

The intermediate SG lateral support is oriented normal to the hot leg and located on the lower shell just below the transition cone. It consists of two rigid struts that are mounted on the SG compartment wall at the elevation of the operating deck. The SG loads are transferred to the struts through trunnions on the SG lower shell “C” barrel. The upper lateral support is

oriented in the direction of the hot leg and located on the upper shell just above the transition cone. It consists of two large hydraulic snubbers oriented parallel with the hot leg centreline. One snubber is mounted on each side of the generator on top of the SG compartment wall. The hydraulic snubbers are valved to permit relatively unrestricted SG movement during thermal transient conditions, and to "lock up" and act as a rigid strut under dynamic loads.

20C.1.5.1.2 **SG Primary Side**

The principal SG primary side components include the Channel Head, Tubesheet, and tube bundle. The Channel Head, Tubesheet, and tube bundle form part of the RCS pressure boundary, which provides a barrier against the release of radioactivity generated within the reactor. The Channel Head and Tubesheet form part of the SG shell and are described in the previous sub-section.

10,025 heat-transfer U-tubes are provided per SG and are welded to the Tubesheet inside the SG shell. The SG tubing is approximately 17.48 mm (0.688 in) outside diameter and 1.02 mm (0.041 in) nominal wall thickness. The nominal minimum U-bend radius is 82.55 mm (3.25 in). The tubes are fabricated of nickel-chromium-iron Alloy 690 and undergo thermal treatment following tube-forming operations. The tubes are tack-expanded, welded, and are expanded over the full thickness of the Tubesheet to minimise secondary water access to the tube-to-tube-sheet crevice. The method by which the tubes are expanded into the Tubesheet is determined based on consideration of the residual stresses and the resultant susceptibility of the tube to degradation. Residual stresses (and the expanded tube's susceptibility to degradation) are limited, in part, through tight control of the pre-expansion clearance between the tube and Tubesheet hole.

20C.1.5.1.3 **SG Secondary Side**

The secondary side of the SG shell, consisting of the lower shell, transition cone, upper shell, feedwater nozzles, elliptical head knuckle, elliptical head and steam outlet nozzle, is the pressure boundary for the secondary side steam/water mixture[2]. These are described in Section 20C.1.5.1.1.

Within the SG shell, the principal secondary side components include the feedwater ring, moisture separating equipment and tube supports. Support of the tubes is provided by ferritic stainless steel tube support plates. Holes in the tube support plates are broached with a hole geometry to promote flow along the tube and to provide an appropriate interface between the tube support plate and the tube. Anti-vibration bars are installed in the U-bend region of the tube bundle. The tube bundle is surrounded by a wrapper, forming an annulus for secondary side feedwater between the wrapper and the shell of the SG. The wrapper is supported by lugs attached to the inside of the SG Shell.

Secondary side feedwater enters the SG at an elevation above the top of the U-tubes through the feedwater nozzle in the SG shell. A welded thermal sleeve connection connects the nozzle to a feedwater ring fitted with debris filtering nozzles and located in the SG upper shell. The feedring is elevated above the feedwater nozzle to minimise feedwater thermal stratification at the nozzle location. The debris filtering nozzles feature perforated outlets above the feedwater ring with 7.3 mm (0.29 in) nominal diameter holes to help prevent loose parts ingress into the SG.

2. The SG upper shell, feedwater nozzles, elliptical head knuckle, elliptical head and steam outlet nozzle are collectively referred to as the steam barrel.

Feedwater then flows down the annulus between the tube bundle wrapper and the SG shell, passes through a gap between the wrapper and the Tubesheet and flows up past the U-tubes where it boils and arrives in the SG upper shell as a mixture of saturated liquid and steam. This saturated mixture passes through moisture separators. Moisture is removed and re-circulated in the SG, while dried steam exits the SG via the steam nozzle and venturi flow restrictors. The primary moisture separators comprise 33 swirl vane riser columns that induce centrifugal separation. The secondary separator contains eight banks of hook-and-pocket vanes that subject the flow to multiple changes in direction.

20C.1.5.2 Functional Description

The basic function of the SG is to transfer heat from the single-phase reactor coolant water through the U-shaped heat exchanger tubes to the boiling, two-phase steam mixture in the secondary side. The SG separates dry and saturated steam from the boiling mixture, and delivers the steam to a nozzle from which it flows to the turbine. Water from the feedwater system continuously replenishes the SG water inventory, entering the SG through the feedwater nozzle and feedring. In addition to its steady-state heat transfer function, the SG secondary side provides a water inventory which is available as a heat sink to mitigate primary side high temperature transients and to accommodate accident conditions.

20C.1.5.2.1 Primary Side – Reactor Coolant Flow

On the primary side, the reactor coolant flow enters the primary chamber of the Channel Head via the hot leg nozzle and enters inverted U-tubes via the Tubesheet, transferring heat to the secondary side during its traverse of the tubes. During its approximately 21.3 m (69.9 ft) traverse of the tubes, the primary water is cooled from approximately 322°C to 279°C (612°F to 534°F). The reactor coolant flow then returns to the cold leg side of the primary chamber via the Tubesheet. The primary coolant flow exits the SG via two cold leg nozzles to which the RCPs are directly attached.

20C.1.5.2.2 Secondary Side – Feedwater Flow

Secondary side feedwater enters the SG via the feedwater nozzle and passes through a feedring fitted with spray nozzles, located in the SG upper shell. The incoming secondary side feedwater mixes with saturated water that has been separated from the steam outlet flow. The result is subcooled water in the SG downcomer region. This water flows down the annulus between the tube bundle wrapper and shell and enters the tube bundle region via a 304.8 mm (12 in) diameter opening at the bottom of the wrapper just above the Tubesheet. The direction of flow then turns and is directed upward along the tube bundle U-tubes.

As it flows upward, the fluid on the secondary side is heated by the primary side fluid via heat transfer through the U-tube walls. The secondary side fluid boils and becomes a mixture of saturated liquid and steam. This saturated mixture continues to flow upward into the moisture separator assembly in the SG upper shell.

The two phase flow leaving the tube bundle enters the primary moisture separator assembly with integral swirl vanes. The swirl vanes impart a centrifugal acceleration to the flow, causing the heavier liquid droplets to collect along the inner surface of the riser pipe. This liquid flow, along with some steam (carry under), is returned to the SG downcomer plenum through openings in the riser pipes and at the outlet of the riser.

Additional separation takes place by gravity as the relatively low velocity flow travels upward to the entrance of the single tier secondary separator. The secondary separator

contains banks of hook-and-pocket vanes that subject the flow to multiple changes in direction. These changes in flow direction produce flow accelerations that act to separate out the remaining liquid in the steam-water mixture. The liquid then flows down the vanes to collection troughs that return it to the downcomer plenum via the drain manifold system. The steam flow exits the secondary separator then leaves the SG through the steam outlet nozzle. The moisture carryover limit of the exiting flow is 0.25% as measured by tracer technique and the design goal moisture carryover of the exiting flow is 0.10% or less.

All saturated water separated out from the steam-water mixture is returned to the SG upper downcomer plenum. Here it mixes with incoming subcooled feedwater, completing the recirculating loop.

20C.1.6 Boundaries

As identified in Reference 20C.1, the physical boundaries of the SG are illustrated in Figure 20C-5 to Figure 20C-9. Interfaces, which form part of a pressure boundary, are at the first circumferential weld joint joining the piping or pump casing to the SG nozzles. The connecting weld between the SG outlet nozzle and the RCP casing is considered a pressure boundary weld per the ASME Code. These physical limits are identified to specify the scope of this report and also represent the limit of applicability of the ASME Code, Section III to the SG.

20C.2 Safety Case Requirements

This key objective of this CSR is to establish that the structural reliability of the SG is commensurate with the consequences of gross failure. This is achieved by means of a structured safety argument, supported by suitable and sufficient evidence. The safety argument is presented in Section 20C.3 according to an established four legged structure (Reference 20C.3), to demonstrate an appropriate level and diversity of defence in depth by identifying evidence to satisfy safety claims and objectives identified within each leg of the argument, as follows:

Leg 1	**Interpolation/Extrapolation of Experience – 'Good' Design and Manufacture**
Objective:	To provide evidence of good design and manufacture based on a proven track record. This forms a keystone for a demonstration of high reliability and embodies the code and plant operating experience with objective of achieving quality of build, high integrity (HI) and the avoidance of defects.
Claim:	High quality is achieved through good design and manufacture.
Leg 2:	**Functional Testing**
Objective:	To incorporate build experience as embodied in design codes, and provides some diversity and redundancy to the pre-service inspection (PSI).
Claim:	Components are shown to be fit for purpose through effective functional testing.

Leg 3: **Failure Analysis**

Objective: By means of an assessment of through-life degradation mechanisms, to show that such mechanisms will not threaten integrity over a specific interval. This goes beyond design code requirements to provide a further demonstration of integrity. This leg acknowledges that flaws may be present and demonstrates tolerance to them. This supplements the Leg 1 aim of avoidance of defects to provide a safety case with both defect avoidance and defect tolerance.

Claim: Components are tolerant to through life degradation over the design life of the plant.

Leg 4 **Forewarning of Failure**

Objective: To confirm the absence of a degradation mechanism or that a known degradation mechanism is not significant to integrity or will have limited consequences. This provides a means of safely controlling any anticipated component degradation and also a contingency for the unexpected.

Claim: Effective systems are in place to provide forewarning of failure

The four legged safety argument will substantiate specific SFRs for the SG and these support nuclear safety claims made for AP1000 plant. The SG SFRs are identified in Section 20C.2.1.

The safety argument is tailored according to the structural reliability claims derived from a process of component classification, with the purpose of demonstrating that component structural reliability is commensurate with the consequences of gross failure. Classification of the SG and its component parts is established in Section 20C.2.2.

The four legged safety argument is provided in Section 20C.3 and the strength of the argument is discussed in Section 20C.4.

20C.2.1 Safety Functional Requirements

The SG is allocated the following SFRs, reiterated here from Table 20-1:

- **SFR 20.3.1** The SG pressure boundary is required to maintain the integrity of the primary and secondary coolant boundaries during standby, normal operation and under design basis faulted conditions for the design life of the plant.

- **SFR 20.3.2** The SG secondary side is required to provide a heat sink for the RCS during power operations and anticipated transients and under natural circulation conditions in accordance with component performance requirements (not required to provide safe shutdown of the plant).

Postulated failure modes which result in a loss of these SFRs lead to identification of structural reliability targets commensurate with the consequences of gross failure, as determined through the process of component classification as described in Section 20C.2.2. The safety argument in Section 20C.3 is provided to substantiate that these structural reliability targets will be achieved and thus demonstrate that the above SFRs will be maintained at all times.

20C.2.2 Structural Integrity Classification

A clear understanding of the potential radiological consequences of any postulated gross failure mode is a key starting point for the SG structural integrity safety argument. This forms a structured and systematic basis to establish an appropriate level of rigour to be applied in the design assessment, material procurement, fabrication, in-manufacture inspection, testing and in-service testing, maintenance, inspection and safety case assessment of the SG. Details of the approach for developing AP1000 component structural integrity safety cases are given in Reference 20C.4.

The approach to structural integrity classification is discussed in Section 20.5 and is consistent with the overall AP1000 safety classification scheme as detailed in Chapter 5. Reference 20C.4 details the approach taken whereby a more detailed assessment of selected individual components is made to establish the consequences of gross failure, due to both direct consequences such as a loss-of-coolant accident (LOCA), and indirect consequences, such as the effect of missiles, jet loading or pipe whip on essential safety systems. Based on this assessment, and in accordance with the scheme identified in Chapter 5, components are allocated one of the five structural integrity classifications described in Section 20.5.2:

The tolerable failure frequency, available mitigation and consequences associated with these classifications is summarised in Table 20-2. There are three regions of the SG where gross failure has been assessed in Reference 20C.4 as having the potential to lead to the most severe off-site consequences against which there is no claimed protection. These are the Secondary Shell, Channel Head, and Tubesheet; all three of which have been allocated a classification of Highest Safety Significance (HSS). Table 20-4 to Table 20-6 respectively, reproduced from Reference 20C.4, identify the basis for the classification of these three regions.

Other components of the SG are allocated a classification of Standard Class 1, since gross failure at other SG locations has been assessed as not having the potential to lead to the most severe and unprotectable off-site consequences. The classification of all individual SG components is presented in Table 20C-4.

20C.3 Safety Argument

This section provides a structured safety argument to demonstrate that the SG is fit for purpose for the required component lifetime of 60 years. The safety argument is presented according to a four-legged structure articulated in section 20C.2.

Consistency with the appropriate ASME rules for design, manufacture and inspection forms the basis to substantiate fitness-for-purpose for SG components with Standard Class 1 classification. Evidence to demonstrate appropriate code compliance for these components is presented in Sections 20C.3.1 (design & manufacture) and 20C.3.4 (in-service inspection).

Compliance with the relevant rules of the ASME Code is generally inferred as providing substantiation of satisfactory reliability for a component classified as Standard Class 1. In the case of the HSS components, i.e., the Channel Head, Tubesheet and Secondary Shell, it is necessary to substantiate a lower frequency of failure, such that the probability of gross failure is so low that it can be discounted. This is achieved by identifying supplementary measures to ensure high quality and by demonstrating the tolerance to manufacturing defects above qualified detection limits. In addition to evidence presented to demonstrate compliance with ASME rules given in Section 20C.3.1, further qualitative arguments are presented in Sections 20C.3.2, 20C.3.3 and 20C.3.4 to demonstrate evidence of defence in depth and

substantiate a level of structural reliability commensurate with HSS classification for the relevant SG components.

20C.3.1 Leg 1: Interpolation/Extrapolation of Experience – Good Design and Manufacture

The principal claim for Leg 1 of the safety argument is that the quality of design and manufacture is commensurate with the classification of each component of the SG. This supports the structural reliability targets associated with the classification of each SG component. Structural reliability targets, expressed in terms of tolerable frequencies of failure, are identified for each level of component classification in Table 20.2.

The Design Specification (Reference 20C.1) provides a diverse range of evidence to ensure the quality of design and manufacture, as identified within this leg of the safety argument. Reference 20C.1 establishes the basis for the materials, design, operability, regulatory requirements, manufacture, inspection, testing, packaging and preparation for shipment of the AP1000 SGs. This provides the basis to demonstrate that the design and construction of the SG conforms to the ASME Code, Section III, Rules for the Construction of Nuclear Power Plant Components and the applicable Code Cases and Addenda for Class 1 and Class 2 vessels. The ASME Section III Rules embody extensive international industry-wide operating experience and compliance with these rules provides a keystone for a demonstration of high structural reliability.

A series of subordinate safety arguments are established to substantiate appropriate quality of SG design and manufacture as follows:

- **Section 20C.3.1.1** SG design is well founded.
- **Section 20C.3.1.2** SG design parameters are suitably well defined.
- **Section 20C.3.1.3** Compliance with relevant design code requirements supports SG structural reliability claims.
- **Section 20C.3.1.4** SG components are manufactured from suitable materials.
- **Section 20C.3.1.5** Suitable controls ensure SG manufacturing quality.
- **Section 20C.3.1.6** Manufacturing and Pre-Service inspections confirm quality of manufacture.
- **Section 20C.3.1.7** Definition and control of plant operation and maintenance ensure continued fitness-for-purpose.

Collectively these arguments identify evidence to demonstrate that the SG is well designed, will enter service free from structurally significant defects and that the effects of through-life degradation on material properties will not have a safety-significant deleterious effect on SG structural reliability.

20C.3.1.1 SG Design is Well Founded

To demonstrate that SG design is well founded, evidence to substantiate the following arguments is provided:

- SG design is well established.

- SG design takes due account of relevant experience.
- Appropriate codes, standards & regulations are specified to control the quality of design and manufacture.

20C.3.1.1.1 **SG Design is Well Established**

The design of the SG is fundamentally similar to previous well established designs and thus supported by a substantial record of safe operating experience. This leads to a comprehensive understanding of the in-service performance of SGs and the management and mitigation of through-life degradation. This understanding has influenced SG design and manufacture to eliminate, minimise and control issues that can adversely affect through-life structural integrity.

Westinghouse has substantial proven experience, knowledge, and capability to design and manufacture SGs. Westinghouse has more than fifty years' experience of nuclear power plant (NPP) design, development and manufacture, and has designed and delivered more than 100 commercial NPPs worldwide including Sizewell B in the UK. The SG design is, therefore, supported by unparalleled experience in design and manufacture, benefitting from substantial operating experience that demonstrates an excellent record of safe operation.

Two SGs are used in the AP1000 plant. The design of the AP1000 SG is similar to earlier Westinghouse design SGs, and also to typical PWR SG design with similar proven materials and manufacturing processes. The design has been the subject of regulatory scrutiny overseas: the Nuclear Regulatory Commission (NRC) of the United States (US) approved the AP1000 design in December 2005 following the earlier approval of AP600 NPP design certification in 1999.

The design of the AP1000 SG is based on standard Westinghouse Model-F technology. There are some 75 Model F-type units in commercial operation, with the highest level of reliability achieved by any SG worldwide. The high reliability of similar SG designs is well proven; examples of currently operating NPP that employ similar SG design include the Delta-75 replacement SGs for V.C. Summer and other plants; Delta-94 replacement SG for South Texas plant; replacement SGs for Arkansas and Waterford.

The SG design is based on well proven preceding designs and therefore novel design features are largely avoided. The design is not, however, identical to earlier designs but has evolved to include a number of enhancements to improve safety and reliability, as described in Section 20C.3.1.1.2 below.

20C.3.1.1.2 **SG Design Takes Due Account of Relevant Experience**

The design of the AP1000 SG benefits from lessons learned over many years of safe operation. This experience has led to design enhancements that improve the structural reliability of the SG. The general arrangement of the SG shell is designed to maximise structural reliability and is comprised of a series of forgings to minimise the number of circumferential welds and eliminate longitudinal welds. The SG design includes several enhancements to improve safety and reliability by mitigating against various issues relating to SG degradation experienced in similar NPP. These enhancements include the following:

- Full-depth hydraulic expansion of the heat transfer tubes in the Tubesheet to minimise secondary water access to the tube-to-Tubesheet crevice,

- Thermally treated Inconel 690 (I-690) heat transfer tubing provides enhanced resistance to tube degradation,

- Modified triangular pitch of heat transfer tubes provides enhanced resistance to tube degradation,

- Broached tube support plates and modified anti-vibration bars (AVBs) to minimise tube degradation due to vibration,

- Upgraded (more robust) primary and secondary moisture separators,

- Enhanced access arrangements for maintenance and inspection, including a modified Channel Head design that facilitates access for robotic tooling.

The SG design includes measures to minimise degradation due to water hammer, stratification, and striping. SG bubble collapse water hammer has occurred in certain early pressurised water reactor SG designs having feedrings equipped with bottom discharge holes. Prevention and mitigation of feedline-related water hammer has been accomplished through an improved design and operation of the feedwater delivery system. The AP1000 SG and feedwater system incorporate features designed to eliminate the conditions linked to the occurrence of SG water hammer. The SG features include introducing feedwater into the SG at an elevation above the top of the tube bundle and below the normal water level by a top discharge feedring. The top discharge of the feedring helps to reduce the potential for vapour formation in the feedring. This minimises the potential for conditions that can result in water hammer in the feedwater piping. The feedwater system features designed to prevent and mitigate water hammer include a short, horizontal or downward sloping feedwater pipe at SG inlet. These features minimise the potential for trapping pockets of steam which could lead to water hammer events.

Stratification and striping are reduced by an upturning elbow inside the SG which raises the feedring relative to the feedwater nozzle. The elevated feedring reduces the potential for stratified flow by allowing the cooler, denser feedwater to fill the nozzle/elbow arrangement before rising into the feedring.

The potential for water hammer, stratification, and striping is further reduced by the use of a separate start-up feedwater nozzle. The start-up feedwater nozzle is located at the same elevation as the main feedwater nozzle and is rotated circumferentially away from the main feedwater nozzle. A start-up feedwater spray system independent of the main feedwater feedring is used to introduce start-up feedwater into the SG. The layout of the start-up feedwater piping includes the same features as the main feedwater line to minimise the potential for waterhammer. The feedwater and startup feedwater nozzles are clad on the inner surface, as described in Section 20C.1.5.1.1, to minimise the potential for corrosion-related degradation.

The SG steam outlet nozzle incorporates flow-limiting venturi designed to limit the pressure drop in the SG during steam line break so as not to exceed allowable loads on the internals and to limit the rate of mass and energy release into containment.

The SG is designed for a component lifetime of 60 years, and the design accommodates facilities for maintenance activities over this period including provision for repair and replacement if necessary. The arrangement of the Channel Head primary chamber provides enhanced access to all tubes, including those at the periphery of the bundle, with robotic equipment. This enhances the ability to inspect, replace and repair portions of the AP1000

unit compared to the more spherical primary chamber of earlier designs. All heat transfer tubes in the SG are accessible for sleeving, if necessary.

Additional measures to control the quality of design and manufacture, based on industry-wide experience, are embodied in the codes, standards and regulations identified below in Section 20C.3.1.1.3.

20C.3.1.1.3 Appropriate Codes, Standards & Regulations are Specified to Control the Quality of Design and Manufacture

Compliance with relevant and internationally well established codes, standards and regulations to control the quality of SG design and manufacture provides assurance that an appropriate level of structural reliability will be achieved. Compliance with the ASME Code provides assurance over a diverse range of relevant aspects including material procurement, component design, selection of manufacturing consumables, qualification of welders, specification of heat treatment, manufacturing quality checks and nondestructive examination (NDE), testing, installation and pre-service and in-service inspection requirements.

The SG is designed, fabricated and installed in accordance with the codes, standards, guidelines and regulations identified in Table 20C-5. These include elements of the ASME Code and Code Cases, American National Standards Institute and ASME Standards, US Code of Federal Regulations, US NRC Regulatory Guides, Electric Power Research Institute (EPRI) Guidelines, and miscellaneous standards and recommended practises.

The applicability of the codes, standards and regulations identified in Table 20C-5 to a particular component of the SG is primarily based on the AP1000 equipment classification of the component. Table 20C-6 identifies the AP1000 equipment classification for the subcomponents of the SG, as well as the corresponding American Nuclear Standards Institute (ANSI) safety class and seismic classification. Class A, B and C components are designed to nuclear codes and standards, such as the ASME Code. AP1000 Equipment Class A components are designed to ASME Code, Section III, Class 1 requirements. For conservatism, all pressure retaining components on the secondary side of the steam generator are also designed to ASME Code, Section III, Class 1 requirements. Class D or E components are designed to meet the design, material, fabrication, inspection and testing requirements of industry codes and standards.

The AP1000 NPP design originates in the US. As such, many of the specified codes, standards and regulations originate in that country. These codes represent internationally established good practice and as such are considered to be applicable in the UK. Where additional or alternative requirements or procedures specifically applicable to the UK are warranted, such as those associated with inspection and defect tolerance, this is identified within the appropriate section of this safety argument.

The codes, standards and regulations that are specified to control quality of SG design and manufacture embody extensive experience relevant to the SG. This experience helps to ensure a structurally robust design and provides a means to prevent, minimise and control component degradation at the design stage. Compliance with the codes, standards and regulations, therefore, provides a foundation for assuring that SG structural integrity will be maintained for the design lifetime.

Evidence of compliance with ASME requirements is provided by ASME certification of the SG at the construction stage of AP1000 NPP development, supported by an assessment to

demonstrate compliance with relevant design code requirements as described in Section 20C.3.1.3.

20C.3.1.2 SG Design Parameters are Suitably Well Defined

To substantiate claims based on ASME Code compliance and also to demonstrate that a safe plant operating envelope is clearly established, SG design parameters must be suitably well defined. Evidence is provided to substantiate the following claims:

- Specification of design load parameters is suitably comprehensive.
- Specification of environmental conditions is suitably comprehensive.

20C.3.1.2.1 Specification of Design Load Parameters is Suitably Comprehensive

Section III Subsection NB of the ASME Code requires that the SG design is evaluated against design, service, and test conditions and that the stresses within the SG are shown to comply with specified allowable stress limits appropriate to the material of construction. The assessment to demonstrate compliance with these requirements is described in Section 20C.3.1.3.

Design conditions include those pressure, temperature, and mechanical loadings selected as the basis for the design. Service conditions cover those normal operating conditions, anticipated transients, and postulated accident conditions expected or postulated to occur during operation. The evaluation of the service and testing conditions includes an evaluation of fatigue due to cyclic stresses. References that establish transient specification are identified in the index of technical reports (see Table 20C-7).

The following five categories of operating condition, as defined in ASME Code, Section III, encompass all operating conditions within the design basis of the SG:

- Level A Service Conditions – Normal Conditions.
- Level B Service Conditions – Upset Conditions, Incidents of Moderate Frequency
- Level C Service Conditions – Emergency Conditions, Infrequent Incidents
- Level D Service Conditions – Faulted Conditions, Limiting Faults
- Testing Conditions

The load parameters used in the design evaluation are summarised below to demonstrate that these have been determined using well established and conservative procedures and capture all conditions within the design basis.

The design basis of the SG is specified in Reference 20C.1. The structural design of the SG is based upon the following maximum steady state internal conditions:

Primary Chamber Components:	
Primary Side Design Temperature:	343.3°C (650°F)
Primary Side Design Pressure:	17.24 MPa (2500 psi)
Secondary Chamber Components:	
Secondary Side Design Temperature:	315.6°C (600°F)
Secondary Side Design Pressure:	8.27 MPa (1200 psi)

Primary-to-Secondary Chamber Components (both sides pressurised concurrently):

Maximum Temperature:	343.3°C (650°F)
Maximum primary-to-secondary differential pressure:	11.38 MPa (1650 psi)
Maximum secondary-to-primary differential pressure:	4.62 MPa (670 psi)

Design thermal-hydraulic conditions and transients are specified in Reference 20C.1, where load combinations for Design, Level A, Level B, Level C, Level D and Test conditions are identified. The load combinations for the SG stress analyses are listed in Table 20C-8. The load combinations are expressed in terms of the nomenclature identified in Table 20C-9.

As identified in Reference 20C.1, the load combinations listed in Table 20C-8 are documented in the interface control document (ICD) (Reference 20C.6). The design analysis includes the RCS pressure, temperature, and flow transients, as specified in Reference 20C.7. SG thermal-hydraulic conditions are determined under the design basis transient conditions specified in Reference 20C.7, with respect to secondary side pressures, temperatures, and heat transfer coefficients throughout the SG. Primary side condition inputs and loadings on SG internals are also determined based on the conditions specified in Reference 20C.7. Additionally, for SG No. 1 only, the scope of the design stress analysis includes consideration of the CVS and PRHR nozzles based on transients defined in the ICD. For the purpose of SG design evaluation, the number of transient occurrences is based on a plant design life of 60 years. In addition to the summary of load combinations listed in Table 20C-8, Reference 20C.1 details load levels and combinations at the following locations:

- SG primary inlet and primary outlet nozzle load combinations
- Support System and Support Loads
- SG Inlet Piping Loads
- SG/RCP Loads
- SG/PRHR Pipe Loads
- SG/Feedwater Pipe Loads
- SG/Steam Line Pipe Loads
- SG/Blowdown Pipe Loads
- SG Level/Pressure Tap Connection Loads
- SG Start-Up Feedwater Nozzle Connection Loads
- SG CVS Nozzle Connection Loads
- Support and Piping Stiffness Values

Cyclic loads, such as those introduced by normal power changes, reactor trips, startup and shutdown operations, are identified as part of the Level A and Level B service loads and are included in the design base transients for fatigue evaluation. Twenty safe shutdown earthquake (SSE) transients are included as Level B loads in the fatigue analysis. The transient conditions selected for equipment fatigue evaluation are based on a conservative estimate of the magnitude and frequency of the temperature and pressure transients that may occur during plant operation.

The AP1000 plant design assessment includes consideration of a postulated circumferential break of the feedwater pipe at the junction of the feedwater nozzle and the 90º, downturning, pipe elbow connecting to the feedwater nozzle. To limit the motion of the end of the feedwater pipe under such a postulated pipe break, a pipe whip restraint is provided at an elevation approximately equal to the bottom end of the 90º pipe elbow. The pipe whip restraint is attached to the SG with two welded lugs, and pipe break loads are reacted through the pipe whip restraint back to the SG shell lugs and upper shell. The loads are provided in Reference 20C.6.

The AP1000 plant design assessment (Section 20C.3.1.3) includes consideration of seismic loading, based on the SSE transient, as part of the assessment of the Level D Service Conditions. The reports describing seismic analysis of the SG are identified in the index of technical reports (see Table 20C-11). The peak ground acceleration of the SSE has been established as 0.30g for the AP1000 design. The vertical peak ground acceleration is conservatively assumed to equal the horizontal value of 0.30g. Both horizontal and vertical design response spectra are based on the Regulatory Guide 1.60 spectra augmented at the higher frequencies. In Chapter 12, a comparison is made between these spectra and the UK generic design basis Principia Mechanica Limited (PML)[3] spectra, which are based on a 0.25g event. SSE seismic response spectra are provided in Reference 20C.1, these are the upper envelope of all reactor coolant loop (including the SG) support locations.

20C.3.1.2.2 **Environmental Specification is Clearly Defined**

The materials selected for use in the SG are selected to be compatible with the full range of internal and external environmental conditions which may be encountered over the plant life. These environmental conditions include temperature humidity, radiation, chemistry of fluid and materials in contact with the SG, and other external conditions which may affect the suitability of a material for its intended service.

During start-up, normal operation, wet layup, and heatup conditions, the SG primary and secondary sides will be exposed to a range of fluid chemistry conditions. Time dependent evaluations in the design analysis are based on adherence to controls on the internal environment of both the primary side (as specified in Table 20-22) and secondary side of the SG, which are based on the well established guidelines of References 20C.8 and 20C.9, respectively. The values presented in Table 20-22 are bounding for chemistry operational control of primary fluids that are in contact with primary system materials and nuclear fuel. The operational chemistry program may apply stricter limits as deemed appropriate. Chapter 21 provides a detailed description of water chemistry.

During hydrostatic testing, the primary and secondary sides of the SG are exposed to a test water internal environment. The quality of the test water is specified in Reference 20C.1.

The SGs will be operating in a containment building and the external environment will vary in terms of temperature, pressure, humidity, and radiation levels depending upon plant conditions. The range of environmental conditions to which external surfaces of SG will be exposed are specified in Reference 20C.1. These include all normal and abnormal operating conditions and accident conditions that are within the design basis.

3. PML spectra were developed for use as broad band spectra for use in design of UK critical facilities. They are based on the anticipated peak ground acceleration at the site and the site ground conditions.

20C.3.1.3 Compliance of SG Design with Relevant Code Requirements will Support SG Structural Reliability Claims

Section III of the ASME Code provides a well established methodology for stress analysis to provide assurance of structural integrity before a component enters service. The SG design will be assessed to confirm that stress, sizing and fatigue limits specified in Section III of the code are met.

To demonstrate that SG design will be assessed against relevant design requirements, and that future operation will be dependent upon satisfying the stress, sizing and fatigue limits specified in Section III of the ASME Code, the following analyses are discussed:

- SG design assessment against relevant stress limits.
- SG design assessment of end-of-life fatigue usage factors (FUFs).

20C.3.1.3.1 SG Design Assessment Against Relevant Stress Limits

Section III of the ASME Code establishes stress limits for design, operational, accident and testing conditions. Reference 20C.1 specifies the requirements for the design stress report that demonstrates that these stress limits are met. Analysis of the following regions of the SG is included in the scope of the SG stress analysis:

- Primary Chamber (Channel Head, Tubesheet, and Support Pad)
- Divider Plate
- Upper Shell, Transition Cone, and Lower Shell
- Steam Nozzle and Upper Head
- Heat Transfer Tubes
- Feedwater Nozzle and Thermal Sleeve
- Feedring, Feedring Supports, and Spray Nozzles
- Recirculation Port (for Maintenance Recirculation)
- Start-up Feedwater Nozzle
- Tube-to-Tubesheet Weld
- Hand Hole
- Inspection Port
- Support Trunnion
- Snubber Support Pad
- Wrapper and Support
- Tube Support Plates, Anti-Vibration Bars and Stay Rods (Lower Internals)
- Minor Nozzles (Blowdown Nozzle, Instrumentation Tap)
- Separator Region (Upper Internals)
- Secondary Manway
- Primary Manway
- Primary Nozzles

Definition of the loading conditions associated with all ASME service and testing conditions is discussed in Section 20C.3.1.2.1. The material strength properties from the ASME Code Section II are used in the design stress report. Materials used in the fabrication process will have material strength properties that meet or exceed the material strength properties used in the design basis for the design stress report as discussed in Section 20C.3.1.4.2.

The ASME stress limits are identified for each of the Level A to D Service Conditions and Testing Conditions included in the code. These form the acceptance criteria for the design

assessment, and SG components classified as HSS and Standard Class 1 are required to meet criteria specified in Section III of the ASME Code for Class 1 components. The SG design report (Reference 20C.10) provides the evidence that these criteria are satisfied. Consistency with the appropriate ASME rules provides the basic demonstration of fitness-for-purpose. The results of stress and fatigue analysis, therefore, form an important element in substantiating the structural reliability of SG components classified as HSS and Standard Class 1.

The AP1000 SG Design Report (Reference 20C.10) summarises the results of detailed analyses against the requirements of ASME Code, Section III. The scope of the analyses includes all locations identified above and all of the required loading conditions specified in Reference 20C.1. The report concludes that the results of the analyses demonstrate that all locations satisfy the structural requirements of Section III of the ASME Code.

The SG supports are described in Section 20C.1.5.1.1. The adequacy of each member of the supports is verified by solving the stress and interaction equations of ASME Code, Section III, Subsection NF and Appendix F.

Section 20.6.1 addresses the design code requirements applicable to ASME Code Class 1 components.

20C.3.1.3.2 SG Design Assessment of End-of-Life Fatigue Usage Factors

The SG is designed to meet the fatigue design criteria as defined in the ASME Code, Section III without compromising other aspects of the design. The FUFs are determined as:

- Membrane plus bending plus peak component at each location (end points of each cut).
- A combination of the total components for all thermal cases, resulting in alternating stress intensity ranges in decreasing order until all usage cycles are exhausted.
- A partial usage factor is determined by computing the ratio of the number of cycles applicable to the alternating stress range, divided by the allowable number of cycles for the same alternating stress range, as defined in the applicable ASME fatigue curve.
- A cumulative FUF is determined by summing the partial usage factors. The cumulative FUF at end of design basis component lifetime must be less than 1.0.

Critical SG design features, as identified in the previous section for stress analysis, are analysed to demonstrate that the fatigue design criteria are met. The SG Design Report (Reference 20C.10) provides evidence that the end-of-life FUFs at all locations analysed are below unity.

20C.3.1.4 SG Components are Manufactured from Suitable Materials

The recommended materials for SG fabrication are specified in Reference 20C.1 and listed in Table 20C-2 of this report. To demonstrate that suitable materials have been chosen for the fabrication of SG components, evidence to substantiate the following arguments is provided.

- AP1000 SG materials have a proven service performance.
- Material specifications meet or exceed the specifications of ASME.
- Chemical composition of materials is well controlled.
- Materials are compatible with each other and with the environment.

- Mechanical testing demonstrates compliance with relevant material specifications.

20C.3.1.4.1 **AP1000 Steam Generator Materials have a Proven Service Performance**

The selection of the AP1000 SG materials reflects international experience in PWR design, manufacture and operation to minimise the effects of through-life degradation.

The material of the Channel Head, Tubesheet and all components of the secondary shell is SA-508 Grade 3 Class 2. UK practice for PWR SGs has been to use SA-508 Grade 3 Class 1 for these components. SA-508 Grade 3 Class 2 has higher strength than SA-508 Grade 3 Class 1. This is achieved during manufacture by SA-508 Grade 3 Class 2 being tempered at a lower temperature than SA-508 Grade 3 Class 1: the nominal chemical compositions being the same. All components of the SG shell are ring forgings, this reduces the number of welds and eliminates axial shell welds.

The hot leg inlet nozzle weld and the PRHR nozzle weld incorporate safe ends, of SA-336 CL F 316LN SS and SB-564 UNS N06690 material, respectively. These are well established in the nuclear industry for application in nozzle welds.

The surfaces of the primary shell that are designed to be in contact with primary coolant are clad with austenitic stainless steel or equivalent corrosion-resistant material; the cladding is Type 308L/309L welded overlay.

Wrought Alloy 600 and its weld metals (Alloy 182 and Alloy 82) were previously used in PWRs due to the materials' inherent resistance to general corrosion in a number of aggressive environments and because of a coefficient of thermal expansion that is closer to that of low alloy and carbon steel. Primary water stress corrosion cracking has been observed in numerous Alloy 600 component items and associated welds in PWR plant, sometimes after relatively long incubation times. Alloy 600 is not used. The use of nickel-chromium-iron alloys in the SG is limited to Alloy 690 and its compatible weld metals (Alloy 152 and Alloy 52). Alloy 690 and its associated weld materials have been shown to be highly resistant to primary water system stress corrosion cracking (PWSCC). A buttering layer of Alloy 690 may be applied to the outlet nozzle and to the RCP casing in order to avoid field PWHT of the outlet nozzle to RCP casing weld.

20C.3.1.4.2 **Material Specifications Meet or Exceed ASME Specifications**

The material recommended for the SG assembly is identified in Table 20C-2. As part of the quality assurance (QA) programme, certified material test reports are to be provided to demonstrate compliance of SG materials with relevant requirements of the ASME Code Section II, where applicable. The material specification requirements include limitations on manufacturing techniques, the use of weld repairs, heat treatment, chemical composition, mechanical testing, inspection and QA. The certified material test report (CMTR) will include material test results and information on the following:

- Chemical analyses: heat and product
- Mechanical properties: tensile stress-strain, Charpy, drop weight, temperature for nil ductility transition (T_{NDT}) and reference temperature for nil ductility transition (RT_{NDT}).
- Heat treatments
- Information on archive/weldment material

- Sketches or drawings with dimensions
- A statement certifying that no weld repairs had been made (where applicable)
- Start-of-life inspection results

Supplementary Requirements are specified for SG shell components (both the primary and secondary shell) which exceed the requirements specified in ASME Section II. The Supplementary Requirements, as detailed in Reference 20C.11, are as follows:

- S1 Simulated PWHT of mechanical test samples
- S2 Ultrasonic Testing (UT) Reference Block Calibration
- S4 Additional Charpy Data
- S9 Additional restrictions on chemical composition
- S10 Alternative Fracture Toughness Requirements to establish a valid T0 fracture toughness reference temperature
- S15 Product Analysis

The heat transfer tubing is subject to heat treatment which exceeds the requirements of ASME Section II, as specified in Reference 20C.12.

Additional Supplementary Requirements are specified for SG nozzle safe-ends which exceed the requirements specified in ASME Section II. The Additional Supplementary Requirements, as detailed in Reference 20C.26, are as follows:

- Fracture Toughness of SA-336/SA-376 Type 316LN and Stainless Steel Weld Material of Nozzle Safe-Ends
- Minimum Yield Strength of SA-336/SA-376 Type 316LN and Stainless Steel Weld Material of Nozzle Safe-Ends
- Minimum Yield Strength of Inconel 52/152 (N06690) Material Associated with Nozzle Safe-Ends

Supplementary fracture toughness testing will be performed to underpin the values assumed in the defect tolerance assessment as described in Reference 20C.37.

20C.3.1.4.3 Chemical Composition is Well Controlled

The chemical composition of SG materials is controlled to minimise the content of elements that could have a detrimental effect of structural integrity. The CMTR will provide evidence to demonstrate that the composition of the materials of construction for the SG comply with the requirements of ASME Code, Section II.

SG material specification is summarised in Reference 20C.1, which provides a point of reference for detailed specification for particular materials. The cobalt content of materials in contact with the primary coolant is restricted to a maximum of 0.05% by weight. All austenitic stainless steel are solution-annealed to ensure an unsensitised condition. All

nickel-chromium-iron alloy base materials are supplied in a thermally treated condition. As identified on Reference 20C.1, the chemical composition of stainless steel and nickel-alloy materials is controlled according to requirements specified in Reference 20C.13.

References 20C.11 and 20C.12 provide detailed specification of the chemical composition of SG shell material and heat transfer tube material, respectively. The cobalt content of the tubing is limited as specified in Reference 20C.12. The chemical composition of the SG shell material is controlled to minimise the potential for material degradation. In addition, chromium content for the SG shell material is required to be greater than 0.10%.

20C.3.1.4.4 **Materials are Compatible with Each Other and with the Environment**

SG materials are selected to be compatible with each other and with the environment on the basis of proven service performance as discussed in Section 20C.3.1.4.1. The environmental characteristics both outside and within the SG are well defined as established in Section 20C.3.1.2.2, and the effect of these environments on SG materials is well understood based on the experience embodied in the codes and standards that control SG design (described in Section 20C.3.1.1.3). This ensures that the materials are resistant to age-related degradation and that material degradation characteristics are known and understood. Key aspects of design materials that help to minimise degradation in the SG environment are summarised below.

Stainless steel cladding on surfaces of the SG primary shell that are in contact with reactor coolant minimises the potential for corrosion-related degradation. The feedwater and startup feedwater nozzles are also clad on the inner surface, as described in Section 20C.1.5.1.1, to minimise the potential for corrosion-related degradation. Details of the SG insulation are specified in Reference 20C.6. In the event of coolant leakage, the ferritic materials are likely to corrode at an increased rate. Ferritic materials potentially exposed to primary coolant leakage can be readily observed as part of the in-service visual and/or nondestructive inspection programme to confirm the integrity of the component for subsequent service.

Austenitic stainless steel materials, such as those used on the nozzle safe ends, and nickel-chromium-iron alloy base materials, such the Alloy 690 heat transfer tubes, are used in the solution-annealed or thermally treated conditions. Sensitised stainless steel is not used in the SG.

High margins against PWSCC over the range of anticipated operating environments exist due to the specification of thermally treated Alloy 690 for the heat transfer tubes. Materials with a low resistance to PWSCC, such as alloy 600, are not used in the SG.

The chemical composition of all stainless steel and Ni-Cr-Fe Alloy materials is controlled, as described in Section 20C.3.1.4.3, to ensure ductility of these materials by minimising the content of low melting-point elements, their alloys and compounds. The use of low melting point elements and other contaminants in expendable materials, such as adhesives, NDE penetrant materials, rust preventatives, marking paints, tapes, ultrasonic testing couplings etc., is restricted according to limits specified in Reference 20C.1.

20C.3.1.4.5 Mechanical Testing Demonstrates Compliance with Relevant Material Specifications

SG material properties are confirmed to comply with relevant design specifications by a test programme summarised in this section. Reference 20C.1 specifies archive material that is to be retained to permit further mechanical testing of SG materials throughout plant life if required.

The mechanical testing requirements for each material are contained within the relevant material specifications as identified in Reference 20C.1. For the SG shell main forgings, the mechanical property tests will consist of Tensile Tests, Drop Weight Tests and Charpy V-Notch Impact Tests. These will be carried out in accordance with ASME Section III Section NB-2000. Mechanical property test specimens are subject to simulated PWHT following quenching and tempering. Orientation of test specimens will be as described in the ASME Code Section III, NB-2322 except that the material is not considered to be subjected to high neutron irradiation.

Charpy V-notch and dropweight fracture toughness tests will be performed on pressure boundary materials in accordance with ASME Code Section III, NB-2320 requirements.

As established by the drop weight tests, a reference temperature for nil ductility transition (RT_{NDT}) of -20.6°C (-5°F) maximum, is required of all ferritic pressure retaining material (except bolting materials). The RT_{NDT} value of -20.6°C represents a design requirement, and an RT_{NDT} of -12.2°C (10°F) is conservatively adopted in the design analyses for many of the SG forgings, with the exception of the Tubesheet and transition cone which require -20.6°C. An RT_{NDT} of -28.9°C (-20°F) maximum, is required of the main feedwater nozzle and startup feedwater nozzle materials.

On pressure boundaries, material for bolting and other fasteners with nominal diameters exceeding 25.4 mm (1 in) will meet the minimum requirements of 25 mils lateral expansion and 61 Nm in terms of Charpy V-notch tests conducted at the lesser of 0°C, the lowest service temperature or the preload temperature.

20C.3.1.5 Suitable Controls Ensure SG Manufacturing Quality

The processes used to manufacture the SG are controlled by well established codes and standards to ensure a quality of manufacture commensurate with structural reliability targets. Procedural controls of manufacturing processes are identified in the index of technical reports (Section 20C.7) and the codes, standards and regulations applied to ensure manufacturing quality are identified in Table 20C-5. The evidence to demonstrate suitable control of manufacturing quality is summarised in this section as follows:

- The SG manufacturer will be suitably experienced.
- SG manufacturing quality will comply with ASME Section III requirements as a minimum.
- Welding will be conducted by suitably qualified and experienced operators in accordance with suitable and well-established procedures.
- Repairs and deviations from the design intent are controlled and will be recorded.
- Manufacturing and procedural controls ensure quality of forging material.
- SG manufacture is supported by a robust QA programme.

20C.3.1.5.1 The SG Manufacturer will be Suitably Experienced

The supplier for the SG has not yet been selected and a technical evaluation of the suppliers' ability to comply with the Design Specification (Reference 20C.1) will form part of site specific justification following generic design assessment (GDA). The Design Specification identifies a range of documentation to be provided by the supplier to demonstrate compliance with the specification and to demonstrate that all responsibilities defined in ASME Code, Section III for the "Manufacturer" have been fulfilled.

QA requirements are specified, giving particular attention to the suppliers' ability with regard to achievement of the material compositional requirements including minimum fracture toughness requirements, the methods for the qualification of weld procedures and the ability to carry out the required range of inspections during manufacture. QA arrangements are discussed in Section 20C.3.1.5.6; these include requirements for the supplier to provide detailed fabrication and inspection plans for Westinghouse review and approval. The plans are subject to Westinghouse approval prior to commencement of manufacturing activities, and will define hold or witness points throughout the manufacturing process to provide an additional means of monitoring the quality of manufacture.

20C.3.1.5.2 SG Manufacturing Quality will Comply with ASME Section III Requirements as a Minimum

Design and fabrication of the SG is carried out in accordance with ASME Code, Section III. The pressure-retaining parts of the SG, including the primary and secondary pressure boundaries, are designed to satisfy the relevant criteria of the ASME Code. Compliance with the code and the experience embodied within the code provides a high degree of confidence that high quality will be achieved and also that the SG will be to tolerant to minor variations in material properties and minor imperfections in fabrication. Supplementary requirements that are more stringent than those in the ASME Code provide additional assurance of the quality of SG design and manufacture and further support to structural integrity claims.

The Design Specification (Reference 20C.1) provides the basis to establish how the design and construction of the SG is to conform to the rules set forth in the ASME Code, as described throughout Leg 1 of this safety argument. The manufacturer will provide a certificate of compliance or equivalent document as evidence that the SG is in conformance with all standards, specifications, codes and procedures specified in Reference 20C.1. Sections 20C.3.1.4.2 and 20C.3.1.6.1 identify supplementary requirements, more stringent than those specified in the ASME Code, relating to SG material specification and manufacturing inspection, respectively.

20C.3.1.5.3 Welding will be Conducted by Suitably Qualified and Experienced Operators in Accordance with Suitable and Well-established Procedures

All SG pressure boundary welding procedures and welder qualifications will be in accordance with ASME Sections IX and III Subsection NB, and all non-pressure boundary welding procedures and welder qualifications will be in accordance with ASME Section IX or equivalent pre-approved standards. Supplementary codes and standards to control welding procedures and welder qualification are identified in Table 20C-5. Specification of weld materials, together with controls on weld procedures and qualification are identified in the index of technical reports (see Table 20C-11).

Fracture toughness testing of weld qualification samples and weld filler metal will be in accordance with ASME Section III and the supplementary requirements identified in

Section 20C.3.1.4.2. The manufacturer is required to provide plans describing welding procedures, along with PWHT procedures, for Westinghouse approval prior to initiating any welding. Welder qualification records are to be retained by the manufacturer.

20C.3.1.5.4 **Repairs and Deviations from the Design Intent are Controlled and will be Recorded**

A requirement to record major/minor repairs and deviations for the design intent is identified in the SG Design Specification (Reference 20C.1). Reporting of defects and noncompliance is carried out in accordance with United States Code of Federal Regulations 10 CFR 21, as identified in Table 20C-5. Deviation notices and nonconformance reports provide the manufacturer with a procedure to record all conditions that do not meet design requirements.

All major repairs to base material and pressure boundary welds will be subjected to formal review by Westinghouse before approval to proceeding with the repair is granted. As specified in Reference 20C.11, weld repairs to the SG shell are not permitted.

The manufacturer is required to provide a certificate of compliance or equivalent document to confirm that the SG conforms with all standards, specifications, codes and procedures identified in the Design Specification (Reference 20C.1) with the exception of any referenced approved deviation notices. Westinghouse will provide a Certificate of Conformance to confirm the acceptability of the certificate of compliance as part of the QA records described in Section 20C.3.1.5.6. These documents are to provide safety justification of any repairs and deviations from the design intent for site specific AP1000 safety cases following the GDA.

20C.3.1.5.5 **Manufacturing and Procedural Controls Ensure Quality of Forging Material**

Reference 20C.11 provides the material specification for the SG forgings that are of SA-508 Grade 3 Class 2 and details aspects including control of chemical composition, microstructure, heat treatment, materials testing, grain size evaluation and NDE. These represent a range controls to ensure that the forging material complies with the requirements of the ASME Code, Section III, Subsection NB for Code Class 1 components. Reference 20C.11 also specifies certain requirements more stringent than and/or supplemental to those in the Code, as identified in Section 20C.3.1.4.2.

20C.3.1.5.6 **SG Manufacture is Supported by a Suitable Quality Assurance Programme**

Quality assurance for the design, procurement, fabrication, inspection, and testing of the SG is performed in accordance with the quality plan described in Westinghouse Electric Corporation Quality Management System (QMS) (Reference 20C.14) to, as a minimum, satisfy the requirements of References 20C.15 to 20C.17. In addition, for all SG pressure boundary components and services, the QA programme will be in compliance with the requirements of Reference 20C.18. Supplementary QA requirements are also identified in Table 20C-5.

The QA programme is to be supported by a clear auditable trail of records that are to be maintained as part of the manufacturing process. These are to be provided during the construction stage of the AP1000 plant to provide evidence that the manufacturing programme is compliant with QA requirements and the codes and standards applied in SG design and manufacture. The Design Specification identifies requirements for records to be maintained by the manufacturer that are to identify details of the following aspects:

- Weld procedures
- Heat treatment

- Material Records including CMTRs
- A certificate of compliance with Reference 20C.1, including deviation notices and non-conformance reports (NCRs)
- Manufacturing Inspections
- Dimensional checks
- Cleaning and contamination protection procedures

20C.3.1.6 Manufacturing and Pre-Service Inspections Confirm Quality of Manufacture

Manufacturing inspections and PSI includes NDE that are conducted to confirm the absence of structurally significant defects. These examinations are carried out according to well established and suitably rigorous techniques that provide a capability for detection of structurally significant defects that is commensurate with the structural reliability claimed for the SG component to which they are to be applied. Evidence to substantiate this claim is provided in Sections 20C.3.1.6.1 to 20C.3.1.6.3 as follows:

- Manufacturing and Pre-Service inspections meet or exceed the requirements of the ASME Code.

- NDE Qualification for HSS Components Ensures Suitably Rigorous Inspection.

- SG design facilitates effective NDE.

20C.3.1.6.1 Manufacturing and Pre-Service Inspections Meet or Exceed the Requirements of the ASME Code

As identified in Section 20C.3.1.4, experience shows that the materials used in the manufacture of the SG lead to a low frequency of defect occurrence. NDE applied at key stages in the manufacturing programme provide further evidence to demonstrate a low frequency of significant defects in forgings and welds.

The manufacturing inspection and PSI programme for the SG will include a diverse range of methods for NDE. A NDE programme is to be produced by the manufacturer to identify how the requirements of the ASME Code and the Design Specification (Reference 20C.1) will be satisfied. The plan will list components and weldments versus the type of NDE to be made. The manufacturer will provide a NDE Inspection Report for each required examination and will include the following in addition to the information required by ASME Code Section III, Section V, and Section XI:

- Fabricator's name
- Purchase order number
- Name of part and part identification number
- Method and procedure used
- Records of Examination Calibrations
- Results of examination
- Personnel qualifications

Any repairs made as a result of NDE findings are subsequently inspected using the same NDE method(s) that originally detected the defect leading to the repair.

NDE will be carried out only by personnel qualified and certified in accordance with the following:

- "Recommended Practice No. SNT-TC-1A, Non-Destructive Testing, American Society for Non-destructive Testing"

- ANSI/ASNT CP-189 "ASNT Standard for Qualification and Certification of Non-destructive Testing Personnel, as amended by ASME Section XI, IWA 2300 and ASME Section III, NB-5500."

NDE results will be interpreted only by personnel certified as Level II, IIa (ET only), or III.

Each of the heat transfer tubes, prior to installation, is to be subjected to a hydrostatic test in accordance with the requirements of ASME Section II SB-163, except that the hydrostatic test pressure will be in accordance with Reference 20C.12. All tubes exhibiting leakage will be rejected.

A gas leak test will be performed to confirm the integrity of the tube-to-Tubesheet welds. The tube-to-Tubesheet helium gas leak test is to be performed after tack expansion and tube welding but before liquid penetrant testing of the tube-to-Tubesheet weld and hydraulic expansion of the tubes.

Sensitive volumetric and surface NDE methods are applied at specified points in the manufacturing programme to ensure any necessary repairs are undertaken at the earliest possible stage and that any degradation resulting from processes such as PWHT is identified. Supplemental inspections, additional to those specified by ASME Section III, are performed that match the pre-service inspection and in-service acceptance criteria of ASME Section XI. Here the objective is to reconcile the difference in acceptance standards between ASME Section III and ASME Section XI and ensure that the PSI does not report rejectable defects that were not identified during the standard manufacturing NDE. The codes, standards and other requirements applied to the diverse range of NDE techniques for manufacturing inspection and PSI are summarised below:

Ultrasonic Testing (UT)

UT examination will be performed in accordance with the following requirements and the codes referenced in the Design Specification:

- Materials – ASME Section III, NB-2000

- Cladding – ASME Section III, NB-5000

- Welds – ASME Section III, NB-5000

- Thickness – ASME Section V, Article 5

- Pre-service Inspection – ASME Section III and ASME Section XI, IWA 2000, IWB 2000, IWC 2000

UT examination of the SG heat-transfer tubes is specified in Reference 20C.12. Cladding on surfaces of the Channel Head bowl, nozzles, manways, and the Tubesheet primary flat face will be UT inspected for 100% of the volume for bond, defects, and thickness by the straight beam method where accessible. Cladding on the steam outlet nozzle for venturi attachment will be UT inspected for bond and defects by the straight beam method. Clad thickness will be measured in accordance with a procedure that will be submitted to the designer for review

and approval. After welding of the divider plate to the Channel Head, the cladding beneath the divider plate will be inspected for lack of bond.

Magnetic Particle Inspection (MT)

MT will be conducted in accordance with ASME Code Section V, Article 7 and to the applicable sub-articles of Section III, Subsection NB-5000 of the ASME Code. In addition to ASME Code requirements, magnetic particle inspection is specified for the following components:

- Tubesheet forging
- Channel Head forging
- Nozzle forgings
- Nozzle to shell (if not integral) weldment
- Support bracket weldments
- Instrument connections (secondary) weldments
- Temporary attachment, after removal, weldments
- Accessible pressure-retaining welds after hydrostatic test

Eddy Current Test (ECT)

Each straight finished heat-transfer tube will be tested during manufacture but before bending in accordance with ASME Section III and Reference 20C.12. ECT of each finished U-bend tube will be examined along the entire tube length using the guidelines of ASME Section XI and Reference 20C.12. After expanding the tubes in the Tubesheet, a 100% inspection will be conducted to measure the inside diameter of each expanded tube throughout the entire thickness of the Tubesheet in order to assess the quality of the expansion operation. Periodic ECT of SG tubes during service is described in section 20C.3.4.2.

Radiography

Radiographic inspection and acceptance will be in accordance with ASME Code Section V, Article 2, except as modified by the requirements of ASME Code Section III, Subsection NB-5000 and as follows:

- Compliance with radiographic density limitations will be determined using calibrated densitometers and density strips.

- Fluorescent screens are not permitted.

- All production radiographs are to be reviewed and approved by the manufacturer.

- Film processing and storage practice will be identified in the radiographic procedure. Storage will be in accordance with the requirements of ANSI N45.2.9.

Liquid Penetrant Test

Liquid penetrant inspection of pressure boundary components will be performed in accordance with ASME Code Section V, Article 6 and to the applicable sub-articles of Section III, Subsection NB-5000 of the ASME Code. Liquid penetrant inspection of non-pressure boundary components will be performed in accordance with ASME Code Section V, Article 6 and to the applicable sub-article of Section III Subsection NB-5000 or NG-5000 of the Code. Liquid penetrant examination will be performed whenever radiography or UT examination of nonmagnetic material is required or when accessibility limitations prohibit the use of MT equipment in magnetic materials. In addition to ASME Code requirements, liquid penetrant examination is required for the following components:

- Weld deposited Tubesheet cladding
- Channel Head cladding
- Divider plate-to-Tubesheet weldment
- Divider plate-to-Channel Head weldment
- Weld deposit cladding

Visual Examination of Welds

Visual examinations will be in accordance with ASME Code Section III and the supplemental requirements and acceptance criteria specified in Reference 20C.1.

Pre-Service Testing

Upon completion of the ASME Section III hydrostatic pressure test (Section 20C.3.2.1) and prior to shipment of the SG assemblies, a baseline Pre-Service NDE programme is to be conducted. This will include volumetric UT and surface examinations of all welds requiring in-service inspection (ISI) as defined by Section XI of the ASME Code. The Design Specification defines the Weld Surface Requirements to facilitate these inspections.

20C.3.1.6.2 **NDE Qualification for HSS Components Ensures Suitably Rigorous Inspection**

HSS welds and forgings are identified in Table 20C-4. Qualified UT volumetric inspections are to be conducted on the HSS locations to provide a very high level of confidence that the SG enters service free of any structurally significant defects. The qualified inspections provide additional high reliability inspections at the end of all manufacturing stages and also generate a “finger-print” set of data against which future ISI results can be compared.

The requirement for qualified inspection of HSS locations is specific to the UK AP1000 Safety Justification and supplements the requirements of the design specification (Reference 20C.1). As described in Section 20C.3.3, target sizes for manufacturing defects for selected HSS welds have been derived from elastic-plastic fracture mechanics by calculating the end-of-life limiting defect sizes and fatigue crack growth in accordance with the R6 methodology.

NDE performed with well established UT techniques will provide a “detect and reject” capability that demonstrates a defect size margin (DSM) of 2 or greater. The basis for this is discussed in Section 20C.3.3. High reliability for these inspections will be demonstrated through qualifying aspects of the inspection system, including procedure, equipment, and personnel, using the principles specified in the European Network for Inspection and Qualification (ENIQ) methodology for qualification of nondestructive tests (Reference 20C.20). For each of the selected HSS locations, a manufacturing inspection plan

has been produced which provide the physical reasoning underpinning the claimed inspection capability. These are discussed in Section 20C.3.3.1.3 below. The manufacturing inspection plans were developed following a process (Reference 20C.36) which is based on the preparation of technical justifications described in ENIQ methodology. A process will be developed in due course to address parent material associated with HSS locations.

20C.3.1.6.3 SG Design Facilitates Effective NDE

The SG design has been assessed to satisfy ASME Code Section III requirements for inspectability, as reported in Reference 20C.19. The design of the SG includes enhancements to facilitate inspection, as described in Section 20C.3.1.1.2. Aspects of SG design to facilitate inspection include access arrangements for personnel and equipment, access for deploying angle beam UT to give full volumetric coverage and provision for access to as many inspection surfaces/scanning directions as possible. Requirements specifying the quality of surface finish to facilitate inspection are specified in Reference 20C.1.

The SGs permit access to tubes for inspection, repair, or plugging, if necessary. Tooling to install mechanical and welded plugs, tube repair sleeves, or effect other repair processes remotely can be delivered robotically. In addition, the SG includes features to enhance robotics inspection of SG tubes without manned entry of the channel head. These include a cylindrical section of the channel head, primary manways, and provisions to facilitate the remote installation of nozzle dams.

20C.3.1.7 Plant Operation and Maintenance

Detailed specification of the control of plant operation and maintenance is to be defined at the nuclear site licencing stage. Issues of safety with respect to generic design and design measures identified in this section demonstrate that well defined and conservative operating parameters will be established. These measures provide a foundation for subsequent definition of site-specific operating rules and maintenance controls. The SG design includes engineered protection against transgression of operating rules. The following aspects are addressed:

- Procedural Control of Thermal and Hydraulic Operating Parameters
- Control of water chemistry to minimise SG corrosion.
- Overpressure Protection.

Plant operating and maintenance procedures, records of operation and maintenance to confirm compliance with procedural controls, and the record and investigation of any transgression of operating parameters will form part of the site-specific QA programme to be specified subsequent to the GDA.

20C.3.1.7.1 Procedural Control of Thermal and Hydraulic Operating Parameters

Procedural controls of thermal and hydraulic operating parameters are defined to identify a safe operating envelope for the SG. Operating within these limits of pressure and temperature minimises the possibility of brittle fracture.

Pressure and temperature (P/T) limits for primary coolant are to be determined for each fluence period in a pressure and temperature limits report. Further details of the P/T limits for the RCS are provided in section 20A.2.1.7.1, and their derivation has been carried out in accordance with an approach defined in Reference 20C.21. Limiting conditions for operation

(LCOs) specify minimum requirements for ensuring safe operation of the plant. The following LCOs are relevant to the control of primary side P/T limits.

- LCO 3.4.3, "RCS P/T Limits"
- LCO 3.4.14, "Low Temperature Overpressure Protection (LTOP) System"
- LCO 3.4.2, "RCS Minimum Temperature for Criticality"

Operation within the LCOs ensures the plant is operated under analysed conditions and brittle failure of the reactor coolant pressure boundary (RCPB) is unlikely. In the event that these limits are exceeded, an evaluation must be performed to determine the effect on the structural integrity of the RCPB components. ASME Code, Section XI, Appendix E provides a recommended methodology for evaluating an operating event that causes an excursion outside the limits.

A Thermal-Hydraulic Design Data Report is produced at the manufacturing stage to describe expected performance of the SG at steady state from 0 to 100% power in design basis and best-estimate conditions.

20C.3.1.7.2 Control of Water Chemistry to Minimise SG Corrosion

Specification of primary coolant and feedwater chemistry is identified in Section 20C.3.1.2.2. The CVS provides a means for adding chemicals to the reactor coolant water and the SG Channel Head incorporates a CVS nozzle to facilitate chemical dosing of primary coolant. The chemicals perform the following functions:

- Control the pH of the coolant during pre-startup testing and subsequent operation
- Scavenge oxygen from the coolant during heatup
- Control radiolysis reactions involving hydrogen, oxygen, and nitrogen during power operations following startup

These functions serve to minimise the potential for degradation due to corrosion of SG primary side internal surfaces that are exposed to primary coolant. Details of the secondary chemistry are presented in Chapter 21.

20C.3.1.7.3 SG Design Includes Protection Against Over Pressurisation

Transgression of the procedural control of thermal and hydraulic operating parameters discussed in Section 20C.3.1.7.1 could potentially result in over pressurisation of the SG. The SG design includes engineered safeguards to provide diversity of protection against over pressurisation.

Reference 20C.1 specifies that relief devices are to be provided to limit the maximum primary and secondary side pressure to 110% of the design pressure. The relief devices, if necessary, may be located outside of the SG jurisdictional boundary so that the overpressure protection requirements of the SG are fully complied with and the safety relieving devices cannot be isolated from the SG during operation. The primary side overpressure protection will comply with ASME Code, Section III rules for Class 1 components and the secondary side overpressure protection with the equivalent rules for Class 2 components.

20C.3.2 Leg 2: Functional Testing

Functional testing provides confirmation that the high standards applied in SG design, fabrication and installation identified in Section 20C.3.1 result in an installed component that is fit for purpose. Evidence of planned pre-service testing, to demonstrate that the SG will enter service fit-for-purpose, is identified as follows:

- **Section 20C.3.2.1** Hydrostatic pressure tests are specified to verify that the SG is proofed against its design pressure.
- **Section 20C.3.2.2** An initial plant testing programme confirms functionality of the SG.

20C.3.2.1 Hydrostatic Pressure Tests are Specified to Verify that the SG is Proofed Against its Design Pressure

Pressure testing is specified to verify integrity of SG pressure boundaries at design pressure prior to operation. Hydrostatic pressure testing of both the primary and secondary sides provides assurance regarding the basic strength of the assembled SG, confirms the absence of gross manufacturing defects and provides early warning of any out of specification material properties. Details of the SG hydrostatic pressure testing requirements are specified in Reference 20C.1; these include testing of the heat transfer tubes, the primary side pressure boundary and the secondary side pressure boundary. At locations where defect tolerance may be dominated by thermal stresses additional assurance of structural reliability is provided by manufacturing and pre-service inspections to confirm the absence of structurally significant defects at start of component life (section 20C.3.1.6.1). In the case of the HSS components of the SG, these are qualified inspections supported by defect tolerance justifications (section 20C.3.3.1). The programme of hydrostatic testing specified for the SG is summarised below.

Hydrostatic pressure testing is planned for both the primary and secondary sides of the SG both at the end of the manufacturing process and following installation, before entering service. These are known as shop and field tests, respectively. For design purposes it is conservatively assumed that the SG will experience 10 cycles of these tests and these hydrostatic test cycles are included in the stress and fatigue analyses. Additional, lower-pressure primary side hydrostatic tests may be performed to meet the in-service inspection requirements of ASME Code, Section XI, Sub article IWB-5200. Four such tests are expected over the design lifetime. The increase in the FUF caused by these tests is covered by the primary-side leakage tests that are considered for design.

The manufacturer is required to conduct hydrostatic tests of the primary and secondary sides of the SGs in accordance with ASME Section III, Subsection NB of the ASME Code. Compliance with these well established rules for the proof testing of pressure vessels against design pressure provides a demonstration of structural reliability before the SG enters service.

The required hydrostatic test pressure of 1.25 times the design pressure for both primary and secondary sides will be applied for a minimum of 10 minutes. The pressure will then be reduced to the design pressure and held for at least four hours while the primary side or secondary side is examined for leaks. No tubes will be plugged before hydrostatic testing without prior written approval by the appropriate authority (normally the buyer).

The primary side hydrostatic test pressure is to be applied at metal and water temperatures high enough to ensure that the metal is at least 33°C above its nil-ductility transition

temperature. The nil-ductility transition temperature (T_{NDT}) is determined as an outcome of the material properties testing described in Section 20C.3.1.4.2. In no case will the hydrostatic test temperature be less than 21.1°C (70°F). The maximum primary side hydrostatic test temperature is 121.1°C (250°F). The temperature for the secondary side hydrostatic test will not exceed 82.2°C (180°F).

Controls on the chemistry of water used for hydrostatic tests and final equipment flushes are detailed in Reference 20C.1. A report will be provided by the manufacturer to confirm that the results of the hydrostatic test of the SG conform to the requirements of the ASME Code Section III.

Section 20C.3.1.6 describes the NDE to be conducted following the SG hydrostatic pressure tests. These are to ensure that the ASME Section XI pre-service examination acceptance criteria can be satisfied and confirm that the SG has sustained no significant damage as a result of the hydrostatic testing.

20C.3.2.2 An Initial Plant Testing Programme Confirms Functionality of the SG

Section 7.5 identifies an initial testing programme for AP1000 plant. The overall objective of the programme is to demonstrate that the plant has been constructed as designed, that systems perform consistent with the plant design, and that activities culminating in operation at full licensed power including initial fuel load, initial criticality, and power ascension are performed in a controlled and safe manner.

The pre-operational tests are applied to entire systems, rather than specific components. A series of start-up test procedures are also specified to confirm safe and controlled operation during activities culminating in operation at full licensed power. As is the case for pre-operational testing, these start-up tests are applicable to systems rather than individual components such as the SG.

The purpose of the RCS pre-operational testing is to verify that the as-installed RCS properly performs the following safety-related functions:

- Provide RCS pressure boundary integrity.
- Provide core cooling and boration in conjunction with the passive core cooling system.
- Measure process parameters required for safety-related actuations and safe shutdown.
- Measure selected process parameters required for post-accident monitoring.
- Vent the reactor vessel head.

Pre-operational testing of the RCS is also performed to verify that the system properly performs the following defence in depth functions:

- Provide forced circulation cooling of the reactor core in conjunction with heat removal by the SGs.

- Provide core cooling by natural circulation of coolant in conjunction with heat removal by the SG(s).

- In conjunction with the SG(s) and normal residual heat removal system, provide the capability to remove core decay heat and cool the reactor coolant to permit the reactor to be refuelled and started up in a controlled manner.

- Provide pressuriser pressure control during normal operation.

- Provide pressuriser level control in conjunction with the CVS.
- Provide pressuriser spray.

The purpose of the SGS pre-operational testing is to verify that the as-installed components properly perform the following safety-related functions:

- Provide SG isolation, including isolation of the main steam lines, feedwater lines, and blowdown lines.
- Remove heat from the RCS and provide secondary side overpressure protection.
- Measure process parameters required for safety-related actuations.
- Measure process parameters required for post-accident monitoring.

SGS pre-operational testing is also to verify that the as-installed components properly perform the following defence in depth functions:

- Provide heat removal from the RCS
- Provide overpressure protection for the SGs to minimise required actuations of spring-loaded safety valves
- Measure process parameters and provide actuation signals for the diverse actuation system

20C.3.3 Leg 3: Failure Analysis

Leg 3 of the safety case provides an assessment of the effects of through-life degradation mechanisms on potential manufacturing defects to show that such mechanisms will not threaten vessel integrity over the plant design lifetime. This goes beyond ASME design code requirements to provide a further demonstration of integrity for HSS components of the SG, specifically by recognising that flaws may be present following manufacture and demonstrating tolerance to them over the design lifetime of 60 years. The arguments supplement the Leg 1 aim of avoidance of defects, by the stringent control of quality of design and manufacture, to provide a safety case with both defect avoidance and defect tolerance.

20C.3.3.1 HSS Components of the SG are Tolerant to Manufacturing Defects for the Design Life of the Plant

This section describes the scope of the analyses undertaken as part of the GDA process to demonstrate that the SG is tolerant to potential defects that could remain undetected after manufacturing inspection. Evidence to demonstrate that the analyses substantiate the claimed defect tolerance of the HSS components is provided in this section as follows:

- The methods planned for defect tolerance assessment are well established.
- The defect tolerance assessments will adequately address through-life crack growth
- Defect tolerance assessments establish allowable start of life (SoL) defect sizes that are to be judged against the qualified examination defect size (QEDS).

20C.3.3.1.1 The Methods Planned for Defect Tolerance Assessment are Well Established

As discussed in section 20.6.4.2, the following sections describe the results of the R6 assessment for the SG and present a summary of the existing linear elastic fracture mechanics (LEFM) assessment carried out in accordance with ASME Code, Section III, Appendix G.

Assessment using the R6 Methodology

In combination with the use of rigorous manufacturing controls and inspection qualification, the defect tolerance assessment provides the necessary understanding to support the claim, to an appropriate degree of confidence, that the SG will enter service free from defects that could be of concern throughout the designed life. The approach to determination of the limiting defect size in a particular orientation and location and the maximum allowable SoL defect size is discussed in section 20.6.4.2. As has been stated in Reference 20C.23, the regulatory expectation is that a defect size margin of 2 will be achieved.

Phase 1: Weld Defect Tolerance and NDE Ranking

A detailed evaluation of selected, limiting weld locations has been made available to provide confidence that there are no regions of the SG where either low defect tolerance or low NDE inspectability would preclude the SG design from being able to satisfy regulatory expectations and support the safety claims for the SG. To evaluate those locations with the greatest risk of entering service with defect of structural significance, either as a result of small allowable SoL defect sizes or a large QEDS, a ranking exercise has been undertaken to consider, on a relative basis, the defect tolerance and the NDE inspectability at each of the AP1000 SG weld locations. The details of this evaluation are reported in Reference 20C.24 and provide the justification for selection of the following SG welds for assessment in Phase 2:

- Lower Shell Barrel A to Tubesheet
- SG Main Feedwater Nozzle to Shell
- Inlet Nozzle to Safe-End

Phase 2: Assessment of Bounding Locations

A limited number of locations were selected for more detailed evaluation in Phase 1. By examination of the primary and secondary loading, it is possible to present quantitative arguments to show that other regions are bounded by the locations that have been assessed. The justification that these locations bound other SG locations classified as HSS is established in Reference 20C.24.

For each of the selected locations, the R6 methodology (Reference 20C.22) was used to determine the defect size margin, which is the margin between the QEDS and the allowable SoL defect size. The allowable defect size is determined using the end of life limiting defect size (ELLDS) and the lifetime fatigue crack growth (LFCG). Details of the assessment methodology are provided in Reference 20C.26. Assessments have been carried out for defects both parallel and transverse to the weld. Material fracture toughness properties reflect the end of life and the supplementary testing described in Reference 20C.37 will be performed to underpin the values assumed. LFCG) was evaluated using appropriate upper bound crack growth laws.

As discussed in Section 20C.3.3.1.3, the results of the defect tolerance assessment can be used to inform an evaluation of the adequacy of the NDE capability at each of the highest ranked locations.

Phase 3: Assessment of Remaining Locations

The full defect tolerance assessment of the remaining HSS locations, including the selected locations in the parent material, will be carried out as part of subsequent assessments. Once completed, the R6 assessment work for the SG will provide assurance that the QEDS is based on a robust assessment of the maximum allowable SoL defect size with appropriate consideration of materials ageing and degradation and through life crack growth.

ASME Code, Section I III, Appendix G Linear Elastic Fracture Mechanics Assessment

The ASME Code, Section III, Appendix G, "Protection against Non-ductile Failure", presents a method for obtaining the allowable loadings to protect against non-ductile failure for ferritic pressure-retaining materials in Class 1 components. Although this approach is not considered sufficient in a UK regulatory context, the results of the assessment nonetheless provide a conservative assessment of defect tolerance which is recognised internationally.

The method given in Appendix G of the ASME Code, Section III is based on the principles of LEFM. At each evaluated location, a postulated defect is assumed. Typically, this is conservatively based on a quarter wall defect; although at certain locations, ASME permits smaller defects to be used. At each location, the mode-I stress intensity factor, K_I, produced by each of the specified loadings is calculated. Then, the summation of the K_I values due to primary and secondary stresses resulting from mechanical and thermal loading during normal, upset, and test conditions is compared to a referenced stress intensity factor, K_{IR}. This reference K_{IR} is the highest critical value of K_I allowed for the material and the temperature involved. An Appendix G assessment is specified in Reference 20C.1. The results of the Appendix G non-ductile failure evaluation are provided in Reference 20C.10. This confirms that the ASME requirements are satisfied.

20C.3.3.1.2 The Defect Tolerance Assessments will Adequately Address Through-life Crack Growth

As part of the R6 assessment the through life crack growth has been calculated in accordance with the procedures specified in the R6 procedure. This includes the use of suitable conservative crack growth rates appropriate to the reactor coolant environment. As discussed in Reference 20C.26, these are based on the ASME upper bound fatigue crack growth curves. These are considered to be conservative for modern steels with low sulphur content. The upper bound nature of these curves is supported by extensive testing worldwide.

20C.3.3.1.3 Defect Tolerance Assessments Establish Allowable SoL Defect Sizes that are to be Judged Against the Qualified Examination Defect Size

The results of the R6 defect tolerance assessments for the three limiting SG welds identified in Section 20C.3.3.1.1 are reported in Reference 20C.29. A limiting QEDS, i.e., that leading to a DSM equal or larger than 2, is calculated for one of two different defect aspect ratios according to flaw orientation. For flaws perpendicular to the weld axis, the QEDS is established for a defect aspect ratio of 2, since the potential length of flaws with that orientation is naturally limited by the weld width. For flaws oriented parallel to the weld axis, it is recognised that flaws with higher aspect ratios may potentially occur, and a defect aspect ratio of 6 is additionally considered in determining QEDS.

Reference 20C.29 reports the calculated limiting QEDS for the SG welds as follows:

Weld	Limiting QEDS (mm)	
	Aspect Ratio = 2	Aspect Ratio = 6
SG Primary Inlet Nozzle to Safe End	6	6
SG Lower Barrel A to Tubesheet	15	15
SG Main Feedwater Nozzle to Shell	15	10

Demonstrating the capability for qualified inspection of these SG welds is considered bounded by the inspection techniques defined and assessed for other AP1000 HSS welds as summarised below:

- Inspection qualification of the SG primary inlet nozzle to safe end weld is considered bounded by the inspection plan for the reactor pressure vessel (RPV) inlet nozzle to safe end weld (Reference 20C.30) where a QEDS surface/near surface defect height of 6mm (approximately 0.24 in) is technically justified. Both are dissimilar metal welds with a coarse-grained austenitic structure and both welds allow inspection access to both the inner and outer surfaces as well as the safe-end end face.

- Inspection qualification of the SG lower barrel A to Tubesheet weld is considered bounded by the inspection plan for the pressuriser (PZR) surge nozzle to safe end weld (Reference 20C.31) where a QEDS surface/near surface defect height of 5mm (approximately 0.2 in) is technically justified. The lower barrel A to Tubesheet weld is a ferritic weld joint between two ferritic forgings with no austenitic stainless steel cladding and good access to both the inner and outer surfaces for inspection techniques. The PZR surge nozzle to safe end weld is a dissimilar metal weld and difficult to effectively inspect. Inspection techniques can be applied in line with previous work associated with the Sizewell B manufacturing non-destructive test (NDT) inspections, the United Kingdom Atomic Energy Agency defect detection trials (DDT), qualified inspections used in Sweden and the US, and common industry approaches.

- Inspection qualification of the SG main feedwater nozzle to shell weld is considered bounded by the inspection plan for the PZR upper head to upper shell weld (Reference 20C.32) where a QEDS surface/near surface height of 10mm (approximately 0.4 in) is technically justified. Both welds are ferritic steel, however the main feedwater nozzle to shell weld does not have stainless steel cladding and benefits from greater accessibility for applying the inspection techniques.

The inspection plans identified above are considered to demonstrate that the capability exists to develop and justify suitable inspection techniques for the SG HSS welds, each to be qualified against a limiting QEDS, as determined by defect tolerance assessment, such that a satisfactory DSM (DSM $\geq$ 2) can be justified. Specific inspection plans for the SG HSS welds will be developed and validated as part of the future safety case development.

20C.3.4 Leg 4: Forewarning of Failure

Legs 1 to 3 of the safety argument identify measures aimed at the avoidance of defects at start of service and throughout component lifetime. Leg 4 provides additional assurance that structural integrity will be maintained by identifying measures to provide timely warning of any structurally significant defects that, in spite of the diverse measures identified in Legs 1 to 3, may be present at SoL or develop during service. The measures identified to provide forewarning of failure are intended to reveal component degradation before any defect could grow to an extent that may threaten the structural integrity of the SG, and thus enable corrective action to be taken to ensure that plant safety is maintained. ISI and detection of leakage provide forewarning of structural failure of the SG, as described below.

20C.3.4.1 Planned In-Service Inspection will Provide Forewarning of Failure

In order to provide assurance that any defects will be detected prior to becoming a threat to the structural integrity of the SG, a programme of ISI is planned. This provides a means of detecting degradation due to anticipated damage mechanisms, provides a means of monitoring any growth of known defects to provide assurance that these remain of a tolerable size, and also provide a contingency measure to detect defects that may unexpectedly arise as a result of unanticipated degradation mechanisms. Qualified techniques and operators are planned for inspection of the most safety-significant (HSS) locations of the SG to ensure that the measures to provide forewarning of failure at these locations are highly reliable. The aspects of the ISI programme described below provide evidence of effective arrangements to provide forewarning of failure:

- An extensive programme of ISI will identify any degradation long before failure.
- Qualified inspection of HSS welds provides highly reliable ISI.
- ISI provides data to monitor and judge in-service defect formation and growth.
- Planned locations for ISI are accessible and inspectable.

20C.3.4.1.1 An Extensive Programme of ISI will Identify any Degradation Long Before Failure

ISI is the preferred method for provision of forewarning of failure. The role of an effective ISI programme is twofold: firstly to detect and monitor anticipated degradation, and secondly to confirm the absence of any unanticipated degradation. ISI is used to confirm the absence of defects that could give rise to gross structural failure: such judgements are based on a comparison of the size of detected defects with a maximum tolerable defect size, as determined by fracture analyses (Section 20C.3.3), combined with a conservative assessment of in-service defect growth throughout the inspection interval.

To be effective, ISI requirements should be identified according to established good practice relevant to the characteristics of each inspection location. Evidence to substantiate that this is the case for the SG is provided in References 20C.27 and 20C.28, where, the proposed ISI arrangements for SG components are outlined to address the requirements of IWA-1400(b) and IWA-1500 of the ASME Code Section XI, supplemented where applicable by 10 CFR 50.55a. Reference 20C.27 identifies inspection requirements for ASME Class 1 components, and Reference 20C.28 identifies requirements for ASME Class 2 and

3 components. These references provide a statement of the inspection techniques, inspectability and access arrangements applicable to ISI for AP1000 NPP and do not constitute a fully developed Inspection Plan: this is to be developed by the utilities as part of the site-specific safety case following GDA.

Reference 20C.27 identifies inspection requirements for primary side SG locations based on those prescribed in ASME Code Section XI for Class 1 pressure retaining components, including the various types of welds, bolting, and heat-transfer tubing. Reference 20C.28 identifies inspection requirements for secondary side SG locations based on those prescribed in ASME Code Section XI for Class 2 components, including shell and nozzle welds.

The planned ISI programme includes the SG components and welds of importance to nuclear safety. A summary of the examination requirements for the SG, as identified in Reference 20C.19, is shown in Table 20C-10. ASME Code Section XI requirements are identified for each location, and relevant code cases are taken into account.

20C.3.4.1.2 Qualified Inspection of HSS Welds Provides Highly Reliable ISI

The ISI arrangements described in section 20C.3.4.1.1 are generic to AP1000 plant worldwide. This section describes supplementary or alternative ISI arrangements planned specifically for the AP1000 SG in the UK.

The Structural Integrity Classification for the SG components is shown in Table 20C-4. For the SG welds classified as HSS, qualified in-service-inspections are to be specified. This requirement, additional to the ISI described in the previous section, is specifically applicable to UK AP1000 plant only and represents a more onerous inspection regime than is applied elsewhere.

Qualified inspection is specified for the most safety-significant regions of the SG to provide the most robust demonstration that there are no defects of concern in these HSS components. The reliability of the ISI for HSS welds of the SG is to be qualified by applying the principles of the ENIQ Methodology as contained in Reference 20C.20.

Adherence to the ENIQ Inspection Qualification methodology provides evidence of good practice for ISI of HSS locations. Reference 20C.20 identifies how inspection requirements and performance objectives are laid down in an inspection specification and provides a method for Inspection Qualification based on technical justification of the inspection method and practical trials on simplified or representative test pieces resembling the component to be inspected. For each of the HSS locations, a qualified inspection plan will be produced which will provide justification for the claimed inspection capability. The qualified inspection plans, for both PSI and ISI, are to be developed following GDA.

20C.3.4.1.3 ISI Provides Data to Monitor and Judge In-service Defect Formation and Growth

In Section 20C.3.1.6.2 qualified manufacturing inspections of HSS welds are described. The resulting data constitute a “finger-print” against which ISI results can be compared. Comparison of ISI data with the manufacturing inspection fingerprint is used to confirm the absence of significant degradation or that build defects are stable i.e., defects detected during ISI must have started life as no greater than the manufacturing inspection validation defect size. Manufacturing inspections are to be performed using the same equipment that is likely to be used for the periodic ISI.

20C.3.4.1.4 Planned Locations for ISI are Accessible and Inspectable

For effective ISI, the SG design should accommodate requirements for inspection equipment and personnel access in accordance with current inspection technology and strategies. Aspects of SG design intended to facilitate effective pre-service and in-service inspection are discussed in Section 20C.3.1.6.3 and an inspectability assessment is provided in Reference 20C.19.

Reference 20C.19 establishes that provisions for inspectability are consistent with good practice, based on compliance with requirements set out in established codes and regulations including NCA-3200(r) of the ASME Code Section III, IWA-1400 and IWA-1500 of the ASME Code Section XI and 10CFR50.55a(g)(3)(i) and 10CFR50.55a(g)(3)(ii). Compatibility with the requirements of these elements of the ASME Code and Federal Regulations provides assurance that the ISI planned for the SG will be effective.

The inspectability assessment is based, in part, on ASME Code, inspectability and access requirements for ISI identified in References 20C.27 and 20C.28. These references address the inspection of SG pressure retaining welds, full penetration nozzle welds, pressure retaining dissimilar metal welds, pressure retaining bolting, pressure retaining welds in pump casings attached to the SG outlet nozzle and SG heat-transfer tubing. ISI requirements are identified as follows:

- Preferred or prescribed inspection technique(s).
- Surface finish requirements.
- Access for personnel and equipment for manual and/or mechanical inspection techniques.
- Access to welds to facilitate UT inspection of the full section.

20C.3.4.2 Diverse Systems are Provided to Detect, Locate and Monitor Leakage from the SG

ISI, as described in section 20C.3.4.1, is the preferred method of demonstrating forewarning of failure. Whilst leak detection and monitoring provide forewarning of failure, this safety argument does not seek to establish a quantitative case for excluding the gross failure of the SG as a result of this forewarning. The leak detection measures described in this section are provided as qualitative evidence of defence in depth in support of this leg of the safety argument. Leak detection provides warning of unforeseen or unexpected loss of coolant from the SG, and monitoring provides a means to confirm that any leakage of the coolant is kept within the limits specified in the technical specifications. To demonstrate that leaks of reactor coolant from the SG will be detected before they compromise plant safety, the following arguments are presented.

- Diverse systems are provided to detect leakage of primary coolant from the SG heat transfer tubes.

- Leak detection of the RCPB provides warning of reactor coolant leakage from the SG.

- SG design includes provision for in-service heat transfer tube monitoring and leakage tests.

20C.3.4.2.1 **Diverse Systems are Provided to Detect Leakage of Primary Coolant from the SG Heat Transfer Tubes**

An important potential identified leakage path for reactor coolant is through the SG heat transfer tubes into the secondary side of the SG. Identified leakage from the SG primary side will be detected by one, or a combination, of the following:

- High condenser air removal discharge radioactivity, as monitored and alarmed by the turbine island vent discharge radiation monitor.
- SG secondary side radioactivity, as monitored and alarmed by the SG blowdown radiation monitor.
- Secondary side radioactivity, as monitored and alarmed by the main steam line radiation monitors.
- Radioactivity, boric acid, or conductivity in condensate as indicated by laboratory analysis.

20C.3.4.2.2 **RCPB Leak Detection Provides Warning of Reactor Coolant Leakage from the SG**

The RCPB is monitored for leaks from the reactor coolant and associated systems as described in section 20.6.4.3.2. The leak detection system provides a means to detect and, to a limited extent, identify the source of the RCPB leakage and provides warning of leakage from all components of the RCS, including the SGs.

20C.3.4.2.3 **SG Design Includes Provision for In-service Heat Transfer Tube Monitoring and Leakage Tests**

The SG design includes provision for tests to detect tube leakage and tube-to-Tubesheet leakage. These tube leakage tests are to be carried out if necessary while the plant is in a cold shutdown state.

Steam generator tubing is subject to a variety of degradation mechanisms. Steam generator tubes may experience tube degradation related to corrosion phenomena, such as wastage, pitting, intergranular attack, and stress corrosion cracking, along with other mechanically induced phenomena such as denting and wear. These degradation mechanisms can impair tube integrity if they are not managed effectively.

Technical specification 3.4.18 of the generic Technical Specifications (Reference 20C.34) includes provisions for steam generator heat transfer tube integrity. Technical Specification 3.4.7 also imposes limits applicable to SG tube integrity. A SG Programme will be developed by the Licensee in accordance with Technical Specification 5.5.4 to manage steam generator integrity. Technical Specification 5.5.4 includes prescriptive criteria to ensure tube integrity that incorporate the good practice of NEI 97-06 and its referenced EPRI Guidelines (References 20C.35 and 20C.33).

Use of the SG Programme ensures that the inspection is appropriate and consistent with accepted industry practices. The SG Programme determines the scope of the inspection and the methods used to determine whether the tubes contain flaws satisfying the tube repair criteria. Inspection scope (i.e., which tubes or areas of tubing within the SG are to be inspected) is a function of existing and potential degradation locations. The SG Programme also specifies the inspection methods to be used to find potential degradation. Inspection

methods are a function of degradation morphology, NDE technique capabilities, and inspection locations.

The steam generators permit access to tubes for inspection, repair, or plugging, if necessary, per the requirements of the SG Programme.

A secondary side leakage test is performed after each opening of the secondary system to check closures for leakage. For design purposes, it is assumed that the steam generator secondary side is pressurised to just below its design pressure to prevent the safety valves from lifting. So that a secondary-side to primary-side pressure differential of 4.62 MPa (670 psi) is not exceeded, the primary side must also be pressurised. The 4.62 MPa differential is the steam generator design differential pressure for secondary-to-primary pressure. The primary system must be above the minimum temperature imposed by reactor vessel material ductility requirements (that is, between 120°F and 250°F (48.8°C and 121.1°C)). It is assumed that this test is performed 80 times for design purposes.

It may become necessary to check the steam generator for tube leakage and tube-to-Tubesheet leakage. This is done by inspecting the underside (channel-head side) of the Tubesheet for water leakage whilst the secondary side is pressurised. This would be done while the plant is shut down.

For this test, the secondary side of the SG is pressurised with water, initially at a relatively low pressure, and the primary system remains depressurised. The underside of the Tubesheet is examined for leaks. If any are observed, the secondary side is depressurised and the leaking tube is plugged. The secondary side is then re-pressurised (to a higher pressure), and the underside of the Tubesheet is again checked for leaks. This process is repeated until the leaks are repaired. The maximum secondary-side test pressure reached is approximately 5.792 MPa (840 psi) gauge.

During these tests, both the primary and the secondary sides of the SGs are at ambient temperatures. Neither the primary-side nor secondary-side design pressure is exceeded. The expected secondary-to-primary pressure differential exceeds the design value of 4.62 MPa (670 psi) for some of the test cycles. The following is a breakdown of the anticipated number of occurrences at each secondary side test pressure:

Test Pressure MPa gauge (psi)	Number of Occurrences
1.379 (200)	400
2.758 (400)	200
4.137 (600)	120
5.792 (840)	80

The total number of tube leakage test cycles is defined as 800 for design purposes. These tests are also accounted for in the design transients for ASME qualification of the RCPB components reflected in Table 20-22.

20C.4 Strength of the Safety Case

20C.4.1 Objective

SFRs for the SG, as given in Table 20-1, are identified in Section 20C.2.1. This report provides a safety argument which identifies evidence to substantiate that the SFRs of the SG will be maintained for all conditions within the design basis. This is achieved by demonstrating that the structural integrity of the SG will be maintained for all conditions within the design basis for a 60-year component lifetime.

The availability and reliability of the SFRs should demonstrably be commensurate with the significance of the radiological hazards to be controlled. This demonstration is achieved by a process of component structural integrity classification which, for the safety justification of each class of component, establishes the degree of rigour to be applied commensurate with the potential radiological consequences of any postulated gross failure mode.

As described in Section 20C.2.2, structural integrity classification of the components of the SG is identified in Table 20C-4; these have been determined according to a process detailed in Reference 20C.4. All welds and forgings of the SG shell, including both the primary and secondary sides, are classified as HSS components. As established in Reference 20C.4, this classification necessitates substantiation of a higher level structural reliability such that the probability of gross structural failure of these SG components is so low it can be discounted.

The structural integrity classification of all SG components, other than the shell welds and forgings, is Standard Class 1. A summary of the evidence presented in the safety argument to substantiate the structural reliability claims for the HSS and Standard Class 1 SG components is given in Section 20C.4.2. This summary and review of the safety argument provides the basis for the conclusions of this report which are presented in Section 20C.6.

20C.4.2 Evidence

It is necessary that the structural integrity of HSS components of the SG is substantiated to a higher degree of rigour than that required for the Standard Class 1 components. The four legged safety argument provides diverse evidence to substantiate the very high structural reliability claimed for HSS components; this evidence is summarised in section 20C.4.2.1. The evidence to substantiate the structural reliability claimed for Standard Class 1 components is effectively a sub-set of that presented in the four legs of the safety argument, as identified in section 20C.4.2.2.

20C.4.2.1 HSS Components

To substantiate the claim that gross structural failure of the HSS components of the SG can be discounted, a safety argument is presented in Section 20C.3. Various elements of sound engineering practice are identified which provide evidence that there is defence in depth against structural failure within the SG arrangement and design. The safety argument comprises four conceptually different legs, within each of which multiple subordinate arguments are supported by diverse sources of substantiating evidence. Robustness is achieved by considering the combined contribution from the four legs. In combination the four legs provide sufficient confidence that gross failure of the HSS components will not occur during normal operation, during design basis transient or fault conditions. The combined strength of the claims, arguments and evidence presented in Section 20C.3 is discussed in this section.

The safety argument is founded upon a high standard of manufacture sufficient to achieve an appropriately high level of structural integrity. Design and fabrication of the SG HSS components is to be in accordance with ASME Code, Section III, Class 1 requirements as a minimum. Supplemental requirements are identified that enhance the quality of SG design and fabrication beyond ASME Class 1 standards. These are detailed in Section 20C.3.1, where multiple arguments and supporting evidence to substantiate achievement of SG integrity are presented. Section 20C.3.1 includes claims, arguments and evidence to address the following aspects:

- The design is well founded and in accordance with internationally recognised standards. Design of PWR SGs is long established and Westinghouse has an established track record. The AP1000 SGs benefit from this historical experience which is embodied in the codes, standards and regulations applied in design and fabrication.

- Procurement of materials is specified and controlled to ensure that well proven materials are chosen, that the materials have good resistance to fracture and are of suitable chemical composition to limit the effect of through-life degradation mechanisms. SG materials comply with the corresponding material specification permitted by the ASME Code, Section II. Supplementary requirements are specified for the HSS forgings which exceed the requirements specified in the ASME Code. Materials testing is specified to confirm that material properties comply with the relevant specifications.

- Very high standards have been applied that control the quality of SG manufacture. HSS components will be manufactured by experienced suppliers and evidence to confirm the suitability of the chosen manufacturer will form part of the Site Specific Justification. Compliance with ASME III Class 1 requirements and the experience embodied within the Code provides high confidence in manufacturing quality. Supplemental requirements have been identified which enhance the standards applied in fabrication beyond those prescribed in the ASME Code. Approved welding procedures and qualified operators are used. Stringent QA arrangements control manufacturing procedures and records are maintained to provide a clear auditable trail that will confirm this. There are procedural controls to limit deviations from the design intent and all repairs and deviations will be recorded to confirm acceptability.

- The HSS components are designed in accordance with the requirements of the ASME Code, Section III for Class 1 components[4]. Consideration of Levels A to D and Test conditions encompass the design basis for the purposes of the analysis. The parameters used in the design evaluation are robustly determined using established and conservative procedures, as detailed in section 20C.3.1.2. Section 20C.3.1.3 describes the analyses that demonstrate compliance with stress and fatigue limits prescribed by the Code, and thus demonstrate fitness-for-purpose for the HSS components at SoL.

- Manufacturing inspections and PSI with appropriate levels of redundancy and diversity will confirm the absence of defects which have the potential for causing, or developing into a failure mode. This will be based on the calculated allowable SoL defect sizes determined using the R6 methodology. Where appropriate, the inspections are subject to independent validation and in the case of HSS components of the SG, a programme of

4. N.b. Secondary side components of the shell, including the Feedwater and Steam Outlet Nozzles, are assigned Class B AP1000 Equipment Classifications, which would normally correspond to ASME III Class 2. The construction of these components is, however, specified in accordance with the requirements applicable to ASME Class 1 components for conservatism.

qualified PSI is specified. These requirements exceed those prescribed by the ASME Code. In the unlikely event that defects are found, they will be repaired in accordance with accepted techniques.

The diverse evidence summarised above demonstrates that the HSS components will be designed and fabricated against well established and appropriate deterministic engineering rules, verified by application of rigorous inspections. The various elements identified establish defence in depth for preventing failure of structural integrity. Functional hydrostatic testing to demonstrate that the HSS components meet the design intent, as described in Section 20C.3.2, supplements the arguments to demonstrate achievement of SG integrity, ensuring that the SG enters service fit for purpose and free of safety-significant defects.

The measures established to ensure good design and construction are supplemented with additional claims and evidence to demonstrate continued structural integrity throughout the planned SG lifetime. Careful control of operating conditions enables the SG to fulfil its safety function for its projected lifetime. The controls that will govern plant operation and maintenance, in accordance with well established procedures, are described in section 20C.3.1.7. Section 20C.3.3 and Section 20C.3.4 provide evidence to substantiate SG integrity under all design basis conditions by demonstrating that any defect which may have gone undetected during manufacture will not cause failure during the lifetime of the plant. The elements that substantiate this claim are as follows:

- Fracture Analyses – The fracture analyses, comprising LEFM analyses, as per in Appendix G of ASME Section III, supplemented by elastic-plastic fracture mechanics procedures specified in the R6 Defect Assessment code, are described in section 20C.3.3.1. The fracture analysis demonstrates that the sizes of defect which are of safety concern are large in relation to those which could be present in the component following qualified NDT.

- Pre-Service and In-Service Inspection – The SG is designed to facilitate effective PSI and ISI, which provide assurance that defects will be detected long before growing to a size that could threaten structural integrity of the SG. Qualification of inspection methods for HSS locations establishes the sizes of defects that can be reliably detected, and provides more robust control of the efficacy of PSI and ISI than the requirements of ASME Section XI. Qualification is to be achieved through a combination of Technical Justification of inspection procedures and equipment, supported by trials. ISI data enables judgement of in-service defect formation and growth by comparison with PSI data.

- Leakage Monitoring – Diverse systems are provided to detect, locate and monitor leakage of reactor coolant from the SG, including leakage via the heat transfer tubes to the secondary side of the SG. Alarm and indication of reactor coolant leakage from the SG in excess of specified limits provides diverse means to detect failure. Periodic tests are planned to confirm the integrity of the primary and secondary side pressure boundaries.

20C.4.2.2 Standard Components

As asserted in Reference 20C.4, the failure statistics for industrial pressure vessels and piping that are built to according to the good practice embodied in modern codes and standards supports a failure rate to be inferred that is in accordance with the structural reliability target for Standard Class 1 (or lower classification) components. Substantiation of the structural reliability of the SG Standard Class 1 components is therefore largely based on demonstrating

compliance with relevant aspects of the ASME Code and with additional regulations as applicable.

General principles that ensure the quality of construction for all SG components are discussed in Section 20C.3.1. These are reinforced by a demonstration of adherence to the requirements of the ASME Code which establishes rules of safety governing the design, fabrication, and inspection of boilers and pressure vessels that are internationally recognised and well established. As identified in section 20C.3.1.1.3, the following sections of the ASME Code establish requirements governing aspects of SG design:

- Section II – Materials
- Section III – Rules for construction.
- Section XI – ISI

Materials of manufacture are discussed in section 20C.3.1.4, where it is established that all materials used in Standard Class 1 components are specified to be in accordance with the requirements of Section II of the ASME Code. In addition, the heat treatment specified for the heat transfer tubing exceeds the requirements of ASME Section II.

The requirements of ASME Code, Section III are identified on the basis of the ASME safety classification of a particular structure, system, or component. The components of the SG forming the reactor coolant pressure boundary are designed in accordance with the rules applicable to ASME Code, Section III, Class 1 components. The subcomponents of the SG performing ASME Class 2 functions are also designed in accordance with the rules applicable to ASME Code, Section III, Class 1 components, for conservatism. AP1000 Class D and AP1000 Class E components of the SG will be designed and manufactured to industry codes and standards. The applicable standards will be specified as part of the site-specific safety justification.

The integrity of the SG pressure boundaries, including the Standard Class 1 components that have a pressure-retaining function, is confirmed by the hydrostatic testing described in section 20C.3.2.1. Gas leak testing is conducted during manufacture to confirm the integrity of the tube-to-Tubesheet welds as described in section 20C.3.2.2.

The ISI requirements for the SG are described in section 20C.3.4.1.1. For the Standard Class 1 components included within the ISI programme, this will be in accordance with the requirements of ASME Code Section XI, IWB-2500 and IWC-2500, and supplemented by requirements specified in 10 CFR 50.55a. A SG programme described in section 20C.3.4.2.3 will dictate the periodicity of examinations for characterisation of tube wear, which will identify degradation and allow implementation of corrective action as needed while the plant is in a safe state. In addition to the planned ISI for Standard Class 1 components, forewarning of failure is also provided by leak monitoring, in particular to detect leakage of primary coolant from the SG heat transfer tubes (section 20C.3.4.2.1). In the event leakage at the heat transfer tubes or Tubesheet is suspected, a tube leakage test can provide indication of failed tubes or leaking tube-to-Tubesheet welds.

20C.5 Review of Open Issues

There are no open issues for the SG that may affect the basis of the safety case arguments.

20C.6 Conclusions

This CSR for the UK AP1000 SG design presents a safety argument to establish that the structural reliability of the SG is commensurate with the consequences of gross failure. SFRs have been identified for the SG. These are to be maintained to ensure plant nuclear and radiological safety. For the SG, assurance that SFRs will be maintained for the design life of the component is provided by substantiating structural integrity against appropriate reliability targets.

Structural reliability targets have been identified for the SG that are based on a procedure of structural integrity classification. Several components of the SG have been ascribed a classification of HSS, for which the highest level of structural reliability must be demonstrated. Other SG components are Standard Class 1, a classification that requires a somewhat less stringent and extensive substantiation of structural reliability.

The components of both the primary and secondary sides of the SG shell have been classified as HSS. The structural reliability target associated with HSS classification is to substantiate a probability of gross structural failure that is so low it can be discounted. The safety argument for the HSS components is presented in a four legged format that is well established in the UK for the safety justification of nuclear plant components similar to the SG that share similar structural reliability targets. The safety argument identifies diverse defence in depth measures to substantiate the structural reliability claimed for the HSS components of the SG:

- The intent and principles that govern the design, future manufacture and operation of the SG in the UK are identified to substantiate fitness for purpose within a pre-construction safety case. The safety argument demonstrates how modern and well established good practice is to be implemented in SG design, manufacture, defect tolerance assessment, and in the provision for through-life inspection.

- The SG design benefits from the long operating history and good safety record of similar components. The design incorporates measures to minimise frequency of failure which are based on substantial operating experience, and this has influenced the design for the SG, for example in terms of the materials selected, the choice of inspection techniques and selection of locations to be inspected. Much of this experience is embodied in the codes, standards and regulations that have been specified to ensure the quality of manufacture.

- Structural integrity of the HSS components is secured largely by passive means and is not significantly reliant on control systems, active safety systems or human intervention. As such, the diverse defence in depth measures identified focus on prevention of failure through conservative, robust design. Surveillance, inspection, leakage monitoring and periodic testing provide secondary defence in depth measures to detect and provide forewarning of structural failure. The SG design facilitates effective inspection which supports a programme of qualified inspection for the HSS components.

- Extensive QA measures covering aspects of design, manufacture, material specification, materials testing and inspection ensure a level of structural reliability that is commensurate with the consequences of gross structural failure of the HSS components. The strength of the safety case is founded on the achievement of integrity. Analyses are specified to deterministically justify the structural integrity of the HSS components of the SG in accordance with ASME Code Section III requirements for Class 1 components. Additional arguments specify robust analyses to provide evidence that

these components are tolerant to structurally significant defects, and this is supported by the qualified inspections.

The structural integrity classification of all other SG components has been determined to be Standard Class 1. The structural reliability target associated with this classification is less onerous than that for HSS components. Failure statistics for industrial pressure vessels and piping built in accordance with the good practice embodied in modern codes and standards are judged to support inference of a failure rate that is commensurate with the structural reliability target for Standard Class 1 components. Substantiation of the structural reliability of the SG Standard Class 1 components is thus based on demonstrating compliance with relevant aspects of the ASME Code. Evidence is presented within various elements of the four-legged safety argument to show that, as a minimum, the Standard Class 1 components of the SG comply with the relevant requirements of the ASME Code.

It is concluded that the safety argument presented in Section 20C.3 identifies a suitable and sufficient diversity of evidence to substantiate the structural reliability claimed for both the HSS and Standard Class 1 components of the SG.

20C.7 Index of Technical Reports

Table 20C-11 provides a list of technical references supporting the safety case and summarises the function of each document within the safety case. Codes, standards and regulations that will be applied to the design, manufacture and operation of the SG are identified separately in Table 20C-5.

20C.8 References

20C.1 Westinghouse Report APP-MB01-Z0-101, Rev. 11, "Design Specification for AP1000 Steam Generator for System RCS," November 2016.

20C.2 Not used.

20C.3 R Bullough, et al., "The Demonstration of Incredibility of Failure in Structural Integrity Safety Cases," International Journal of Pressure Vessels and Piping 78, 2001, pages 539-552.

20C.4 Westinghouse Report, UKP-GW-GLR-004, Rev. 3, "AP1000 UK Structural Integrity Classification," January 2017.

20C.5 Not Used.

20C.6 Westinghouse Report APP-RCS-M8-002, Rev. 5, "AP1000 Steam Generator – Interface Control Document (ICD)," May 2015.

20C.7 Westinghouse Report, APP-RCS-M1-001, Rev. 4, "Reactor Coolant System Design Transients," February 2013.

20C.8 EPRI, "Pressurized Water Reactor Primary Water Chemistry Guidelines," Rev. 6, Electric Power Research Institute, 2007.

20C.9 EPRI, "Pressurized Water Reactor Secondary Water Chemistry Guidelines," Rev. 6, Electric Power Research Institute, 2004.

20C.10 Westinghouse Report APP-MB01-Z0R-100, Rev. 6, "AP1000 Steam Generator Generic Design Report," October 2016.

20C.11 Westinghouse Report, APP-VL51-Z0-002, Rev. 4, "Material Specification for SA-508/SA-508M Grade 3 Class 2 Forgings (Section III-NB)," August 2011.

20C.12 Westinghouse Report APP-VL53-Z0-011, Rev. 4, "Material Specification for Thermally Treated Alloy UNS N06690 (Alloy 690) Tubing for AP1000," September 2010.

20C.13 Westinghouse Report, APP-GW-VLR-002, Rev. 2, "Technical Requirements of Stainless Steels, Nickel-based Alloys, Carbon and Low Alloy Steels, and Welding Materials for the AP1000," January 2016.

20C.14 Westinghouse Document "Quality Management System (QMS)," Rev. 7, August 2013.

20C.15 NRC 10CFR50 Appendix B – "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants," US Nuclear Regulatory Commission.

20C.16 Regulatory Guide 1.28, "Quality Assurance Program Requirements (Design and Construction)," Rev. 3, US Nuclear Regulatory Commission, August 1985.

20C.17 ASME NQA-1-1994, "Quality Assurance Requirements for Nuclear Facility Applications," American Society of Mechanical Engineers.

20C.18 ASME Boiler and Pressure Vessel Code, "Quality Assurance." Section III, Subsection NCA, Article NCA- 4000, American Society of Mechanical Engineers Boiler and Pressure Code.

20C.19 Westinghouse Report APP-MB01-VMR-001 Rev. 0, "AP1000 Component ISI Inspectability Assessment: Steam Generator," April 2011.

20C.20 ENIQ "European Methodology For Qualification Of Non-Destructive Testing," European Network for Inspection Qualification Report nr. 31, EUR 22906 EN Issue 3, August 2007.

20C.21 Westinghouse Document WCAP-14040-NP-A, Rev. 2, "Methodology Used to Develop Cold Overpressure Mitigating System Setpoints and RCS Heatup and Cooldown Limit Curves," January 1996.

20C.22 R6, Rev. 4, "Assessment of the Integrity of Structures Containing Defects," British Energy Generation Ltd., 2007.

20C.23 HSE, "Nuclear Directorate Generic Design Assessment – New Civil Reactor Build, Step 3 Structural Integrity Assessment of the AP1000," Assessment Report No. AR 09/013-P. Health and Safety Executive.

20C.24 Westinghouse Report UKP-MV01-Z0R-100, Rev. 3, "Results of Weld Ranking Process for Reactor Vessel, Steam Generator, Pressurizer, Main Steam Line and Main Coolant Loop Piping," December 2015.

20C.25 Not Used.

20C.26 Westinghouse Report UKP-MV01-Z0R-101, Rev. 2, "Methodology and Input Data for the Application of the R6 Flaw Evaluation Procedure and Fatigue Crack Growth Analysis to the UK AP1000 Components," December 2016.

20C.27 Westinghouse Report APP-GW-VW-001, Rev. 1, "AP1000® Design for Inspectability Program: ISI Requirements and Design Guidance for Class 1 Components," June 2014.

20C.28 Westinghouse Report APP-GW-VW-002, Rev. 0, "AP1000 Design for Inspectability Programme: ISI requirements for class 2 and 3 components," June 2007.

20C.29 Westinghouse Report UKP-MB01-Z0C-004, Rev. 1, "Flaw Evaluation of the UK AP1000 Steam Generator Welds," April 2016.

20C.30 Westinghouse Report WDI-TJ-1051, Rev. 1, "Manufacturing NDT Inspection Plan for the RPV Inlet Nozzle to Safe End Weld of the AP1000 RPV in Response to Regulatory Observation Action RO-AP1000-19.A3," December 2010.

20C.31 Westinghouse Report WDI-TJ-1054, Rev. 1, "Manufacturing NDT Inspection Plan for the Surge Nozzle to Safe End Weld of the AP1000 Pressurizer in Response to Regulatory Observation Action RO-AP1000-19.A3," January 2011.

20C.32 Westinghouse Report WDI-TJ-1055, Rev. 1, "Manufacturing NDT Inspection Plan for the upper head to upper shell and manway to shell welds of the AP1000 Pressurizer in Response to Regulatory Observation Action RO-AP1000-19.A3," February 2011.

20C.33 "Steam Generator Management Program: Pressurized Water Reactor Steam Generator Examination Guidelines," Electric Power Research Institute,.

20C.34 Westinghouse Report UKP-GW-GL-501, Rev. 0, "AP1000® UK Generic Technical Specifications," January 2016.

20C.35 NEI 97-06, "Steam Generator Program Guidelines," Nuclear Energy Institute.

20C.36 Westinghouse Report WDI-PJF-2405360-TCR-003, Rev. 2, "Westinghouse Process for the Development of AP1000 Related Manufacturing NDT Inspection Plans as Part of the GDA Process (UK)," Wesdyne International, February 2016.

20C.37 Westinghouse Report UKP-GW-M0R-001, Rev. 0, "Additional Fracture Toughness Testing for the UK AP1000 Plant," January 2017.

Table 20C-1. AP1000 Steam Generator Nominal Design Parameters(3)

Type	Vertical U-tube Feedring
Number of tubes per SG	10,025
Heat Transfer Surface area per SG	11,477 m^2
Tube OD	17.48 mm
Tube wall thickness	1.02 mm
Tube ID	15.42 mm
Tube pitch	24.89 mm
Overall length of SG shell	22.45 m(1)
Upper shell I.D	5.33 m
Lower shell I.D	4.19 m
Channel Head thickness (base metal wall thickness)	254 mm
Tubesheet thickness (base metal vertical thickness)	791.4 mm
Primary side design pressure	17.24 MPa
Primary side design temperature	343.3°C
Secondary side design temperature	315.6°C
Secondary side design pressure	8.27 MPa
Primary to secondary maximum differential pressure	11.38 MPa
Secondary to primary maximum differential pressure	4.62 MPa
No Load Temperature	291.7°C
Primary water volume per SG	58.8 m^3
Water volume in plena	16.7 m^3
Water volume in tubes	42.2 m^3
Secondary water volume per SG(2)	103.2 m^3
Secondary steam volume per SG(2)	147.9 m^3
Secondary liquid mass per SG(2)	79,722 kg

Notes:

1. Measured from steam outlet nozzle to the flat, exterior portion of the Channel Head.
2. At full power design conditions. Actual volumes and masses are dependent on final design and operating conditions.
3. All dimensions are nominal. Construction tolerances apply.

Table 20C-2. AP1000 Steam Generator Material Recommendation

SG Sub-Component	Material
Heat Transfer Tubes(1)	SB-163 UNS N06690 Special Thermally Treated
Tubesheet	SA-508 GR. 3 CL. 2 plus supplementary requirements S1, S2, S4, S9, S10, S15
Channel Head and Nozzles	SA-508 GR. 3 CL. 2 plus supplementary requirements S1, S2, S4, S9, S10, S15
Transition Cone and Secondary Shell	SA-508 GR. 3 CL. 2 plus supplementary requirements S1, S2, S4, S9, S10, S15
AVBs	SA-479 Type 405 with SB-166 UNS N06690 end caps
Tube Bundle Wrapper	SA-516 Grade 70
Feedwater, Start-up Feedwater, and Steam Outlet Nozzles	SA-508 GR. 3 CL. 2 plus supplementary requirements S1, S2, S4, S9, S10, S15
Blowdown/Drain Nozzle and Instrumentation Nozzles	SA-508 GR. 1A plus supplementary requirements S1, S2, S4, S10, S15
Tubesheet Cladding	SFA-5.11/SFA-5.14 Weld Metal, (ENiCrFe-7/ ERNiCrFe-7) (Primary Surface), and SFA-5.4/SFA-5.9 Stainless Steel (E308L, ER308L, E309L, ER309L) (Upstand region)
Access Opening Covers	SA-533 Type B Class 2
Channel Head Divider Plate	SB-168 UNS N06690
Stay Rods	SA-739 Grade B22
Feedwater Spray Nozzles	SB-167 UNS N06690
Feedwater Ring Assembly	SA-335 Grade P11 , SA-234 Grade WP11, SB-167 UNS N06690, SB-564 UNS N06690, SB-168 UNS N06690
Primary Moisture Separator Assembly	SA-516, Grade 70, ASTM A517/A514 Grade B, SA-36, SA-106 Grade B, SA-105
Secondary Moisture Separator Assembly	ASTM A36, ASTM A106 Gr. B, ASTM A234 Gr. WPB, ASTM 285 Gr. C, ASTM A516 Gr. 70
Steam Outlet Nozzle Flow Limiting Venturi (at Steam Outlet Nozzle Interface)	SB-564 UNS N06690 Forging
External Bolting (Bolts and Nuts)	SA-193 Grade B7 (Studs and/or Studs Bolts), SA-194 Grade 7 (Nuts)
Primary Inlet Nozzle Safe Ends	SA-336 Class F 316LN
PRHR Nozzle Safe End	SB-564 UNS N06690

Table 20C-2. AP1000 Steam Generator Material Recommendation (cont.)

SG Sub-Component	Material
Upper Elliptical Head	SA-508 GR. 3 CL. 2 plus supplementary requirements S1, S2, S4, S9, S10, S15
Sludge Collector	SA-516 Grade 70, SA-36, SA-105, SA-106 Grade B
Upper Lateral Support	SA-508 GR. 3 CL. 2 plus supplementary requirements S1, S2, S4, S9, S10, S15
Lower Shell Trunnion	SA-508 GR. 3 CL. 2 plus supplementary requirements S1, S2, S4, S9, S10, S15
Channel Head Cladding	Austenitic stainless weld deposited with SFA-5.9, ER309L/ER308L and SFA-5.4, E309L/E308L.
Pipe Whip Restraint	SA-533 Type B Class 2

Notes:

1. Heat transfer tubing will meet all of the requirements of Reference 20C.12.

Table 20C-3. AP1000 Steam Generator Interfaces

1	Upper, Intermediate, and Lower Lateral Supports
2	Vertical Column Support
3	1-Primary Inlet Nozzle
4	1-Steam Outlet Nozzle
5	1-Feedwater Nozzle
6	1-PRHR Nozzle, (SG No. 1 only)
7	2-Secondary Manways
8	2-Primary Manways
9	1-Start-up Feedwater Nozzle
10	1-Drain/Blowdown Nozzle
11	4-Upper Level Taps shared by narrow and wide range
12	4-Lower Narrow Range Taps
13	4-Lower Wide Range Taps
14	4-Top-of-Tubesheet handholes and 2 U-bend Inspection Ports, 1 Maintenance Recirculation Access Port
15	1-CVS Nozzle, (SG No. 1 only)
16	Sludge collector piping (internal to the SG near a secondary manway)
17	3 – Steam Pressure Taps
18	2-Primary Outlet Nozzle-to-RCP Casing

Table 20C-4. Structural Integrity Classification of Steam Generator Components

Location	Classification	Comment
WELDS		
Primary Shell		
Channel Head to Tubesheet to weld	HSS	See Table 20.4 to Table 20.6
Primary Inlet Nozzle to Safe End butt weld	HSS	
Primary Outlet Nozzle to RCP casing weld	HSS	2 Primary Outlet Nozzles per SG
PRHR Nozzle to Safe End butt weld	HSS	SG 1 Only
CVS Nozzle to Channel Head weld	HSS	SG 1 Only
Secondary Shell		
Elliptical Head to Elliptical Head Knuckle weld	HSS	See Table 20.4. Note: Steam Outlet Nozzle to Feedwater Pipework weld not included in the scope.
Elliptical Head Knuckle to Upper Shell weld	HSS	
Tubesheet to Lower Shell weld	HSS	
Start-Up Feedwater Nozzle to Shell weld	HSS	
Main Feedwater Nozzle to Shell weld	HSS	
Manway Welds	HSS	
FORGINGS		
Primary Shell		
Channel Head and nozzles	HSS	See Table 20.5 and Table 20.6
Tubesheet	HSS	
Secondary Shell		
Lower Shell A Barrel	HSS	See Table 20.4.
Lower Shell B Barrel	HSS	
Lower Shell C Barrel	HSS	
Transition Cone	HSS	
Upper Shell D Barrel (including nozzles)	HSS	
Upper Shell E Barrel	HSS	
Elliptical Head Knuckle	HSS	
Elliptical Head (including nozzle)	HSS	

Table 20C-4. Structural Integrity Classification of Steam Generator Components (cont.)

Location	Classification	Comment
OTHER REGIONS		
Heat Transfer U-Tubes	Standard Class 1	Failure of a single tube is considered within the design basis and assessed in Chapter 9. Multiple tube failure is not assessed and is considered beyond the design basis.
Tube-to-Tubesheet welds	Standard Class 1	
AVBs	Standard Class 1	
Tube Bundle Wrapper	Standard Class 1	
Support Plates and Flow Distribution Baffle (if used)	Standard Class 1	
Blowdown/Drain Nozzle and Instrumentation Nozzles	Standard Class 1	
Manway Covers	Standard Class 1	
Channel Head Divider Plate	Standard Class 1	
Stay Rods	Standard Class 1	
Spacer Pipes (if used)	Standard Class 1	
Feedwater Spray Nozzles	Standard Class 1	
Feedwater Ring Assembly	Standard Class 1	
Primary Moisture Separator Assembly	Standard Class 1	
Secondary Moisture Separator Assembly	Standard Class 1	
Steam Outlet Nozzle Flow Limiting Venturi	Standard Class 1	
External Bolting (Bolts and Nuts)	Standard Class 1	
Sludge Collector	Standard Class 1	
Upper Lateral Support	Standard Class 1	
Lower Shell Trunnion	Standard Class 1	

Table 20C-5. Codes and Standards Related to SG Design and Manufacture

ASME Boiler and Pressure Vessel Code	
Section II	Material Specification.
Section III	Nuclear Power Plant Components.
Section V	Non Destructive Examination.
Section IX	Welding and Brazing Qualification.
Section XI	Rules for ISI of Nuclear Power Plants Components.
ASME Code Cases	
2142-2	F-Number Grouping for Ni-Cr-Fe Filler Metals Section IX (Applicable to all Sections, including Section III, Division 1, and Section XI).
N-643-2	Fatigue Crack Growth Rate Curves for Ferritic Steels in PWR Water Environment, Section XI, Division 1.
N-782	Use of Code Editions, Addenda, and Code Section III Division 1.
N-759-2	Alternative Rules for Determining Allowable External Pressure and Compressive Stresses for Cylinders, Cones, Spheres, and Formed Heads, Class 1, 2, and 3 Section III, Division 1.
ANSI/ASME Standards	
ASME NQA-1 1994	"Quality Assurance Requirements for Nuclear Facility Applications."
ANSI/ANS-51.1	"Nuclear Safety Criteria for the Design of Stationary Pressurized Water Reactor Plants."
U. S. Code of Federal Regulations	
10CFR21	"Reporting of Defects and Non-compliance."
10CFR50	Appendix A "General Design Criteria for Nuclear Power Plant," Criteria 1, 2, 4, 14, 30, 31, 32 and 34 apply.
10CFR50	Appendix B "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants."
10CFR50	Appendix G "Fracture Toughness Requirements."
10CFR50.55(a)	"Codes and Standards."
US NRC Regulatory Guides	
RG 1.31 Rev. 3	"Control of Ferrite Content in Stainless Steel Weld Metal," April 1978.
RG 1.37, Rev. 0	"Quality Assurance Requirements for Cleaning of Fluid Systems and Associated Components of Water-Cooled Nuclear Power Plants," March 1973.
RG 1.43 Rev. 0	"Control of Stainless Steel Weld Cladding of Low-Alloy Steel Components," May 1973.
RG 1.44 Rev. 0	"Control of the Use of Sensitized Stainless Steel," May 1973.

Table 20C-5. Codes and Standards Related to SG Design and Manufacture (cont.)

US NRC Regulatory Guides (cont.)	
RG 1.50 Rev. 0	"Control of Preheat Temperature for Welding of Low-Alloy Steel," May 1973.
RG 1.84 Rev. 32	"Design and Fabrication Code Case Acceptability ASME Section III, Division 1," June 2003.
RG 1.121 Rev. 0	"Basis for Plugging Degraded Pressurized Water Reactor Steam Generator Tubes," (exception for Section C.1 and C.2.a(1)), August 1976.
RG 1.125 Rev. 1	"Physical Models for Design and Operation of Hydraulic Structures and Systems for Nuclear Power Plants," October 1978.
RG 8.8 Rev. 3	"Information Relevant to Ensuring That Occupational Radiation Exposure at Nuclear Power Stations Will Be As Low As Reasonably Achievable," (confirms Sections 1.d, 2.a, 2.b-g, 2.h, 2.i, 4.a and 4.3. Sections 1 and 1.a-c are not applicable for AP1000), June 1978.
RG 8.19 Rev. 1	"Occupational Radiation Dose Assessment in Light-Water Reactor Power Plants," June 1979.
RG 1.71, Rev. 0	"Welders Qualification for Areas of Limited Accessibility," December 1973.
RG 1.147, Rev. 12	"In-service Inspection Code Case Acceptability – ASME Section XI, Division 1," May 1999.
RG 1.28, Rev. 3	"Quality Assurance Program Requirements (Design and Construction)," August 1985.
RG 1.20, Rev. 2	"Comprehensive Vibration Assessment Program for Reactor Internals During Preoperational and Initial Startup Testing," May 1976.
RG 1.92, Rev. 1 and Rev. 2	"Combining Modal Responses and Spatial Components in Seismic Response Analysis," February 1976 and July 2006.
Electric Power Research Institute (EPRI) Guidelines	
NP-3009	"Steam Generator Chemical Cleaning Process Development."
NP-5652	"Guidelines for Utilization of Commercial Grade Items in Nuclear Safety-Related Applications."
TR-107569	"PWR Steam Generator Examination Guidelines," Vol. 1 & 2.
NP-6617	"Electropolishing Qualification Program for PWR Steam Generator Channel Heads."
NP-6618	"Electropolishing Qualification Program for PWR Steam Generator Divider Plates."
TR-103296	"Cobalt Reduction Guidelines."
TR-016743	"Guidelines for PWR Steam Generator Tubing Specifications and Repair Specifications for Alloy 690 Steam Generator Tubing," Vol. 2.
TR-1013706	"Steam Generator Management Program: Pressurized Water Reactor Steam Generator Examination Guidelines."

Table 20C-5. Codes and Standards Related to SG Design and Manufacture (cont.)

Miscellaneous	
IEEE-344-1987	"Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations."
AWS A2.4-1998	"Standard Symbols for Welding, Brazing, and Non-destructive Examination."
ASTM E140-1997	"Standard Hardness Conversion Tables for Metals Relationship Among Brinell Hardness, Vickers Hardness, Rockwell Hardness, Superficial Hardness, Knoop Hardness, and Scleroscope Hardness."
TEMA, 9th Edition	"Standards of the Tubular Exchanger Manufacturers' Association."
ASTM A262	"Standard Practices for Detecting Susceptibility to Intergranular Attack in Austenitic Stainless Steels."
SNT-TC-1A-1992	"Recommended Practice for Non-destructive Testing, Personnel Qualification and Certification as amended by ASME Section III, NB-5520 and ASME Section XI, IWA-2300 for the In-service Inspection requirements."
ANSI/ ASNT CP-189-2001	"Standard for Qualification and Certification of Non-destructive Personnel as amended by ASME Section XI, IWA-2300."
NEI 97-06	"Steam Generator Program Guidelines."

Table 20C-6. SG Equipment Classification#1 (Reference 20C.1)

Major Assembly or Part Description	AP1000 Equipment[1] Classification	ANSI Safety Class[3]	Seismic Design
Primary Side Pressure Boundary	Class A	SC-1	Cat. I
Tube-to-Tubesheet Weld	Class A	SC-1	Cat. I
Primary Channel Head Divider Plate	Class B	SC-2	Cat. I
Secondary Side[4] Pressure Boundary	Class B	SC-2	Cat. I
Tube Bundle Support Assembly	Class C	SC-3	Cat. I
Feedwater Nozzle[4]	Class B	SC-2	Cat. I
Instrumentation Tap[4]	Class B	SC-2	Cat. I
Steam Outlet Nozzle[4]	Class B	SC-2	Cat. I
Flow Limiting Venturi	Class B	SC-2	Cat. I
Primary & Secondary Separator Assemblies and Supports	Class D	NNS	Cat. II
Feedwater Ring Pressure Boundary Interface	Class B	SC-2	Cat. I
Feedwater Distribution Ring Assembly & Supports (Except Pressure Boundary Interface)	Class C	SC-3	Cat. I
Nozzle Dam Support Feature	Class C	SC-3	Cat. I
Lifting & Handling Lugs	Class E	NNS	N/A
Pipe Whip Restraint	Class B	SC-2	Cat. I
Anti-Vibration Bars	Class C	SC-3	Cat. I
AVB End Caps, AVB Retaining Rings, and AVB Retaining Bars	Class D	NNS	Cat. II
All Other Assemblies	Class E	NNS	N/A

Notes:

1. For those items designated with Equipment Classification as Class D&E (Non-Nuclear Safety) the design, material, fabrication, inspection and testing will be to industry codes and standards.
2. Not used.
3. The safety classification is based on ANSI-51.1. Compliance with safety classification requirements is demonstrated if the assembly or part meets the same level of Code classification or a more stringent level.
4. The secondary side is classified as Class B. However, all pressure retaining components on secondary side will be designed to ASME Code, Section III, Class 1 (AP1000 Equipment Classification – Class A) requirements.

Table 20C-7 SG Equipment Classification#2 (Ref. 20C.1)

AP1000 Code Letter[1]	ANS Equipment Safety Class[2]	RG 1.29 Seismic Design Requirements	ASME Code, Sec. III Class[3]	IEEE Requirements	RG 1.26 NRC Quality Group[4]	10 CFR 50 Appendix B[5]	Inspection & Testing Requirements	Required Test & Maintenance
A	SC-1	I	1	NA	GROUP A	YES	YES[6]	See Note 7
B	SC-2	I	2	NA	GROUP B	YES	YES[6]	See Note 7
C	SC-3	I	3	1E	GROUP C	YES	YES[6]	See Note 7
D	NNS[2]	N/A	N/A	N/A	GROUP D	NO	YES[8]	See Note 8
E	NNS[2]	N/A	N/A	N/A	N/A	N/A	N/A	N/A
N/A – Not Applicable								

Notes:

1. A single letter equipment classification identifies the safety class, quality group, and other classifications for AP1000.
2. AP1000 safety classification is an adaptation of that defined in ANSI 51.1. The NNS defined in the ANSI 51.1 standard is divided into several AP1000 equipment classifications namely, Classes D, E, F, L, P, R, and W.
3. ASME Code, Section III defines various classes of structures, systems and components (SSCs) for NPPs. It defines criteria and requirements based on the classification.
4. The quality group classification corresponds to those provided in Regulatory Guide 1.26.
5. "Yes" means QA programme is required according to 10 CFR 50 Appendix B. "No" means QA programme is not required according to 10 CFR 50 Appendix B.
6. Class A, B, and C structures, systems, and components built to ASME Code, Section III, are inspected to ASME Code, Section XI requirements.
7. Class A, B, and C structures, systems, and components that are required to function to mitigate design base accidents have some testing requirements included in the plant technical specifications. In addition to the requirements in the technical specifications, testing and maintenance requirements are included in an administratively controlled reliability assurance plan.
8. Class D SSCs determined to be risk important have selected technical requirements programme requirements and procedures to assure defence in depth availability. Class D SSCs not identified as risk important have select reliability assurance programmes and procedures to ensure reliability where needed. These programmes are administratively controlled programmes and may be included in the technical requirements manual or general availability controls manual, as appropriate.

Table 20C-8 Design Loading Combinations Applicable For Steam Generator

Condition	Design Loading Combinations[10]	Notes
Design	P + DW + DML + XL[11]	DML may include normal vibration loading/bldg settlement. XL contains max thermal for service levels A.
Level A Service	PMAX[1] + DW + XL[3]	Normal 100% power operating condition pressure and thermal (XL).
	PMAX + DW + DN + XL[6]	Max level A loadings of coincident pressure, thermal (XL) and normal dynamic
Level B Service	PMAX + DW + DU + XL[6]	DU is service level B dynamic (if applicable)
Level C Service	PMAX + DW + DE + XL[6]	DE is service level C dynamic (if applicable)
	PMAX + DW + DY + HYDSP + XL[7]	DY, HYDSP, and XL (thermal) are loads associated with ADS sparger discharge
Level D Service	PMAX + DW + DF + XL[6]	DF is some other dynamic level D event (other than SSE or DBPB) with corresponding level D thermal (XL) If no other level D dynamic then evaluate thermal faulted without dynamic
	PMAX + DW + SRSS((SSE + SSES) + DBPB)[5] + XL[3]	This case uses normal operation thermal for XL
	PMAX + DW + RVOS + SRSS(SSE + SSES)[5]+ XL[9]	This case uses thermal loads for XL associated with RVOS condition
	PMAX + DW + DYS + DBPBS + SRSS((SSE+ SSES)[5] + DY + HYDSP) + XL[7][8]	XL for this case corresponds to thermal associated with the long term steady state pipe break condition

Table 20C-8 Design Loading Combinations Applicable For Steam Generator (cont.)

Condition	Design Loading Combinations(10)	Notes
Test	P + DW + DML	DML may include normal vibration loading/bldg settlement.

Notes:

1. The values of PMAX in the load combinations may be different for different levels of service conditions as provided in the design transients. For earthquake loadings PMAX is equal to normal operating pressure at 100% power.
2. Not used.
3. In combining loads, the timing and causal relationships that exist between PMAX, and XL, are considered for determination of the appropriate load combinations.
4. Not used.
5. For components that behave as anchors to the piping system, such as equipment nozzles, SSE and SSES are combined by absolute sum. For other components, such as straight pipe, tees, and valves, SSE and SSES are combined by SRSS method.
6. In combining loads, the timing and causal relationships that exist between PMAX, DN, DU, DE, DF, and XL, are considered for determination of the appropriate load combinations.
7. In combining loads, the timing and causal relationships that exist between PMAX, DY, HYDSP, and XL, are considered for determination of the appropriate load combinations.
8. In combining loads, the timing and causal relationships that exist between PMAX, DY, and XL, are considered for determination of the appropriate load combinations.
9. In combining loads, the timing and causal relationships that exist between PMAX, RVOS, and XL, are considered for determination of the appropriate load combinations.
10. 10% SSE is used as the allowable load for the unknown loads defined for each service level (DML, DN, DU, DE, DY + HYDSP, DF, RVOS, and DYS + SRSS(DY+HYDSP) loads). For the Level A and B conditions, 10% SSE is assumed to have an infinite number of cycles.
11. Thermal loads are combined with Design Condition loads for inside the limit of reinforcement, as specified in subsection NB of the ASME Code.

Table 20C-9 Load Nomenclature

Load	Description
P	Internal design pressure.
PMAX	Peak pressure.
DW	Dead weight.
DML	Design Mechanical Loads (other than DW). This includes Service Level A loads and RVOS loads that are Service Level B.
XL	External mechanical loads, such as the nozzle reactions associated with piping systems, will be combined with other loads in the loading combination expressions.
SSE	SSE (inertia portion).
FV	Fast valve closure.
RVC	Relief/safety valve – closed system (transient).
RVOS	Relief/safety valve – open system (sustained).
RVOT	Relief/safety valve – open system (transient).
DY	Dynamic load associated with various service conditions including FV, RVC, and RVOT is applicable (transient).
DN	Dynamic load associated with Level A (Normal) service conditions including FV, RVC, and RVOT as applicable (transient).
DU	Dynamic load associated with Level B (Upset) service conditions including FV, RVC, and RVOT as applicable (transient).
DE	Dynamic load associated with Level C (Emergency) service conditions including FV, RVC, and RVOT as applicable (transient).
DF	Dynamic load associated with Level D (Faulted) service conditions during which, or following which, the piping system being evaluated must remain intact including FV, RVC, and RVOT as applicable. This includes postulated pipe rupture events (transient).
DYS	Dynamic load associated with various service conditions (sustained).
SSES	Seismic anchor motion portion of SSE.
ES	Seismic anchor motion of earthquake smaller than SSE.
DBPB	Design basis pipe break, includes LOCA and non-LOCA (transient).
HYDSP	Building structure motions due to automatic depressurisation system sparger discharge.
DBPBS	Design basis pipe break, includes LOCA and non-LOCA (sustained).
SRSS	Square root of the sum of the squares (mathematical operator).

Table 20C-10 Summary of Examination Requirements for the Steam Generator

Description	Examination Method		
	Volumetric	Surface	Visual
Primary Side			
Tubesheet to Channel Head weld	X	–	–
Inlet nozzle inside radius section	See Note 1	–	See Note 1
Outlet nozzle inside radius section	See Note 1	–	See Note 1
PRHR nozzle inside radius section	See Note 1	–	See Note 1
Inlet nozzle to safe end butt weld	X	X	–
Outlet nozzle to RCP casing butt weld	X	X	–
PRHR nozzle to safe end butt weld	X	X	–
Studs and nuts	–	–	X
CVS nozzle to Channel Head weld	–	X	–
Pressure retaining boundary	–	–	X
SG heat transfer tubing	X	–	-
Secondary Side			
Elliptical head knuckle to upper shell weld	X	–	–
Tubesheet to lower shell weld	X	–	–
Start-up feedwater nozzle to shell weld	X	X	–
Start-up feedwater nozzle inside radius section	See Note 3	–	–
Main feedwater nozzle to shell weld	X	X	–
Main feedwater nozzle inside radius section	X	–	–
Steam outlet nozzle inside radius section	See Note 2	–	–
Welded attachments(4)	–	X	–

Notes:

1. Inspection requirements allow for substitution of volumetric examination with enhanced magnification visual examination.
2. The main steam outlet nozzle is not considered to have an inside radius section. It is integrally forged with elliptical head.
3. IWC-2500 excludes this examination; only applicable to nozzles having NPS > 12.
4. Associated with the full penetration welded intermediate and upper lateral support trunnions and support pads respectively.

Table 20C-11. Index of Technical Reports

Document Reference	Document Title	Description
Reports		
APP-MB01-Z0-101	SG Design Specification	Establishes the basis for the materials, design, operability, regulatory requirements, manufacture, inspection, testing, packaging and preparation for shipment of the AP1000 SGs. This provides the basis to ensure that the design and construction of the SG conforms to the rules set forth in the ASME Code for Class 1 and Class 2 vessels.
APP-MB01-Z0R-100	AP1000 SG Generic Design Report	Consolidates the results of the detailed analyses required to demonstrate the adequacy of the structural design to sustain and meet, in every respect, the requirements and provisions of the ASME Code and of the Design Specification APP-MB01-Z0-101.
APP-RCS-M1-001	RCS Design Transients	Defines the transients used to qualify the reactor coolant system to design requirement.
WCAP-14040-NP-A	Methodology Used to Develop Cold Overpressure Mitigating System Setpoints and RCS Heatup and Cooldown Limit Curves	Method to develop overpressure protection set-points and heat-up/ cool-down curves.
APP-GW-VH-002	Packaging Nuclear Components and Spare Parts for Shipment and Storage	Provides details of the requirements for the packaging of nuclear components and spare parts when being shipped or placed in storage.
APP-GW-Z0-602	Cleaning and Cleanliness Requirements of Equipment for Use in Nuclear Steam Supply System and Associated Systems	Provides details of the cleaning and cleanliness requirements of equipment for use in the nuclear steam supply system along with associated systems.
APP-MB01-VMR-001	AP1000 Component ISI Inspectability Assessment: SG	Identifies general code, inspectability and access requirements for SG components.

Table 20C-11. Index of Technical Reports (cont.)

Document Reference	Document Title	Description
Reports (cont.)		
UKP-MV01-Z0R-100	Results of Weld Ranking Process for Reactor Vessel, SG and Pressurizer – Defect Tolerance	Identifies welds to be included in the phased programme planned for defect tolerance assessments.
APP-GW-VW-001	AP1000® Design for Inspectability Program: ISI Requirements and Design Guidance for Class 1 Components	Identifies general code, inspectability and access requirements for ASME Class 1 components.
APP-GW-VW-002	AP1000 Design for inspectability programme: ISI requirements for class 2 and 3 components	Identifies general code, inspectability and access requirements for ASME Classes 2 & 3 components.
APP-GW-VLR-010	AP1000 Supplemental Fabrication and Inspection Requirements	Provides details of the AP1000 supplemental fabrication and inspection requirements.
APP-GW-Z0-608	Material Test Specification for Austenitic Stainless Steel Cladding	Provides details of the test specification for materials testing of austenitic steel cladding.
Process Specifications		
APP-GW-VW-011	Additional Requirements for AP1000 SG Welding Consumables	Identifies additional requirements for SG welding consumables.
APP-MB01-VW-011	Supplemental Welding Requirements for SG Fabrication	Identifies supplemental welding requirements for SG fabrication.
APP-MB01-VW-021	Engineering Requirements for Welding Procedure Qualifications for ASME Code Section III-NB Pressure Boundary Overlay and Attachment Welds	Identifies welding qualification requirements.

Table 20C-11. Index of Technical Reports (cont.)

Document Reference	Document Title	Description
Materials Specification		
APP-VL52-Z0-022	SA-240 Type 304 (UNS S30400) Stainless Steel Plate (Section III-NB)	Specification for SG component/weld material.
APP-VL52-Z0-201	SA-479 Type 410, UNS S41000 (Section II)	Specification for SG component/weld material.
APP-VL53-Z0-012	SB-167, UNS N06690, Alloy 690 Seamless Pipe and Tube (Section II)	Specification for SG component/weld material.
APP-VL52-Z0-011	SB-168, UNS N06690, Section III-NB (Alloy 690 Plate)	Specification for SG component/weld material.
APP-VL52-Z0-012	SB-168, UNS N06690, Alloy 690 Plate, Sheet and Strip Section II	Specification for SG component/weld material.
APP-VL51-Z0-021	SB-564, UNS N06690, Section III-NB (Alloy 690 Forgings)	Specification for SG component/weld material.
APP-VL51-Z0-020	SB-564, UNS N06690, Section II (Alloy 690 Forging)	Specification for SG component/weld material.
APP-VL52-Z0-002	SB-166, UNS N06690, Alloy 690 Rod and Bar (Section II)	Specification for SG component/weld material.
APP-VL52-Z0-001	SB-166, UNS N06690, Alloy 690 Rod and Bar (Section III-NB)	Specification for SG component/weld material.
APP-VL53-Z0-011	Thermally Treated Alloy UNS06990 (Alloy 690) Tubing for AP1000	Specification for SG component/weld material.

Table 20C-11. Index of Technical Reports (cont.)

Document Reference	Document Title	Description
Materials Specification (cont.)		
APP-GW-VH-001	AP1000 Site Receiving, Inspection, and Storage Requirements for System Materials and Equipment	Specification for SG component/weld material.
APP-GW-Z0-620	AP1000 Requirements for Marking of Reactor Plant Components and Piping	Specification for SG component/weld material.
APP-VL52-Z0-021	SA-240 Type 405 Stainless Steel Plate (Section III-NB)	Specification for SG component/weld material.
APP-VL52-Z0-030	SA-516 Grade 70 Plate (Section II)	Specification for SG component/weld material.
APP-VL52-Z0-029	SA-516 Grade 70 Plate (Section II)	Specification for SG component/weld material.
APP-VL52-Z0-031	SA-516 Grade 70 Carbon Steel Plate (Section III-NB)	Specification for SG component/weld material.
APP-VL51-Z0-001	SA-508 Grade 1A Forgings (Section III-NB)	Specification for SG component/weld material.
APP-VL52-Z0-004	SA-479, Stainless Steel Anti-Vibration Bar, Type 405 (UNS S40500) ASTM Standard	Specification for SG component/weld material.
APP-VL52-Z0-003	SA-479 Type 405 (UNS S40500) Stainless Steel Hot-Rolled Bar (Section II)	Specification for SG component/weld material.
APP-VL51-Z0-011	SA-336 Grade F316LN Forging (Section III-NB)	Specification for SG component/weld material.

Table 20C-11. Index of Technical Reports (cont.)		
Document Reference	**Document Title**	**Description**
Materials Specification (cont.)		
APP-VL51-Z0-002	SA-508/SA-508M Grade 3 Class 2 Forgings (Section III-NB)	Specification for SG component/weld material.
APP-VL52-Z0-071	SA-36 Carbon Steel Shapes, Plates, and Bars (Section II)	Specification for SG component/weld material.
APP-VL52-Z0-042	SA-533 Type B Class 2 Plate (Section III-NB)	Specification for SG component/weld material.
APP-VL53-Z0-031	SA-335 Grade P11 Seamless Ferritic Steel Pipe (Section II)	Specification for SG component/weld material.
APP-VL52-Z0-091	SA-194 Ferritic Steel Nuts Grade 7, Chromium-Molybdenum (Section III-NB)	Specification for SG component/weld material.
APP-VL52-Z0-301	SA-739 Grade B11 Bar (Section II)	Specification for SG component/weld material.
APP-VL53-Z0-231	SA-234 Grade WP11 Seamless Alloy Steel Fittings (Section II)	Specification for SG component/weld material.
APP-VL53-Z0-131	SA-234 Grade WPB Seamless Carbon Steel Piping Fittings (Section II)	Specification for SG component/weld material.
APP-VL53-Z0-232	SA-234 Grade WP11 Class 1 Seamless Alloy Steel Fittings (Section II)	Specification for SG component/weld material.
APP-VL52-Z0-081	SA-193, Ferritic Steel Bolting Material Grade B7, Chromium-Molybdenum (Section II)	Specification for SG component/weld material.
APP-VL52-Z0-005	SA-193, Ferritic Steel Bars and Bolting Grade B7, Chromium-Molybdenum (Section III-NB)	Specification for SG component/weld material.

Materials Specification (cont.)		
APP-VL53-Z0-111	SA-106 Grade B Seamless Carbon Steel Pipe (Section II)	Specification for SG component/weld material.
APP-VL51-Z0-031	SA-105 Carbon Steel Forgings (Section II)	Specification for SG component/weld material.
APP-VL53-Z0-001	SA-213 Grade TP304 (UNS S30400) Stainless Steel Tubing (Section III-NB)	Specification for SG component/weld material.
APP-VL52-Z0-007	Material Specification for SA-194 Grade 1 Carbon Steel Nuts (Section II – Special Requirements)	Specification for SG component/weld material.
APP-VL52-Z0-302	Material Specification for SA-739 Grade B22 Bar (Section II)	Specification for SG component/weld material.
APP-VL52-Z0-051	Material Specification for SA-696 Grade C Carbon Steel Bars (Section II with Additional Requirements)	Specification for SG component/weld material.

Figure 20C-1. Not Used

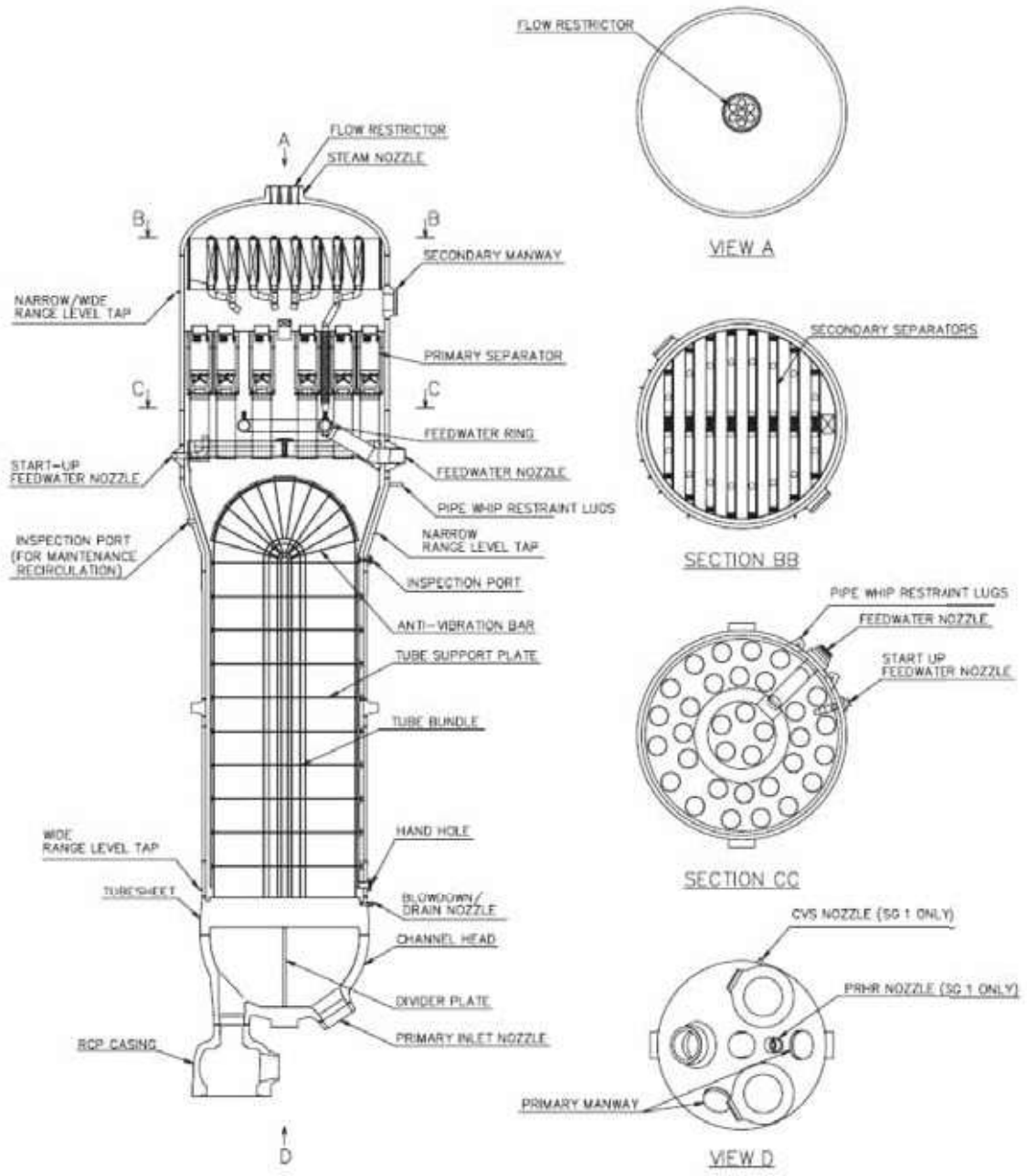


Figure 20C-2. AP1000 Steam Generator

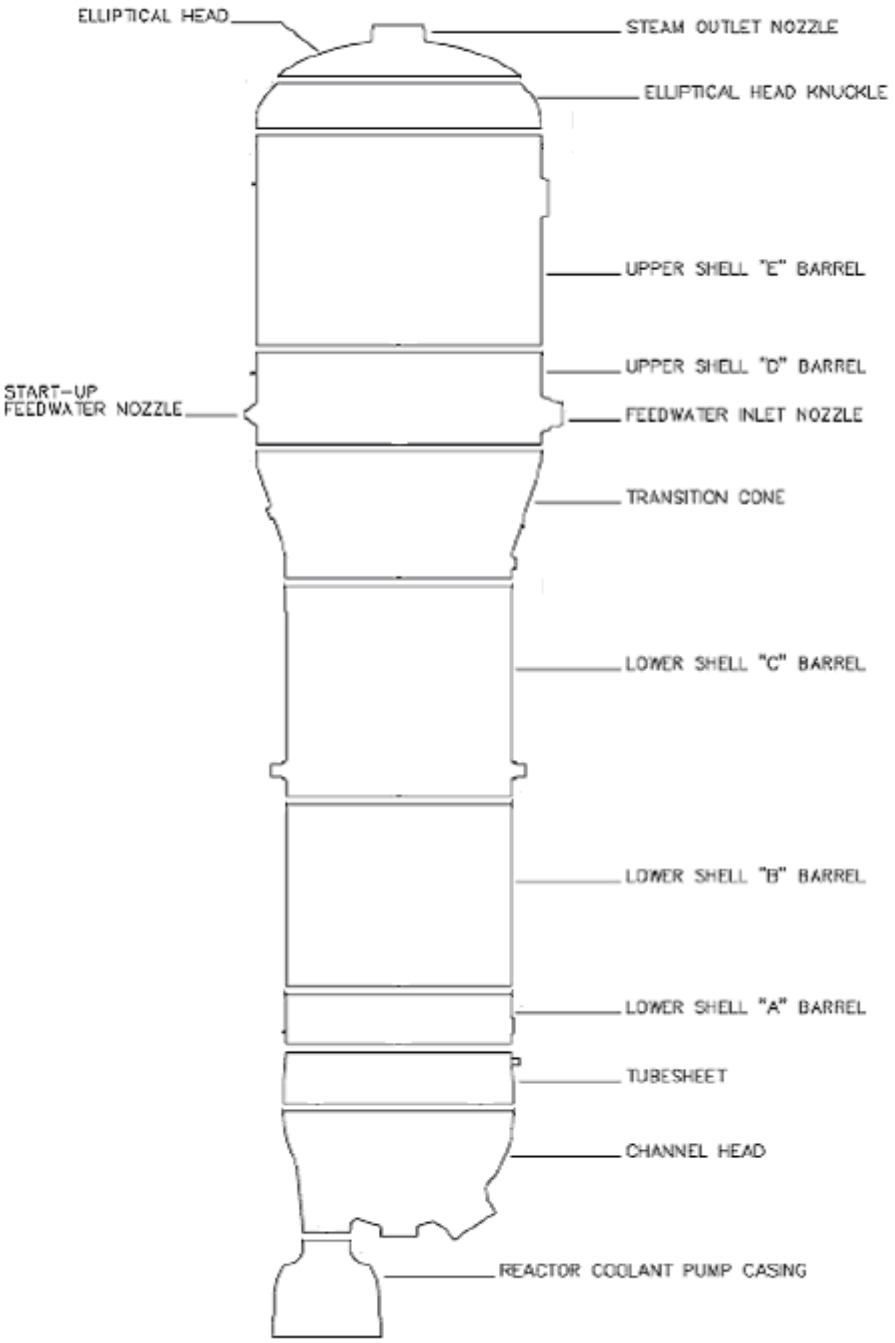


Figure 20C-3. AP1000 Steam Generator Shell

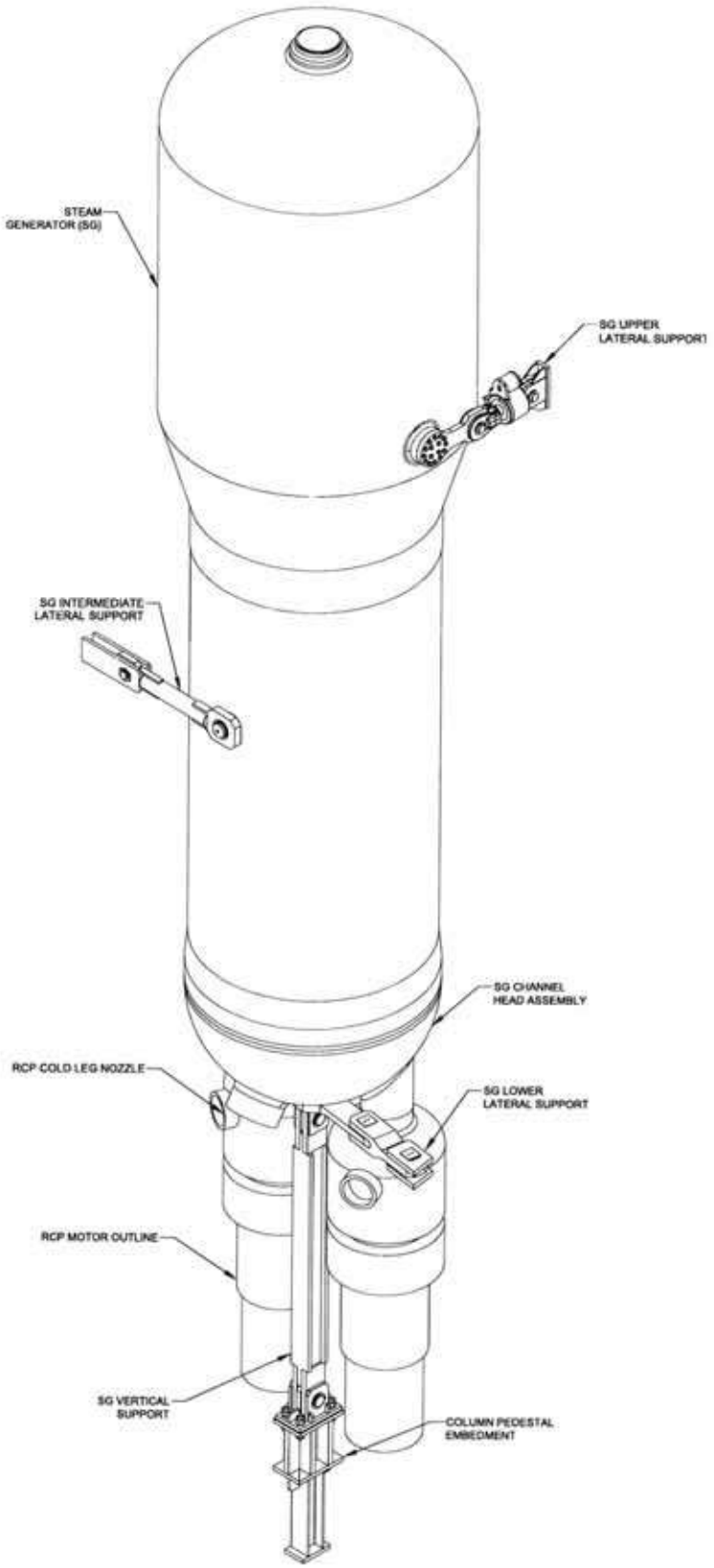


Figure 20C-4. AP1000 Steam Generator Supports

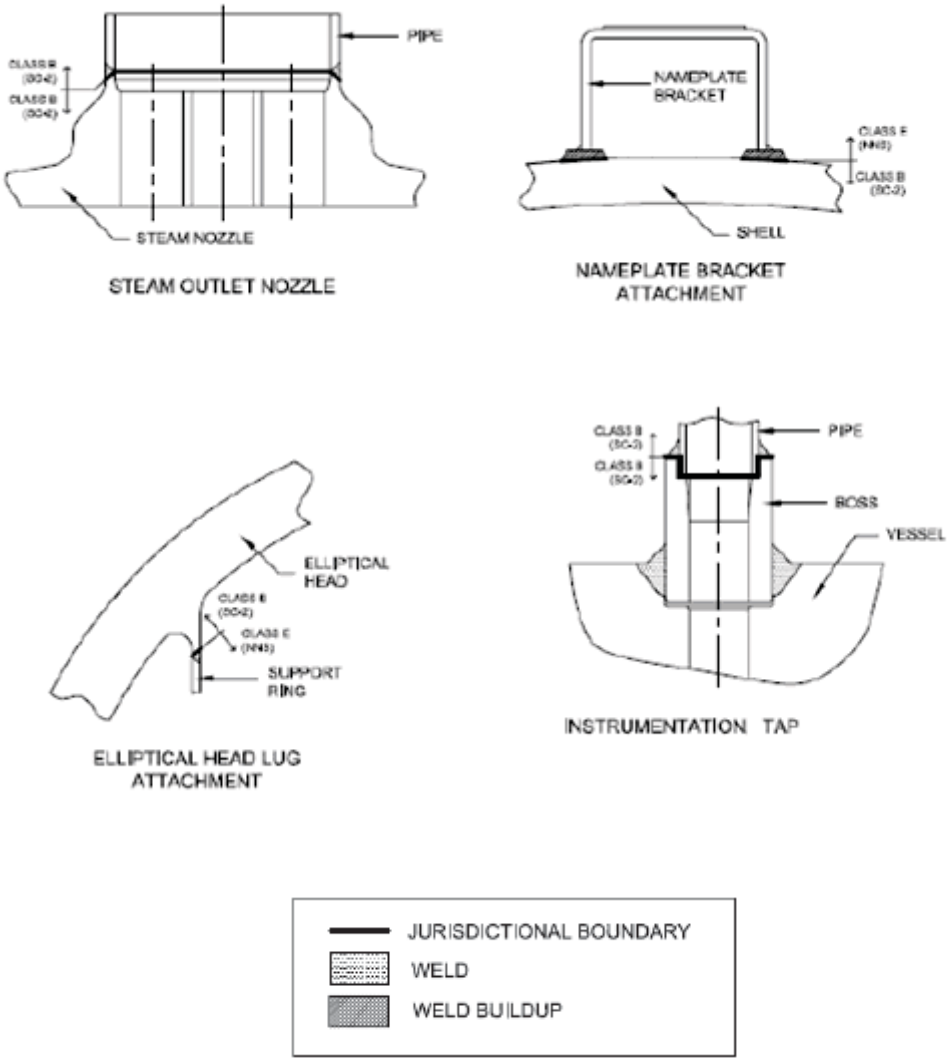


Figure 20C-5. Steam Generator Boundaries (#1)

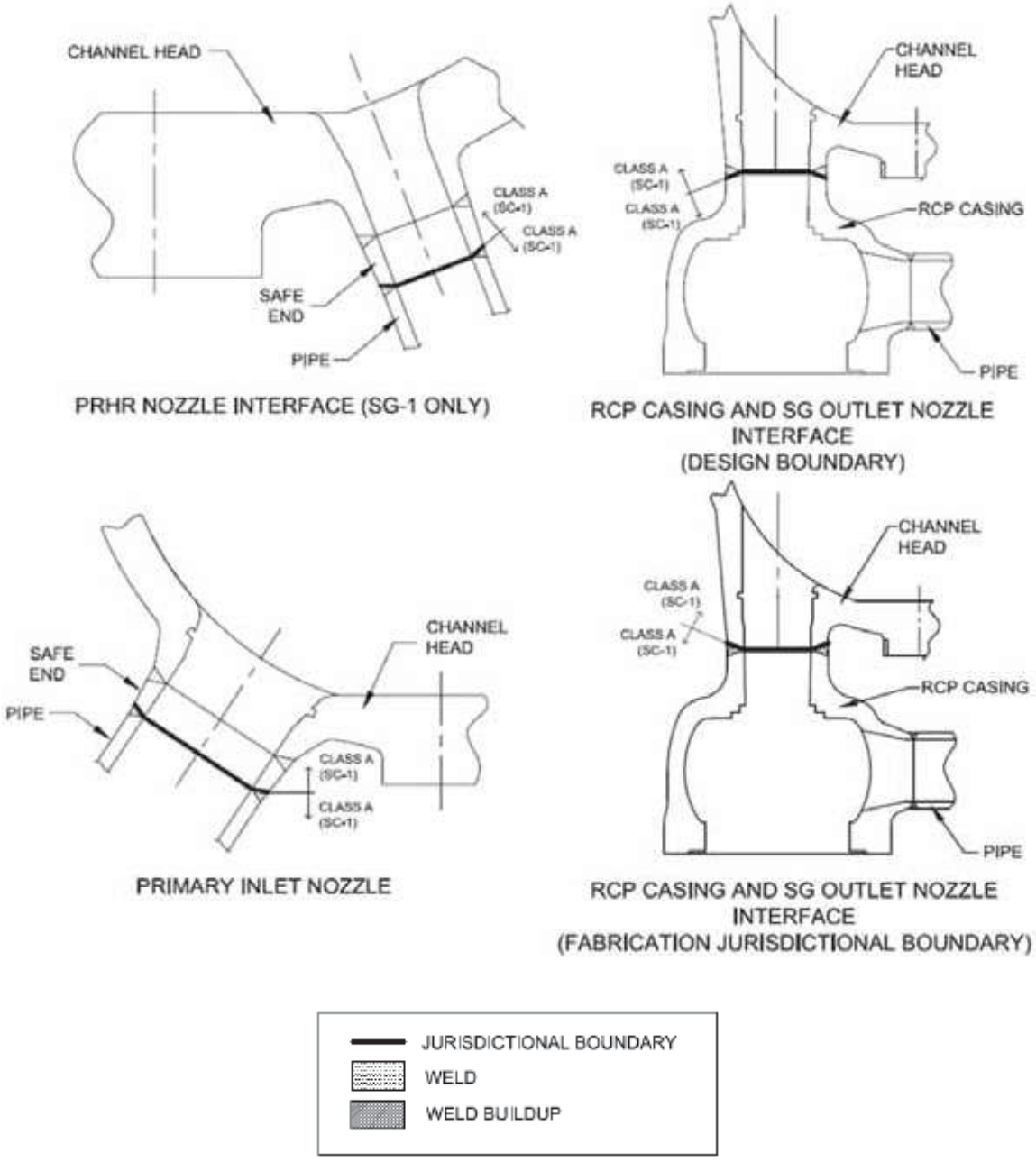


Figure 20C-6. Steam Generator Boundaries (#2)

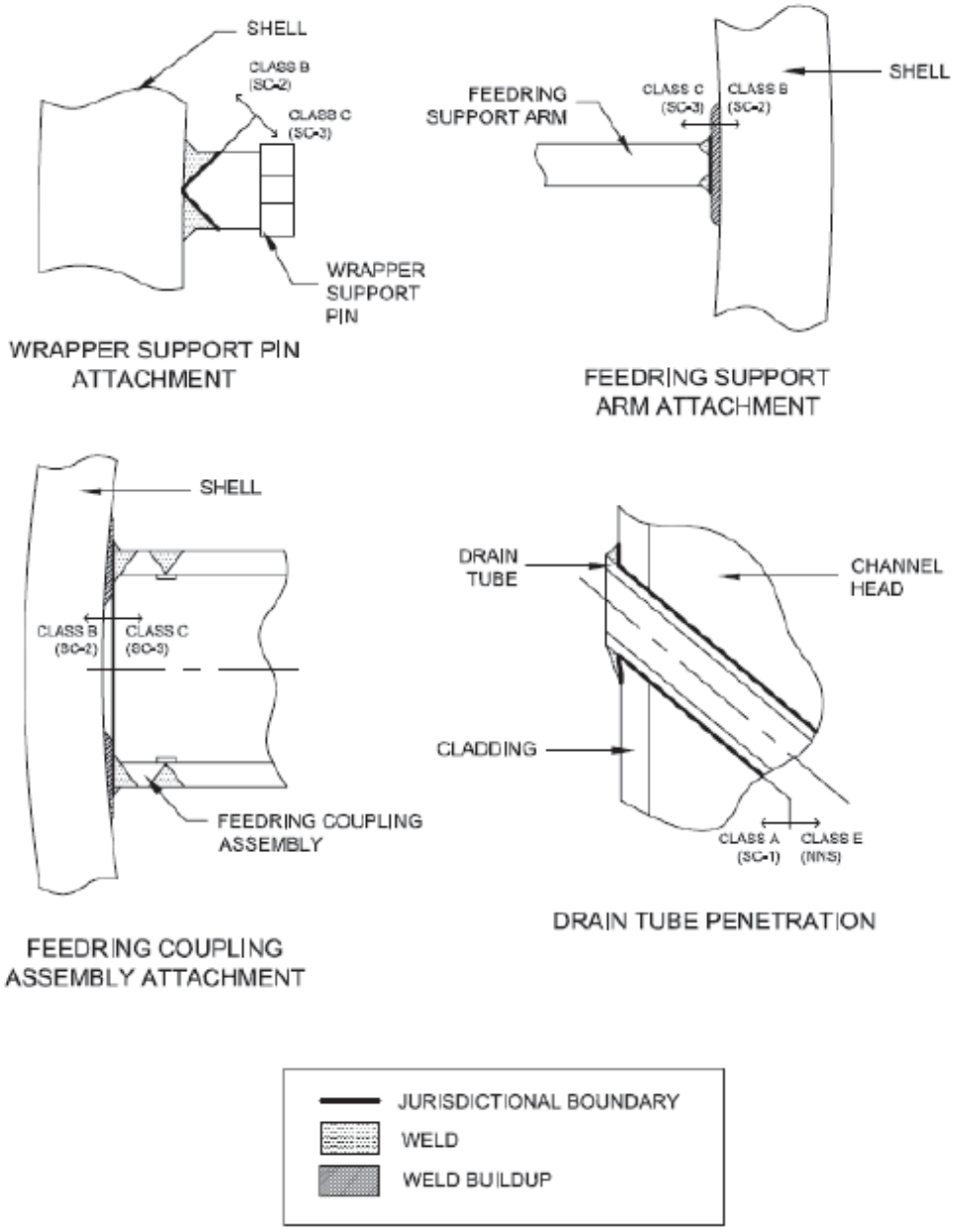


Figure 20C-7. Steam Generator Boundaries (#3)

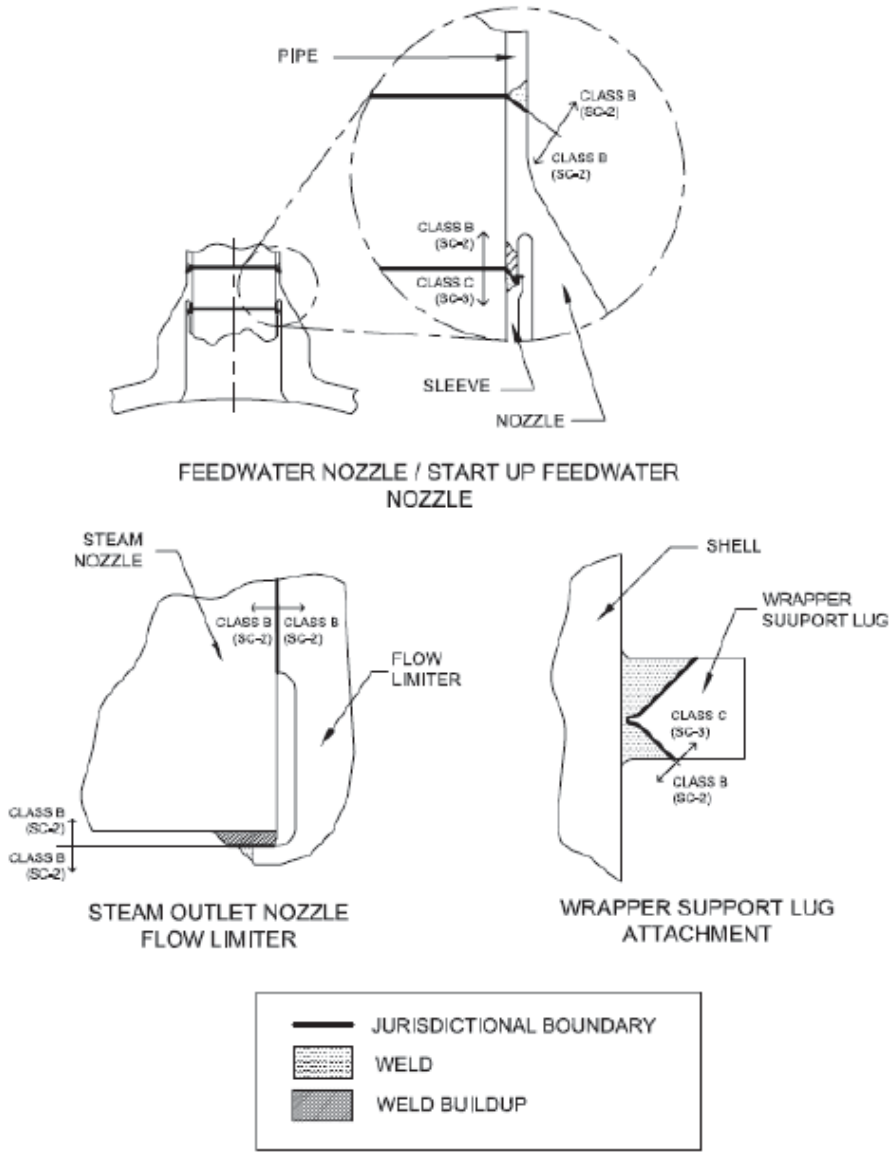


Figure 20C-8. Steam Generator Boundaries (#4)

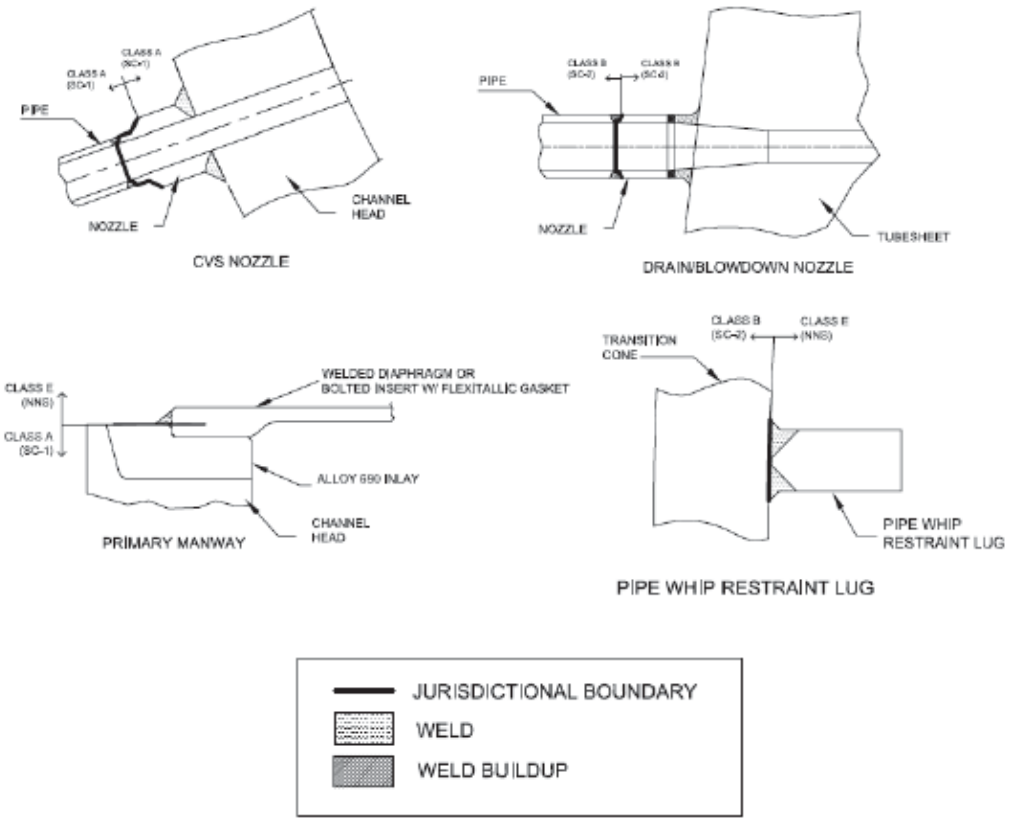


Figure 20C-9. Steam Generator Boundaries (#5)

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS AND ACRONYMS

ALARP	as low as reasonably practicable
ANSI	American National Standards Institute
ASME	America Society of Mechanical Engineers
AVT	all-volatile treatment
CFR	Code of Federal Regulations
CSR	Component Safety Report
CV	containment vessel
GDA	generic design assessment
GTAW	gas tungsten arc welding
HI	high integrity
HSS	highest safety significance
ISI	in-service inspection
LOCA	loss-of-coolant accident
MSIV	main steam isolation valve
MSL	main steam line
MSLB	main steam line break
MSS	main steam system
MTS	main turbine system
NDE	nondestructive examination
NRC	Nuclear Regulatory Commission
PCSR	Pre-construction safety report
P&ID	Piping & instrumentation diagram
PORV	power-operated relief valve
PWHT	post-weld heat treatment
RCS	reactor coolant system
SCC	stress corrosion cracking
SFR	safety functional requirement
SG	steam generator
SGS	steam generator system
SSC	system, structure, or component
TIG	tungsten inert gas
UK	United Kingdom
US	United States

APPENDIX 20D
MAIN STEAM LINE

20D.1 Introduction

This is the component safety report (CSR) for the AP1000 main steam line (MSL) as introduced in Section 20.2. The safety argument herein substantiates the structural integrity of the MSL to a degree of rigour commensurate with the consequences of gross structural failure. The safety argument is supported by identification of a suite of documentary evidence outlined in Section 20D.5 regarding the quality of design, manufacture, installation and operation of the MSL.

20D.1.1 Scope

This report addresses all nuclear and radiological hazards potentially arising from gross structural failure of the MSL for the entire design lifetime objective of 60 years. Conventional hazards to personnel safety are outside the scope of this Appendix 20D.

This assessment is limited to the piping running from the steam generator (SG) steam outlet nozzle to the Line 11 anchor point on the Auxiliary Building wall where the piping is connected to the main steam system (MSS). The scope does not include any other components of the steam generator system (SGS), MSS or any other systems. The physical boundaries of the MSL are identified in Section 20D.1.6.

The scope of this report is restricted to consideration of those pressure, temperature, and mechanical loadings within the design basis. The design basis includes normal operating conditions, anticipated transients, and postulated accident conditions.

20D.1.2 Objectives

This CSR supports that the claim that the AP1000 plant risk remains both tolerable and as low as reasonably practicable (ALARP) for the design lifetime. For the purposes of the structural integrity assessment, this claim is substantiated by satisfying structural integrity safety design bases for all safety-significant systems, structures, or components (SSCs). The safety design bases, applied across the operational, process and lifecycle scope of the safety case, embody the technical scope of the safety case: if these can be maintained at all times, the plant will be acceptably safe. Specific safety functional requirements (SFRs) for the MSL are developed from the structural integrity safety design bases, and correspond to the functions that need to be maintained to provide assurance of nuclear and radiological safety. The SFRs applicable to the MSL are identified in Section 20D.2.1.

20D.1.3 Interface with other Safety Case Documents

The safety argument presented in this report is supported by a dossier of technical data, specifications and analyses. These are listed in the Technical Index (Section 20D.5).

20D.1.4 Main Steam Line Description

The MSL is part of the SGS, which supplies steam to the MSS and subsequently to the main turbine system (MTS) over a range of flows and pressures covering the entire operating range from system warmup to maximum calculated turbine conditions at full power operation. There are two MSLs in the AP1000 plant. Each MSL is routed from the top of its respective SG, dropping to a horizontal run below the containment operating deck. From there, the

MSLs separately penetrate the containment vessel (CV) and are each routed through their own physically separated main steam and feedwater isolation valve compartment in the auxiliary building to the pipe anchors located at the structural interface between the auxiliary building and the turbine building (Wall 11), where the MSL terminates into the MSS piping. Each MSL within the SGS has one main steam isolation valve (MSIV), six main steam safety valves, one power-operated relief valve (PORV), and one PORV block valve.

Key system pressures, temperatures and flowrates are given in Table 20D-1. A sectional elevation of the nuclear island is shown in Figure 20D-1, where the MSLs can be seen running from the top of the steam generators. A general arrangement of the nuclear island is provided in Reference 20D.1 which shows the MSL pipework running through the containment penetration in the containment vessel, and into the individual MSIV (main steam isolation valve) compartments. Isometric drawings of both MSLs are given in References 20D.2 to 20D.9. Figure 20D-2 shows a detailed view of the containment penetration. This includes bellows to minimise piping loads applied to the CV and a guardpipe to protect the bellows and to prevent over pressurisation of the containment annulus in a postulated pipe rupture event. Similar features are present on feedwater penetrations.

The MSL pipe is 965 mm (38") nominal outside pipe diameter with 44.2 mm (1.74") minimum wall thickness after American Society of Mechanical Engineers (ASME) allowable wall thickness is adjusted for bending. The MSL is manufactured from the ASME SA-335 Gr P11 seamless ferritic alloy-steel pipe for high temperature service. The MSL is fabricated from various pipe lengths using the tungsten inert gas (TIG) method (known as gas tungsten arc welding (GTAW)) in the US).

Codes and standards utilised in the design of the MSL are applied according to the AP1000 equipment class of the component. The MSL piping is designed in accordance with relevant requirements of the ASME Boiler & Pressure Vessel Code (Code), Section III, as discussed in Section 20D.3.2. Schematics of MSL Loops A and B are shown on the Steam Generator System piping and instrumentation diagram (P&ID) in Reference 20D.10 and 20D.11.

20D.1.5 Function

The SGS (and hence MSL) is required during start-up and operation at power, to remove the heat produced by the reactor core; and also in the initial phase of shutdown operation before the normal residual heat removal system can be connected, to remove the decay heat from the reactor core. The heat sinks are provided either by venting steam to the atmosphere or by the turbine bypass system dumping steam to the condenser. Each MSL passes through the containment boundary.

The system is provided with a MSIV and associated MSIV bypass valve on each MSL from its respective SG. These valves are located outside the containment boundary and provide the ability to isolate the secondary side of each SG to prevent the uncontrolled blowdown of more than one SG, and also to isolate downstream portions of the system. Also located in each MSIV compartment are the six (6) main steam safety valves; every one of these safety valves vents to atmosphere through two discharge pipes and vent paths. The safety valves are spring operated and are designed to ensure that the pressure limitations of the SG, and subsequently the MSL, are not exceeded. Downstream of the safety valves is the power-operated atmospheric relief valve, which vents to atmosphere through a vent pipe and silencer. The operation of the power-operated relief valves is automatically controlled by steam line pressure during plant operations: the power-operated relief valves automatically modulate open and exhaust to atmosphere whenever the steam line pressure exceeds a

predetermined set point; as steam line pressure decreases, the relief valves modulate closed. Their capacity is sufficient to exhaust the steam produced during any design basis initiating event before the pressure rise threatens the integrity of the steam generator or the MSLs. They also provide defence-in-depth safety by cooling down the SGs and the reactor coolant system (RCS) in conjunction with the power-operated atmospheric relief valves when the condenser is not available. Each MSL is anchored at the point where it passes through the wall between the auxiliary building and the turbine building; the section of it from the SG to the anchor has sufficient flexibility to accommodate thermal expansion. Beyond this wall the two MSLs are cross-connected into a common header, which itself subsequently branches into four lines to the turbine stop valves; the connections to the two moisture-separator reheaters, the gland sealing system and the turbine bypass are also in this common header.

A postulated gross failure of MSL piping has been considered to establish appropriate structural reliability targets. Such failure could also result in consequential damage to nearby SSCs, through pipe whip, explosion or missiles. The layout configuration and material of construction of the MSLs are designed to maintain low pipe stresses in these areas. Thus, pipe rupture restraints are not required, and the loop is analysed for pipe ruptures only for small auxiliary lines.

20D.1.6 Boundaries

The physical boundaries for safety case assessment of the MSL, are identified below:

- SG steam outlet nozzle safe end weld;
- Circumferential girth weld to MSS piping at Line 11.

20D.2 Safety Case Requirements

As identified in Section 20D.1.2, the principal objective of this CSR is to demonstrate that the SFRs allocated to the MSL piping, established in Section 20D.2.1, will be maintained for all conditions within the design basis. This objective is to be achieved by substantiating the structural reliability of each component of the MSL piping against targets that are commensurate with the consequences of gross failure of that component. These targets are determined by means of a United Kingdom (UK) AP1000 component structural integrity classification process as described in Section 20D.2.2, where structural reliability targets for all MSL piping components are identified. The safety argument presented in Section 20D.3 identifies evidence to support the following nuclear safety claims for the MSL piping.

Claim:	**High quality is achieved through good design and manufacture.**
Objective:	Provides evidence of good design and manufacture based on established design and manufacturing processes and use of proven materials. It provides a keystone for a demonstration of high reliability and embodies the code and plant operating experience with an objective of achieving quality of build and the avoidance of defects.
Claim:	**Good design is achieved through compliance with ASME.**
Objective:	Incorporates the build experience as embodied in the design codes.
Claim:	**Components are tolerant to through-life degradation over the design life of the plant**
Objective:	Provides an assessment of through-life degradation mechanisms and shows that such mechanisms will not threaten integrity over a specific interval.

The safety argument is tailored according to the structural reliability claims derived from a process of component classification, with the purpose of demonstrating that component structural reliability is commensurate with the consequences of gross failure.

The elements of the safety argument are provided in Section 20D.3 and the strength of the argument is discussed in Section 20D.4.

20D.2.1 Safety Functional Requirements

The pre-construction safety report (PCSR) identifies structural integrity safety design bases for AP1000 SSCs. These are requirements of plant systems, some duty, some accident response, which must be maintained at all times to provide assurance of plant nuclear and radiological safety. As identified in Table 20-1, the MSL is allocated the following SFRs:

SFR 20.5.1 The MSL is required to maintain the integrity of the primary coolant pressure boundary during standby, normal operation and under design basis faulted conditions for the design life of the plant.

SFR 20.5.2 MSLs are required to exhibit leak behaviour in the event of a through wall defect developing (defence in depth).

SFR 20.5.3 The pipework in the vicinity of the containment penetrations is required to maintain the integrity of the pressure boundary during standby, normal operation and under design basis faulted conditions for the design life of the plant.

SFR 20.5.4 The pipework in the vicinity of the containment penetrations above 50 mm (2 in) is required to exhibit leak behaviour in the event of a through wall defect developing (defence in depth).

The associated MSL containment penetrations also form part of the CV and the following relevant SFR for the containment penetrations applies from the performance and safety design bases allocated to the CV, as follows:

SFR 20.9.1 The CV is required to provide a leak tight barrier against the uncontrolled release of radioactivity to the environment under postulated accident conditions for the design life of the plant and to assure that the containment design conditions important to safety are not exceeded for as long as postulated accident conditions require.

Postulated failure modes which result in a loss of these SFRs lead to identification of structural reliability targets commensurate with the consequences of gross failure, as determined through the process of component classification as described in Section 20D.2.2. The safety argument in Section 20D.3 is provided to establish that structural integrity of the MSL and associated containment penetrations will be maintained for all conditions within the design basis and thus demonstrate that all of the above SFRs will be maintained at all times.

20D.2.2 Main Steam Line Structural Integrity Classification

Key to the MSL structural integrity safety case is the clear understanding of the potential radiological consequences of any postulated gross failure mode. Based on this understanding, a structured and systematic basis can be established for setting the level of rigour applied during the design assessment, material procurement, fabrication, in-manufacture inspection, testing and in-service testing, maintenance, inspection and safety case assessment of the component. Details of the approach for developing AP1000 component structural integrity safety cases are given in the 'UK AP1000 Structural Integrity Classification' report at Reference 20D.13.

The approach to structural integrity classification is consistent with the overall AP1000 safety classification scheme as detailed in Chapter 5. In this, three broad classifications for UK SSCs are defined, requiring judgment to be made with respect to the component's importance to safety, these are defined as Class 1, Class 2 and Class 3. In practice, for the MSL and other AP1000 components, this classification scheme is too coarse to determine component structural integrity requirements, since Class 1 covers a very broad range of initiating event frequencies and consequences and hence a commensurately broad range of structural reliability targets. Reference 20D.13 details the approach taken whereby a more detailed assessment of selected individual components is made to establish the consequences of gross failure, due to both direct consequences such as a loss-of-coolant accident (LOCA), and indirect consequences, such as the effect of missiles, jet loading or pipe whip on essential safety systems. Based on this, and in accordance with the scheme identified in Reference 20D.13, components are ascribed one of the following five structural integrity classifications:

- Highest safety significance (HSS)
- High integrity (HI)
- Standard Class 1
- Standard Class 2
- Standard Class 3

The unmitigated direct consequences of gross failure of the MSL have been assessed in Reference 20D.13 and gross failure of the MSL is analysed within the design basis main steam line break (MSLB) and is protectable without core damage and does not result in over-pressurisation of the containment. A failure of the MSL (MSLB) is analysed at hot zero power (section 9.1.5) and at full power (section 9.1.6) to demonstrate the event can be mitigated without core damage. The analysis of the peak containment pressure incurred due to a MSLB is provided in Section 9D.3. However, considering the possible indirect consequences, there is potential for pipe whip since pipe supports are not specifically designed to prevent this. A review based on detailed interrogation of 3D models indicated that damage to containment as a result of pipe whip is not credible. The potential for pipe whip of the casualty line to rupture the non-casualty MSL leading to a double MSLB was also evaluated. The double MSLB is outside the design basis and could lead to core damage and over-pressurisation of the containment, which consequently could lead to the most severe off-site consequences against which there is no claimed protection. However, evaluation of the potential for a double MSLB due to pipe whip determined the geometry does not allow for pipe whip of the casualty line to affect the non-casualty line. As such, the MSL inside containment is classified as a Standard Class 1 component.

Other parts of the MSL lie outside containment in the MSIV. Failure of the MSL is analysed within the design basis MSLB. Flow restrictors in the outlet nozzle on the SG serve to limit the magnitude of the resulting plant transient and hence the direct consequences of an MSLB

would not lead to unacceptable radiological consequences. The wall between the MSIV compartment and the main control room, and the floor slab between the MSIV compartment and the Class 1 electrical equipment room are evaluated for pipe whip and jet impingement loads for worst case breaks in either the MSL or the main feedwater line due to their proximity to the main control room and Class 1 electrical room. UK Class 1 equipment inside containment is protected against the indirect consequences of an MSLB that occurs outside containment. Indirect consequences from a gross failure of a main steam line have the potential to affect the equipment upper elevations of the auxiliary building. The loss of equipment in the upper elevations of the auxiliary building would not affect the passive system used to put the plant in a safe shutdown condition should an event occur. Additionally, supplemental deterministic design controls are required which include additional analysis, design criteria, fabrication and construction criteria, and in-service inspection criteria.

On the basis that unacceptable consequences would not occur, the MSL and feedwater line in the MSIV compartments outside containment are classified as Standard Class 1 components, but they are subject to supplemental deterministic design controls.

20D.3 Safety Argument

For a Standard Class 1 component, the primary safety argument is that design and manufacture in accordance with the ASME Code provides the basis against which adequate structural reliability can be claimed for a Standard Class 1 component. The basis of the safety case for the MSL is, therefore, the arguments and evidence to substantiate the following claims.

- Claim 1: High quality will be achieved during manufacture (Section 20D.3.1).
- Claim 2: Good design is achieved through compliance with ASME (Section 20D.3.2).
- Claim 3: In-Service Degradation is Avoided (Section 20D.3.3).

20D.3.1 High Quality is Achieved During Manufacture

The design, manufacture and inspection of the MSL piping and welds will accord with the appropriate requirements of relevant sections of the ASME Code. This demonstrates that the measures applied to achieve a high quality of build and the avoidance of defects are suitably robust and appropriate to the safety classification of the piping.

To ensure that there is a high degree of control over the achievement of high quality during manufacture, the following controls on the manufacturing records and procedures are specified in References 20D.15 (for shop fabricated piping) and 20D.14 (for field fabricated piping and installation) as part of the piping design specification.

Materials Specification

The materials specified for the different parts of the main steam piping from the SGs to the turbine stop valves is presented below.

Description of Main Steam Piping	
Segment	**Material Specification**
SG outlet to containment penetration	SA-335 Gr. P11 seamless pipe
Containment penetration to MSIV	SA-335 Gr. P11 seamless pipe
MSIV to auxiliary/turbine building wall	SA-335 Gr. P11 seamless pipe

The AP1000 MSL materials comply with the corresponding material specification permitted by the ASME Code, Section III, Division 1. All ASME III material will be manufactured in accordance with the ASME II material specifications included in the 1998 edition, 2000 Addendum of ASME II.

The mechanical testing requirements for each material are contained within the relevant material specifications. For the MSL these will be carried out in accordance with ASME III Section NC-2000.

Code Class 2 pressure retaining material, except as exempted by NC-2311, will be impact tested and accepted in accordance with NC-2300. Code Class 3 pressure retaining material, except as exempted by ND-2311, will be impact tested and accepted in accordance with ND-2300. The acceptance standards for both Class 2 and 3 piping tests will satisfy the applicable lowest service temperature requirements as per NC-2332 and ND-2332.

Materials for parts within the jurisdiction of the ASME Code will have certified material test reports clearly presenting the results of all ASME Code required testing. All other materials will be designed to be certified as required by the applicable material specifications, but as a minimum by a certificate of compliance.

Bending Procedures

Prior to bending any of the piping being undertaken copies of the manufacturer's bending procedures, including qualification test results for ASME III Piping for each material to be bent will be submitted to Westinghouse. Bending will not be started until the Contractor's bending procedures are approved.

Heat Treatment after Bending or Forming

Heat treatment procedure will be submitted for review by Westinghouse prior to the start of heat treatment. Carbon and low-alloy steel piping such as that used in the MSL does not require heat treatment if it has been bent or formed in the temperature range of 1,650°F to 2,000°F (899°C to 1,093°C) and cooled in still air.

Weld Procedures

As detailed in References 20D.14 and 20D.15, welding of all materials will be done in accordance with welding procedures and using certified welders that have been qualified according to the rules of Sections III and IX of the ASME Code and the supplemental requirements detailed in Reference 20D.18. Control of welding variables (as well as

examination and testing) during procedure qualification and production welding is performed according to ASME Code requirements. Specific details of welding processes, selection and control of welding consumables, welding procedure qualification, pre-heat, interpass temperatures and post heating requirements are provided in Reference 20D.18. All welding, welding procedure qualification, and welder qualification will be in accordance with the requirements of ASME III for Code Classes 1, 2, and 3 piping, and the additional requirements of Reference 20D.14.

Post Weld Heat Treatment

Post weld heat treatment (PWHT) procedures will be submitted to Westinghouse for review and approval prior to the start of heat treatment. For carbon and low-alloy steel piping such as that used in the MSL, PWHT is to be in accordance with ASME III, NB-4600, NC-4600, or ND-4600 as applicable.

Manufacturing Inspections

Reference 20D.15 and Reference 20D.14 specify the test and inspection requirements for shop fabricated pipework and field fabricated and installed pipework, respectively. A summary of the examinations and tests for pipework and fittings is provided. These include requirements for materials and welds. Supplemental inspection requirements are defined in Reference 20D.18.

All NDE for Code Classes 1, 2, and 3 piping welds will be performed in accordance with ASME III NB-5000, NC-5000, or ND-5000, as applicable. All personnel performing NDEs will be qualified and certified in accordance with SNT-TC-1A and ASME III NB-5500, NC-5500 or ND-5500, as applicable. The MSL welds are all to be subject to 100% volumetric ultrasonic manufacturing inspections from the outer diameter.

Mechanical Testing

In accordance with ASME II SA-335 a hydrostatic test of each length of pipe supplied will be carried out. Shop hydrostatic tests are also carried out on the MSL containment penetrations, and these are checked prior to their installation on plant.

After installation, Code Classes 1, 2 and 3 piping systems will be pressure tested in accordance with ASME III (Reference 20D.14). The requirements for hydrostatic testing are given in ASME III NC-6200. The test temperature is selected so that the possibility of brittle fracture is minimised. The test pressure is 1.25 times the design pressure, and is 10.343 MPa abs (1500 psia) for the MSL. The test is held at the design pressure and then reduced to the design pressure of 1200 psia (8.274 MPa abs) and examined for leaks.

Cleaning and Contamination Protection Procedures

Materials used in the fabrication, installation, and testing of nuclear steam supply components and systems are handled, protected, stored, and cleaned according to recognised, accepted methods designed to minimise contamination that could lead to deterioration.

20D.3.2 **Good Design is Achieved Through Compliance with ASME**

Compliance with relevant and internationally well-established codes, standards and regulations to control the quality of design and manufacture provides assurance that an appropriate level of structural reliability will be achieved. Compliance with the ASME Code provides assurance over a diverse range of relevant aspects including material procurement,

component design, selection of manufacturing consumables, qualification of welders, specification of heat treatment, manufacturing quality checks and nondestructive examination (NDE), testing, installation and manufacturing, pre-service and in-service inspection requirements.

The codes, standards and regulations that are specified to control quality of MSL piping design and manufacture embody extensive relevant experience that helps to ensure a structurally robust design and provides a means to prevent, minimise and control component degradation at the design stage. Compliance with the codes, standards and regulations, therefore provides a foundation for assuring that MSL piping structural integrity will be maintained for the design lifetime.

The MSL is designed to meet the requirements of ASME Code, Section III class B (ASME III Code Class 2/Class MC), or class C (ASME III Code Class 3). The AP1000 Class 2, 3 Piping and B31.1 Extensions Design Specification report (Reference 20D.16) is the Westinghouse design specification for ASME Class 2 and 3 piping. This document specifies that ASME Class 2 and 3 piping, will be designed, analysed, fabricated, and constructed in accordance with the ASME Code, Section III, 1998 Edition with Addenda up to and including 2000 (Reference 20D.17) with specific conservative usage provisions concerning the application of subsections NC and ND as detailed in the piping design criteria for the AP1000 Plant (Reference 20D.19).

The AP1000 Specification for Field Fabricated Piping and Installation, ASME Code, Section III, Classes 1, 2, and 3 and ASME B31.1 (Reference 20D.16), in conjunction with the Piping Design Specification (Reference 20D.14), and the AP1000 Specification for Shop Fabricated Piping (Reference 20D.15) including references therein, constitute a complete ASME Code, Section III Design Specification and provides the complete basis for the design, fabrication, installation, testing, and Code certification of ASME Code, Section III piping systems.

Appendix 15A summarises the safety classification and categorisation of mechanical and fluid systems, structures, and components. The MSL containment penetrations at SGS-PY-C01A and SGS-PY-C01B respectively, are designed to ASME III, MC.

Evidence of compliance with ASME requirements is provided by ASME certification of the MSL piping at the construction stage of AP1000 NPP development, supported by an assessment to demonstrate compliance with relevant design code requirements.

Other codes, regulations and standards apply to the MSL pipework and are tabulated in References 20D.14, 20D.15 and 20D.16. These include American National Standards Institute (ANSI) and ASME standards, Westinghouse Documents, US Code of Federal Regulations (CFRs), and US Nuclear Regulatory Commission (NRC) Regulatory Guides.

20D.3.3 Mitigation and Management In-Service Degradation

To demonstrate that the design has taken account of in-service degradation mechanisms, evidence to substantiate the following argument is provided:

- A structured process has been applied to identify in-service degradation mechanisms.
- The design has been optimised to mitigate against the risk from in-service degradation mechanisms.

Forewarning of degradation is identified through in-service inspection.

20D.3.3.1 Identification of Degradation Mechanisms

Westinghouse has designed, developed, and manufactured nuclear facilities since the 1950s, beginning with the world's first large central station nuclear plant (Shippingport), which produced power beginning in 1957. Westinghouse has since designed and delivered more than 100 commercial nuclear power plants worldwide, including the design of Sizewell B in the UK, with a combined electrical generating capacity in excess of 90,000 MW. The design of the AP1000 MSL is, therefore, supported by decades of successful plant operating experience which has accumulated many operating years. Westinghouse has substantial proven experience, knowledge, and capability to design, manufacture and furnish technical assistance for the installation, start-up and service of nuclear power plants.

The substantial record of safe operating experience provides confidence that there is a thorough understanding of the in-service performance of the MSL, the management and mitigation of through-life degradation issues and in the avoidance of issues at the design and manufacturing stage that can affect the through life performance.

In high-energy piping, there are material degradation mechanisms that could adversely affect the integrity of the system. The following is a list of potential degradation mechanisms relevant to the MSL:

- Erosion-corrosion induced wall thinning
- Stress corrosion cracking (SCC)
- Water hammer
- Fatigue
- Thermal aging
- Thermal stratification
- Other mechanisms

Erosion-Corrosion Induced Wall Thinning

The MSLs in the AP1000 are fabricated from SA-335 Grade P11 Alloy steel. Erosion-corrosion induced wall thinning is not expected in the main steam line. Extensive work has been done investigating erosion-corrosion in carbon steel pipes. The main steam line has low susceptibility to erosion due to the pipe material composition, which has sufficient levels of chromium to preclude erosion-corrosion material loss. Susceptibility is also low due to the relatively high operating temperature and the high quality steam in the MSL.

Based on the above discussion, erosion-corrosion induced wall thinning does not have an adverse effect on the integrity of the MSL piping.

Stress Corrosion Cracking

The main steam piping is constructed from ferritic steel. SCC in ferritic steels commonly results from a caustic environment. A source of a caustic environment in the main steam piping would be moisture carryover from the SG. However, the secondary side water treatment utilises all-volatile treatment (AVT). AVT effectively precludes causticity in the SG bulk liquid environment. For some operating plants prior to implementing AVT, the phosphate water treatment caused a caustic chemical imbalance resulting in SCC of SG tubing. Under AVT water treatment conditions, there are no instances of caustic SCC on the

ferritic steam lines, indicating no significant caustic carryover. The operating secondary side chemistry precludes SCC on the ferritic main steam line.

Based on the above discussion, SCC does not have an adverse effect on the integrity of MSL piping.

Water Hammer

The steam lines are not subject to water hammer by the nature of the fluid transported. The following system design provisions address concerns regarding steam hammer within the MSL and identify the significant dynamic loads included in the main steam piping design.

Design features that prevent water slug formations are included in the system design and layout. In the MSL, these include the use of drain pots and the proper sloping of lines.

The operating and maintenance procedures that protect against a potential occurrence of steam hammer include system operating procedures that provide for slowly heating up (to avoid condensate formation from hotter steam on colder surfaces), operating procedures that caution against fast closing of the MSIVs except when necessary, and operating and maintenance procedures that emphasise proper draining.

The stress analyses for the MSL piping and components include the dynamic loads from rapid valve actuations, including actuation of the MSIVs and the safety valves.

Based on the above discussion, water hammer does not have an adverse effect on the integrity of MSL piping.

The MSL piping is designed to take account of the potential for damage due to steam-driven slugs of water, as outlined in NUREG-0371.

Fatigue

Low-cycle fatigue due to normal operation and anticipated transients is accounted for in the design of the piping system. The MSL piping complies with the stress range reduction factors of the ASME Code, Section III. Due to the nature of operating parameters, MSL piping is not subjected to any significant transients to cause low-cycle fatigue. Based on the above discussion, low-cycle fatigue is not a concern for the AP1000 MSLs.

To address high-cycle fatigue, a pre-operational test programme is implemented as required by NB-3622.3, NC-3622, and ND-3622 of the ASME Code, Section III to verify that the piping and piping restraints will withstand dynamic effects due to transients, such as pump trips and valve trips, and that piping vibrations are within acceptable levels. The piping systems to be tested include the MSL piping.

Thermal Aging

The main steam piping system does not have cast materials. The welding process used on these lines is GTAW. There are no thermal aging concerns for the carbon steel piping of the MSL and the alloy steel of the main feedwater piping. The material used for the main steam piping system is not susceptible to dynamic strain aging effects.

Thermal Stratification

The design of piping and component nozzles in the AP1000 includes provisions to minimise the potential for and the effects of thermal stratification, cycling, and striping, pursuant to actions requested in several NRC bulletins.

Thermal stratification occurs only in a pipe that has a susceptible geometry and low flow velocities. A temperature difference between the flowing fluid and stagnant fluid is also a prerequisite. The MSL piping is not subjected to thermal stratification by the nature of fluid transported.

Other Mechanisms

The MSL pipe does not operate at temperatures for which creep fatigue must be considered. Creep fatigue is a concern for ferritic steel piping operation at temperatures above 371.11°C (700°F).

Pipe degradation or failure by indirect causes such as fires, missiles, and component support failures is precluded by criteria for design, fabrication, inspection, and separation of potential hazards in the vicinity of the safety-related piping.

The material used in the MSL is highly ductile and resistant to cleavage type failure at operating temperatures. The resistance to failure has been demonstrated by material fracture toughness tests.

Overall Conclusion

Consideration of the above in-service experience and known age related degradation mechanisms confirms that these have been considered in the design process, and that the design of the MSL is not susceptible to them. In the case of fatigue caused by vibration, appropriate pre-operational tests will be carried out on the plant to confirm that this will not be a problem.

20D.3.3.2 In-Service Inspection

ISI provides forewarning of degradation mechanisms and this forms an important element of the safety case argument. The role of an effective in-service inspection (ISI) programme is twofold: firstly to detect and monitor anticipated degradation, and secondly to confirm the absence of any unanticipated degradation. ISI is used to confirm the absence of defects that could give rise to gross structural failure.

To be effective, ISI requirements should be identified according to established good practice relevant to the characteristics of each inspection location. Evidence to substantiate that this is the case for the MSL piping of ISI is provided in Reference 20D.12, where the planned ISI arrangements for MSL piping are outlined to address the requirements of IWA-1400(b) and IWA-1500 of the ASME Code Section XI, supplemented where applicable by 10CFR50.55a. Reference 20D.12 provides a statement of the inspection techniques, inspectability and access arrangements applicable to ISI for AP1000 plant although it does not constitute a fully developed Inspection Plan: this is to be developed and submitted for regulatory approval as part of the site-specific safety case following the generic design assessment (GDA). Inspection intervals are to be established for the Inspection Plan in accordance with Sub articles IWA-2400 and IWC-2400 of the ASME Code, Section XI.

Reference 20D.12 presents a summary of examination requirements for AP1000 Class 2 and 3 Components, including Class 2 and 3 piping.

20D.4 Strength of the Safety Case

All portions of the MSL have been classified as Standard Class 1 components. The safety argument in Section 20D.3 demonstrates how structural integrity of the MSL is established based on extensive quality assurance measures in design, manufacture, materials, testing, and qualified inspection. The strength of the safety case is based on achievement of integrity and that the MSL has been deterministically justified in accordance with ASME Code, Section III. The arguments presented are considered to provide a cogent basis to substantiate reliability claims commensurate with the Standard Class 1 classification of the MSL.

To substantiate this assertion this report provides a structured argument supported by suitable and sufficient evidence to achieve this, three key elements namely; Quality of Build, Good Design and Mitigation and Management In-service Degradation have shown how this will be achieved.

Quality of Build has been demonstrated by compliance with ASME Code, Section III. Material specification control has been achieved in accordance with Section II of ASME Code, NDE in accordance with ASME Code, Section III with adequate fracture toughness demonstrated by compliance with the ASME Code.

Good Design has been demonstrated by providing evidence that design transients including normal, upset, emergency and faulted conditions have been analysed and loadings shown to be within the allowable limits of ASME Code, Section III, Div 1 – 1998 Edition with Addenda up through and including 2000.

The approach to Mitigation and Management of In-service Degradation has been demonstrated by identifying all design characteristics, degradation mechanisms and potential hazards that could lead to injury, fatality or loss of operation of the MSL. ISI will also provide forewarning of degradation with inspection and maintenance carried out at appropriate intervals.

20D.5 Index of Technical Reports

A list of the main supporting documents that have been used in the preparation of this report are given in Table 20D-2, with a summary of their content.

20D.6 Review of Open Issues

There are no open issues that affect the basis of the MSL safety case arguments presented in support of GDA.

20D.7 Conclusions

A safety argument to establish that the structural reliability of the UK AP1000 MSL is commensurate with the consequences of gross failure has been presented. SFRs have been identified for the MSL, based on structural integrity safety design bases established in the PCSR. These requirements are to be maintained to ensure plant nuclear and radiological safety. For the MSL, assurance that these SFRs will be maintained for the design life of the plant is provided by substantiating structural integrity against appropriate reliability targets.

Structural reliability targets have been identified for the MSL based on the procedure of structural integrity classification discussed in Section 20.5 and in Reference 20D.13. All portions of the MSL have been classified as Standard Class 1 components.

The main element of the safety case argument is that the MSL has been designed in accordance with the high standards of the ASME Code as applicable to ASME Class 1 components. This includes tight controls on material properties, manufacturing processes, design, testing, inspection and installation such that there is a high level of confidence in the quality of the MSL and that it will enter service free from significant flaws that could affect the integrity of the MSL over its lifetime. Section 20D.5 identifies the detailed specifications and analyses that provide the evidence to support this argument.

Based on the arguments presented, together with the referenced supporting evidence, it is considered that the structural reliability of the MSL has been justified to a standard commensurate with the consequences of its gross failure.

20D.8 References

20D.1 Westinghouse Report APP-1040-P2-001, Rev. 4, "Nuclear Island General Arrangement Plan at El. 117"-6," March 2012.

20D.2 Westinghouse Report APP-SGS-PLW-30A, Rev. 2, "Steam Generator System Containment Building Rooms 11500/11701 Main Steam Line A," July 2014.

20D.3 Westinghouse Report APP-SGS-PLW-030, Rev. 4, "Steam Generator System Containment Building Room 11500 Main Steam Line A," June 2014.

20D.4 Westinghouse Report APP-SGS-PLW-031, Rev. 4, "Steam Generator System Auxiliary Building Room 12406 Main Steam Line A," June 2014.

20D.5 Westinghouse Report APP-SGS-PLW-032, Rev. 4, "Steam Generator System Auxiliary Building Room 12406 Main Steam Line A," July 2014.

20D.6 Westinghouse Report APP-SGS-PLW-40A, Rev. 2, "Steam Generator System Containment Building Rooms 11500/11702 Main Steam Line B," July 2014.

20D.7 Westinghouse Report APP-SGS-PLW-040, Rev. 5, "Steam Generator System Containment Building Room 11400/11500 Main Steam Line B," July 2014.

20D.8 Westinghouse Report APP-SGS-PLW-041, Rev. 4, "Steam Generator System Auxiliary Building Room 12404 Main Steam Line B," July 2014.

20D.9 Westinghouse Report APP-SGS-PLW-042, Rev. 5, "Steam Generator System Auxiliary Building Room 12404 Main Steam Line B," July 2014.

20D.10 Westinghouse Report APP-SGS-M6-001, Rev. 15, "Piping and Instrumentation Diagram Steam Generator System," April 2013.

20D.11 Westinghouse Report APP-SGS-M6-002, Rev. 15, "Piping and Instrumentation Diagram Steam Generator System," April 2013.

20D.12 Westinghouse Report APP-GW-VW-002, Rev. 0, "AP1000 Design for Inspectability Program: ISI Requirements for Class 2 and 3 Components and Core Internals Structures," June 2007.

20D.13 Westinghouse Report UKP-GW-GLR-004, Rev. 3, "AP1000 UK Structural Integrity Classification," January 2017.

20D.14 Westinghouse Report APP-GW-P0-008, Rev. 6, "AP1000 Specification for Field Fabricated Piping and Installation, ASME III, Code Classes 1, 2, and 3 and ASME B31.1," June 2014.

20D.15 Westinghouse Report APP-GW-P0-007, Rev. 7, "AP1000 Specification for Shop Fabricated Piping," June 2014.

20D.16 Westinghouse Report APP-PL02-Z0-102, Rev. 3, "AP1000 Class 2, 3 Piping and B31.1 Extensions Design Specification," October 2015.

20D.17 ASME Boiler and Pressure Vessel Code, 1998 Edition with 2000 Addenda, Section III, American Society of Mechanical Engineers.

20D.18 Westinghouse Report APP-GW-VLR-010, Rev. 2, "AP1000 Supplemental Fabrication and Inspection Requirements," January 2016.

20D.19 Westinghouse Report APP-GW-P1-001, Rev. 1, "Piping Design Criteria for AP1000," February 2011.

Table 20D-1. Principal System Pressures, Temperatures and Flow Rates

Parameter	Value
Maximum steam flow (lb/hr) per SG	7.49×10^6 (943.72 kg/s)
Design pressure (psia)	1200 (8.274 MPa abs)
Design temperature (°F)	600 (315.6°C)
Full plant load pressure (psia)	821 (5.662MPa abs)
Full plant load temperature (°F)	523.3 (272.9°C)
No load (hot standby) pressure (psia)	1106 (7.626 MPa abs)
No load (hot standby) temperature (°F)	557 (291.7°C)

Table 20D-2. Technical Index

Document Reference	Document Title	Description
APP-GW-P1-001	Piping Design Criteria for AP1000	Defines piping design criteria for AP1000 plant nuclear safety-related and non-nuclear safety-related piping and tubing.
APP-PL02-Z0-102	AP1000 Class 2, 3 Piping and B31.1 Extensions Design Specification	ASME Class 2 & 3 piping design – Part of MSL design specification.
APP-GW-P0-007	AP1000 Specification for Shop Fabricated Piping	Technical and QA requirements for furnishing shop fabricated power piping. Basis of fabrication, installation, testing and Code certification of ASME III piping systems.
APP-GW-P0-008	AP1000 Specification for Field Fabricated Piping and Installation, ASME III, Code Classes 1, 2, and 3 and ASME B31.1	Technical and QA requirements for installing field fabricated power piping. Basis of fabrication, installation, testing and Code certification of ASME III piping systems.
APP-GW-VLR-010	AP1000 Supplemental Fabrication and Inspection Requirements	Extra requirements for safety-related items, when specified.
APP-SGS-PLR-030	Piping Stress Analysis Report for Main Steam Line A from Steam Generator (RCS-MB-01) to Wall 11	The piping stress analysis for as-designed piping to qualify the MSL A to the requirements of the ASME code and the Design Specification.
APP-SGS-PLR-040	Piping Stress Analysis Report for Main Steam Line B from Steam Generator (RCS-MB-02) to Wall 11	The piping stress analysis for as-designed piping to qualify the MSL B to the requirements of the ASME code and the Design Specification.
APP-GW-VW-002	AP1000 Design for Inspectability Program: ISI Requirements for Class 2 and 3 Components and Core Internals Structures	Identifies general code, inspectability and access requirements for ASME Classes 2 & 3 components.

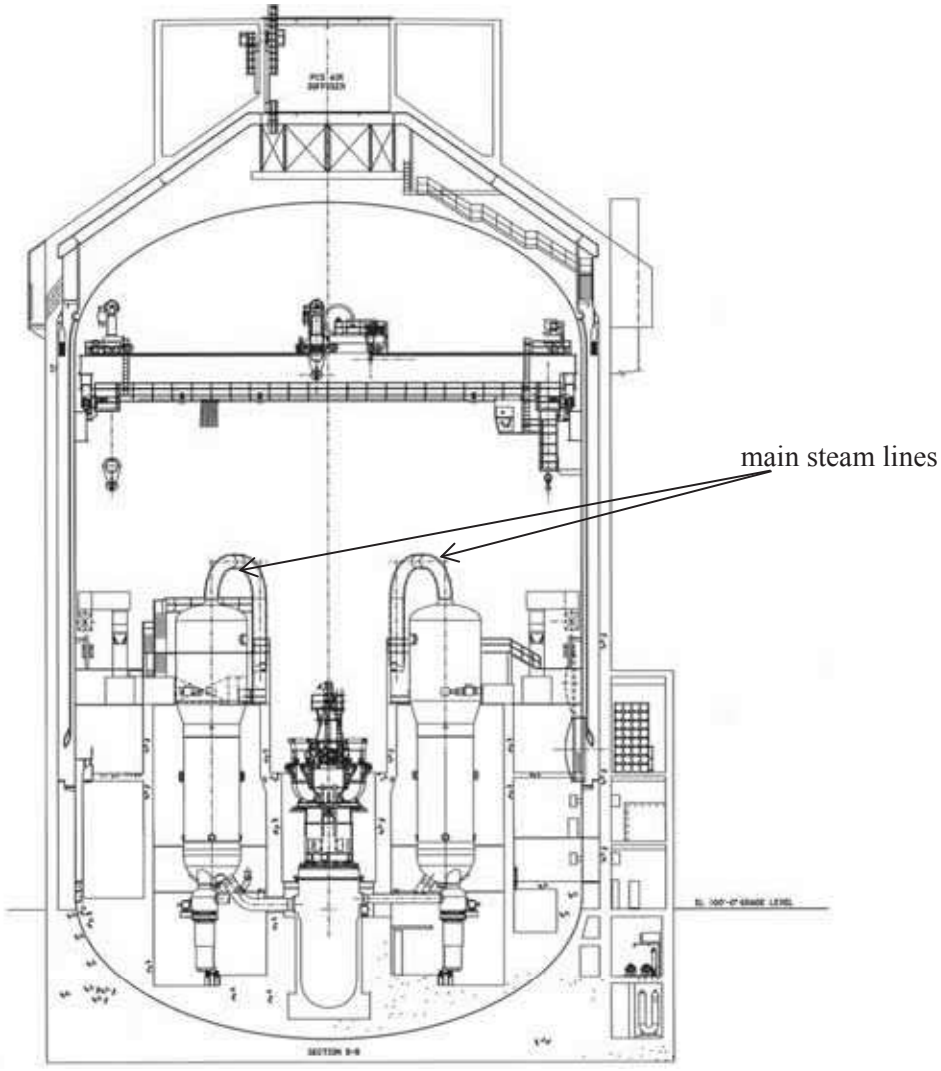


Figure 20D-1. Nuclear Island Sectional Elevation

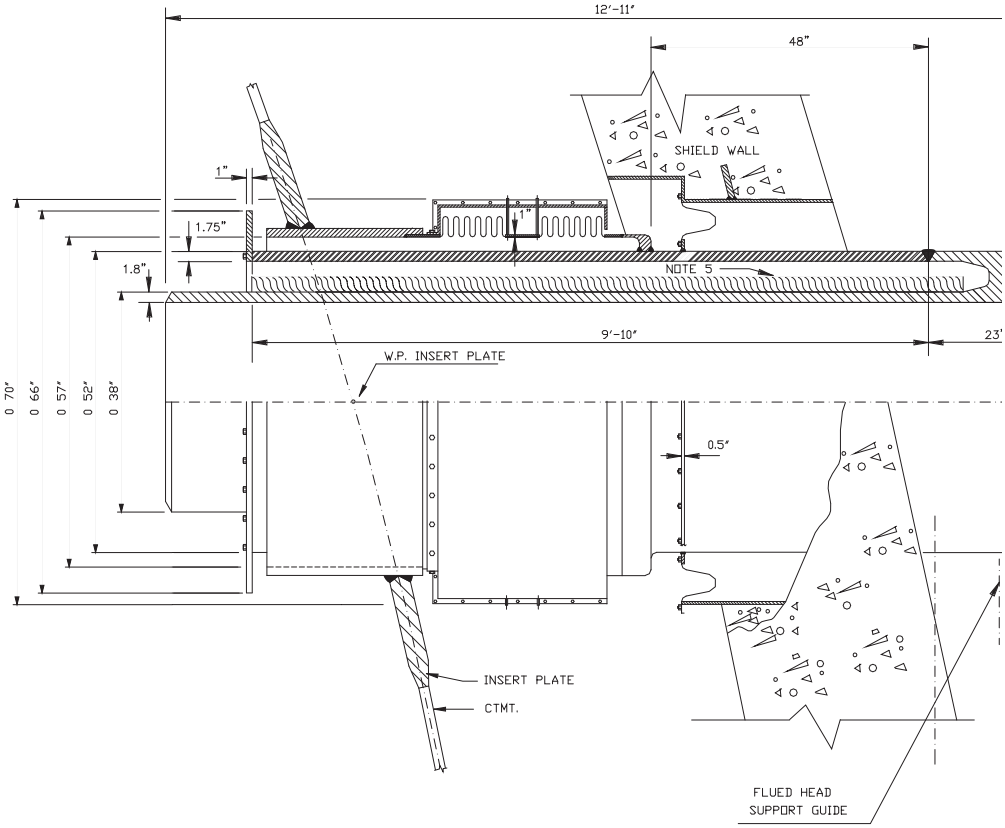


Figure 20D-2. MSL Containment Penetration

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS AND ACRONYMS

ALARP	as low as reasonably practicable
ASME	America Society of Mechanical Engineers
CFR	Code of Federal Regulations
CMTR	certified material test report
CSR	Component Safety Report
DSM	defect size margin
ELLDS	end of life limiting defect size
ENIQ	European Network for Inspection and Qualification
EPRI	Electric Power Research Institute
FUF	fatigue usage factors
GDA	generic design assessment
GTAW	gas tungsten arc welding
HI	high integrity
HSS	highest safety significance
ID	inner diameter
ISI	in-service inspection
LFCG	lifetime fatigue crack growth
LOCA	loss-of-coolant accident
NDE	nondestructive examination
NPP	nuclear power plant
NRC	Nuclear Regulatory Commission
PSI	pre-service inspection
QEDS	qualified examination defect size
RCPB	reactor coolant pressure boundary
RCS	reactor coolant system
RCL	reactor coolant loop
RV	reactor vessel
SFR	safety functional requirement
SG	steam generator
SoL	start of life
SSC	system, structure, or component
SSE	safe shutdown earthquake
TIG	tungsten inert gas
UK	United Kingdom
US	United States

APPENDIX 20E
REACTOR COOLANT LOOP PIPING COMPONENT SAFETY REPORT

20E.1 Introduction

This is the component safety report (CSR) for the reactor coolant loop (RCL) piping as introduced in Section 20.2.The safety argument herein substantiates the structural integrity of the RCL piping to a degree of rigour commensurate with the consequences of gross structural failure. The safety argument is supported by a suite of documentation outlined in Section 20E.4 that supports the design, manufacture, installation, and operation of the RCL piping.

20E.1.1 Scope

This report presents arguments to substantiate the claim that the nuclear and radiological risk potentially arising from gross structural failure of the RCL piping remains tolerably low for the 60 year design lifetime. Structural reliability targets are established on the basis of the nuclear and radiological risks associated with gross structural failure. Conventional (non-nuclear/radiological) hazards to safety are not addressed.

Reliability targets are to be substantiated for the entire design lifetime objective of 60 years. This duration of service is used to calculate fatigue usage, and to establish inspection and maintenance requirements based on anticipated degradation over the design lifetime.

The scope of the assessments includes consideration of all pressure, temperature, and mechanical loadings within the design basis. This includes normal operating conditions, anticipated transients, postulated accident conditions and test conditions.

The scope of the assessment is limited to the structural reliability of the RCL piping only and does not include other components of the reactor coolant system (RCS), of which the RCL is a part, or any other systems. A description of the RCL piping is provided in Section 20E.1.4, and physical boundaries are identified in section 20E.1.4.2 to establish the piping and welds included within the scope of this report.

20E.1.2 Objectives

Safety functional requirements (SFRs) for the safety-significant components of AP1000 nuclear power plant (NPP) are identified in Table 20-1. These SFRs must be maintained in order that AP1000 plant risk is maintained at a level that is both tolerable and as low as reasonably practicable (ALARP) for the design lifetime. The SFRs applicable to the RCL piping are identified in Section 20E.2.1. The principal objective of this CSR is, therefore, to demonstrate that the SFRs will be maintained for all conditions within the design basis.

This strategy to achieve this objective is described in Section 20E.2 and substantiation of the claimed structural reliability is provided by a safety argument in Section 20E.3, where evidence to support the nuclear safety claims is identified.

20E.1.3 Interface with Other Safety Case Documents

The safety argument presented in Section 20E.3 is supported by a dossier of technical evidence. Specific references are identified in the relevant sections of a structured safety argument in Section 20E.3, applicable codes and standards are identified in section 20E.3.1.1, and Westinghouse documents that specify and control the design and manufacture of the RCL are listed in Section 20E.5.

20E.1.4 Reactor Coolant Loop Piping – Description

The RCS includes two (2) heat transfer loops, each of which contains a steam generator (SG). Attached to each SG are two (2) reactor coolant pumps (RCPs), a single hot leg, and two (2) cold legs for circulating reactor coolant between the reactor vessel (RV) and the SGs (Reference 20E.11). In addition, the RCS includes a pressuriser (PZR), interconnecting piping and valves, and instrumentation necessary for operational control and safeguards actuation. All reactor coolant system equipment is located in the reactor containment. Figure 20F-2 and Figure 20E-1 illustrate isometric and plan views of the RCS, respectively. The RCL piping forms part of the reactor coolant pressure boundary (RCPB), which provides a barrier against the release of radioactivity generated within the reactor and is designed to provide a high degree of integrity throughout operation of the plant.

The RCS piping that connects the RV to the SG, RCPs and PZR is known as the RCL and is comprised of the following:

- Two single piece, seamless, forged austenitic stainless steel (ASME SA-376) piping sections, known as hot legs. Each hot leg is connected at one end by a pipe to safe end weld to an outlet nozzle on the RV, and at the other end by a pipe to safe end weld to an inlet nozzle located in the channel head of each SG. The nominal wall thickness of the hot leg piping is 82.6 mm (3.25 in) and the inner diameter (ID) is approximately 787.4 mm (31 in).

- Four single seamless forged austenitic stainless steel (ASME SA-376) piping sections, known as cold legs. Each cold leg is welded at one end to the safe end weld of an inlet nozzle on the RV and at the other end to the casing of a RCP; the RCP casings are in turn connected at the upstream end to SG outlet nozzles. The nominal wall thickness of the cold leg piping is 65.0 mm (2.55 in) and the ID is approximately 558.8 mm (22 in).

- A single piece seamless forged austenitic stainless steel (ASME SA-312) surge line that connects one (1) hot leg (Loop 1) to the PZR. The surge line is welded at one end to a nozzle in one hot leg, and at the other end to the PZR outlet nozzle safe end. The surge line is DN 450 (nominal pipe size (NPS) 18), Schedule 160 piping.

The RCL piping includes nozzles that connect to auxiliary systems piping. The piping associated with these auxiliary systems is not included within the scope of this CSR, but is described here in order that the role of the RCL nozzles that connect to these systems can be understood. Figure 3-1 of Reference 20E.11 provides a simplified sketch of the RCS including depiction of the connecting auxiliary systems. The auxiliary systems are described in the AP1000 class 1 piping and non-class 1 extensions design specification (Reference 20E.2) and include the following:

- PZR safety relief subsystem

- RCS automatic depressurisation subsystem (ADS)

- RV head vent (RVHV) subsystem
- Passive core cooling system (PXS)
- Emergency core decay heat removal subsystem, consisting of one (1) Passive Residual Heat Removal Heat Exchanger (PRHR HX) and associated valves, piping, and instrumentation
- Chemical and volume control system (CVS)
- Normal residual heat removal system (RNS)

The connections of these systems to nozzles in the RCL piping are as follows:

- Two PZR spray line branch connections, welded to nozzles in Loop 1 cold legs. These lines are DN 100 (NPS 4) and merge into a single line that is welded to the PZR spray nozzle safe end.
- Branch connections from the RCL Loop 2 cold legs to the core makeup tanks (CMTs) (DN 200 (NPS 8)).
- Branch connection from the RCL Loop 1 hot leg to the PRHR HX and ADS (DN 450 (NPS 18)).
- Branch connection from the RCL Loop 2 hot leg to the ADS (DN 450 (NPS 18)).
- Branch connection from the Loop 2 hot leg to RNS line (DN 500 (NPS 20)).

20E.1.4.1 Functional Description

During operation, the RCPs circulate pressurised water through the RCL and primary components. The pressurised water, which serves as coolant, moderator, and solvent for boric acid is heated as it passes through the core in the RV. It next flows via the hot legs into the SGs where the heat is transferred to the SG secondary side water, and then is returned to the RV via the RCPs and cold legs to repeat the process. The surge line connects the RCL to the PZR to provide a means of controlling RCS pressure within specified limits. The functions of the auxiliary systems connected to the RCL piping are described in Reference 20E.2.

Figure 20E-2 provides a schematic illustration of the flow within the RCS and Table 20E-1 identifies the principal pressures, temperatures, and flow rates of the RCS piping at the locations identified in Figure 20E-2 under normal steady-state, full-power operating conditions. These parameters are based on the best-estimate flow at the pump discharge.

20E.1.4.2 Physical Boundaries

The physical boundaries of the RCL piping contribute to the definition of the scope of this report, as discussed in Section 20E.1.1. The boundaries are identified as follows:

- The boundaries of the ends of the two (2) RCL hot legs are, at one end, the pipe to safe end welds to outlet nozzles on the RV, and at the other end at the pipe to safe end welds that connect to the inlet nozzles at the channel head of each SG. The physical boundaries at the connections between the hot legs and ancillary systems are at the nozzle to pipe weld connecting to the ancillary piping.

- The boundaries of the ends of the four (4) RCL cold legs are, at one end, the safe end weld to RV inlet nozzles, and at the other end the weld to the RCP. The physical boundaries at the connections between the cold legs and ancillary systems are at the cold leg nozzle to pipe weld connecting to the ancillary piping.

- The boundaries of the surge line are at the circumferential weld connecting a nozzle on the hot leg (Loop 1) and at the other end at the surge line pipe to PZR outlet nozzle safe end weld.

The welds described above are considered as pressure boundary welds per the American Society of Mechanical Engineers (ASME) Code and are included within the scope of this report.

20E.2 Safety Case Requirements

As identified in Section 20E.1.2, the principal objective of this CSR is to demonstrate that the SFRs allocated to the RCL piping, established in Section 20E.2.1, will be maintained for all conditions within the design basis. This objective is to be achieved by substantiating the structural reliability of each component of the RCL piping against targets that are commensurate with the consequences of gross failure of that component. These targets are determined by means of a United Kingdom (UK) AP1000 component structural integrity classification process as described in Section 20E.2.2, where structural reliability targets for all RCL piping components are identified. The safety argument presented in Section 20E.3 identifies evidence to support the following nuclear safety claims for the RCL piping.

Claim 1: High quality is achieved through good design and manufacture

Objective: The safety argument will seek to establish that the design, manufacture and inspection of the RCL piping will be in accordance with the appropriate requirements of relevant sections of the ASME Boiler and Pressure Vessel Code (ASME Code). This code embodies considerable operating experience relevant to the RCL piping and adherence to the relevant code requirements and forms a keystone for demonstrating quality of build, high integrity and the avoidance of defects. Additional requirements for qualified manufacturing inspections of the most safety significant welds are identified.

Claim 2: Design assessment of the RCL will demonstrate compliance with relevant design code requirements

Objective: An assessment of the RCL piping design in accordance with the requirements of Section III of the ASME Code is specified, with the objective of demonstrating that the appropriate design limits for stress and fatigue for all relevant service conditions are satisfied.

Claim 3: Forewarning of failure is provided by in-service inspection

Objective: In-service inspection (ISI) represents the preferred method to provide forewarning of failure. It provides a means of monitoring and controlling anticipated degradation and also can confirm the absence of unanticipated degradation mechanisms. Evidence is provided to demonstrate that the ISI arrangements are sufficient to provide timely warning before structural failure of RCL piping could occur.

Claim 4: Leak behaviour provides further forewarning of gross structural failure of the reactor coolant loop

Objective: Leak monitoring adds defence in depth to the argument that effective forewarning of failure will be provided by ISI. Diverse means to warn of leakage from the RCS are identified.

The elements of the safety argument are provided in Section 20E.3 and the strength of the argument is discussed in Section 20E.4.

20E.2.1 Safety Functional Requirements

Table 20-1 identifies SFRs for AP1000 systems, structures, or components (SSCs). The following SFRs are applicable to the RCL piping:

- **20.4.1**: The pipework is required to maintain the integrity of the RCPB during standby, normal operation and under design basis faulted conditions for the design life of the plant.

- **20.4.2**: Leak behaviour provides forewarning of gross failure of the reactor coolant loop.

Postulated failure modes, which result in a loss of these SFRs, lead to the identification of structural reliability targets commensurate with the consequences of gross failure, as determined through the process of component classification, as described in Section 20E.2.2 below. The safety argument in Section 20E.3 is provided to substantiate that these structural reliability targets will be achieved and thus demonstrate that the SFRs will be maintained at all times.

20E.2.2 RCL Structural Integrity Classification

A structured and systematic approach has been applied to establish the appropriate level of rigour to be applied in the design assessment, material procurement, fabrication, in-manufacture inspection, testing and in-service testing, maintenance, inspection and safety case assessment of the RCL piping. This involves a process of structural integrity classification of the components, as described in Section 20.5 and detailed in the AP1000 UK structural integrity classification (Reference 20E.3). The classification process entails a detailed assessment of AP1000 components to establish the consequences of gross failure due to both direct consequences, such as a loss-of-coolant accident (LOCA), and indirect consequences, such as the effect of missiles, jet loading or pipe whip on essential safety systems.

The RCL piping components have been determined to have a structural integrity classification of Standard Class 1. The basis for the classification of the RCL to RV nozzle safe end welds, the RCL to SG/RCP welds, and the surge line are shown in Table 20-9, Table 20-10, and Table 20-19, respectively.

The Standard Class 1 classification of the RCL components is informed by the LOCA analysis reported in Section 9.6.4. Passive protection systems are identified in Table 20-9, Table 20-10 and Table 20-19 that mitigate the consequences of failure for a range of break sizes up to and including a guillotine break of the largest pipe. The classification is also supported by assessment of pipe whip, jet impingement, asymmetric and subcompartment pressurisation performed in support of Reference 20E.16. Additionally, core depressurisation forces following a loss of coolant accident were evaluated in Reference 20E.17.

As identified in Table 20-9, Table 20-10 and Table 20-19, the anticipated effects arising from a guillotine break of the large bore pipework is not anticipated to result in core damage.

20E.3 SAFETY ARGUMENT

The structural integrity classification for Standard Class 1 necessitates demonstration of compliance with the relevant rules of the ASME Code. The structure of this safety argument is based on substantiation of the nuclear safety claims identified in Section 20E.2. These claims are addressed in this safety argument as follows:

- **Section 20E.3.1** High quality is achieved through good design and manufacture.
- **Section 20E.3.2** Design assessment of the reactor coolant loop will demonstrate compliance with relevant design code requirements.
- **Section 20E.3.3** Forewarning of failure is provided by in-service inspection.
- **Section 20E.3.4** Leak behaviour provides further forewarning of gross structural failure of the reactor coolant loop.

Evidence is presented in Section 20E.3 to show that, as a minimum, all components of the RCL piping comply with the relevant requirements of Sections II (materials), III (construction) and XI (ISI) of the ASME Code.

20E.3.1 High Quality Is Achieved through Good Design and Manufacture

The design, manufacture and inspection of the RCL piping and welds will accord with the appropriate requirements of relevant sections of the ASME Code. This demonstrates that the measures applied to achieve a high quality of build and the avoidance of defects are suitably robust and appropriate to the safety classification of the piping. To demonstrate that high quality is achieved through good design and manufacture, evidence to support the following claims is provided:

- Appropriate codes, standards & regulations are specified to control the quality of design and manufacture.
- RCL design and operation minimises the potential for in-service degradation.
- Materials specifications comply with relevant ASME Code requirements.
- Specification of reactor coolant water chemistry minimises the potential for corrosion.
- Mechanical testing demonstrates compliance with relevant material specifications.

- Welding will be conducted by suitably qualified and experienced operators in accordance with suitable and well-established procedures.
- Manufacturing inspections confirm the absence of structurally significant defects.
- Hydrostatic pressure testing confirms RCPB integrity.

20E.3.1.1 Appropriate Codes, Standards & Regulations Are Specified to Control the Quality of Design and Manufacture

Compliance with relevant and internationally well established codes, standards and regulations to control the quality of design and manufacture provides assurance that an appropriate level of structural reliability will be achieved. Compliance with the ASME Code provides assurance over a diverse range of relevant aspects including material procurement, component design, selection of manufacturing consumables, qualification of welders, specification of heat treatment, manufacturing quality checks and nondestructive examination (NDE), testing, installation and manufacturing, pre-service and in-service inspection requirements.

The RCL piping includes the hot leg and cold leg pipes with their integral branch connection nozzles, and the surge line. The design, manufacture and installation is to be undertaken in accordance with the codes, standards and regulations identified in the reactor coolant loop seamless forged and formed pipe fabrication specification (Reference 20E.4). These are summarised in Table 20E-2 and include elements of the ASME Code, ASME Code Cases, American National Standards Institute (ANSI) and ASME Standards, US Code of Federal Regulations (CFRs), United States (US) Nuclear Regulatory Commission (NRC) Regulatory Guides (RG) and a number of supplementary Westinghouse specifications and other documents. The applicable edition of the ASME Code is the 1998 Edition with addenda up through and including 2000 Addenda with an additional restriction for piping design. The restriction on piping design is that the treatment of dynamic loads, including seismic loads in pipe stress analysis, will satisfy the requirements of the ASME Code, Section III, Subarticles NB-3210, NB-3220, NB-3620, NB-3650, NC-3620, ND-3620, and ND-3650, 1989 Edition, 1989 Addenda.

The AP1000 NPP design originates in the US and as such, many of the specified codes, standards and regulations originate in that country. These are internationally well established and as such, are considered to be applicable in the UK.

The codes, standards and regulations that are specified to control quality of RCL piping design and manufacture embody extensive relevant experience that helps to ensure a structurally robust design and provides a means to prevent, minimise and control component degradation at the design stage. Compliance with the codes, standards and regulations, therefore provides a foundation for assuring that RCL piping structural integrity will be maintained for the design lifetime.

Evidence of compliance with ASME requirements is provided by ASME certification of the RCL piping at the construction stage of AP1000 NPP development, supported by an assessment to demonstrate compliance with relevant design code requirements as described in Section 20E.3.2.

20E.3.1.2 Reactor Coolant Loop Design and Operation Minimises the Potential for In-Service Degradation

The inclusion of integral branch connection nozzles within the design minimises the number of welds in the RCL piping, and thus reduces the potential for in-service degradation. Appendix B of Reference 20E.16 includes an assessment of degradation mechanisms that could adversely affect the structural integrity of AP1000 piping including the RCL. Appendix B of Reference 20E.16 identifies design measures and procedural controls that minimise in-service degradation and these aspects, where relevant to the RCL, are summarised below.

In high-energy piping, there are material degradation mechanisms that could adversely affect structural integrity and may also undermine the validity of a leak behaviour assessment. The following categories of degradation mechanism are addressed in Appendix B of Reference 20E.16:

- Resistance to wall thinning
- Stress corrosion cracking (SCC)
- Water hammer
- Fatigue
- Thermal ageing
- Thermal stratification
- Other mechanisms

These categories are discussed in turn below:

Resistance to Wall Thinning

Wall thinning by erosion and erosion-corrosion effects does not occur in the primary loop piping because Series 300 austenitic stainless steel material is highly resistant to these effects. The coolant velocity in the AP1000 primary loop is approximately 23 m/s (75 ft/s). This flow velocity is not expected to create erosion-corrosion effects, since stainless steels are considered to be virtually immune (Reference 20E.5). A review of erosion-corrosion in nuclear power systems (Reference 20E.6) reported that "stainless steels are increasingly being used due to their excellent resistance to erosion-corrosion, even at high water velocities, 40 m/s (130 ft/s)." The bend radii in the AP1000 hot and cold legs are greater than the bend radii used in the crossover legs of operating plants. There is no record of erosion-corrosion induced wall thinning in the primary loops of operating plants.

Based on the above, erosion-corrosion induced wall thinning will not adversely affect the structural integrity of RCL piping.

Stress Corrosion Cracking

SCC is not anticipated in RCL piping because the three conditions necessary for SCC to take place are not present. The three conditions are:

- There must be a corrosive environment.
- The material itself must be susceptible to SCC.
- Tensile stresses must be present in the material.

During plant operation, the reactor coolant water chemistry is monitored and maintained within specific limits (see section 20E.3.1.4). Contaminant concentrations are kept below the thresholds known to be conducive to SCC. The major water chemistry control standards are considered in the plant operating procedures.

The key to mitigation and management of a corrosive environment is control of oxygen. During normal power operation, oxygen concentration in the RCS is controlled to extremely low levels by controlling charging flow chemistry and maintaining a hydrogen overpressure in the reactor coolant at specified concentrations. Halogen concentration is controlled by maintaining concentrations of chlorides and fluorides within the specified limits and thus the likelihood of SCC in the RCL is very low. As described in Chapter 21 and in section 20E.3.1.4, periodic analysis of the coolant chemistry is performed to verify that the reactor coolant water quality meets specifications.

The elements of a water environment known to increase the susceptibility of austenitic stainless steel to stress corrosion are oxygen, fluorides, chlorides, hydroxides, hydrogen peroxide, and reduced forms of sulphur (for example, sulfides, sulfites, and thionates). Pipe cleaning minimises the potential for contamination and control of water chemistry prevents the occurrence of a corrosive environment during plant operation.

Series 300 stainless steel materials have been chosen for the RCL piping due to recorded operating experience in low-oxygen or no-oxygen environments with no significant safety-related incidents. The use of these materials in the AP1000 coolant environment is in accordance with the requirements of RG 1.44.

Design tensile stresses in the RCL are within the ASME Code, Section III allowable limits, as discussed in section 20E.3.2.2. Residual tensile stresses in RCL welds are not considered when designing in accordance with the ASME Code, Section III, since these are self-equilibrating and do not affect the failure loads. The residual stresses should not be more severe than for the operating Westinghouse pressurised water reactor plants (which have not experienced stress corrosion cracking in the primary loop).

The material used for buttering nozzles at stainless-to-carbon steel safe ends is a high nickel alloy. The nickel-chromium-iron alloy selected and qualified for this application is not susceptible to primary water SCC.

Water Hammer

The RCL is designed to operate at a pressure greater than the saturation pressure of the coolant, thus precluding the voiding conditions necessary for water hammer to occur. The RCS is designed for Level A, B, C, and D (normal, upset, emergency, and faulted) service condition transients. The design requirements are conservative relative to both the number of transients and their severity. Relief valve actuation and the associated hydraulic transients following valve opening have been considered in the system design. Other valve and pump actuations cause relatively slow transients with no significant effect on the system dynamic loads.

To provide dynamic system stability, reactor coolant operating parameters are controlled. Temperature during normal operation is maintained within a narrow range by control rod positioning. Pressure is controlled within a narrow range for steady-state conditions by PZR heaters and PZR spray. The flow characteristics of the system remain constant during a fuel cycle. The operating transients of the RCL piping are such that significant water hammer loads are not expected to occur.

Fatigue

Low-cycle fatigue due to normal operation and anticipated transients is accounted for in the design of the piping system. An assessment to demonstrate that the RCL piping complies with the fatigue usage requirements of the ASME Code, Section III is described in Section 20E.3.2.

High-cycle fatigue loads on the RCL piping and other RCPB components result primarily from pump vibrations. The steam generator is designed so that flow-induced vibrations in the tubes are avoided. The loads from RCP vibrations are minimised by criteria for pump shaft vibrations during hot functional testing and operation. During operation, an alarm signals when the reactor coolant pump vibration is greater than the limits. These measures minimise the potential for high-cycle fatigue in the RCL.

Thermal Aging

RCL piping materials are chosen in preference to cast material so that the potential for thermal ageing is minimised. The welds used in the assembly of the AP1000 plant are gas tungsten arc welds (GTAW). Due to the typically low ferrite content in GTAW, these are essentially as resistant to the effects of thermal ageing as the base metal materials.

Thermal Stratification

Thermal stratification occurs only in a pipe that has a susceptible geometry and low flow velocities. A temperature difference between the flowing fluid and stagnant fluid is also a prerequisite. The design of RCL piping includes provisions to minimise the potential for and the effects of thermal stratification, cycling, and striping as discussed below.

Thermal stratification in the RCL resulting from actuation of passive safety features is evaluated as a design transient. Stratification effects due to both Level B and Level D service conditions are considered. The criteria used in the evaluation of the stress in the loop piping due to stratification is the same as that applicable for other Level B and Level D service conditions. Section 20E.3.2 describes the design assessment which includes consideration of these design basis conditions.

The surge line has been specifically designed and instrumented to minimise the potential for thermal stratification that could increase cyclic stresses and fatigue usage. At the connection of the surge line to the hot leg, the surge line is sloped 24 degrees from the horizontal. The connection to the hot leg is in the portion of the loop piping that is at an angle with the horizontal and adjacent to the steam generator inlet nozzle. The run between the hot leg and PZR continuously slopes up. The surge line has an angle of at least 2.5 degrees to the horizontal. Changes of direction in the surge line are made using pipe bends instead of elbow fittings.

The surge line temperature is monitored for the indication of thermal stratification. The temperature is monitored at three locations using strap-on resistance temperature detectors. One location is on the vertical section of pipe directly under the PZR. The other two locations are on the top and bottom of the pipe at the same diameter on a more horizontal section of pipe near the PZR. Temperatures in the spray lines from the cold legs of one loop are measured and indicated. Alarms from these signals actuate to warn the operator of low spray water temperature or to indicate insufficient flow in the spray lines.

Hot functional testing requirements for the AP1000 plant will ensure that piping thermal deflections result in no adverse consequences. As part of the Westinghouse Owners Group

programme on surge line thermal stratification, Westinghouse collected surge line physical design and plant operational data for all domestic Westinghouse pressurised water reactors (PWRs). In addition, Westinghouse collected surge line monitoring data from approximately 30 plants. This experience was used in the development of the AP1000 thermal stratification loadings.

A monitoring programme will be implemented at the first AP1000 plant to record temperature distributions and thermal displacements of the surge line as well as pertinent plant parameters such as PZR temperature and level, hot leg temperature, and reactor coolant pump status. Monitoring will be performed during hot functional testing and during the first fuel cycle to provide evidence that the RCS is operating within specified limits of temperature and displacement.

Other Mechanisms

Creep fatigue is a concern for austenitic stainless steel piping operating at temperatures above 426°C (800°F). RCL piping does not operate at temperatures for which creep fatigue must be considered.

Pipe degradation or failure by indirect causes, such as fires, missiles, and component support failures, is precluded by criteria for design, fabrication, inspection, and separation of potential hazards in the vicinity of the safety-related piping. A deterministic justification of RCL piping against seismic event transients is provided in Reference 20E.18.

The potential for cleavage failure of RCL piping is precluded by the high ductility of the material at operating temperatures.

20E.3.1.3 Materials Specifications Comply with Relevant ASME Code Requirements

The RCL piping materials are specified in accordance with applicable requirements of the ASME Code Section II. This is confirmed following manufacture by certified material test reports (CMTRs). There is a full scale mockup test in place to confirm the material properties could be achieved (Reference 20E.7). A summary of the Section II requirements applicable to the RCL piping is provided in this section. The following elements of the ASME Code Section II are applicable to the RCL piping:

- SA-312, “Specification for Seamless and Welded Austenitic Stainless Steel Pipes.”
- SA-370, “Mechanical Testing of Steel Products.”
- SA-376, “Seamless Austenitic Steel Pipe for High-Temperature Central-Station Service.”
- SA-745, “Ultrasonic Examination of Austenitic Steel Forgings.”
- SFA-5.9, “Specification for Bare Stainless Steel Welding Electrodes and Rods.”

The RCL piping is made from austenitic stainless steels as identified in Section 20E.1.4. These are supplied in the final heat-treated condition required by the respective ASME Code, Section II materials specification for the particular type or grade of alloy. The use of sensitised stainless steels in the RCS is restricted in accordance with RG 1.44, and sensitised stainless steels are not used for the RCL piping. RCL piping is stress-relieved subsequent to bending or other fabrication operations which could result in significant residual stress in the pipe. Processes such as welding or heat treating, which apply heat to stainless steel, are controlled to minimise the potential for sensitisation of the stainless steel. During the latter stages of fabrication, the stainless steel piping is not heated above 426°C (800°F) other than locally by welding operations. The solution-annealed surge line material is subsequently formed by hot-bending followed by a solution-annealing heat treatment.

The hot and cold leg pipe material are specified in accordance with the applicable requirements of ASME Code, Section II, SA-376, TP316LN and all RCL forgings will comply with the requirements of ASME Code, Section III, Subsection NB, Article 2000. The surge line pipe material is specified in accordance with the applicable requirements of ASME Code, Section II, SA-312, TP316LN.

Reference 20E.4 identifies the following restrictions for material composition of the RCL piping. Limits are specified with regard to the concentration of elements including sulphur, phosphorous, carbon, copper, lead, tin, arsenic, and antimony. Any quantities detected will be recorded for information as part of the CMTR.

In Reference 20E.4 the grain size determination for the RCL piping is specified in accordance with ASTM E-112. The photomicrographs illustrating the microstructure (including identification, magnification, and etchant) will be provided in the CMTR. The flattening test will comply with the applicable requirements of ASME Code, Section II, SA-376, TP316LN.

Welding materials used for fabrication and installation of welds of austenitic stainless steel materials and components meet the requirements of Section III of the ASME Code. For applications using austenitic stainless steel welding material, the material conforms to ASME weld metal analysis A-8, Type 308, 308L, 309, 309L, 316, or 316L.

Austenitic stainless steel materials used in the fabrication, installation, and testing of nuclear steam supply components and systems are handled, protected, stored, and cleaned accordance with ASME NQA-1 and RG 1.37 to minimise the potential for contamination that could subsequently result in degradation of the piping.

20E.3.1.4 Specification of Reactor Coolant Water Chemistry Minimises the Potential for Corrosion

The RCS water chemistry is specified to minimise the potential for corrosion and the materials selected for RCL piping are well established for use in a PWR reactor coolant environment. Time dependant evaluations in the design analysis are based on adherence to controls on the internal environment, and Chapter 21 provides a detailed specification of water chemistry, the limits of which are summarised in Table 20A-3. The specification of reactor coolant is in accordance with the well established pressurised water reactor primary water chemistry guidelines (Reference 20E.8). The RCL piping will be exposed to a range of fluid chemistry conditions during start-up, normal operation, wet layup, and heatup conditions.

The CVS and sampling system provide an effective means to monitor and control reactor coolant water chemistry. Periodic analyses of the coolant chemistry are performed to verify that the reactor coolant water quality meets the specifications, and the CVS provides a means of chemical dosing to maintain water chemistry quality.

20E.3.1.5 Mechanical Testing Establishes Compliance with Relevant Material Specifications

RCL piping material properties are confirmed to comply with relevant design specifications by a test programme. Mechanical, metallographic, and hardness test requirements of hot leg and cold leg piping are specified in Reference 20E.4. Similar tests for the Surge Line are specified.

The mechanical testing programme for RCL piping is specified to be in accordance with ASME Code, Section II, SA-370, “Mechanical Testing of Steel Products”. A limit on the

hardness of the Type 316LN material in the final fabricated condition is specified and the procedure for hardness testing will be in accordance with SA-370 or ASTM A1038. Additional mechanical testing of RCL material is summarised below:

- Tensile testing at room temperature on finished, heat treated hot and cold leg forgings is specified in accordance with the ASME Code, Section II, SA-376.
- Grain size determination in accordance with ASTM E-112.
- Corrosion sensitisation tests in accordance with ASTM A262, Practice E.

Tensile testing of weld filler material is specified in Reference 20E.9. The results of all mechanical testing of RCL piping materials are to be included in the CTMRs to confirm that material specifications are satisfied.

20E.3.1.6 Welding Will be Conducted by Suitably Qualified and Experienced Operators in Accordance with Suitable and Well-Established Procedures

The RCL piping will use narrow gap tungsten inert gas (TIG) welding, a high quality process with low likelihood of flaw occurrence. As specified in Reference 20E.9, all welding of RCL piping is conducted in accordance with the rules of Sections III and IX of the ASME Code. Additional detailed requirements for welding processes and consumables are specified in the AP1000 supplemental fabrication and inspection requirements (Reference 20E.10). All welding is to be performed by operators who have been qualified in accordance with the ASME Code Sections III and IX. The practices for storing and handling welding electrodes and fluxes comply with ASME Code, Section III, Paragraphs NB-2400 and NB-4400.

The welding of austenitic stainless steel is controlled to mitigate the occurrence of microfissuring, or hot cracking, in the weld. Also, it has been well documented that delta ferrite is one of the mechanisms for reducing the susceptibility of stainless steel welds to hot cracking. The minimum delta ferrite level below which the material will be prone to hot cracking lies between 0 and 3% delta ferrite. Delta ferrite control is generally appropriate for welding processes used to join stainless steel parts in components designed, fabricated, or stamped according to the ASME Code, Section III, Classes 1 and 2, and core support components, except where no filler metal is used, or where such control is not applicable, such as the following: electron beam welding; autogenous gas shielded tungsten arc welding; explosive welding; welding using fully austenitic welding materials. The welding specifications also include the delta ferrite determinations for the austenitic stainless steel welding materials used for welding qualification testing and for production processing.

20E.3.1.7 Manufacturing Inspections Confirm the Absence of Structurally Significant Defects

The RCL piping is subject to manufacturing NDE in accordance with requirements established in the ASME Code and ASME NQA-1. The manufacturing inspection requirements for RCL piping are specified in Reference 20E.4. The requirements for manufacturing inspection applicable to all RCL piping are summarised, as follows.

Ultrasonic Examination

Ultrasonic examination (UT) examination is specified to be performed throughout 100% of the wall volume of each RCL pipe according to the applicable requirements of Section III of the ASME Code for RCL piping. The finished machined and heat treated forging (hot leg and cold leg piping) will be UT examined by both straight beam method in accordance with

NB-2540 and angle beam method in accordance with NB-2550 requirements. The examinations will be conducted over 100% of the accessible surfaces of the pipe wall volume.

The straight beam UT examination acceptance standard will meet NB-2540 requirements with the additional requirements per SA-745 for QL-1 for straight beam. The angle beam UT examination will be performed in two circumferential and two axial directions, where feasible.

The surge piping material will be UT examined per ASME Code Section III, NB-2550.

In the final configuration for the hot leg, cold leg, and surge line piping, the ends that will be attached to other piping will be examined using UT techniques comparable to those to be applied for ISI.

Liquid Penetrant Examination

Liquid penetrant examinations will be performed on accessible surfaces, including weld surfaces, of each finished RCL pipe and fitting according to the criteria of the ASME Code, Section III. Liquid penetrant examinations will be conducted on the pipe bends both before the bending operation and after the subsequent heat treatment. Liquid penetrant examinations will be performed on all accessible (outside and inside) surfaces of:

- Finished pipe
- Finished or machined branch connection nozzles
- Repair welds and weld overlays
- All machined weld end preparations intended for use in field welds
- Additional pre- and post-bending liquid penetrant examinations

Radiographic Examination

Radiographic examination (RT) examination, in accordance with ASME Code, Section III requirements, are specified for all RCL circumferential butt welds and branch connection nozzle welds exceeding DN 100 pipe size.

All weld repairs are to be approved prior to repair and will be recorded. The examination of any weld repair is to be repeated as required for the original weld. When the defect was originally detected by the liquid penetrant method and the repair cavity does not exceed the lesser of 9.7 mm or 10% of the thickness, it only needs to be re-examined by the liquid penetrant method.

20E.3.1.8 Hydrostatic Pressure Tests Confirm the Integrity of the Reactor Coolant Pressure Boundary

The RCS is subjected to a hydrostatic pressure test to proof the system against design pressure. The system hydrostatic test will be performed rather than a component hydrostatic test for the RCL piping. This is in accordance with the applicable requirements of ASME Code, Section II, SA-376, TP316LN.

The RCS hydrostatic pressure testing complies with IWA-5000 and IWB-5000 of the ASME Code, Section XI. Although it is planned only to conduct a single RCS hydrostatic test before the RCS enters service, ten hydrostatic test transients are included in the design for the evaluation of fatigue of RCS components due to cyclic loads.

The hydrostatic test confirms the integrity of the RCPB before operation of the plant. section 20E.3.4.2 provides details of detection of leakage from the RCS to provide warning of any significant loss of coolant throughout the period of operation.

20E.3.2 Design Assessment of the Reactor Coolant Loop Will Demonstrate Compliance with Relevant Design Code Requirements

Section III of the ASME Code provides a well established methodology for undertaking stress analysis to provide assurance of structural integrity before a component enters service. The RCL design has been assessed to confirm that stress, sizing and fatigue limits specified in Section III of the ASME Code are met.

To demonstrate that RCLs are designed to satisfy the stress, sizing, and fatigue limits specified in Section III of the ASME Code over the required period of service, the following aspects of the analyses are discussed:

- The scope of the ASME III design assessment is comprehensively specified.
- The RCL design assessment will demonstrate that relevant stress limits and end of life fatigue usage factors (FUFs) are satisfied.

20E.3.2.1 The Scope of the ASME III Design Assessment Is Comprehensively Specified

Section III Subsections NB and NC of the ASME Code require that the RCL piping design is evaluated against design, service, and test conditions and that the stresses within the RCL are shown to comply with specified allowable stress limits appropriate to the material of construction. The RCL piping design is to be justified against the requirements of the ASME Code, Section III for Class 1 components for all conditions within the design basis. The material strength properties from the ASME Code Section II (Section 2.3.1-A) are to be used in the design stress report. Materials used in the fabrication process will have material strength properties that meet or exceed the material strength properties used in the design basis for the design stress report as discussed in section 20E.3.1.3. Other parameters to be included within the scope of the design assessment are summarised in this section.

The design basis conditions are specified in terms of pressure, temperature, and mechanical loadings associated with all normal operating conditions, other anticipated transients, and postulated accident conditions. The evaluation of the service and testing conditions includes an evaluation of fatigue due to cyclic stresses. The following five categories of operating condition, as defined in ASME Code, Section III, encompass all operating conditions within the design basis of the RCL piping:

- Level A Service Conditions – Normal Conditions.
- Level B Service Conditions – Upset Conditions, Incidents of Moderate Frequency
- Level C Service Conditions – Emergency Conditions, Infrequent Incidents
- Level D Service Conditions – Faulted Conditions, Limiting Faults
- Testing Conditions

The RCL design transients are discussed in Section 20.6.1 and summarised in Table 20-22. Principal RCS pressures, temperatures, and flow rates are shown in Table 20E-1. The structural design of the RCL piping is based upon the following maximum steady state conditions:

Design Pressure	17.13 MPa (2485 psi)
Design Temperature	343°C (650°F)

The ASME stress limits, generally expressed as ratios of calculated stress vs. design allowable stress intensity (Sm), are identified for each of the Level A to D service conditions and testing conditions included in the Table 20-22. The ASME stress limits form the acceptance criteria for the design assessment, and the RCL piping meets the criteria specified in Section III of the ASME Code, Section III, subsection NB for Class 1 components.

The scope of the RCL design assessment will, as a minimum, include the loading combinations listed in Table 20E-3. These are described according to the nomenclature given in Table 20E-4. The RCL piping is to be analysed for the normal loads of weight, pressure, and temperature; mechanical transients of safe shutdown earthquake (SSE) and auxiliary line pipe ruptures; and pressure and temperature transients are outlined in Section 3.2 of Reference 20E.2

The transient conditions selected for ASME Code, Section III fatigue evaluation are based upon a conservative estimate of the magnitude and frequency of the temperature and pressure transients that may occur during plant operation. The design transients and the number of events used for the fatigue evaluation of RCS components, including the RCL piping, are presented in Table 20-22. Generally, only Level A and B service condition design transients are evaluated in the analysis of cyclic fatigue. Up to 25 stress cycles for Level C service conditions may be excluded from cyclic fatigue analysis in conformance with ASME Code, Section III criteria. Any Level C service conditions which are in excess of the 25-cycle limit are evaluated for the effect on cyclic fatigue using Level B criteria. For the evaluation of cyclic fatigue, the cycles included for seismic events are evaluated using Level B criteria and are not excluded from the fatigue evaluation regardless of the size of the stress range considered.

20E.3.2.2 The Reactor Coolant Loop Design Assessment Will Demonstrate that Relevant Stress Limits and End of Life Fatigue Usage Factors Are Satisfactory

The ASME Code, Section III establishes stress and fatigue limits for design, operational, accident and testing conditions. The ASME design report demonstrates that the requisite stress limits, as specified in the AP1000 Class 1 Piping Design Specification, are met for the RCL piping. This is presented in Reference 20E.14 and includes the assessment of support loads, nozzle loads and functional capability. Equivalent analyses for other sections of the RCS piping and branch lines are identified in Table 20E-6. The fatigue analysis is reported separately in Reference 20E.15.

The FUFs for the RCL piping have been evaluated using the 1998 Edition of the ASME Code (with addenda up through and including 2000 Addenda) fatigue design curves. Generic design assessment (GDA) Assessment Finding AF-AP1000-SI-39 has set the expectation that the future Licensee will undertake a fatigue design evaluation for locations in stainless steel and ferritic components that are in contact with the wetted environment to ensure that the effects of environment have been properly accounted for in the fatigue design analysis. GDA Assessment Finding AF-AP1000-SI-40 has also set the expectation that the future Licensee will review the changes to the design which would be required if the current version of the

ASME Code were used and either make these changes or justify why these changes are not practical.

20E.3.3 Forewarning of Failure Is Provided by In-Service Inspection

Effective ISI provides a well established means of monitoring and controlling anticipated degradation, confirms the absence of unanticipated degradation mechanisms and provides forewarning of failure. Evidence is provided to demonstrate that suitable ISI arrangements will effectively provide timely warning before structural failure of RCL piping could occur as follows:

- ISI of RCL piping is specified in accordance with established codes and standards.
- ISI provides data to monitor and judge in-service defect formation and growth.
- Arrangement for inspectability and access are specified to facilitate effective inspection.

Reference 20E.13 presents the component ISI assessment for the main loop and surge line piping. Leak monitoring adds defence in depth to the argument that effective forewarning of failure will be provided, and diverse means to warn of leakage from the RCS are identified, as described in section 20E.3.4.2.

20E.3.3.1 In-Service Inspection of Reactor Coolant Loop Piping Is Specified in Accordance with Established Codes and Standards

ISI is the preferred method for provision of forewarning of failure. The role of an effective ISI programme is twofold: firstly to detect and monitor anticipated degradation, and secondly to confirm the absence of any unanticipated degradation mechanisms. ISI is used to confirm the absence of defects that could give rise to gross structural failure.

To be effective, ISI requirements should be identified according to established good practice relevant to the characteristics of each inspection location. Evidence to substantiate that this is the case for the RCL piping of ISI is provided in the AP1000 design for inspectability programme: ISI requirements for class 1 components (Reference 20E.12), where the planned ISI arrangements for RCL piping are outlined to address the requirements of IWA-1400(b) and IWA-1500 of the ASME Code Section XI, supplemented where applicable by 10 CFR 50.55a. Reference 20E.12 provides a statement of the inspection techniques, inspectability and access arrangements applicable to ISI for AP1000 NPP and does not constitute a fully developed Inspection Plan, as required by 10 CFR 50.55a. A fully developed Inspection Plan is to be submitted for regulatory approval as part of the site-specific safety case following GDA. Inspection intervals are established for the Inspection Plan in accordance with Sub articles IWA-2400 and IWB-2400 of the ASME Code, Section XI and it is intended that in-service examinations be performed during normal plant outages, such as refuelling shutdowns or maintenance shutdowns occurring during the inspection interval.

Reference 20E.12 identifies inspection requirements for the RCL piping, based on those prescribed in ASME Code Section XI for Class 1 components.

The planned ISI programme includes the RCL components and welds of importance to nuclear safety. ASME Code Section XI requirements are identified for each location, and relevant code cases, as approved by NRC, are taken into account. The ISI requirements are summarised in Table 20E-5.

For the pressure retaining welds in piping DN 100 (NPS 4) or larger the ASME Code, Section XI examination category is B-J. The pipe to safe end welds, pump casing to pipe welds and pipe to pipe welds in the surge line are to be inspected by volumetric UT and liquid penetrant surface examinations. These are required over essentially 100% of the length of each weld during each inspection interval.

20E.3.3.2 In-Service Inspection Provides Data to Monitor and Judge In-Service Defect Formation and Growth in High Integrity Welds

Pre-service inspection will be undertaken in which the resulting data constitute a "fingerprint" against which ISI results can be compared. Comparison of ISI data with the manufacturing inspection fingerprint is used to confirm the absence of significant degradation or that build defects are stable i.e., defects detected during ISI must have started life as no greater than the manufacturing inspection validation defect size. Manufacturing inspections are to be performed using the same equipment that is likely to be used for the periodic ISI.

20E.3.3.3 Arrangement for Inspectability and Access Are Specified to Facilitate Effective Inspection

For effective ISI, the RCL design should accommodate requirements for inspection equipment and personnel access in accordance with current inspection technology and strategies. A design for inspectability programme for the UK AP1000 plant included an assessment for main loop and surge line piping welds. This assessment was, in part, based on the ISI Requirements Report for AP1000 Class 1 piping (Reference 20E.12), which identifies inspectability and access requirements for RCL locations. The following inspectability assessment for ISI of pressure retaining welds in RCL piping provides an evidence of the level of detail obtained from the inspectability programme.

Inspectability

- Pipe weld liquid penetrant examinations will be conducted on the outside diameter (OD) surface of the pipe. The examination area is defined as the area comprised of the weld plus approximately 12 mm (0.5 in) on each side of the weld. These inspections are performed manually.

- Pipe weld UT examinations are to be conducted on the OD surface of the pipe. The examination volume is defined as the volume comprised of the inner 1/3 thickness of the weld plus approximately 6 mm (0.25 in) on each side of the weld. Manual or mechanised contact equipment can be applied. Probes having 45° and 60° angles are typically applied, 45° is the predominant approach.

Access

- Application of the surface examination technique requires access to the examination surface plus approximately 150 mm (6 in) beyond to allow for sufficient space to use inspection equipment. Since the examination is performed manually, sufficient access and space must be provided for at least one operator to have hand contact and direct visual contact with the examination surface. At least 300 mm (12 in) of radial clearance from the component surface is required.

- Application of the volumetric examination techniques requires an OD examination surface free from obstructions for an axial distance on each side of the weld of (2 x thickness + 51 mm (2 in)). This includes thermal insulation adjacent to the OD surface, attachments and abrupt changes in the surface contour including counterbores and thickness changes in nozzles. The weld crown should be flush. It is noted that the required length of both sides of the weld may be reduced depending on the latest qualified techniques.

20E.3.4 Forewarning of Failure is Further Provided Through Leakage Detection

The RCPB is monitored for leaks from the reactor coolant and associated systems by a variety of components located in multiple systems as described in section 20.6.4.3.2. The leakage detection provisions forewarn of failure by providing timely warning of leakage before gross structural failure of the RCL piping would occur. Leak detection measures supplement the ISI arrangements (Section 20E.3.3) in providing forewarning of failure.

Unidentified leakage from through-wall cracks in the RCL piping would be released through the reflective insulation to the containment atmosphere. During normal operation, variations in airborne radioactivity, containment pressure, temperature, or specific humidity above the normal level signify a possible increase in unidentified leakage rates and alert the plant operators that corrective action may be required. Similarly, increases in containment sump level signify an increase in unidentified leakage.

20E.4 Strength of the Safety Case

20E.4.1 Objective

SFRs for the RCL piping are identified in Section 20E.2.1. This report provides a safety argument which identifies evidence to substantiate that the SFRs of the RCL piping will be maintained for all conditions within the design basis. This is achieved by demonstrating that the structural integrity of the RCL piping will be maintained for a 60 year component lifetime.

The availability and reliability of the SFRs should demonstrably be commensurate with the significance of the radiological hazards to be controlled. This demonstration is achieved by a process of component structural integrity classification which, for the safety justification of each class of component, establishes the degree of rigour to be applied commensurate with the potential radiological consequences of any postulated gross failure mode.

The structural integrity classifications of the components of the RCL piping are identified in Section 20E.2.2; these have been determined according to a process detailed in Reference 20E.3. The structural integrity classification of all components of the RCL piping is Standard Class 1.

A synthesis of the evidence presented in the safety argument to substantiate the structural reliability claims for the Standard Class 1 components of RCL piping is given in Section 20E.4.2, below. This summary and review of the safety argument provides the basis for the conclusions of this report which are presented in Section 20E.7.

20E.4.2 Evidence

The evidence to substantiate the structural reliability claimed for Standard Class 1 components, as identified in Sections 20E.3.1 to 20E.3.4, is based on a demonstration of compliance with relevant requirements of the ASME Code, supplemented by forewarning of failure to augment substantiation of the claimed structural reliability.

As asserted in Reference 20E.3, the failure statistics for industrial pressure vessels and piping that are built according to the good practice embodied in modern codes and standards supports inference of a failure rate that is in accordance with the structural reliability target for Standard Class 1 components. Substantiation of the structural reliability of the RCL components is, therefore, largely based on demonstrating compliance with relevant aspects of the ASME Code and with additional regulations as applicable.

The good practice that will control design and manufacture ensure quality of construction for all RCL components and these are described in Section 20E.3.1. The ASME Code prescribes rules of safety governing the design, fabrication, and inspection of boilers and pressure vessels that are internationally recognised and well established. As identified in section 20E.3.1.1, the following sections of the ASME Code establish requirements governing the following aspects of RCL design:

- Section II – Materials
- Section III, Rules for construction.
- Section XI: ISI

Procurement of materials is specified and controlled to ensure that well proven materials are chosen, that the materials have good resistance to fracture and are of suitable chemical composition to limit the effect of through-life degradation mechanisms. Materials of manufacture are discussed in section 20E.3.1.3, where it is established that all materials used in all RCL piping is specified to be in accordance with the requirements of Section II of the ASME Code.

All RCL components are designed and manufactured in accordance with the rules applicable to ASME Code, Section III for Class 1 components. Compliance with these requirements, and the experience embodied within the code, provides high confidence in manufacturing quality. Section 20E.3.1 identifies how various aspects of the Section III requirements are addressed for the RCL, these include mechanical testing to confirm material properties, welding procedures and welder qualification, manufacturing inspections to confirm the absence of defects, and hydrostatic pressure testing to confirm the integrity of the pressure boundary. Section 20E.3.2 describes assessments which deterministically justify the structural integrity of RCL piping against stress and fatigue limits established by the ASME Code, Section III for Class 1 components. The RCL design features integral branch nozzles connections that minimise the number of welds required in fabrication.

The planned programme of ISI for the RCL piping is described in Section 20E.3.3. This will be undertaken in accordance with the requirements of ASME Code Section XI and IWB-2500, and supplemented by requirements specified in 10 CFR 50.55a. In addition to the

planned ISI, forewarning of failure in RCL piping is also provided by leak monitoring for the RCS (section 20E.3.4.2).

20E.5 Index of Technical Reports

The Codes, Standards and other documents specified in Reference 20E.9 to control the quality of RCL design and manufacture are listed in Table 20E-2. Table 20E-6 lists design and analysis documents germane to the assessment of the RCL structural integrity safety case. A number of these Westinghouse reports are also specified in Reference 20E.9 and therefore are listed in both Table 20E-2 and Table 20E-6.

20E.6 Review of Open Issues

There are no open issues that affect the basis of the RCL piping safety case arguments presented in support of GDA.

20E.7 Conclusions

This CSR for the UK AP1000 RCL piping design presents a safety argument to establish that the structural reliability of the RCL piping is commensurate with the consequences of gross failure. SFRs have been identified for the RCL piping. These are to be maintained to ensure plant nuclear and radiological safety. For the RCL piping, assurance that SFRs will be maintained for the life of the component is provided by substantiating structural integrity against appropriate integrity targets.

Structural integrity targets have been identified for the RCL piping based on the procedure of structural integrity classification discussed in Section 20.5. All RCL components are classified as Standard Class 1, a classification that requires a less stringent and extensive substantiation of structural reliability than that of High Integrity or Highest Safety Significance.

The structural reliability target associated with a Standard Class 1 classification can be achieved through consideration of actuarial failure statistics. Industrial pressure vessels and piping built in accordance with the good practice embodied in modern codes and standards are judged to support inference of a tolerably low failure rate. Substantiation of the structural reliability of the RCL Standard Class 1 components is, thus, based on demonstrating compliance with relevant aspects of the ASME Code.

Evidence is presented within the structured safety argument to show that, as a minimum, all components of the RCL piping comply with the relevant requirements of Sections II (materials), III (construction) and XI (ISI) of the ASME Code for Class 1 components.

The scope of the code requirements provides a diversity of measures for the prevention of failure through conservative, robust design and stringent control of manufacture. ISI and leak detection monitoring provide further assurance of structural reliability by detecting and warning of any in-service degradation.

The evidence identified is judged to substantiate a tolerably low frequency of failure which is commensurate with the consequences of failure.

It is concluded that the safety argument presented in Section 20E.3 identifies a suitable and sufficient diversity of evidence to substantiate the structural reliability claimed for the

components of the RCL piping. The final results of the ASME III design analyses confirm that the RCL piping design satisfies the relevant stress and fatigue limits of the ASME Code.

20E.8 References

20E.1 Not used

20E.2 Westinghouse Report APP-PL02-Z0-101, Rev. 3, "AP1000 Class 1 Piping and Non-Class 1 Extensions Design Specification," October 2015.

20E.3 Westinghouse Report UKP-GW-GLR-004, Rev. 3, "UK AP1000 Structural Integrity Classification," January 2017.

20E.4 Westinghouse Report APP-PL01-Z0-200, Rev. 6, "Reactor Coolant Loop Seamless Forged and Formed Pipe Fabrication Specification," January 2014.

20E.5 Electric Power Research Institute (EPRI), EPRI NP-3944, "Erosion-Corrosion in Nuclear Plant Steam Piping: Causes and Inspection Program Guidelines," April 1985.

20E.6 G. Cragnolino, "Erosion-Corrosion in Nuclear Power Systems – An Overview," Corrosion '87, Paper No. 86, March 1987.

20E.7 Westinghouse Report APP-PL01-T1-001, Rev. 3, "AP1000 SA-376 TP316LM Hot Leg Piping Forging (ASME Section III-NB) Full Scale Mock-Up Qualification Test Specification," December 2014.

20E.8 Electric Power Research Institute (EPRI), 1014986, "Pressurized Water Reactor Primary Water Chemistry Guidelines – Revision 6," 2007.

20E.9 Westinghouse Report APP-PL01-Z0-201, Rev. 1, "Reactor Coolant Loop Piping Fabrication Specification Including Welding," December 2013.

20E.10 Westinghouse Report APP-GW-VLR-010, Rev. 2, "AP1000 Supplemental Fabrication and Inspection Requirements," January 2016.

20E.11 Westinghouse Report APP-RCS-M3-001, Rev. 8, "Reactor Coolant System Specification Document," June 2015.

20E.12 Westinghouse Report APP-GW-VW-001, Rev. 1, "AP1000 Design for Inspectability Program, ISI Requirements and Design Guidance for Class 1 Components," June 2014.

20E.13 Westinghouse Report APP-PL01-VMR-001, Rev. 0, "AP1000 Component ISI Inspectability Assessment: Main Loop and Surge Line Piping," August 2011.

20E.14 Westinghouse Report APP-RCS-PLR-050, Rev. 4, "AP1000 Reactor Coolant Loop (RCL): Piping Qualification," December 2015.

20E.15 Westinghouse Report APP-RCS-PLC-061, Rev. 1, "AP1000 Reactor Coolant Loop Piping Component Fatigue Evaluation," August 2014.

20E.16 Westinghouse Report UKP-GW-GLR-114, Rev. 1, "UK AP1000® Plant Internal Hazards Topic Report – Pressure Part Failure," January 2017.

20E.17 Westinghouse Report UKP-GW-GLR-035, Rev. 0, "UK AP1000® Fuel Tolerability of Depressurisation of the Primary Circuit Assessment," August 2016.

20E.18 Westinghouse Report APP-RCS-PLC-056, Rev. 2, "AP1000 Reactor Coolant Loop (RCL): Seismic Time History Analysis," November 2015.

Table 20E-1. Nominal System Pressures, Temperatures, and Flow Rates

Location (Figure 20E-2)	Description	Fluid	Pressure (psig (MPa gauge))	Nominal Temp. (°F (°C))	Flow[1] (gpm (m^3/hr))
1	hot leg 1	Reactor Coolant	2248 (15.499)	610 (321.11)	177,645 (40347.57)
2	hot leg 2	Reactor Coolant	2248 (15.499)	610 (321.11)	177,645 (40347.57)
3	cold leg 1A	Reactor Coolant	2310 (15.927)	537.2 (280.67)	78,750 (17886.07)
4	cold leg 1B	Reactor Coolant	2310 (15.927)	537.2 (280.67)	78,750 (17886.07)
5	cold leg 2A	Reactor Coolant	2310 (15.927)	537.2 (280.67)	78,750 (17886.07)
6	cold leg 2B	Reactor Coolant	2310 (15.927)	537.2 (280.67)	78,750 (17886.07)
7	Surge Line Inlet	Reactor Coolant	2248 (15.499)	610 (321.11)	–
8	Pressuriser Inlet	Reactor Coolant	2241 (15.451)	653.0 (345.00)	–
9	Pressuriser Liquid	Reactor Coolant	2235 (15.410)	653.0 (345.00)	–
10	Pressuriser Steam	Steam	2235 (15.410)	653.0 (345.00)	–
11	Pressuriser Spray 1A	Reactor Coolant	2310 (15.927)	537.2 (280.67)	1-2 (0.23-0.45)
12	Pressuriser Spray 1B	Reactor Coolant	2310 (15.927)	537.2 (280.67)	1-2 (0.23-0.45)
13	Common Spray Line	Reactor Coolant	2310 (15.927)	537.2 (280.67)	2-4 (0.45-0.91)

Table 20E-1. Principal System Pressures, Temperatures, and Flow Rates (cont.)

Location (Figure 20E-2)	Description	Fluid	Pressure (psig (MPa gauge))	Nominal Temp. (°F (°C))	Flow[1] (gpm (m^3/hr))
14	ADS Valve Inlet	Steam	2235 (15.410)	653.0 (345.00)	–
15	ADS Valve Inlet	Steam	2235 (15.410)	653.0 (345.00)	–

Note:
1. At the conditions specified.

Table 20E-2. Codes and Standards Related to RCL Design and Manufacture

ASME Boiler and Pressure Vessel Code	
Section II	Material Specification. The following elements are specified: • SA-312, "Specification for Seamless and Welded Austenitic Stainless Steel Pipes." • SA-370, "Mechanical Testing of Steel Products." • SA-376, "Seamless Austenitic Steel Pipe for High-Temperature Central-Station Service." • SA-745, "Ultrasonic Examination of Austenitic Steel Forgings."
Section III	Nuclear Power Plant Components
Section V	Non Destructive Examination
Section IX	Welding and Brazing Qualification
Section XI	Rules for ISI of Nuclear Power Plants Components
ASME Code Cases	
N-782	This Code case allows for the design, procurement, manufacture, etc., of the reactor coolant loop piping in accordance with Section III of the ASME Boiler and Pressure Vessel Code, 1998 Edition with addenda up through and including the 2000 Addenda. This Code case states that as an alternative to NCA-1140(a)(2)(a) and NCA-1140(a)(2)(b), the edition and addenda endorsed for a design certified or licensed by the regulatory authority may be used.
Standards	
ASTM Standard, A262	Standard Practices for Detecting Susceptibility to Intergranular Attack in Austenitic Stainless Steels.
ASTM Standard, E112	Standard Test Method for Determining Average Grain Size.
NUREG CR-0371	Stress Indices for Girth Welded Joints, Including Radial Weld Shrinkage, Mismatch and Tapered Wall Transitions.
ASME NQA-1	Quality Assurance Program Requirements for Nuclear Facilities," 1994.
ANSI/ANS-51.1-1983	Nuclear Safety Criteria for the Design of Stationary Pressurized Water Reactor Plants.

Table 20E-2. Codes and Standards Specified for RCL Design and Manufacture (cont.)

US Code of Federal Regulations	
10 CFR Part 20	Standards for Protection Against Radiation.
10 CFR Part 21	Reporting of Defects and Noncompliance.
10 CFR Part 50	Domestic Licensing of Production and Utilization Facilities The following appendices are specified in Reference 20E.4:
	Appendix A, "General Design Criteria for Nuclear Power Plants." (The applicable design criteria are identified in Reference 20E.4)
	Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants."
US NRC Regulatory Guides	
RG 1.26 Rev. 3	Quality Group Classification and Standard for Water, Steam, and Radioactive- Waste-Containing Components of Nuclear Power Plants
RG1.31 Rev. 3	Control of Ferrite Content in Stainless Steel Weld Material
RG1.37 Rev.0	Quality Assurance Requirements for Cleaning of Fluid Systems and Associated Components of Water-Cooled Nuclear Power Plants
RG 1.38 Rev.2	Quality Assurance Requirements for Packing, Shipping, Receiving, Storage and Handling of Items for Water Cooled Nuclear Power Plants
N.b. The N45-2 series standards have been replaced by ASME NQA-1. Therefore, reference may be made to ASME NQA-1 rather than the N45-2 series standards identified in the RGs listed above.	
RG 1.44 Rev.0	Control of the Use of Sensitized Stainless Steel
RG1.71 Rev. 0	Welder Qualification for Areas of Limited Accessibility
RG 1.84 Rev. 32	Design and Fabrication Code Case Acceptability ASME Code, Section III

Table 20E-3. ASME III Design Loading Combinations for RCL Piping

Condition	Design Loading Combinations[3]
Design	P + DW + DML + XL
Level A Service	PMAX[1] + DW + XL
	PMAX + DW + DN + XL
Level B Service	PMAX + DW + DU + XL
Level C Service	PMAX + DW + DE + XL
	PMAX + DW + DY + HYDSP + XL
Level D Service	PMAX + DW + DF + XL
	PMAX + DW + SRSS[2] ((SSE + SSES) + DBPB) + XL
	PMAX + DW + RVOS + SRSS (SSE + SSES) + XL
	PMAX + DW + DYS + DBPBS + SRSS ((SSE + SSES) + DY + HYDSP) + XL

Notes:

1. The values of PMAX in the load combinations may be different for different levels of service conditions as provided in the design transients. For earthquake loadings PMAX is equal to normal operating pressure at 100% power.
2. SRSS equals the square root of the sum of the squares.
3. See Table 20E-4 for description of loads.

Table 20E-4. Loading Nomenclature

Load	Description
P	Internal design pressure
PMAX	Peak pressure
DW	Dead weight
DML	Design Mechanical Loads (other than DW). This includes Service Level A loads and RVOS loads that are Service Level B.
XL	External mechanical loads, such as the nozzle reactions associated with piping systems, will be combined with other loads in the loading combination expressions.
SSE	Safe shutdown earthquake (inertia portion)
E	Earthquake smaller than SSE (inertia portion)
FV	Fast valve closure
RVC	Relief/safety valve – closed system (transient)
RVOS	Relief/safety valve – open system (sustained)
RVOT	Relief/safety valve – open system (transient)
DY	Dynamic load associated with various service conditions including FV, RVC, and RVOT as applicable (transient)
DN	Dynamic load associated with Level A (Normal) service conditions including FV, RVC, and RVOT as applicable (transient)
DU	Dynamic load associated with Level B (Upset) service conditions including FV, RVC, and RVOT as applicable (transient)
DE	Dynamic load associated with Level C (Emergency) service conditions including FV, RVC, and RVOT as applicable (transient)
DF	Dynamic load associated with Level D (Faulted) service conditions during which, or following which, the piping system being evaluated must remain intact including FV, RVC, and RVOT as applicable. This includes postulated pipe rupture events (transient)
DYS	Dynamic load associated with various service conditions (sustained)
SSES	Seismic anchor motion portion of SSE
ES	Seismic anchor motion of earthquake smaller than SSE
TH	Thermal loads for the various service conditions
TNU	Service Level A and B (normal and upset) plant condition thermal loads; including thermal stratification and thermal cycling
TN	Service Level A (normal) plant condition thermal loads
TU	Service Level B (upset) plant condition thermal loads
TE	Service Level C (emergency) plant condition thermal loads

Table 20E-4. Loading Nomenclature (cont.)

Load	Description
TF	Service Level D (faulted) plant condition thermal loads
SCVNU	Static displacement of steel containment vessel – normal and upset conditions
SCVE	Static displacement of steel containment vessel – emergency condition
SCVF	Static displacement of steel containment vessel – faulted condition
HTDW	Hydrostatic test dead weight
DBPB	Design basis pipe break, includes LOCA and non-LOCA (transient)
LOCA	Loss-of-coolant accident
HYDSP	Building structure motions due to automatic depressurisation system sparger discharge
DBPBS	Design basis pipe break, includes LOCA and non-LOCA (sustained)

Table 20E-5. Summary of Examination Requirements & Methods for AP1000 Class 1 Piping

Description	Exam. Method		
	UT	PT	MT
Pipe to Safe End Welds, Pump Casing to Pipe Welds, Valve Body to Pipe Welds, Pipe to Pipe Welds (NPS 4 or Larger)	✓(2)	✓	
Branch Connection Welds (NPS 4 or Larger)	✓(2)	✓	
Branch Connection Welds (Less Than NPS 4)		✓	
Circumferential Piping Welds (Less Than NPS 4)		✓	
Socket Welds		✓	
Piping Welded Attachments		[3]	[3]

Notes:

1. Man. – manual, Mach. – mechanised scanner
2. Alternative UT approach
3. PT or MT required, depending on material

Table 20E-6. Index of Technical Reports

	Document Reference	Document Title	Description of Role in Safety Case
Specifications/Reports			
1.	APP-PL02-Z0-101	AP1000 Class 1 Piping and Non-Class 1 Extensions Design Specification	Provides requirements for the design, fabrication, and construction of ASME Class 1 piping and connected Class 2, 3 piping extensions and provides the requirements for the connected ASME B31.1 piping extensions in accordance with the ASME Code.
2.	APP-PL01-Z0-200	Reactor Coolant Loop Seamless Forged and Formed Pipe Fabrication Specification	Establishes the design, manufacture, forming, machining, grinding, heat treatment, inspection, testing, documentation, packaging, storage, and shipping requirements for the austenitic stainless steel reactor coolant loop pipe forgings.
3.	APP-PL01-Z0-201	Reactor Coolant Loop Piping Fabrication Specification including Welding	Establishes the design, fabrication, welding, machining, grinding, inspection, testing, documentation, packaging, storage, and shipping requirements for the subassemblies of the austenitic stainless steel reactor coolant loop hot and cold leg piping.
4.	APP-RCS-PLR-050	AP1000 Reactor Coolant Loop (RCL): Piping Qualification	Summarises the results of the piping analysis for the piping connecting the reactor vessel, steam generators, and reactor coolant pump.
5.	APP-RCS-PLR-040	AP1000 Piping Analysis Report for Pressurizer Surge Line	Details the complete basis, except for the fatigue evaluation, for the static and dynamic analysis of AP1000 RCS Surge Line to the requirements of the Design Specification.
6.	APP-RCS-PLC-003	AP1000 Pressurizer Surge Line Piping Component Fatigue Analysis	Documents the fatigue evaluations for ASME Class 1 piping components of the pressuriser surge line piping.
7.	APP-RCS-M1-001	Reactor Coolant System Design Transients	Describes the fluid systems transients to be considered when designing the major RCS components.
8.	APP-GW-G1-003	Seismic Design Criteria	Documents the seismic design criteria used for safety-related and non-safety-related structures, systems, and components (SSC) that must be seismically designed.

Table 20E-6. Index of Technical Reports (cont.)

	Document Reference	Document Title	Description of Role in Safety Case
Specifications/Reports			
9.	APP-GW-GEM-200	AP1000™ Chemistry Manual	Presents Westinghouse Electric Company's expectations for chemistry control requirements for the successful commissioning and operation of the AP1000 Standard Plant.
10.	APP-GW-Z0-602	AP1000 Cleaning and Cleanliness Requirements of Equipment for use in Nuclear Steam Supply and Associated Systems	This document provides details of the cleaning and cleanliness requirements of equipment for use in the nuclear steam supply system along with associated systems.
11.	APP-GW-VW-001	AP1000 Design for Inspectability Program: ISI Requirements for Class 1 Components	This document provides details of the AP1000 design for the inspectability programme: ISI requirements for Class 1 components.
12.	APP-PL01-T1-001	AP1000 SA-376 TP316LN hot leg Piping Forging (ASME Section III-NB) Full Scale Mockup Qualification Test Specification	Describes the controls and test procedures to assess the soundness, integrity, metallurgical structure and mechanical properties of the reactor coolant loop hot leg.
13.	APP-PL01-T1-002	AP1000 RCL Pipe Grain Size Monitor for Production Pieces	Procedure for remote metallographic preparation, surface replication, and grain size measurement at the critical locations of the hot leg, cold leg, and reactor coolant loop piping production pieces
14.	APP-GW-VLR-010	AP1000 Supplemental Fabrication and Inspection Requirements	Provides details of the AP1000 supplemental fabrication and inspection requirements.
15.	APP-GW-VLR-002	Technical Requirements of Stainless Steels, Nickel-Based Alloys, Carbon and Low Alloy Steels, and Welding Materials for AP1000	Contains technical requirements of stainless steels, nickel-base alloys, and carbon and low alloy steels used in the AP1000 design.

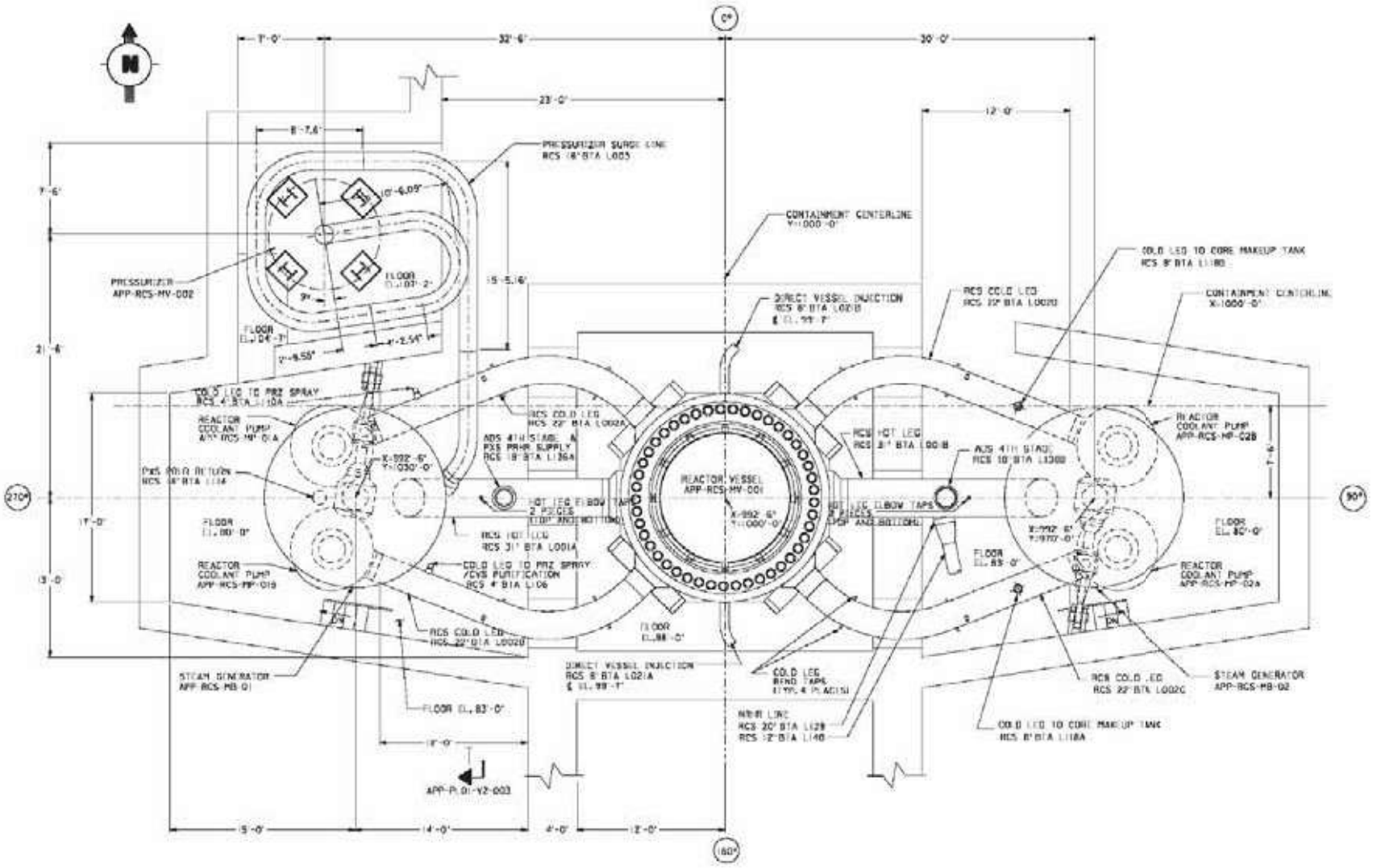


Figure 20E-1. Reactor Coolant System Plan View

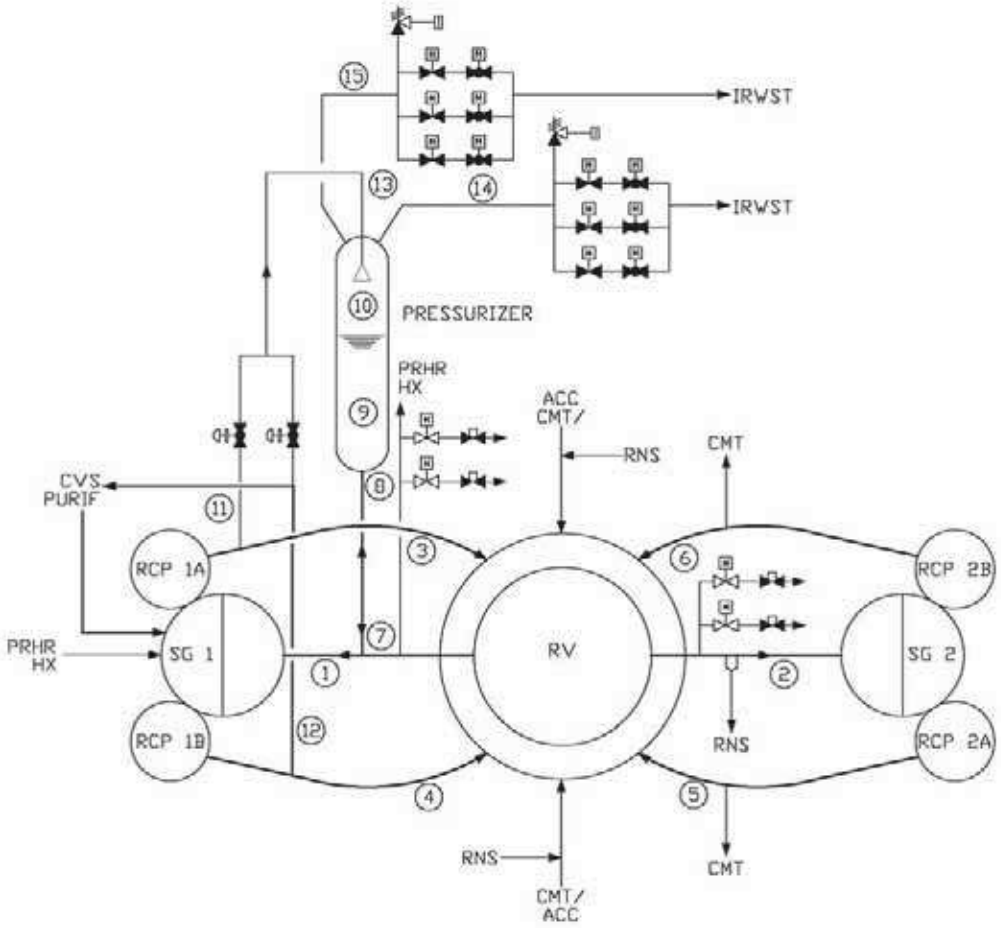


Figure 20E-2. Reactor Coolant System Schematic Flow Diagram

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS AND ACRONYMS

ALARP	as low as reasonably practicable
ANSI	American National Standards Institute
ASME	American Society of Mechanical Engineers
ASTM	American Society for Testing and Materials
CSDRS	certified seismic design response spectra
CSR	Component Safety Report
DEGB	double-ended guillotine break
HSS	highest safety significance
ISI	in-service inspection
LOCA	loss-of-coolant accident
NDE	nondestructive examination
NRC	Nuclear Regulatory Commission
PWSCC	primary water stress corrosion cracking
R&D	research and development
RCP	reactor coolant pump
RCS	reactor coolant system
RT_{NDT}	reference temperature for nil ductility transition
SCL	stress classification line
SFR	safety functional requirement
SG	steam generator
SI	structural integrity
SSC	system, structure, or component
SSE	safe shutdown earthquake
TAGSI	Technical Advisory Group on Structural Integrity
UK	United Kingdom
US	United States

APPENDIX 20F
REACTOR COOLANT PUMP COMPONENT SAFETY REPORT

20F.1 Introduction

This is the component safety report (CSR) for the reactor coolant pump (RCP) as introduced in Section 20.2.The safety arguments herein substantiate the structural integrity (SI) of the RCPs to a degree of rigour commensurate with the consequences of gross structural failure. The safety arguments are supported by a suite of documentation outlined in Section 20F.5 that supports the design, manufacture, installation and operation of the RCP.

20F.1.1 Scope

This CSR presents a structural integrity argument for the RCPs in relation to their pressure retention function; withstand to design basis internal and external hazards, including the effects of postulated flywheel disintegration and rotor locking. These arguments support the claim that the nuclear and radiological risks, potentially arising from gross structural failure of an RCP casing are tolerably low for the entire design lifetime objective of 60 years. The mechanical and electrical aspects of the RCP design are considered in sections 17.3.1 and 18, and are outside the scope of this appendix.

20F.1.2 Objectives

This CSR establishes arguments to support the claim that the AP1000 plant risk remains both tolerable and as low as reasonably practicable (ALARP) for the design lifetime. These claims are substantiated by satisfying structural integrity safety design bases for all safety-significant AP1000 systems, structures, or components (SSCs). The safety design bases, applied across the operational, process and lifecycle scope of the safety case, embody the technical scope of the safety case: if these can be maintained at all times, the plant will be acceptably safe. Specific safety functional requirements (SFRs) for the RCP are developed from the structural integrity safety design bases, and correspond to the functions that need to be maintained to provide assurance of nuclear and radiological safety. The SFRs applicable to the structural integrity aspects of the RCP are identified in Section 20F.2.

The approaches to achieving this objective are:

- To support the nuclear safety claims made for the AP1000 RCP design.
- To present arguments that support the claim that the structural reliability of the RCPs is commensurate with the consequences of failure and remains so throughout their design life. That is, where failure is intolerable, the probability of gross failure should be shown to be so low that such failure can be discounted, or where failure does not lead to intolerable consequences, the target reliability is linked to the consequences in accordance with the methodology in Reference 20F.1. This is discussed in Section 20F.2.2.

20F.1.3 Interface With Other Safety Case Documents

The RCP Final Research and Development (R&D) Report, Reference 20F.2, which details the proposed design solution, references a dossier of technical data and supporting analyses. In addition to this report, the Final Design Report (Reference 20F.12) summarises the supporting design process, including dedicated design reviews, the main conclusions and supporting and reference documentation, and updates to the design as part of the design finalisation process, especially in resolution to the open issues (chits) identified during the design reviews.

A full index of technical documentation is provided in the final design review package, which also includes a synopsis of the main design reviews and analyses. Table 20F-5 shows the reports, calculations, and analysis supporting the RCP design.

20F.1.4 Reactor Coolant Pumps Description

20F.1.4.1 Overview

Reference 20F.3 provides the AP1000 RCP design specification for the sealless, wet winding RCP, while Reference 20F.12 provides a review of the RCP design. This Final Design Review package provides a summary and synopsis of the design and design process. Its main reference is the technical report in Reference 20F.2, as updated in Reference 20F.12 to the design finalisation in support of the final design review, and in resolution of open items identified during previous intermediate design reviews. These two reports and the design specification, and the extensive supporting documentation therein referenced, provide the basis of the design for this CSR. Although these documents cover all aspect of the pump design, including the hydraulic characteristics and electrical performance, this CSR covers those aspects of the design relevant to structural integrity.

The RCPs are an integral part of the reactor coolant system (RCS) pressure boundary and are designed to circulate pressurised water to extract heat from the core delivering it to the steam generators (SGs) and then back to the core. The reactor coolant system consists of two heat transfer circuits, each with a single SG, two RCPs, and a single hot leg and two cold legs. Figure 20F-1 shows the schematic flow diagram for the AP1000 RCS; the principal pressures, temperatures and flow rates under normal steady-state, full-power operating conditions relating to the various numbered locations are presented in Table 20F-1. SG number 1 has RCP 1A and RCP 1B attached whilst SG number 2 has RCP 2A and RCP 2B attached. Figure 20F-2 is an isometric figure depicting the reactor coolant loops and the RCPs. Figure 20F-3 is an elevation figure showing the RCP configuration below one of the SGs.

The AP1000 RCPs are high-inertia, high-reliability, sealless pumps that circulate the reactor coolant through the reactor vessel, loop piping, and SGs. Each pump is a compact, vertical pump/motor unit, designed to fit into the SG compartment. The pump casings are welded to the channel head by the suction nozzle. The integration of the pump suction into the bottom of the SG channel head is a significant pressurised water reactor design development. By eliminating the coolant loop piping cross-over leg associated with traditional pump pairs, the loop pressure drop is reduced, reducing the pumping requirements and promoting passive circulation, the foundation and support system for the steam generator and associated piping is simplified, the overall plant footprint is reduced, and the potential for uncovering of the core is reduced by eliminating the need to clear the loop seal during a small loss-of-coolant accident (LOCA).

20F.1.4.2 Description

Each AP1000 RCP is a vertical, single-stage centrifugal pump designed to pump large volumes of main coolant at high pressures and temperatures. Owing to its sealless design, it is more tolerant of beyond design basis conditions that could adversely affect shaft seal designs. The main impeller attaches to the rotor shaft of the driving motor, which is an electric induction motor. Primary coolant circulates between the stator windings and along the rotor which obviates the need for a seal around the motor shaft. Additionally, the motor bearings are lubricated by primary coolant. The motor is, thus, an integral part of the pump. The basic pump design has been proven by many years of service in similar applications around the world and in other applications. Evidence to support this argument is presented in Reference 20F.2.

The pump motor size is minimised through the use of a variable frequency drive to provide speed control in order to reduce motor power requirements during pump startup from cold conditions. The variable frequency drive is used not only during heatup and cooldown, but also during all operational modes. To provide the rotating inertia needed for flow coast-down, a bi-metallic flywheel assembly is attached to the pump shaft. The flywheel ensures that, following a loss of electrical power supply to the main coolant flow, the resulting coastdown meets the requirements for the design basis analysis.

Pressure Boundary

The pressure boundary consists of three parts, the pump casing, heat barrier assembly, and motor casing assembly. These parts are clamped together by 24 high strength closure bolts. The reactor coolant pump casing is a single-piece forging, constructed of ferritic material (SA-508 Grade 3) and includes an austenitic cladding of the wetted surfaces. Cladding is applied using weld overlay consistent with the application process used for similar portions of the reactor coolant system. The use of SA-508 material offers high strength, greater ease of manufacture and compatibility with the SG channel head material thereby reducing the number of potential on dissimilar metal welds. Weld buttering or post weld heat treatment will be utilised on the remaining dissimilar metal welds to reduce the risk of welds failing. The specific method will be determined during the detailed design phase. The heat barrier and motor casing components are also single-piece forgings constructed of high-strength (Gr. F6NM) martensitic stainless steel material.

The pressure boundary components are designed to meet the requirements of the American Society of Mechanical Engineers (ASME) Boiler & Pressure Vessel Code (Code), Section III, Division 1, Class 1998 edition, including 2000 Addenda; and are designed and analysed according to the requirements in Subarticle NB-3400 of the Code. This is discussed further in Section 20F.3.2.

Impeller/Diffuser

The pump/motor unit consists of a pump hydraulic part, where a semi-axial impeller/diffuser combination is mounted in a flow-optimised, single-piece casing. The impeller/diffuser combination is of a very high hydraulic efficiency and is based on well proven designs that have been used by Westinghouse for more than 30 years.

Flywheel

The flywheel is located between the impeller and the motor, and consists of a single-piece forged stainless steel cylinder, with several smaller heavy metal cylinders inside. The inclusion of very high density materials such as tungsten alloy is required to minimise the

size of the flywheel, thereby, allowing incorporation within the pressure boundary as well as reducing the drag on the flywheel and associated heat production caused by the location of the flywheel within the pressure boundary. However, these high density materials do not have the required strength. Hence, a bi-metallic design has been selected, which has the following advantages over the alternatives:

- The forged stainless steel base can be selected to meet the operating conditions.
- It is possible to produce large stainless steel forgings without structurally significant flaws.
- The high density material is not relied upon structurally.
- The amount of material needed in order to provide the same inertia as a monolithic flywheel is considerably lower.

A short and rigid shaft, supported by a radial bearing, connects the impeller with the high-inertia flywheel. In order to avoid potentially high circumferential stress in the central bore, the flywheel is connected to both pump shaft and motor shaft via Hirth-type spline face adapters. In addition, no shrink fit to a shaft is needed to transmit the torque.

The flywheel is located inside the heat barrier, which forms part of the pressure boundary. A complex arrangement of cooling water circuits provides a homogeneous temperature distribution in and around the flywheel, minimises the friction losses of the flywheel, and protects the motor from hot coolant.

Motor/Electrical Components

The driving torque is transmitted by the motor shaft, which itself is supported by two radial bearings. A three-phase, high voltage squirrel cage induction motor generates the driving torque. The speed of the motor is variable by the variation of the output frequency of the variable frequency drive. The motor is mounted in a single-piece forged motor casing with a bolted cover at the lower end side. Due to the wet winding concept, it is possible to achieve an optimal cooling of the stator and avoid internal hotspots with positive effects regarding motor lifetime. The cooling water is forced through the stator windings and the gap between the rotor and stator by an auxiliary impeller. Furthermore, this wet winding motor concept is of very high efficiency as compared to a canned motor with its high eddy current losses.

Supports

The RCPs are supported entirely by the SGs; consequently, there are no RCP supports.

20F.1.5 Boundaries

The physical boundaries for safety case assessment of the RCP are as follows:

- RCP casing suction nozzle end. The weld of the suction nozzle to the SG is considered as part of the SG.
- RCP casing to discharge nozzle end. The weld of the discharge nozzle to the cold leg pipe is considered part of the RCS piping.
- Heat exchanger cooling water supply and return flanges.

- Flange for the RCP fill and drain line.

The RCP casing boundaries are indicated in Figure 20F-4.

20F.2 Safety Case Structure

The main focus of this CSR is to provide a structured safety argument, supported by suitable and sufficient evidence, to substantiate the reliability appropriate to the classification of the RCP as a Standard Class 1 component, as outlined in Section 20F.2.2. To achieve this, the safety argument is presented as three key elements, as follows:

Claim 1:	Quality of Build: High quality will be achieved during manufacture.
Objective:	Provides evidence of good design and manufacture based on established practices and track record. It provides a keystone for a demonstration of appropriate reliability and embodies the code and plant operating experience with the objective of achieving a good quality of build and the avoidance of defects.
Claim 2:	Good Design: Good design is achieved through compliance with ASME.
Objective:	Incorporates the build experience as embodied in the design codes.
Claim 3:	Mitigation and Management of In-service Degradation: RCP pressure boundary components are tolerant to through-life degradation over the design life of the plant
Objective:	Provides an assessment of through-life degradation mechanisms and shows that such mechanisms will not threaten integrity over a specific interval. It is also established that potential degradation mechanisms are understood and that the inspection and maintenance programme will detect degradation before it affects the performance requirements.

The safety argument has been tailored according to the structural reliability claims derived from a process of component classification, with the purpose of demonstrating that component structural reliability is commensurate with the consequences of gross failure.

The three elements of the safety argument are provided in Section 20F.3 and the strength of the argument is discussed in Section 20F.4.

20F.2.1 Safety Functional Requirements

The basis for the selection of the SFRs is discussed in Section 20.4. These are based on the safety design bases established for each component and include the duty functions and accident response requirements of plant systems, which must be maintained at all times or upon demand as appropriate to provide assurance of plant nuclear and radiological safety. Identification of the SFRs for the RCP follow from the performance and safety design bases allocated in Reference 20F.3, as follows:

- **SFR 20.11.1** The RCP is required to maintain the integrity of the primary coolant pressure boundary during standby, normal operation and under design basis faulted conditions for the design life of the plant.

- **SFR 20.11.2** The RCP is required to retain missile fragments arising from a disruptive failure of the RCP flywheel without gross failure of the RCS pressure boundary.

Postulated failure modes which result in a loss of these functional requirements lead to the identification of structural reliability targets commensurate with the consequences of gross failure, as determined through the process of component classification as described in Section 20.5.

20F.2.2 Reactor Coolant Pump Structural Integrity Classification

For the United Kingdom (UK) AP1000 plant, a structural integrity classification methodology detailed in Reference 20F.1 and summarised in Section 20.5 has been applied to pressurised components with the aim of determining the required level of structural reliability for each of the major plant components based on an evaluation of the direct consequences and indirect consequences of gross failure. Direct consequences include the effect of LOCA or reactivity addition, indirect consequences include missile generation, pipe whip, blast and flood.

The assessment of the RCP pressure boundary and flywheel is presented in Table 20-8. This includes the conclusion that a gross failure of the RCP pressure boundary would lead to a large LOCA, bounded by the double-ended guillotine break (DEGB) of the primary loop. This is within the analysis presented in Chapter 9 and therefore mitigated by the Class 1 AP1000 passive systems. Considering the indirect consequences, the assessment of the potential for high energy missiles to be generated concluded that these missiles would be contained within the SG compartment without threatening the operability of the plant passive safety systems or containment boundary. Specific consideration was given to the potential for missile fragments from the RCP to lead to a disruptive failure of the SG channel head or secondary shell, which would in itself attract a highest safety significance (HSS) classification. The assumption of two consecutive disruptive failures is considered outside the methodology and hence was dismissed. Consideration was also given to the failure of the SG support column arising from missile damage. Analysis performed demonstrates that core cooling is maintained in the unlikely event that the vertical support should fail as a result of missile damage. Based on these arguments, the RCP pressure boundary has been assessed as a Standard Class 1 component. The basis for the safety case is presented in Section 20F.3.

The RCP to SG Channel Head weld has been assessed as highest safety significance. The justification for this weld is presented in Appendix 20C.

20F.3 Safety Case Arguments

For a Standard Class 1 component, the primary safety argument is that design and manufacture in accordance with the ASME Code provides the basis against which adequate structural reliability can be claimed for a Standard Class 1 component. Evidence to support this claim is provided by pressure vessel failure statistics, as indicated in the UK Technical Advisory Group on Structural Integrity (TAGSI) paper on the presentation of incredibility of failure safety cases (Reference 20F.4).

The basis of the safety case for the RCP is, therefore, the arguments and evidence to substantiate the following claims.

- Claim 1: High quality will be achieved during manufacture (Section 20F.3.1).
- Claim 2: Good design is achieved through compliance with ASME (Section 20F.3.2).

- Claim 3: In-Service Degradation is Avoided (Section 20F.3.3).

20F.3.1 High Quality Is Achieved During Manufacture

The reliability and integrity of the RCP pressure boundary is dependent upon the achievement of high quality during design, manufacture and installation. The design intent is translated into a manufacturing process which is controlled by a Quality Assurance Programme complying with rigorous design codes including the ASME Code. The RCP Design Specification (Reference 20F.3) provides the complete list of the industry codes, specification and standards which are to be complied with. These include:

- Westinghouse specifications and standards, including supplementary fabrication and inspection requirements.
- The ASME Code and applicable Code cases.
- American National Standards Institute (ANSI)/ASME Standards
- United States (US) Code of Federal Requirements
- US Nuclear Regulatory Committee (NRC) Regulatory Guides and NUREGS
- American Society for Testing and Materials (ASTM) Standards

Fabrication and manufacturing for the RCP will meet the specifications described in Reference 20F.3 to satisfy the requirements of ASME Code, Section III, Subsection NB, Article NB-4000. The following sections outline design requirements to assure the manufactured RCP is of high quality.

20F.3.1.1 Fabrication

The Class 1 parts of the RCP pressure boundary will be fabricated per the requirements of ASME Code, Section III, Subsection NB, Article NB-4000. The heat exchanger structural support will be fabricated to Subsection NF, Article NF-4000.

20F.3.1.2 Material Specifications

The pressure boundary materials for the AP1000 RCP will all comply with the material specifications of ASME Code, Section II. The RCP Design Specification (Reference 20F.3) specifies the requirements for the RCP pressure boundary materials including welding and bolting materials. Allowable pressure boundary materials are summarised in Table 20F-2. SA-508 Grade 3 was selected for the casing material as the selection of SA-508 Grade 3 material provides the following benefits:

- Existing world-wide manufacturing experience in forging large diameter, thick ring sections thus ensuring predictable through-thickness material properties.
- Extensive world-wide operating experience in light water reactor environments with no fatigue driven failures.
- Reduces the number of reactor coolant system pressure boundary materials.
- Minimises the reliance on dissimilar metal welds.

- Industry proven chemistry specification and mechanical property database
- Mechanical property balance between yield strength and thermal conductivity.
- Extensive welding and nondestructive examination (NDE) inspection experience related to heavy section forgings utilising established techniques.

To prevent corrosion of low alloy steel components in contact with primary coolant, the pump casing will have corrosion-resistant cladding on surfaces exposed to the reactor coolant. Clad surfaces will be austenitic stainless steel weld overlay. For multiple layer austenitic stainless steel cladding, the cladding will be Type 308L weld metal with Type 309L weld metal used for the first layer. The approach to cladding provides the following benefits:

- Extensive world-wide operating experience in light water reactor environments
- Corrosion resistance of cladding material equivalent to corrosion resistance of Types 304 and 316 austenitic stainless steel alloys or nickel-chromium-iron alloy, martensitic stainless steel, and precipitation-hardened stainless steel
- Equivalent inspectability to other clad application approaches

The heat barrier and motor casing are to be fabricated from Gr. F6NM forged high-strength martensitic stainless steel (Table 20F-3). Reference 20F.3 specifies the design requirements for martensitic stainless steel.

The materials used for the pressure boundary bolting will be examined and tested as per paragraph NB-2300 and NB-2500 of the ASME Code. Ferritic pressure boundary bolting materials will meet the minimum requirements of 0.63 mm (0.025 in) lateral expansion and 61J for Charpy V notch tests conducted at 10°C (50°F) maximum.

20F.3.1.3 Welding

External pressure boundary welds are limited to the interface to connecting components as the casing is a single forging. The pump casing, heat barrier assembly, and motor casing assembly components are manufactured as single-piece forgings; no fabrication welding is included.

Welding, welder qualifications and welding inspection will be in accordance with ASME III and Section IX as described in Reference 20F.3. The same standards apply to welds within the flywheel enclosure even though they are not external pressure boundary welds.

20F.3.1.4 Nondestructive Testing

As specified in Reference 20F.3, nondestructive testing will be carried out by personnel qualified and certified in accordance with the requirements of ASME III, NB-5000. The requirements with respect to testing and examination techniques are specified. The results of these tests on the pressure boundary components and the structural components of the flywheel will be documented.

Examination will be performed in accordance with the following requirements:

- Materials – ASME Section III, NB-2000.

- Cladding – ASME Section III, NB-5000.
- Welds – ASME Section III, NB-5000.
- Thickness – ASME Section V, Article 5.

Any ultrasonic testing weld examination zone includes the weld and heat affected zone. The weld heat affected zone will extend 12.7 mm (0.5 in) beyond the weld fusion line.

Radiographic inspection or magnetic particle inspection will be performed in accordance with ASME Section III, Subsection NB. Magnetic particle examination will be performed after any required post-weld heat treatment.

The final NDE of pressure boundary materials will be conducted in the stage of fabrication indicated in the ASME Section III, Subsection NB and the following:

- Low alloy materials will be magnetic particle inspected after quench and temper.
- Surfaces to be clad will be magnetic particle examined prior to cladding.

Liquid penetrant inspection will be performed in accordance with ASME Section III, Subsection NB.

The weld between the RCP and the SG channel head has been classified as a HSS weld. This weld has been considered as part of Appendix 20C and will be subjected to inspection qualified in accordance with the European Network on Inspection Qualification methodology and supported by elastic-plastic defect tolerance studies.

The flywheel structural components will be inspected prior to final assembly in conformance with Regulatory Guide 1.14 (Reference 20F.5). Inspection of the flywheel will be in accordance with the fabrication methods used and the procedures in ASME Section III, Article NB-2500. To ensure the integrity of the flywheel following final assembly, a penetrant test will be performed on the enclosure welds.

20F.3.1.5 Quality Control

The requirements of a quality control programme relevant to the RCPs is summarised in Reference 20F.3. A compliant programme will be produced for the fabrication and installation of the RCP.

20F.3.1.6 Hydrostatic Testing

ASME Code provides hydrostatic requirements which will be carried out for each RCP as specified in Reference 20F.3. A shop hydrostatic test will be performed at a test temperature established to be safe from brittle fracture. Reference 20F.3 recommends that the test temperature should not be lower than the reference temperature nil-ductility temperature (RT_{NDT}) plus 33°C.

20F.3.1.7 Prototype/Production Testing Requirements

Testing requirements relating to the pressure boundary are specified in Reference 20F.3. This includes a requirement for testing of a full sized first-of-a-kind pump. Reference 20F.12 and Reference 20F.2 summarise the design, fabrication and testing programme of a ½-scale prototype pump used to test and verify the response of the RCP components. The scaled pump testing was completed as part of the design refinement process and has been used to provide comparison between calculated performance data and measured data including temperature distributions and bearing performance.

Reference 20F.12 and Reference 20F.2 summarise the results of testing performed on a ½-scale flywheel with tungsten alloy inserts including balancing and overspeed testing. The maximum speed for the flywheel prototype was 2,437 rpm, which exceeds the 2,250 rpm required in the design specification for the full-sized flywheel (Reference 20F.3). Overspeed testing is required for the full size flywheel during factory acceptance testing.

Together these arguments provide a basis for a demonstration that each RCP will achieve a high quality during manufacture and will enter service free from significant structural defects. The outcome of the materials testing and NDE will provide supporting evidence on a case-by-case basis in due course.

20F.3.2 Good Design Is Achieved Through Compliance With ASME.

As stated in section 20F.1.4.2, the pressure boundary components have been designed to meet the design, analysis and testing requirements of the ASME Code, Section III, paragraph NB-3400.

Summaries of the calculations against these criteria are presented in Reference 20F.2. These summaries have been developed from the detailed design calculations.

Pressure Boundary Stress Analysis

The RCP Design Specification, Reference 20F.3, presents the loading combinations used to analyse and justify the RCP assembly: The resulting RCP pressure boundary stress intensities are not to exceed the limits specified in ASME III, NB-3400. The rules to be used for evaluation of the Level D conditions are defined in Appendix F of ASME Code, Section III.

Reference 20F.3 presents the allowable design nozzle loads for outlet and inlet nozzles. These loads are applied at the nozzle safe ends where applicable or at the nozzle-piping interface during the design of the RCP.

Reference 20F.2 summarises the results of the ASME sizing calculations and stress analyses for the pressure retaining parts, which provides evidence that the ASME sizing requirements have been satisfied. Reference 20F.12 also describes the results of the stress and fatigue analysis against the mechanical and thermal loads described above. The analysis, which was performed using the ANSYS Code, covers the following components:

- Pump Casing
- Lower Part of Motor Housing
- Thrust Bearing Housing
- Bearing Bracket
- Upper Part of Motor Housing
- Heat Barrier
- Main Closure Studs

The conclusion from this analysis is that all pressure retaining parts of the RCP comply with the rules and limits set forth in the ASME Code.

As stated in section 20F.1.4.2, the pump casing is ferritic material with austenitic stainless steel cladding. The existing ASME analysis for the pump casing was completed for a martensitic pump casing. Reference 20F.12 documents in detail the comparison of the different materials and justifies why it is not considered necessary to update the stress analysis at this stage. It is recognized that prior to shipment, the analysis is required to be

updated for the material change. The following arguments support the applicability of the existing ASME stress analyses to the current pump casing design:

Material Properties

Reference 20F.12 provides a summary of important parameters for three different microstructures of ASME Code compliant pressure boundary materials including the ferritic material chosen for the pump casing and two other materials – martensitic stainless steel (the material analysed in the ASME stress analysis referenced in Reference 20F.12) and austenitic stainless steel (for comparison). The impact of these parameters is discussed in the following reconciliation.

Evaluation and Reconciliation with Regard to Stress Analysis

The stress analysis performed for the martensitic casing material was reviewed with regard to changes that would be needed to reflect the ferritic pump casing material. Because the material strength of SA-508 is not as high as of the Grade F6NM material, the locations of stress classification lines (SCLs) and nodes with maximum stresses and usage factors were evaluated. The relevant positions are shown in Reference 20F.12.

The design and test conditions produced the maximum stresses. Service Levels A to D are covered by these conditions. The general maximum usage factor was found away from the discharge nozzle; however, the absolute value was so low that this area did not require any further consideration. A local usage factor needed to be evaluated for the area in and around the discharge nozzle, because the stress intensity range at this location needed special justification. The reconciliation therefore focused on the section through the discharge nozzle.

It is expected that a change in pump casing material will not lead to major changes in the stress analysis. The following facts have positive or supporting influence on the stress analysis:

1. Sizing Calculations (wall thickness, reinforcement) were re-performed for the ferritic material (Reference 20F.12). All requirements of ASME Code, Section III, Division 1, Subsection NB-3300 are fulfilled.

2. Ferritic material has a higher thermal conductivity than martensitic (Section 5.1.2 of Reference 20F.12). Therefore, the same thermal loads would result in lower stresses in a ferritic material of similar thickness during steady state and especially during transient conditions.

3. Since general usage factors are very low, even an increased alternating stress would be compared to the same fatigue curve and would not exceed the limits.

4. The ferritic casing design also includes a reinforced transition area per ASME Code.

5. The circumferential groove at the bottom of the casing in the analysed case was eliminated in the ferritic design, resulting in a thicker and more homogeneous casing bottom.

These factors combine to mitigate the effects of reduced material strength. Should these contributors turn out to be insufficient to meet ASME code requirements, the appropriate measure would be to reinforce the transition to the discharge nozzle further by adding material to the outside. In order to keep the required distance to the weld (for in-service inspection (ISI)), the nozzle length would have to be increased. This would also cause

changes in the raw part of the pump casing. However, the general design of the casing or the pump would not be affected. The ASME stress analysis using ferritic material will be performed during the detailed design phase of the RCP and acceptable results are necessary to meet the requirements specified in the design specification (Reference 20F.3).

20F.3.3 Seismic Operability Analysis

The RCP is classified as AP1000 Class A with Seismic Category I requirements (Reference 20F.6). The AP1000 design earthquake is referred to as the AP1000 certified seismic design response spectra (CSDRS). Figures 1 and 2 of Reference 20F.6 depict the horizontal and vertical design response spectra for the AP1000 plant, scaled to the safe shutdown earthquake at 0.3g. The design response spectra are applied at foundation level (87.96 m) in the free field at hard rock sites and at finished grade (100 m) in the free field at firm rock and soil sites. In addition to the CSDRS, the AP1000 design has been enhanced to meet hard rock high frequency seismic response associated with earthquakes representative of Central and Eastern United States rock sites.

The RCP is welded to the SG and will predominantly be driven by the seismic response of the SG through this support, which is justified in Appendix 20C. The RCP pressure boundary itself is a seismically rugged structure that will not be prone to failure due to the inertial forces. Nevertheless, a series of analyses have been undertaken to investigate the additional stresses due to a seismic event as summarised in Reference 20F.2. This discusses the results of analyses which provide the evidence that the RCP is seismically designed and qualified for the safe shutdown earthquake (SSE), that it can withstand the effect of specified earthquakes, that the pump will perform its safety shutdown functions during and after SSE and that it will maintain the safe shutdown condition.

Flywheel Integrity

The AP1000 plant is designed such that components important to safety are protected against the effects of missiles. The AP1000 RCP is therefore designed such that, in the event of a postulated worst-case flywheel assembly failure, the surrounding structure can contain the energy of the fragments without causing gross failure of the pressure boundary. In the design and fabrication of the flywheel, the intent of US NRC Regulatory Guide 1.14 (Reference 20F.5) is followed. The Final R&D Report (Reference 20F.2) provides a summary of the analysis undertaken using the energy absorption equations of Hagg and Sankey (Reference 20F.9). This analysis assumes that fracture of the flywheel has occurred and seeks to prove the energy of the fragments is insufficient to penetrate the pump pressure boundary walls. The analysis covers a range of fragment sizes. The results show that for the worst case fragment size, the fragments will be retained within the pressure boundary as they possess insufficient energy to perforate the RCP casing. This supports the argument that in the unlikely event of flywheel failure, any fragments will be contained within the pressure boundary.

Rotor Seizure

The design of the pump is such as to preclude the instantaneous stopping of any rotating component of the pump or motor. The rotating inertia would overcome interference between components for a period of time. To analyse the mechanical and structural effect of a rapid slowdown of the rotating assembly, a failure of the rotating assembly is postulated that results in deformation that causes an interference with the surrounding RCP components. For such interference, the pump and motor are postulated to come to a rapid stop. This bounds other postulated mechanisms involving a rapid slowdown of the pump.

For normal operating conditions, the connection of the pump with the steam generator and discharge piping is analysed for the vibration of the pump, hydraulic effects and the torque due to rapid slowdown of the rotating assembly. The stresses in the pump casing, motor housing, steam generator channel head, and piping are analysed using ASME Code, Section III, Service Level D limits for this condition. The evidence to support this is presented as part of the Final R&D Report (Reference 20F.2) which considers the deceleration from a normal operating rotational speed of n = 1,780 rpm to standstill during one revolution. The report discusses the results of the analysis undertaken using finite element methods. The conclusion in this report is that the stress intensities from the postulated locked rotor event are always lower than the allowable Service Level D stress limits. Therefore, the integrity of the pump is not jeopardised by such an event.

Flywheel Overspeed

Reference 20F.2 presents the results of an overspeed analysis of the flywheel considering both ductile and non-ductile failure. This analysis concludes that the maximum allowable stress intensity in the load carrying part of the flywheel would be reached at 3,640 rpm, considerably above the design speed (125% of nominal) of 2,250 rpm. Considering non-ductile failure, the stress intensity factor for an assumed crack with length equal to the minimum that can be detected by NDE is evaluated against a lower bound fracture toughness of 50 MPa√m. Based on this calculation, the limiting speed was determined to be 7,140 rpm, demonstrating a considerable margin against non-ductile failure of the flywheel.

Dynamic Analysis

The rotating components of the pump have been analysed for dynamic characteristics, including damped natural frequencies, stability, and forced responses to normal operational load (Service Level A), and upset conditions (Service Level B) associated with the rotating masses. A linear modal and stability analysis has been performed with the aid of the computer programme ANSYS. The linear modal and harmonic responses were performed for different pump speeds within the operating frequency range or at the natural frequencies of the housing. The computer code NIROD has been applied for non-linear rotating dynamic calculations. The results of this analysis are summarised in Reference 20F.2.

20F.3.4 Mitigation and Management of In-Service Degradation

The design of the AP1000 RCP takes account of potential through life degradation mechanisms which could threaten the integrity of the pressure boundary. Design and manufacture in accordance with established codes, standards and regulations provides assurance of high reliability, in addition to supplemental requirements based on Westinghouse's extensive experience with such mechanisms and practices for mitigation and management. The degradation mechanisms are summarised below.

Degradation Mechanism	AP1000 Mitigation
Material Defects	• Selection of appropriate material product types (forging vs. casting) • Good design and manufacture (ASME) • High degree of control of manufacturing processes • Material and manufacturing inspections (NDE) • Pressure testing
Corrosion/Erosion	• Selection of materials • Good design and manufacture (ASME)

Degradation Mechanism	AP1000 Mitigation
Fatigue Cracking	• Selection of materials • Good design and manufacture (ASME) • In-service inspection
Stress Corrosion Cracking	• Selection of materials • Detrimental material control during manufacturing • Control and limitation of material compositions • Identification (design) and control (operation) of plant fluid chemistry parameters
Primary Water Stress Corrosion Cracking (PWSCC)	• Selection of materials • Prohibiting use of materials susceptible to PWSCC
Underclad cracking	• Selection of materials • High degree of control of welding processes • Material and manufacturing inspections (NDE)
Irradiation embrittlement	The AP1000 RCP is located away from the Reactor Vessel such that the pump is not considered to be susceptible to irradiation effects.

These mechanisms are primarily mitigated and managed through design, manufacturing, and inspection requirements for the RCP:

- Use of forgings instead of castings to provide a higher quality of material and alleviate the potential for internal flaws and defects
- Experienced-based selection of corrosion/erosion resistant materials
- Design, analysis, manufacturing, inspection and testing in accordance with ASME Boiler and Pressure Vessel (B&PV) Code to promote inherent quality and good design
- Identification of bounding plant chemistry values within design requirements
- Requirements for controls of materials and manufacturing:
  - Fracture toughness requirements
  - Material and Post-Weld Heat Treatment requirements
  - Delta ferrite limitation requirements
  - Limitation or prohibition of unacceptable materials and/or composition of materials (low melting point metals, detrimental materials such as halides, etc.)
  - Welding qualifications and process requirements (ASME Section IX)
  - Cladding material specifications and processes restrictions (preheat, heat input)
- Examination and testing requirements for materials and manufacturing:
- Volumetric examination (UT) of base material and final as-clad material

- Surface examination (MT) of base material after quench and temper and also prior to cladding
- Surface examination (PT) of final cladding
- Hydrostatic testing

Through these requirements and in-service inspection activities, such aforementioned degradation mechanisms are properly managed or even precluded.

20F.3.4.1 Compatibility with Environment

The RCP will be designed to operate satisfactorily with the reactor coolant water chemistry guidelines provided by Electric Power Research Institute (Reference 20F.7) and the primary coolant chemistry specification as given in Reference 20F.3. As noted in Reference 20F.2, there is over two decades nuclear industry experience of pumps utilising similar design materials for the pump pressure boundary while operating in contact with borated water without experiencing problems.

20F.3.4.2 In-Service Inspection

The design of the RCP is such that access is provided in the installed condition for inspections as specified by Section XI of the ASME code. The AP1000 design philosophy includes a design for inspectability programme to ensure that the design has been optimised to minimise uninspectable regions, to reduce the occupational radiation exposure, reduce inspection times, to allow state of the art inspection systems to be used and to enhance flaw detection and characterisation reliability. Full details of the inspectability assessment of the RCP are not yet available.

Based on the review presented in the AP1000 ISI requirements (Reference 20F.11), the components requiring in-service examination include, at a minimum, the pump casing to cold leg welds, the pump casing, the flange surface and bolting, and the terminal assembly to the RCP shell. The following design features help minimise the number of regions that require ISI.

- The pump casing, heat barrier assembly, and motor casing assembly components are manufactured as single-piece forgings; no fabrication welding is included.
- The flywheel is designed for low stress to meet the requirements of US NRC Regulatory Guide 1.14.

The final ISI requirements will be specified by the relevant utility as part of the site specific justification.

20F.3.4.3 Vibrational and Loose Parts Monitoring

The RCP is equipped with a three-axis vibration monitoring system that continuously monitors pump structure vibrations. This provides early warning of factors which could lead to premature failure of the pumps rotating component or higher than anticipated vibrational loading which could lead to fatigue crack growth.

20F.4 Strength of the Safety Case

The RCP has been subject of an extensive design development process, starting in 2004/2005 and culminating with the Final Design Review in December 2010. The final design review information package is documented in Reference 20F.12. The design review package demonstrates the level of maturity of the design and the robustness of the development process. Based on the robust design process and supporting evidence strong arguments are presented, which justify the integrity of the RCP to a standard appropriate to a Standard Class 1 component.

The RCP Final R&D Report, Reference 20F.2 references a dossier of technical data and supporting analyses. In addition to this report, the Final Design Report (Reference 20F.12) summarises the supporting design process, including a series of dedicated design reviews on the flywheel and thermal barrier, hydraulic design, pressure boundary, motor, bearing material, high pressure cooler and rotor dynamics.

In addition to this design process, a ½-scale hydraulic test as well as a ½-scale model pump test was conducted to support the design process, confirm the appropriateness of the design solution, and to confirm the analytical methods used in the design development and substantiation, as well as to demonstrate the manufacturability of the design.

The analyses and testing summarised in References 20F.2 and 20F.12 and the safety arguments based around compliance with ASME Section III requirements in Section 20F.3 demonstrate how RCP integrity will be achieved based on extensive quality assurance measures in analysis, design, fabrication, manufacture, materials, testing and inspection. The development and subsequent application of a testing and inspection programme in accordance with specifications will provide evidence and assurances that the RCP will be tolerant to through-life degradation and that any defects will be detected in good time.

In combination these elements will provide a cogent argument to substantiate integrity commensurate with the classification of the RCP for the 60-year design life.

20F.5 Index of Technical Reports

A list of the technical references supporting the substantiation is included within Reference 20F.12 and its supporting references, especially Reference 20F.2. The technical index is also provided in Table 20F-5.

20F.6 Review of Open Issues

There are no open issues for the RCP that affect the basis of the safety case arguments. Further updates to the design analyses are planned as part of the design finalisation. These updates will be controlled under robust QA-controlled procedures and will not affect the basis of the safety case arguments made in this report.

20F.7 Conclusions

The RCP has been classified in accordance with the methodology described in Reference 20F.1 as a Standard Class 1 component. This is because a DEGB of the primary loop is within the design basis and can be protected by the AP1000 passive protection systems, further, a disruptive failure of the RCP pressure boundary would be contained within the SG compartment and hence would not lead to the loss of essential safety systems or the containment pressure boundary. A disruptive failure of the RCP leading to a coincident

disruptive failure of the SG pressure boundary is not considered credible. In view of this, the RCP has not been classified as HSS.

For a Standard Class 1 component, the main element of the safety case argument is firstly, that the RCP will be manufactured in accordance with the high standards of the ASME Code, as applicable. This includes appropriate controls on material properties, manufacturing processes, design, testing, inspection and installation, such that there is a high level of confidence in the quality of the component and that it will enter service free from significant manufacturing flaws that could affect the integrity of the component over its lifetime.

The second element of the safety case argument is that the RCP design considers all credible loads and load combinations and complies with the appropriate requirements of the applicable ASME Code. This includes consideration of dynamic effect, flywheel disintegration and rotor seizure. The analyses presented in Reference 20F.2 provide evidence to support this argument.

Thirdly, that measures to prevent, detect or forewarn of in-service degradation, such as the implementation of a suitable ISI regime and vibration monitoring are specified, which will mitigate against the mechanisms identified as threatening the integrity of the component through life. The arguments presented support the claim that the structural reliability of the RCP pressure boundary will be commensurate with its consequences of gross failure.

20F.8 References

20F.1 Westinghouse Report UKP-GW-GLR-004, Rev. 3, “AP1000 UK Structural Integrity Classification,” January 2017.

20F.2 KSB Report P223 09 P086 V, Rev. 0, “Reactor Coolant Pump Type RUV for Westinghouse Reactor AP1000 Final R&D Report,” November 2008.

20F.3 Westinghouse Report EPS-MP01-M2-001, Rev. C, “Design Specification for Wet Winding Reactor Coolant Pump (RCP) for System: RCS,” February 2012.

20F.4 Bullough, R., et al., “The Demonstration of Incredibility of Failure in Structural Integrity Safety Cases,” International Journal of Pressure Vessels and Piping 78, pages 539-552, 2001.

20F.5 Regulatory Guide 1.14, Rev. 1, “Reactor Coolant Pump Flywheel Integrity,” US Nuclear Regulatory Commission.

20F.6 Westinghouse Report APP-GW-G1-003, Rev. 6, “AP1000 Seismic Design Criteria,” August 2011.

20F.7 EPRI Document Number 1014986, “Pressurized Water Reactor Primary Water Chemistry Guidelines,” Rev. 6, Electric Power Research Institute, September 2007.

20F.8 Not Used.

20F.9 ASME Publication 73-WA-PWR-2, “The Containment of Disk Burst Fragments by Cylindrical Shells,” American Society of Mechanical Engineers, 1994.

20F.10 Not Used.

20F.11 Westinghouse Report APP-GW-VW-001, Rev. 1, "AP1000® Design for Inspectability Program: ISI Requirements and Design Guidance for Class 1 Components," June 2014.

20F.12 KSB Report UA4 38793, Rev. 0, "Information Package for Final Design Review. Reactor Coolant Pump Type RUV for Westinghouse Reactor AP1000," November 2010.

Table 20F-1. Principal System Pressures, Temperatures, and Flow Rates

Principal System Pressures, Temperatures, and Flow Rates (Nominal Steady-State at Full Power)					
Location	**Description**	**Fluid**	**Pressure MPa (psi) gauge**	**Nominal Temperature °C (°F)**	**Flow m^3/hour (gpm)**
1	Hot Leg 1	Reactor Coolant	15.50 (2248)	321.11 (620)	40,347.57 (177645)
2	Hot Leg 2	Reactor Coolant	15.50 (2248)	321.11 (620)	40,347.57 (177645)
3	Cold Leg 1A	Reactor Coolant	15.93 (2310)	280.67 (537.2)	17,886.07 (39375)
4	Cold Leg 1B	Reactor Coolant	15.93 (2310)	280.67 (537.2)	17,886.07 (39375)
5	Cold Leg 2A	Reactor Coolant	15.93 (2310)	280.67 (537.2)	17,886.07 (39375)
6	Cold Leg 2B	Reactor Coolant	15.93 (2310)	280.67 (537.2)	17,886.07 (39375)

Table 20F-2. RCP Pressure Boundary Materials Specifications

Reactor Coolant Pump Pressure Materials Specifications		
Component	**Material**	**Class, Grade, or Type**
Pressure forgings	SA-182	F304, F304L, F304LN, F316, F316L, F316LN F6NM
	SA-508 or	GR3 CL1, GR3 CL2
	SA-336	F304, F304L, F304LN, F316, F316L, F316LN, F6NM (per ASME Code Case N774)
Pressure casting	SA-351	CF3A or CF8A
Tube and pipe	SA-213	TP304, TP304L, TP304LN, TP316, TP316L, TP316LN
	SA-376 or	TP304, TP304LN, TP316, TP316LN
	SA-312(c)	TP304, TP304L, TP304LN, TP316, TP316L, TP316LN
Pressure plates	SA-240	304, 304L, 304LN, 316, 316L, 316LN
Closure bolting	SA-193 or	GR B7
	SA-540	GR B24, CL 2 & CL 4, or GR B23, CL 2, CL 3 & 4

Table 20F-3. Heat Barrier and Motor Casing Assembly Pressure Boundary Material Properties

Material	**SA-182 Gr. F6NM (SA-336 Gr. F6NM per ASME Code Case N-774)**
Tensile Strength, Yield (MPa / ksi)	620 / 90
Tensile Strength, Ultimate (MPa / ksi)	790 / 115
Elongation at Break	15%
Brinell Hardness	295 max

Table 20F-4 Not Used.

Table 20F-5. Technical Index of Key Documents Relevant to RCP

Document Number	Revision	Document Title	Date	Remarks
H23 07 P023	0	Hydraulic Test Report	February 2007	Includes performance curve, 4 quadrant curves, calibration protocols
H23 07 P024	0	Pressure Pulsation Report	June 2007	-
Balancing Report KSB Flywheel	0	Flywheel: TA Prototype Balancing Report	July 2007	-
UA4 38783	0	Flywheel: TA Prototype Design Manufacturing & Testing	July 2007	-
H23 07 P033	0	Missile Analysis	September 2007	-
RUV-G-FWTA-004	0	Flywheel Stress Analysis	November 2007	-
RUV-G-FWTA-005	0	Flywheel: Ductile/Nonductile Failure	October 2008	-
P15 08 P003	0	Pressure Boundary Stress Report	October 2008	Selected parts: pump casing, lower part of motor housing, bearing bracket, thrust bearing housing
P15 08 P004	0	Pressure Boundary Stress Report	October 2008	Selected parts: upper part of motor housing, heat barrier, tie bolts; includes calculation of temperature distribution
P15 08 P051	0	Pressure Boundary Stress Report Overview and Summary	October 2008	
P15 08 P046	0	Locked Rotor Analysis	October 2008	

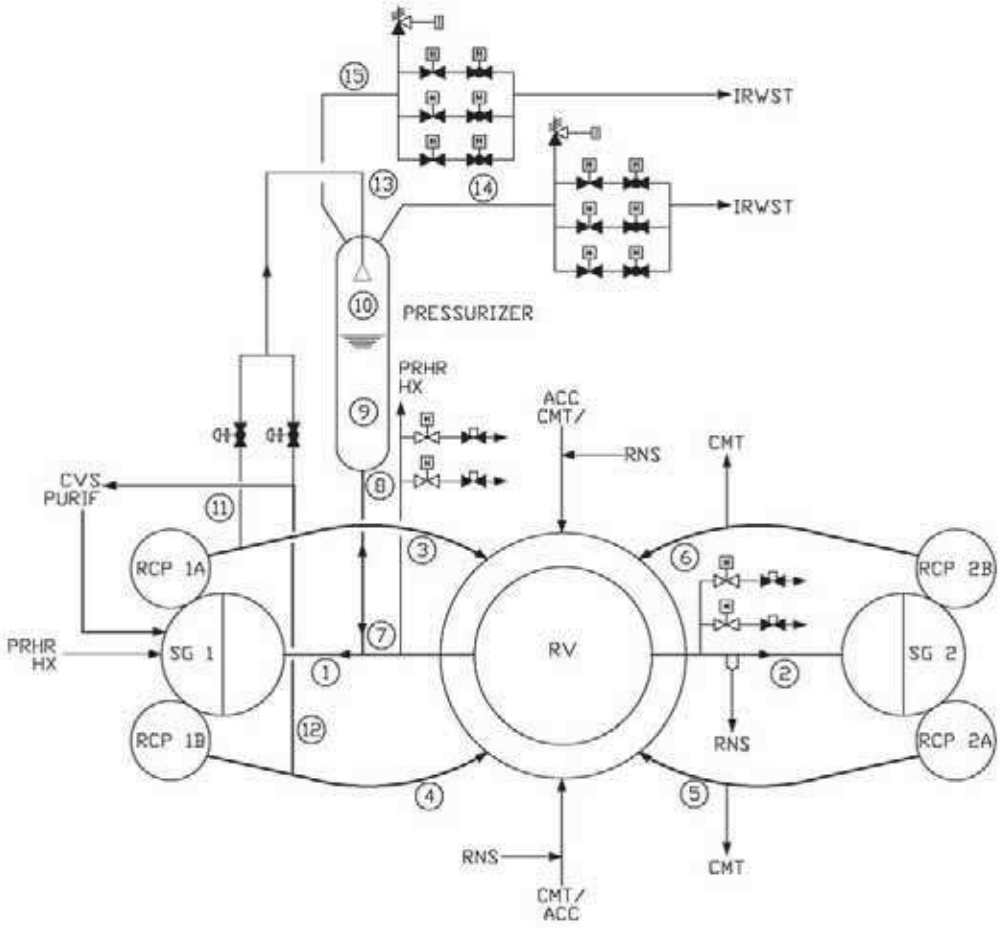


Figure 20F-1. Reactor Coolant System Schematic Flow Diagram

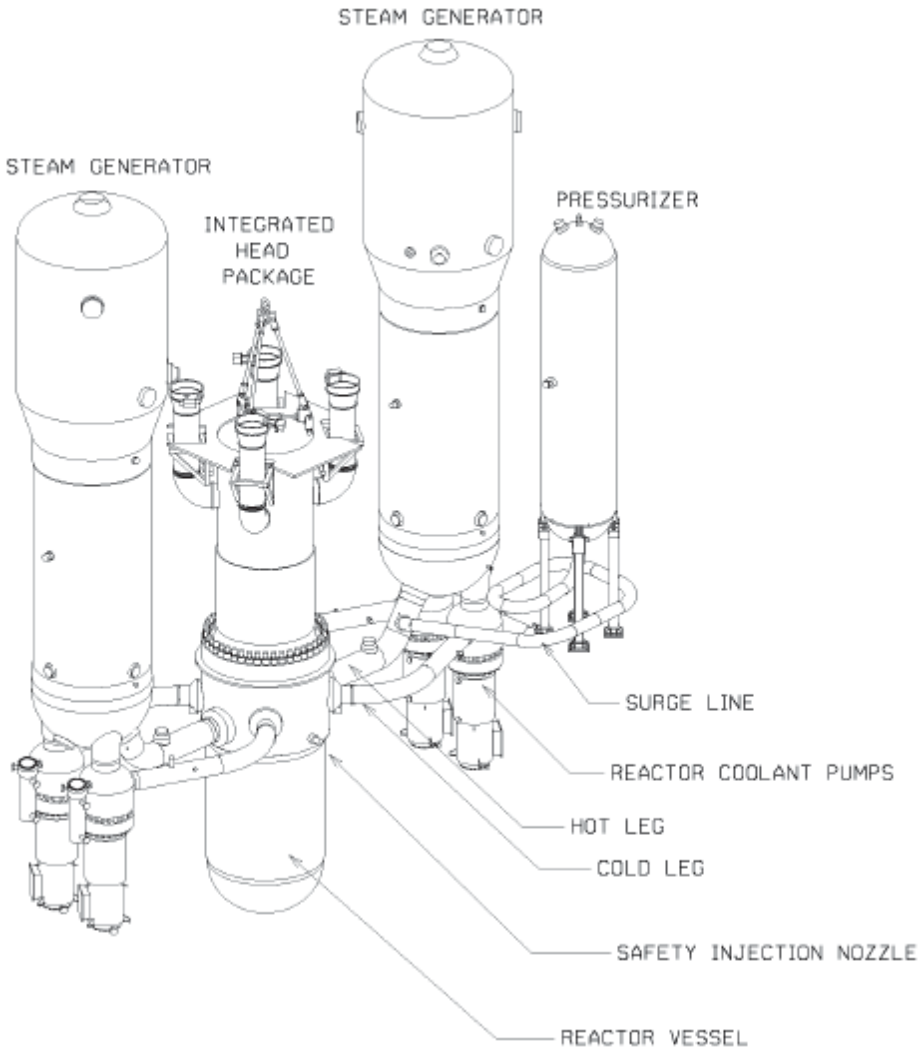


Figure 20F-2. Reactor Coolant Loops Showing RCPs

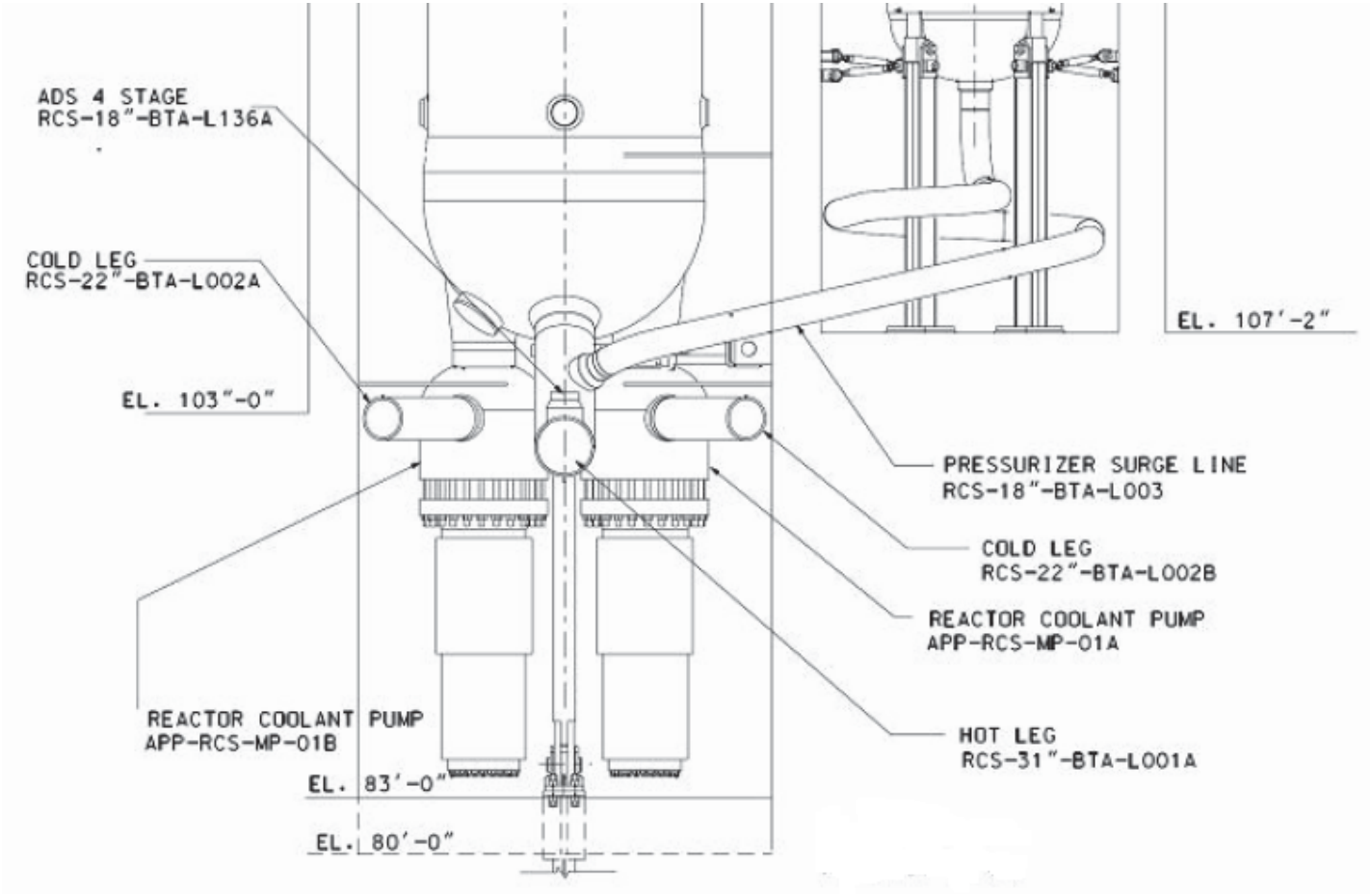


Figure 20F-3. Configuration of Reactor Coolant Pumps Below Steam Generator

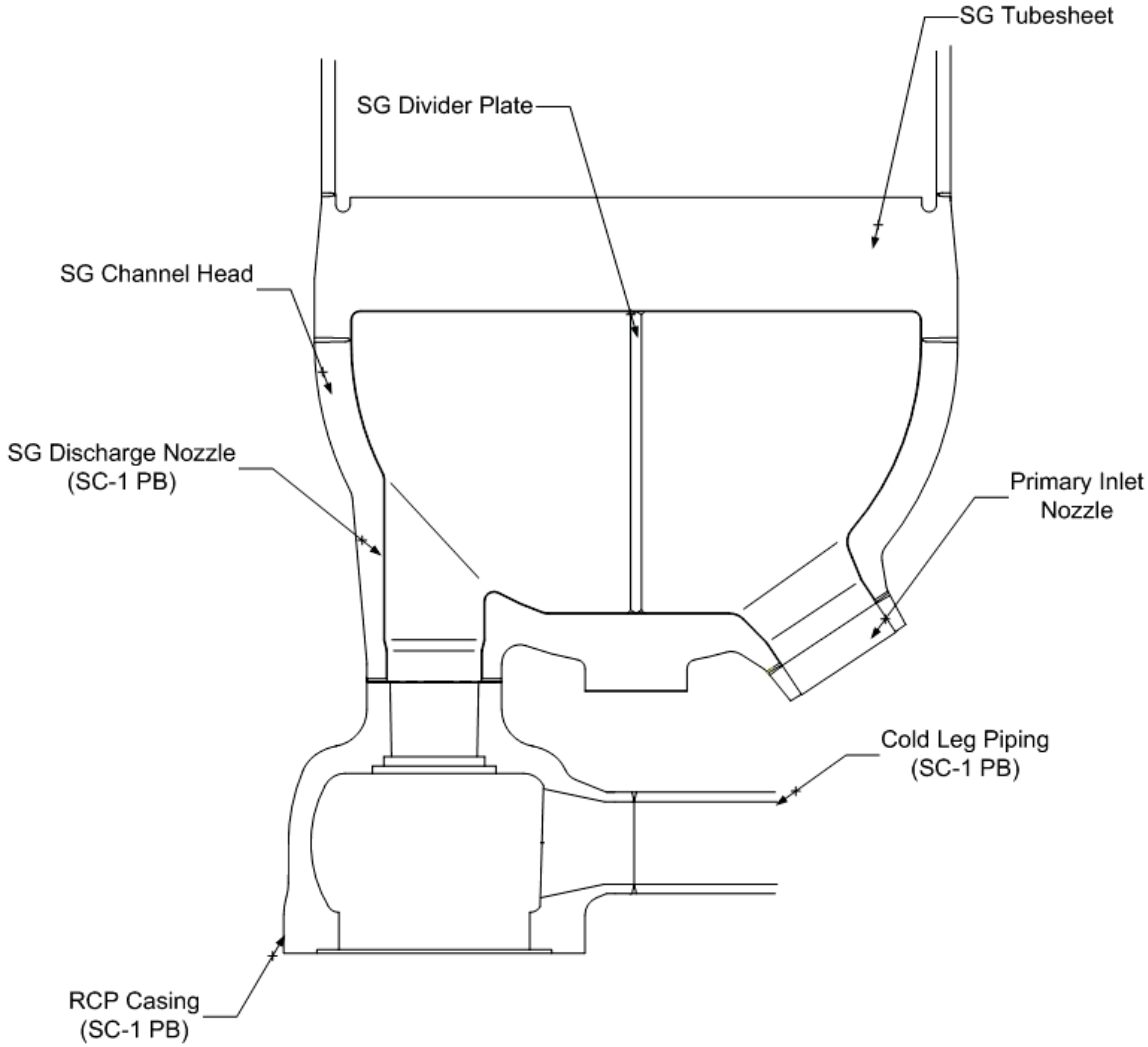


Figure 20F-4. RCP Casing Boundaries

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS AND ACRONYMS

ADS	automatic depressurisation system
ASME	American Society of Mechanical Engineers
CSR	Component Safety Report
EAC	environmentally assisted cracking
FMEA	failure modes and effects analysis
GDA	generic design assessment
HX	heat exchanger
IRWST	in-containment refuelling water storage tank
ISI	in-service inspection
LOCA	loss-of-coolant accident
NDE	nondestructive examination
PRHR	passive residual heat removal
PWSCC	primary water stress corrosion cracking
PXS	passive core cooling system
RCS	reactor coolant system
SFR	safety functional requirement
SSC	system, structure, or component
UK	United Kingdom
UNS	Unified Numbering System (alloys)
US	United States

APPENDIX 20G
PASSIVE RESIDUAL HEAT REMOVAL HEAT EXCHANGER COMPONENT SAFETY REPORT

20G.1 Introduction

This is the component safety report (CSR) for the passive residual heat removal (PRHR) heat exchanger (HX) as introduced in Section 20.2.The safety arguments herein substantiate the structural integrity of the PRHR HX to a degree of rigour commensurate with the consequences of gross structural failure. The safety argument is supported by a suite of documentation outlined in Section 20G.6 that supports the design, manufacture, installation and operation of the PRHR HX.

20G.1.1 Scope

This report presents arguments to support the claim that the nuclear and radiological risks potentially arising from gross structural failure of the PRHR HX are tolerably low for the design lifetime of 60 years. Conventional hazards to personnel safety are outside the scope of this Appendix 20G.

20G.1.2 Objectives

This report supports the claim the AP1000 plant risk remains both tolerable and as low as reasonably practicable for the design lifetime. This claim is substantiated by satisfying structural integrity safety design bases for all safety-significant AP1000 systems, structures, or components (SSCs). The safety design bases, applied across the operational, process and lifecycle scope of the safety case, embody the technical scope of the safety case; if these can be maintained, the plant will be acceptably safe. Specific safety functional requirements (SFRs) for each particular component are developed from the structural integrity safety design bases, and correspond to the functions that need to be maintained to provide assurance of nuclear and radiological safety. The SFRs applicable to the PRHR HX are identified in Section 20G.3.

20G.1.3 Interface with Other Safety Case Documents

The safety argument presented in this report is supported by a dossier of technical data and analyses. These are listed in the Technical Index (Section 20G.6) along with the role of each document in supporting the safety case argument.

20G.2 PRHR HX Description

20G.2.1 Overview

The PRHR HX is a component of the passive core cooling system (PXS) and provides emergency core decay heat removal. The PRHR HX provides core residual heat removal during postulated design basis non-loss-of-coolant accident (non-LOCA) events.

20G.2.2 Description

The PRHR HX consists of inlet and outlet channel heads connected together by 689 vertically oriented, C-shaped, thermally treated Alloy 690 tubes. The tubes are assembled into a tube sheet supported by the wall of the in-containment refuelling water storage tank (IRWST) and are normally submerged below the IRWST water surface. The PRHR HX is AP1000

Equipment Class A and is designed to meet seismic Category I requirements. Figure 20G-1 shows a diagram of the component. The design life of the PRHR HX is 60 years.

The heat exchanger inlet piping connects to an inlet channel head located near the top of the IRWST. The inlet channel head and tube sheet are attached to the tank wall via a support shell. The heat exchanger is supported by a frame attached to the IRWST floor and ceiling. The extended flange is designed to accommodate thermal expansion. The heat exchanger outlet piping is connected to the outlet channel head, which is vertically below the inlet channel head, near the tank bottom. The outlet channel head has a similar structural configuration to the inlet channel head. Materials used in the manufacture of the PRHR HX subcomponents, as detailed in Reference 20G.2, are shown in Table 20G-1. Further details of the PRHR HX design can be found in the PRHR HX Design Specification (Reference 20G.2) and in the Interface Control Document (Reference 20G.8).

20G.2.3 PRHR HX Function

Operation of the PXS is initiated (valves opened) upon receipt of any of the following signals: low steam generator level narrow range with concurrent low startup feedwater flow to any steam generator, low steam generator level wide range, high hot leg temperature, and also core makeup tank or automatic depressurisation system (ADS) actuation. The PRHR actuation signal automatically opens the normally closed valves in the line from the PRHR HX to the steam generator cold leg plenum. Driven by natural circulation, the PRHR HX takes suction from one of the RCS hot legs and injects cooled reactor coolant into the steam generator cold leg plenum on the same loop. The PRHR HX can provide decay heat removal with or without the reactor coolant pumps running. The PRHR HX transfers heat from the reactor coolant system (RCS) to the water contained in the IRWST. The water in the IRWST provides a large heat sink that acts to delay direct steaming into the containment for several hours. For additional details concerning the PRHR HX operation please refer to Chapter 6 and section 9C.

PRHR HX flow inlet and outlet line temperatures are monitored by indicators and alarms. The operator has the capability to manually throttle the discharge valves to control flow through the PRHR HX during a controlled plant cooldown.

The basic functions of PRHR HX are:

1. The PRHR HX removes sufficient heat from the RCS to mitigate loss of main feedwater and/or main feedwater line break accident assuming natural circulation.

2. The PRHR HX is capable of automatically rejecting core decay heat from the RCS to the IRWST for an extended period of time assuming the steam generated in the IRWST is returned to the tank. After a period of approximately two hours, the IRWST water reaches the saturation point and the IRWST water steams to the containment atmosphere. There it condenses on the steel containment shell which is cooled by the passive containment cooling system and is collected by a gutter arrangement at several elevations of the containment vessel and drained back into the IRWST. This process maintains the PRHR HX heat sink.

3. The PRHR HX is capable of reaching safe shutdown conditions within 36 hours, and maintaining these conditions for greater than 14 hours following non-LOCA faults, with or without AC power or the RCPs. This is substantiated using realistic analysis; safe shutdown conditions represent cooling the RCS core average temperature to 215.6°C (420°F) (average of hot leg and cold leg temperatures). Using traditional conservative design basis analysis assumptions, the RCS conditions are brought to a safe and stable

state, below the ADS actuation criteria, and this condition is maintained for greater than 72 hours. This cooldown allows the RCS pressure to be reduced, which reduces the stress in the RCS and connecting pipes to low levels, greatly reducing the chance of a subsequent LOCA. Eventually, PRHR performance is degraded to a point where the RCS conditions would approach ADS actuation criteria, and the operators would transition to open loop cooling should power not be restored (See Appendix 9C). It is important to note that "safe shutdown mode" (Mode 4) only applies to normal operation and does not apply to the post fault condition of "safe shutdown" as discussed here and explained further in Appendix 9C.

Full details of the functional requirements are given in Reference 20G.3.

The plant is allowed to operate within specified limits of PRHR HX tube leakage. The AP1000 Technical Specifications allow for PRHR HX tube leakage of up to 1893 litres/day (500 US gallons/day). If the tube leakage exceeds this rate, the Technical Specifications require that the PRHR HX will be isolated and the plant shut down. A forced plant outage will occur in case of a significant leakage or a rupture of a PRHR HX tube. The design, maintenance, and inspection of the PRHR HX in accordance with ASME requirements make this a highly unlikely event during the 60-year life of the plant.

20G.2.4 PRHR HX Boundaries

The physical boundaries for safety case assessment of the PRHR HX are shown in Reference 20G.2 and identified below:

- All pressure containing materials up to, but excluding, the circumferential welds between the inlet and outlet nozzle safe ends and the attached field piping.
- Vent and drain nozzle terminal ends, excluding field pipe weld.
- Circumferential structural weld between mounting ring and the IRWST wall liner.
- Housing upper lateral support including attachment bolting to its interfacing building embedment plate, but excluding the building attachment plate.
- Housing lower support base plate including the anchor bolts to its interfacing building embedment plate, but excluding the embedment plate.
- Circumferential weld attaching the tube sheet forging to the extended flange.

20G.3 Safety Case Requirements

The main focus of this report is to provide a structured safety argument, supported by suitable and sufficient evidence, to substantiate the classification of the PRHR HX as Standard Class 1, as outlined in Section 20G.3.2 of the report. To achieve this, the safety argument is presented as three key elements, as follows:

Claim 1: Quality of Build: High quality is achieved through good design and manufacture.

Objective: Provides evidence of good design and manufacture based on established design and manufacturing processes and use of proven materials. It provides a keystone for a demonstration of high reliability and embodies the code and plant operating experience with an objective of achieving quality of build

and the avoidance of defects (Section 20G.4.1).

Claim 2: **Good Design: Good design is achieved through compliance with the American Society of Mechanical Engineers (ASME).**

Objective: Incorporates the build experience as embodied in the design codes (Section 20G.4.2).

Claim 3: **Mitigation and Management of In-Service Degradation: Components are tolerant to through-life degradation over the design life of the plant**

Objective: Provides an assessment of through-life degradation mechanisms and shows that such mechanisms will not threaten integrity over a specific interval (Section 20G.4.3).

The safety argument is tailored according to the structural reliability claims derived from a process of component classification, with the purpose of demonstrating that component structural reliability is commensurate with the consequences of gross failure.

The three elements of the safety argument are provided in Section 20G.4 and the strength of the argument is discussed in Section 20G.5.

20G.3.1 Safety Functional Requirements

Chapter 20 identifies structural integrity safety design bases for AP1000 SSCs. These are requirements of plant systems, some duty, and some accident response, which must be maintained to provide assurance of plant nuclear and radiological safety. The Safety Functional Requirements (listed in Table 20-1) for the PRHR HX have been derived from the following performance and safety design basis criteria, which apply when normal heat removal paths are not available:

- During anticipated RCS heatup or makeup transients, the PRHR HX must automatically be actuated to cool the reactor coolant.

- During excessive cooldown events such as a steam line break or an inadvertent PRHR HX operation, the PRHR HX must not remove too much heat such that the core is damaged or cause the ADS to be actuated.

- During a non-LOCA event, the PRHR HX must be capable of cooling the core such that the plant will meet the safety analysis acceptance criteria of maintaining primary and secondary system pressures below 110% of their design values, ensuring that the minimum departure from nucleate boiling ratio remains above the applicable limit, and ensuring that pressuriser water volume is not relieved through the pressuriser safety valves.

Detailed discussion of the emergency core decay heat removal criteria for the PRHR HX is provided in Reference 20G.14. Based on these, the following Safety Function Requirements have been identified which reflect the overall role of the component in plant safety:

- **SFR 20.6.1** The PRHR HX is required to maintain the integrity of the primary coolant pressure boundary during standby, normal operation and under design basis faulted conditions for the design life of the plant.

- **SFR 20.6.2** The PRHR HX is required to remove core decay heat in accordance with the component performance requirements.

Postulated failure modes which result in a loss of these functional requirements lead to identification of structural reliability targets commensurate with the consequences of gross failure, as determined through the process of component classification as described in Section 20G.3.2.

20G.3.2 PRHR HX Structural Integrity Classification

For the United Kingdom (UK) AP1000 plant, a structural integrity classification methodology, described in Section 20.5, has been applied with the aim of determining the required level of structural reliability for each of the major plant components based on an evaluation of the direct (e.g., LOCA) and indirect (e.g., missiles and pipe whip, etc.) consequences of gross failure. The details of the classification for the PRHR HX classification are presented in Table 20-13 and in Reference 20G.1.

Evaluation of the consequences of failure of the PRHR HX concludes that the direct consequences of gross failure of the PRHR HX would be an isolable LOCA that could be protected by the passive protection systems without causing core damage. Although failure of the PRHR HX tube would lead to a LOCA and result in the loss of an important element of the passive protection system, plant performance analyses have shown that loss of the rupture of a PRHR HX tube does not lead to core damage. The analysis to support this is presented in Section 9.6.5.

Considering the indirect consequences, the risk of consequential damage due to a failure of the PRHR HX tubing is considered small primarily because the heat exchanger is located under several feet of water in the IRWST and its configuration is unlikely to lead to the generation of missiles that could challenge the integrity of essential systems or containment. The indirect consequences of gross failure of the inlet and outlet PRHR lines have been evaluated and it is considered that they would not lead to escalated consequences of failure. On this basis the PRHR HX has been categorised as a Standard Class 1 component. The safety case requirements for such components are as described in Section 20G.3.

20G.4 Safety Case Arguments

The PRHR HX has been classified as a Standard Class 1 component in accordance with the structural integrity classification methodology. The structural integrity claim is therefore based on arguments that substantiate the claims listed in Section 20G.3. Consistency with the appropriate ASME III Code Class provides the basic demonstration of fitness-for-purpose for the PRHR HX.

Compliance with ASME III rules for an ASME Safety Class 1 component provides the primary element in the safety case for the AP1000 PRHR HX.

20G.4.1 High Quality Is Achieved through Good Design and Manufacture

In order to demonstrate that high quality is achieved through good design and manufacture, evidence to support the following claims is provided:

- The fabrication specification (Reference 20G.4) complies with ASME Code requirements for Class 1 components, including ASME NQA-1 (Reference 20G.5) quality requirements.

- Supplementary requirements are specified to avoid defects and to ensure quality.

The reliability of the PRHR HX is dependent upon the design quality. The design intent is translated into a manufacturing route controlled by a Quality Assurance Programme that complies with rigorous design codes, including the ASME Boiler and Pressure Vessel Code (Code). Section 2.3 of the PRHR HX Design Specification (Reference 20G.2) provides a list of the industry codes, specifications, and standards applied to the component.

The justification of the quality of build of the PRHR HX and of materials includes:

- Special processes used for manufacturing and fabrication – The PRHR HX is classified as AP1000 Equipment Classification Class A. Design and fabrication of the PRHR HX is carried out in accordance with ASME Code, Section III, Class 1 requirements. Special procedures and supplemental fabrication requirements to avoid manufacturing defects through, for example weld procedures and heat treatment controls, are detailed in References 20G.2 and 20G.6.

- Material Specifications – The applicable PRHR HX materials specifications and testing requirements have been specified in accordance with the requirements of Section II of the ASME Code. Of specific note is the use of Alloy 690 seamless tubing and the special procedures in place to ensure it is not susceptible to environmentally assisted cracking (EAC) through tight compositional control and strict heat treatment procedures.

- Nondestructive Examination (NDE) – The NDE of the PRHR HX is conducted in accordance with ASME Code, Section III requirements using ultrasonic examination, penetrant examination, magnetic particle examination, surface examination and weld examination. Supplemental inspection requirements include but are not limited to those detailed in Reference 20G.6.

- Fracture Toughness – Assurance of adequate fracture toughness of ferritic materials in the PRHR HX (input and output nozzles, channel heads and tube sheets) (ASME Code, Section III, Class 1 component) is provided by compliance with the requirements for fracture toughness testing included in NB-2300 and Appendix G to Section III of the ASME Code. This is described in further detail in Section 20G.4.3.3 of this document.

Together these provide a keystone for a demonstration that the PRHR HX is well designed, will enter service free from structurally significant defects and that the effects of through-life degradation on material properties will not have a deleterious effect on the structural reliability of the component.

20G.4.2 Good Design Is Achieved through Compliance with ASME

In order to demonstrate that good design is achieved through compliance with ASME, evidence to substantiate the following argument is provided:

- The design has been analysed and has been shown to comply with the requirements of ASME Code, Section III for Class 1 components.

The AP1000 PRHR HX has been designed in accordance with the requirements of the ASME Boiler and Pressure Vessel Code Section III, Div 1 – 1998 Edition through 2000 Addenda. The assessment is reported in a suite of calculation notes, as listed in the Technical Index of this report. The ASME Code, Section III subsection applicable to each sub-component is summarised below.

- Channel Heads (Upper & Lower) – Subsection NB

- Tube sheets (Upper & Lower) – Subsection NB
- Tube Sheet to Support Plate Weld – Subsection NB
- Tube Bundle – Subsection NB
- Tube Supports – Subsection NF
- Support Frame Housing, Including Upper & Lower Supports – Subsection NF
- Extended Flange – Subsection NF
- Support Shell to IRWST Liner Seal Weld – Subsection NF
- Support Shell – Subsection NF
- Support Plate – Subsection NF
- Mounting Ring – Subsection NF
- Vent/Drain Nozzle (upper and lower) Flow Restrictor – Subsection NB
- Vent/Drain Nozzle Pipe – Subsection NC

The design transients relevant to the PRHR HX are detailed in detail in Reference 20G.7; and are enveloped by the RCS transients shown in Table 20-22. The load cases considered include normal, upset, emergency and faulted conditions.

The external loads on the PRHR HX are specified in the Interface Control Document (Reference 20G.8). This includes nozzle external loads and seismic loads. In addition to conventional seismic loading, a dynamic assessment has been performed to evaluate the response of the PRHR HX assembly to sloshing effects, as well as the hydrodynamic loads due to pressure waves generated by the activation of the spargers in the IRWST or a PRHR HX tube rupture. The PRHR HX is therefore designed against design basis internal and external hazards.

An ASME sizing assessment of the critical locations of the PRHR HX is undertaken to ensure the designed thicknesses meet the minimum thickness required by the ASME Code, considering required loadings. Adequate sectional thicknesses/areas are specified throughout the component (Reference 20G.11).

The thermal and structural analysis has been undertaken using established procedures to demonstrate that for the load cases analysed, the stresses and cumulative fatigue usage factors are satisfactory and meet the appropriate limits set forth in the ASME Code, Section III. Details of these calculations are presented in the references calculation notes as detailed in the technical index.

20G.4.3 Mitigation and Management of In-Service Degradation

In order to demonstrate that the design has taken account of in-service degradation mechanisms, evidence to substantiate the following argument is provided:

- A structured process has been applied to identify in-service degradation mechanisms.

- The design has been optimised to mitigate against the risk from in-service degradation mechanisms.

20G.4.3.1 Identification of Degradation Mechanisms

Reference 20G.9 provides a failure modes and effects analysis (FMEA) which was carried out in order to identify design characteristics, potential hardware failures, or human errors associated with the design and operation of the PRHR HX that could lead to a potentially hazardous condition such as a LOCA.

The FMEA resulted in the identification of potential hazards or operational problems. Potential through-life degradation mechanisms considered included the following:

- Primary water stress corrosion cracking (PWSCC)
- Corrosion
- Fatigue
- Brittle fracture
- Vibration
- Erosion
- Failure arising from manufacturing defects

The basis of the safety case argument is that mitigation against corrosion, fatigue, vibration, erosion and manufacturing defects is essentially provided by compliance with ASME design and fabrication rules together with the associated in-service inspection (ISI) requirements and the operating experience embodied within the code to mitigate against these degradation mechanisms. Vibration analysis showed wide margin to established criteria for fluid-elastic excitation, vortex shedding and turbulence during the relatively short actuation periods. Further discussion of the measures associated with the mitigation and management of PWSCC in nickel alloys and the avoidance of brittle fracture (nonductile failure) is provided below.

It was determined in the FMEA study (Reference 20G.9) that there is sufficient mitigation in place to offset the potential hazards identified within the report, where the majority of hazards are assumed to be of minimal likelihood and minimal severity.

20G.4.3.2 Mitigation and Management of PWSCC

The main component of the PRHR HX is the Alloy 690 seamless tubing. Reference 20G.10 defines the guidelines for the manufacture, examination, quality assurance, testing and shipment of nickel-chromium-iron Alloy 690 (Alloy Unified Numbering System (UNS) N06690) seamless tubing. Alloy 690 is produced in accordance with the requirements of Section III of the ASME Code for ASME Class 1 components and has proven resistance to PWSCC.

ASME compliance will be achieved as the material manufacture of the seamless tubing complies with the applicable requirements of ASME Code, Section III Division 1 Subsection NB-2000, ASME Code, Section II Part B SB-163, including Supplementary Requirement S2 for high yield strength.

Material testing, for example, Ultrasonic Testing and Eddy Current Testing of Alloy 690 tubing, will be performed in accordance with the requirements stated in Reference 20G.10 supplemented by ASME SE-213 and ASME SE-571 respectively.

20G.4.3.3 Avoidance of Non-Ductile Failure

The Generic Design Report (Reference 20G.11) presents the calculations performed to safeguard the PRHR HX from non-ductile failure during normal, upset and test conditions, as required by the ASME Code, Section III, subsection NB.

Calculated stress intensity factors (K_I) were compared with the allowable critical values (K_{IR}). The analysis is based on the general methodology set forth in Appendix G of the ASME Code and in WRC Bulletin No. 175 (Reference 20G.15). Safety coefficients have

been applied to calculated stress intensity factors K_I in accordance with Appendix G, Articles G-2215 and G-2400.

In accordance with Appendix G of the ASME Code, Section III, the postulated defects for vessel walls are sharp surface defects normal to the direction of maximum stress. The depth of such defects is assumed to be 1/4 the shell section thickness with a length of 1.5 times the section thickness.

Reference 20G.11 provides further detail of the significant results of the fracture toughness calculations. The critical areas were found to be at the shell discontinuities and at the heel of nozzles. These regions cannot satisfy code requirements if a 1/4 thickness defect is assumed. Therefore, flaw depths 1/10 of the shell thickness were postulated, this is permitted by ASME Code, Section III Appendix G-2120 where there is a basis for ensuring smaller postulated defects, such as in regions remote from welds. Based on this assumption, the Heat Exchanger meets the Appendix G requirements for normal, upset and test conditions.

20G.4.3.4 In-Service Inspection

ISI provides forewarning of potential failure and a means of monitoring degradation. ISI forms an important element of the safety case argument. ISI is carried out in accordance with Section XI of the ASME Code. References 20G.12 and 20G.13 provide details of the inspectability assessment and details of the examination requirements for the PRHR HX using different techniques. Consideration is also given to the inspection coverage, limitations and access conditions at each location. A summary of the ISI requirements is shown in Table 20G-3.

Written instructions concerning PRHR HX inspection, maintenance, installation, operation, assembly details and disassembly details will be provided following generic design assessment (GDA). From this information, inspection of the PRHR HX will be carried out in accordance with appropriate maintenance and inspection and testing schedules. This will include as part of the ISI inspection regime, examination of the PRHR HX tubing over the entire tube length (tube end to tube end). NDE personnel performing such examinations will be qualified in accordance with ASME Code, Section XI Appendix VIII.

Inspection and maintenance of the PRHR HX will be performed during refuelling in accordance with the inspection plan and the refuelling frequency.

Both tube sheets can be accessed from outside the IRWST through the manways for inspection and maintenance without draining the IRWST. The channel head is designed to accomplish complete draining of the channel head, including the manway penetrations.

20G.5 Strength of the Safety Case

The PRHR HX is classified as a Standard Class 1 component. The safety argument in Section 20G.4 demonstrates how PRHR HX structural integrity is established based on extensive quality assurance measures in design, manufacture, materials, testing and qualified inspection. The strength of the safety case is underpinned by evidence to show that the PRHR HX has been specified and deterministically justified in accordance with the ASME Boiler and Pressure Vessel Code for Class 1 components. Additional mitigation against the effects of through-life degradation is provided by careful material selection and in-service inspection. In combination these elements provide a cogent argument to substantiate reliability commensurate with the classification of the PRHR HX.

To substantiate this claim, this report provides a structured argument supported by suitable and sufficient evidence. To achieve this, three key elements namely Quality of Build, Good Design and mitigation and management of in-service degradation have shown how this will be achieved.

Quality of Build has been demonstrated by compliance with ASME Code, Section III. Applicable material specification control has been achieved in accordance with Section II of the ASME code. NDE in accordance with ASME Code, Section III with adequate fracture toughness demonstrated by compliance with ASME code specifications.

Good design has been demonstrated by providing evidence, via the Generic Design Report (Reference 20G.11), that stresses arising during normal, upset, emergency and faulted conditions are within allowable limits specified in the ASME Boiler and Pressure Vessel Code Section III, Div 1 – 1998 Edition through 2000 Addenda.

Mitigation and management of in-service degradation has been demonstrated by identifying degradation mechanisms and potential hazards that could lead to loss of integrity of the PRHR HX. ISI will also provide forewarning of degradation with inspection carried out at appropriate intervals.

20G.6 Index of Technical Reports

Table 20G-4 provides a list of technical references supporting the safety case and the function of each document within the safety case.

20G.7 Review of Open Issues

There are no open issues for the PRHR HX that affect the bases of the safety case arguments presented in support of GDA.

20G.8 Conclusions

This report presents arguments that support the claim that the structural reliability of the PRHR HX is commensurate with the consequences of gross failure. To evaluate this, the PRHR HX has been classified in accordance with the procedure for structural integrity classification specified in Reference 20G.1. Based on this, the component has been evaluated as a Standard Class 1 component.

The PRHR HX is designed in accordance with the high standards of the ASME Code as applicable to ASME Class 1 components. This includes tight controls on material properties, manufacturing processes, design, testing, inspection and installation such that there is a high level of confidence the PRHR HX will be constructed with high quality; and will enter service free from significant flaws that could affect the integrity of the component over its lifetime. Secondly, measures to prevent or forewarn of in-service degradation, such as the use of EAC-resistant materials and in-service inspection, are specified, which will mitigate against the identified mechanisms having the potential to threaten the integrity of the component through-life.

20G.9 References

20G.1 Westinghouse Report UKP-GW-GLR-004, Rev. 3, “AP1000 UK Structural Integrity Classification,” January 2017.

20G.2 Westinghouse Report APP-ME02-Z0-101, Rev. 12, "Design Specification AP1000 Passive Residual Heat Removal Heat Exchanger for System PXS," December 2016.

20G.3 Westinghouse Report APP-ME02-Z0-001, Rev. 4, "AP1000 Passive Residual Heat Removal Heat Exchanger Functional Specification," March 2011.

20G.4 Westinghouse Report APP-ME02-Z0-200, Rev. 2, "AP1000 PRHR HX Fabrication Specification," May 2013.

20G.5 ASME NQA-1-1994, "Quality Assurance Program Requirements for Nuclear Facilities," American Society of Mechanical Engineers, 1994.

20G.6 Westinghouse Report APP-GW-VLR-010, Rev. 2, "AP1000 Supplemental Fabrication and Inspection Requirements," January 2016.

20G.7 Westinghouse Report APP-PXS-M3C-205, Rev. 5, "Passive Core Cooling System (PXS) Design Transients," June 2014.

20G.8 Westinghouse Report APP-PXS-M8-003, Rev. 3, "AP1000 PRHR HX Interface Control Document," October 2015.

20G.9 Westinghouse Report APP-ME02-GRA-001, Rev. 1, "AP1000 Passive Residual Heat Removal Heat Exchanger (PRHR HX) Failure Mode and Effects Analysis (FMEA)," February 2010.

20G.10 Westinghouse Report APP-VL53-Z0-014, Rev. 3, "Thermally Treated Alloy UNS N06690 (Alloy 690) Tubing for the AP1000 Passive Residual Heat Removal (PRHR) Heat Exchanger," March 2010.

20G.11 Westinghouse Report APP-ME02-Z0R-100, Rev. 2, "AP1000 Passive Residual Heat Removal Heat Exchanger Generic Design Report," November 2016.

20G.12 Westinghouse Report APP-GW-VW-001, Rev. 1, "AP1000® Design for Inspectability Program: ISI Requirements and Design Guidance for Class 1 Components," June 2014.

20G.13 Westinghouse Report APP-ME02-VMR-001, Rev. 1, "AP1000 Component ISI Inspectability Assessment: Passive Residual Heat Removal Heat Exchanger (PRHR HX)," January 2013.

20G.14 Westinghouse Report APP-PXS-M3-001, Rev. 7, "Passive Core Cooling System, System Specification Document," July 2015.

20G.15 WRC Bulletin No. 175, "PVRC Recommendations on Toughness Requirements for Ferritic Materials," Welding Research Council, Inc., August 1975.

Table 20G-1. PRHR HX Pressure Boundary Materials

Component	Material
HX Tubes	ASME SB-163 Ni-Cr-Fe Alloy UNS N06690, Cobalt 0.015% max, thermally treated
Channel Head Assembly (Head, Tube Sheet, Inlet/Outlet Nozzles and Manway)	SA-508 Grade 3 Class 2
Manway Cover	SA-533 Grade B, Class 1
Manway Insert	SA-240 Type 304L
Nozzle Safe-Ends	SA-336, F316LN
Nozzle/Safe-End Buttering	ASME Nickel Base Alloys plus applicable Code Cases
Channel Head Cladding	ASME Austenitic Stainless Steels plus applicable Code Cases
Tube Sheet Cladding Primary Side Secondary Side	ASME Nickel Base Alloys plus applicable Code Cases ASME Austenitic Stainless Steels plus applicable Code Cases

Table 20G-2. Not Used

Table 20G-3. Summary of PRHR HX ISI Requirements

Weld/Volume	Examination Method[3]			
	PT	MT	UT	Visual
Inlet Channel Head to Tube Sheet Weld			Yes	
Outlet Channel head to Tube Sheet Weld			Yes	
Inlet Nozzle Inside Radius Section			Yes	
Outlet Nozzle Inside Radius Section			Yes	
Inlet Nozzle to Safe End Butt Weld	Yes		Yes	
Outlet Nozzle to Safe End Butt Weld	Yes		Yes	
Studs and Nuts				Yes
Tube Sheet to Support Plate Weld	Yes[2]	Yes[2]		
Tube Sheet to Extended Flange Weld	Yes[2]	Yes[2]	Yes	
Support Plate to Support Shell Weld				Yes
Support Shell to Mounting Ring Weld				Yes
Mounting Ring Welds				Yes
Mounting Ring to IRWST Liner Seal Weld				Yes
Heat Exchanger Tubing			Yes[1]	
Support Structures				Yes

Note:

1. Eddy current testing applied, although ASME Code Section XI, Table IWB-2500-1 only defines this requirement for steam generator tubing.
2. Either dye penetrant or magnetic particle examination satisfies requirement.
3. PT – dye penetrant; MT – magnetic particle; UT – volumetric; Visual – visual detection, various methods.

Table 20G-4. PRHR HX Technical Index

Document Reference	Title	Description of Role in Safety Case
APP-ME02-Z0-001	AP1000 Passive Residual Heat Removal Heat Exchanger Functional Specification	Defines the functional performance and operational requirements for PRHR HX
APP-ME02-Z0-101	AP1000 Passive Residual Heat Removal Heat Exchanger Design Specification	Provides the basis for the design and construction of the PRHR HX to conform to the ASME Code and applicable Code Cases.
APP-ME02-Z0R-100	AP1000 Passive Residual Heat Removal Heat Exchanger Generic Design Report	Contains the detailed analyses required to demonstrate the adequacy of the structural design to sustain the imposed loadings, requirements and provisions identified such that all design requirements of the Design Specification and of the ASME Code are met.
APP-GW-VW-001	AP1000® Design for Inspectability Program: ISI Requirements and Design Guidance for Class 1 Components	Contains requirements and design guidance relative to ISI for ASME Class 1 components, specifically focused on the concept of design for inspectability, to ensure that adequate design and access provisions for meeting ASME Code, Section XI are considered in the overall plant design.
APP-ME02-VMR-001	AP1000 Component ISI Inspectability Assessment: PRHR HX	Presents a detailed assessment of the accessibility and inspectability for in-service inspection of PRHR HX.
APP-ME02-Z0-200	AP1000 PRHR HX Fabrication Specification	Provides details of the specific requirements and special procedures for fabrication of the PRHR HX.
APP-PXS-M8-003	AP1000 PRHR HX Interface Control Document	Interface Control Document.

Table 20G-4. PRHR HX Technical Index (cont.)

Document Reference	Title	Description of Role in Safety Case
APP-GW-VLR-010	AP1000 Supplemental Fabrication & Inspection Requirements	Provides details of supplemental fabrication and inspection requirements that are over and above ASME Code requirements.
APP-RCS-M1-001	Reactor Coolant System Design Transients	Defines the transients used to qualify the reactor coolant system to design requirements.
APP-PXS-M3C-205	PXS Design Transients	Describes the fluid systems transients to be considered when designing the PXS piping and components.
APP-VL53-Z0-014	Thermally Treated Alloy UNS N06690 (Alloy 690) Tubing for the AP1000 Passive Residual Heat Removal (PRHR) Heat Exchanger.	Provides guidelines for the manufacture, examination, quality assurance, testing and shipment of nickel-chromium-iron alloy UNS N06690 (Alloy 690) seamless tubing to be used in the PRHR HX.

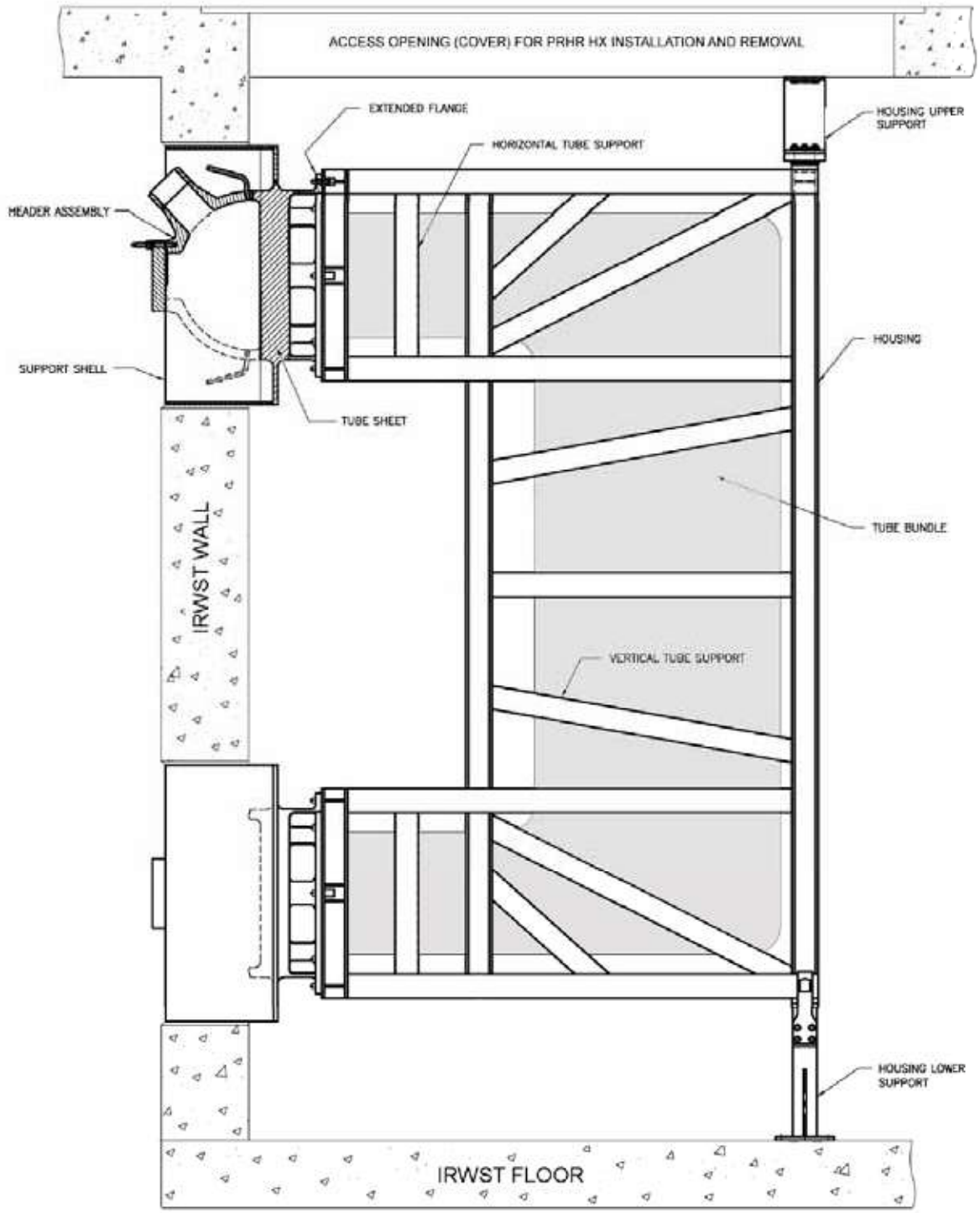


Figure 20G-1. Passive Residual Heat Removal Heat Exchanger

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS AND ACRONYMS

ALARP	as low as reasonably practicable
ANSI	American National Standards Institute
ASME	American Society of Mechanical Engineers
CMT	core makeup tank
CMTR	certified material test reports
CSR	Component Safety Report
CV	containment vessel
DVI	direct vessel injection
FMEA	failure modes and effects analysis
GDA	generic design assessment
HAZ	heat affected zone
ID	inside diameter
ISI	in-service inspection
LOCA	loss-of-coolant accident
NDE	nondestructive examination
PWHT	post-weld heat treatment
PXS	passive core cooling system
RCS	reactor coolant system
RT_{NDT}	reference temperature nil ductility transition
SFR	safety functional requirement
SSC	system, structure, or component
UK	United Kingdom
US	United States

APPENDIX 20H
CORE MAKEUP TANK COMPONENT SAFETY REPORT

20H.1 Introduction

This is the component safety report (CSR) for the core makeup tank (CMT) as introduced in Section 20.2.The safety argument herein substantiates the structural integrity of the CMT to a degree of rigour commensurate with the consequences of gross structural failure. The safety argument is supported by a suite of documentation outlined in Section 20H.5 that supports the design, manufacture, installation, and operation of the CMT.

20H.1.1 Scope

This report presents arguments to support the claim that the nuclear and radiological risks potentially arising from gross structural failure of the CMT are tolerably low for the design lifetime objective of 60 years. Conventional hazards to personnel safety are outside the scope of this Appendix 20H.

20H.1.2 Objectives

The objective of this report is to establish that the AP1000 plant risk remains both tolerable and as low as reasonably practicable (ALARP) for the design lifetime. This claim is substantiated by satisfying structural integrity safety design bases for all safety-significant AP1000 systems, structures, or components (SSCs). The safety design bases, applied across the operational, process and lifecycle scope of the safety case, embody the technical scope of the safety case: if these can be maintained at all times, the plant will be acceptably safe. Specific safety functional requirements (SFRs) for each particular component are developed from the structural integrity safety design bases, and correspond to the functions that need to be maintained to provide assurance of nuclear and radiological safety. The SFRs applicable to the CMT are identified in Section 20H.2.1.

20H.1.3 Interface with Other Safety Case Documents

This report provides a safety argument to support the nuclear safety case claims relevant to the CMT. The safety argument presented in this report is supported by a dossier of technical specifications and analyses. These are listed in the Technical Index (Section 20H.5) and each is specifically identified in the relevant section of the structured safety argument.

20H.1.4 Core Makeup Tank Description

20H.1.4.1 Overview

The CMTs (two), as shown in Figure 20H-1, are components of the passive core cooling system (PXS). They are located inside the containment above the direct vessel injection (DVI) line connections. The basic function of the CMT is to provide reactor coolant system (RCS) makeup and boration during events when the normal makeup system is unavailable or insufficient. Upon receipt of a safeguards actuation signal, valves open to provide makeup water to the RCS.

20H.1.4.2 Description

Details of the CMT design can be found in the CMT design specification (Reference 20H.2). The two CMTs are vertical cylindrical tanks with hemispherical upper and lower heads. They are located inside the containment (on the 102.3-m floor elevation) (i.e., 7'2" above grade) above the DVI line connections to the reactor vessel, which are at an elevation near the bottom of the hot leg (Figure 20H-2).

The CMT is made of carbon steel with stainless-steel clad on the internal surface with hemispherical upper and lower heads supported on columns. The tank has an inlet diffuser welded to the inside of the upper head in the centre. A manway is provided for access to the inside of the tank. There are eight level taps to insert level instrumentation. There are six thermowell penetrations, two level/sample taps, and one fill tap. In addition, three lifting lugs are welded to the upper head. The CMT is designed with a linear-type support having a flanged interface for bolting the CMT to the building structure. The CMT is designed in accordance with the requirements of American Society of Mechanical Engineers (ASME) Boiler and Pressure Vessel Code (Code) Section III, Subsection NB (Reference 20H.3). The CMT supports are qualified to the criteria of subsection NF of the ASME Code. Inside the containment, the secondary shield wall serves as a barrier between the reactor coolant loops and the CMTs.

20H.1.4.2.1 Materials

Materials used in the manufacture of the CMT subcomponents are shown in Table 20H-1. The cylinder and heads are made of low-alloy carbon steel and are clad on the internal surfaces with stainless steel for corrosion resistance. The nominal cladding thickness will be 5.6 mm (0.22 inch). Machining of as-deposited cladding is not required if the surface finish is suitable for required nondestructive examination (NDE) inspections. All clad surfaces including nozzles and manway will be 100 percent ultrasonically inspected for both bond and defects by the straight beam method. Materials in contact with the reactor coolant fluid are fabricated with corrosion resistant materials or are cladded. The cladding and stainless steel is carried through the rest of the tank features which include a manway, various small nozzles (level indicators, thermowells, pressure taps, and sample taps), and larger inlet/outlet nozzles. The cobalt content of materials used in the construction of component surfaces which come into contact with the primary coolant, including screws, bolts, washers, weld cladding and locking cups, has been specified to be no greater than 0.05 percent weight, integrated average. The cobalt content of all other welding materials is excluded from this requirement.

20H.1.4.2.2 Design Temperature and Pressure

The structural design of the CMT is based on the maximum steady state internal design pressure and design temperature values of 17.13 MPa gauge (2485 psig) and 343°C (650°F), respectively. These values are to be used in conjunction with the appropriate values of external pressure and temperature defined in the Design Specification (Reference 20H.2).

During normal operation, the CMTs are completely full of borated water (with a boron concentration of about 3500 ppm). The temperature of the borated water in the CMTs is generally about the same as that of the containment at a nominal operating temperature of 10°C to 48.89°C (50° to 120°F), since the tanks are not insulated or heated. Normally, the CMT outlet is isolated from the RCS and the cold leg pressure balance line is open, which keeps the tank at a pressure generally equal to the RCS.

20H.1.4.2.3 Total Volume/Flowrate

The free internal volume for the CMT is approximately 70.792 m^3 (2500 ft^3).

The discharge line from each CMT contains a flow-tuning orifice that provides a mechanism for the field adjustment of the injection line resistance. The orifice is used to establish the required flow rates assumed in the CMT design. The CMTs provide injection for an extended time after CMT actuation. The duration of injection will be much longer when the CMTs operate in the water recirculation mode as compared to the steam condensation mode.

20H.1.4.2.4 Manway

The CMT has an access manway in the shell of the tank to permit access for inspection and maintenance. The manway cover bolting is designed to facilitate the use of remotely operated stud tensioning and de-tensioning devices. The manway cover assembly is provided with design features to facilitate installation and removal of the cover away from the manway.

20H.1.4.2.5 Nozzles

The mechanical characteristics of the CMT nozzles are shown in Table 20H-2. All nozzles terminate in stainless steel material for compatibility with the interfacing piping material. The stainless steel safe ends are of sufficient length to prevent damage to the transition weld on the nozzle during field welding. Nozzles are buttered prior to final post-weld heat treatment (PWHT). In this way, the heat affected zone (HAZ) of the nozzle receives a PWHT. After final PWHT, the stainless-steel ends are welded to the buttered vessel nozzles. By following this procedure, sensitisation of the stainless steel ends is prevented.

20H.1.4.2.6 Lifting Lugs

The lifting lugs are designed in accordance with the criteria specified in American National Standards Institute (ANSI) N14.6-1993 (Reference 20H.5).

20H.1.4.2.7 Chemistry

The reactor coolant inside the CMT is controlled in accordance with the Electric Power Research Institute pressurised water reactor primary water chemistry guidelines (Reference 20H.6) as discussed in Chapter 21. The CMT water may contain dissolved oxygen at a concentration equal to saturation at atmospheric pressure. Samples from the CMTs are taken periodically to check the boron concentration. Connections are provided for remotely adjusting (if required) the boron concentration in the CMT during normal plant operation. Makeup water for the CMT is provided by the chemical and volume control system.

20H.1.4.2.8 Pressurisation

Overpressure protection of the CMT and RCS is provided by the use of ASME Code, Section III, Class 1 pressure safety valves which are located in the RCS piping.

20H.1.5 Core Makeup Tank Function

The basic function of the CMT is to provide RCS makeup and boration during events when the normal makeup system is unavailable or insufficient. Full details of the functional requirements are given in the AP1000 Core Makeup Tank Functional Specification (Reference 20H.7). CMT level and inlet and outlet line temperatures are monitored by indicators and alarms. The operator can take action (as required) to meet the technical specification requirements for CMT operability.

Each CMT is connected to the RCS through an outlet line that has normally closed isolation valves. Upon receipt of a safeguards actuation signal, these valves open to align the CMT to the RCS. The outlet line from each CMT is connected to one of the two DVI lines, which provides an injection path for the water supplied by the CMT. When the cold legs are filled, the CMTs operate in a water-recirculation mode driven by the density difference between the hot inlet line and the cold CMT. This mode of operation provides RCS water makeup and effective boration appropriate for non-loss-of-coolant accident (LOCA) events.

When the cold legs are voided, the CMTs operate in a steam-displacement (or steam-compensated injection) mode driven by the density difference between the cold leg steam and the cold water in the CMT. This mode provides greater injection rates than the water recirculation mode, which is appropriate for LOCA events. The CMT flow is based on limiting CMT and RCS temperatures and pressures to ensure that the CMTs can provide injection for a minimum of approximately 20 minutes after CMT actuation and the initial steam condensation transient. For non-LOCA events, the duration of injection will be much longer. Each CMTs inlet has an inlet diffuser designed to reduce steam velocities into the cold CMT water, thereby minimising potential water hammer and reducing the amount of mixing that occurs during initial CMT operation.

20H.1.6 Core Makeup Tank Boundaries

The physical boundaries of the CMT are defined in Reference 20H.2, as summarised below.

The equipment boundary of ASME Code jurisdiction includes all components in Figure 20H-3 and Figure 20H-4.

Figure 20H-3 shows the ASME Code jurisdictional boundaries of CMT, which include all pressure retaining materials up to the circumferential welds between the piping and nozzle safe ends or nozzle and piping (nozzle to pipe weld is not in the CMT jurisdictional boundary). The manway cover (including bolts), tank supports, shear block and shear block weld are ASME Code qualified components. As depicted in Figure 20H-4, the anchor bolts and associated hardware, slide and embedment plates are not ASME components.

The CMT is supported by eight columns. Each column support will have an individual base plate at the bottom. This serves as an interface for attaching the CMT to the embedded plate on the building floor. Auxiliary pipe connections including the quantity and size for the nozzles are specified in Reference 20H.2.

20H.2 Safety Case Requirements

The main focus of this report is to provide a structured safety argument, supported by suitable and sufficient evidence, to substantiate a structural reliability commensurate with the requirements of a Standard Class 1 component, as outlined in Section 20H.2.2 of this report. To achieve this, the safety argument is presented as three key elements, as follows:

Claim 1: **Quality of Build: High quality is achieved through good design and manufacture (Section 20H.3.1).**

Objective: Provides evidence of good design and manufacture based on established design and manufacturing processes and use of proven materials. It provides a keystone for a demonstration of high reliability and embodies the code and plant operating experience with the objective of achieving quality of build and the avoidance of defects.

Claim 2: **Good Design: Good design is achieved through compliance with ASME (Section 20H.3.2).**

Objective: Incorporates the build experience as embodied in the design codes.

Claim 3: **Mitigation and Management of In-Service Degradation: Components are tolerant to through-life degradation over the design life of the plant (Section 20H.3.3).**

Objective: Provides an assessment of through-life degradation mechanisms and shows that such mechanisms will not threaten integrity over a specific interval.

The three elements of the safety argument are provided in Section 20H.3 and the strength of the argument is discussed in Section 20H.4.

20H.2.1 Safety Functional Requirements

Chapter 20 identifies structural integrity safety design bases for the SSCs. These are requirements of plant systems, some duty and some accident response, which must be maintained at all times to provide assurance of plant nuclear and radiological safety. Identification of the SFRs for the CMT follows from the performance and safety functional requirements outlined in Reference 20H.7, as follows:

The CMT is a large tank containing borated water (at RCS pressure) that drains into the RCS during certain plant transients and accidents. Based on this, the following SFRs have been identified that reflect the overall role of the component in plant safety:

- **SFR 20.7.1** The CMT pressure boundary must remain intact during standby, normal operation, and under design basis faulted conditions for the design life of the plant.

- **SFR 20.7.2** The CMT is required to store cold borated water under reactor coolant system pressure for high-pressure reactor coolant makeup in accordance with the component performance requirements.

- **SFR 20.7.3** The CMT is required to deliver borated water to the RCS in the event of a LOCA or non-LOCA when the normal makeup system is unavailable or insufficient.

Postulated failure modes that result in a loss of these functional requirements lead to identification of structural reliability targets commensurate with the consequences of gross failure, as determined through the process of component classification as described in Section 20H.2.2.

20H.2.2 Core Makeup Tank Structural Integrity Classification

For the United Kingdom (UK) AP1000 plant, the structural integrity classification methodology (Reference 20H.1), has been applied with the aim of determining the required level of structural reliability for each of the major plant components based on an evaluation of the direct consequences (e.g., LOCA) and indirect consequences (e.g., missiles/pipe whip etc) of gross failure. The detail of the classification for the CMTs is presented in Reference 20H.1.

This concluded that the direct consequences of gross failure of the CMT is bounded by the more limiting DVI line failure which is shown not to lead to core damage and is within the design basis analysis of Section 9.6.5. Considering the indirect failure consequences, due to the proximity of the CMTs to the containment vessel (CV) it is possible that damage to the containment could occur. An analysis of the effectiveness of the containment cooling with damaged containment has been undertaken and results show that the CV pressure is reduced to and maintained near atmospheric pressure. Also, CMT failure cannot impact the containment below elevation (102.1 m), thus the mass loss from the CV does not deplete the water inventory inside the containment quickly. In summary, damage to the containment would not prevent the passive protection system from cooling the core but the release rate would be increased. There is also potential for damage to Category 1 control and instrumentation cables but this would not prevent the redundant train of the affected safety system from operating properly. On this basis, the CMT has been categorised as a Standard Class 1 component.

20H.3 Safety Case Arguments

As discussed in Section 20H.2.2, the CMT has been classified as a Class 1 component in accordance with Reference 20H.1. The structural integrity claim is, therefore, based on arguments which substantiate the claims listed in Section 20H.2. Consistency with the appropriate ASME III Code class provides the basic demonstration of fitness-for-purpose for the CMT.

Compliance with ASME Code, Section III rules for a Class 1 component provides the primary element in the safety case for the AP1000 CMTs.

20H.3.1 High Quality is Achieved through Good Design and Manufacture

In order to demonstrate that high quality is achieved through good design and manufacture, evidence to support the following claims is provided:

- The fabrication specification complies with ASME Code requirements for Class 1 components.
- Supplementary requirements are specified to avoid defects and to ensure quality.

The reliability of the CMT depends upon the equipment design quality. The design intent is translated into a manufacturing route which is controlled by a Quality Assurance Programme which complies with rigorous design codes including the ASME Boiler and Vessel Pressure Code (Reference 20H.3). Section 2.3 of the CMT Design Specification (Reference 20H.2) provides a comprehensive list of the industry codes, specifications and standards applied to the component.

The justification of the quality of build of the CMT and materials includes:

- **Processes used for manufacturing and fabrication** – Design and fabrication of the CMT is carried out in accordance with ASME Code, Section III, Class 1 requirements as defined in the Design Specification (Reference 20H.2).
- **Material Specifications** – The CMT materials specifications and testing requirements have been specified in accordance with the requirements of Section II of the ASME Code. Material specifications also include relevant Westinghouse Standards, ANSI/ASME/ASTM standards, United States (US) Code of Federal Regulations and US Nuclear Regulatory Commission Regulatory Guides as defined in Reference 20H.2. The primary coolant boundary will be fabricated from ASME plate and/or forging material. Charpy V-notch tests and drop weight fracture toughness tests are required. Nozzles will terminate in stainless steel material for compatibility with the interfacing piping material. The stainless-steel safe ends will be of sufficient length to prevent damage to the transition weld on the nozzle during field welding. Nozzles will be buttered prior to final PWHT. In this way, the HAZ of the nozzle will be receiving a PWHT. After final PWHT, the stainless steel ends will be welded to the buttered vessel nozzles. By following this procedure sensitisation of the stainless-steel ends is prevented.
- **Material Test Reports** – Materials for parts within the jurisdiction of the ASME Code will have certified material test reports (CMTR) clearly presenting the results of all ASME Code required testing. All other materials will be certified as required by the applicable material specifications, but as a minimum by a certificate of compliance.

- **Mechanical Testing** – Hydrostatic tests will be carried out in accordance with the requirements of the ASME Code, Section III, using working fluids meeting the appropriate water chemistry specifications. The hydrostatic test will be performed at a test pressure of 1.25 times the design pressure and at a test temperature safe from brittle fracture. The minimum hydrostatic test temperature will be 33.3°C (60°F) above the reference temperature nil-ductility temperature (RT_{NDT}).

- **In-Manufacture NDE** – The NDE of the CMT is conducted in accordance with ASME Code, Section III requirements using ultrasonic examination, liquid penetrant examination, magnetic particle examination, surface examination and weld examination. These provide confidence that the required weld quality is achieved during manufacture. All clad surfaces, including nozzle and manway will be 100% ultrasonically inspected for both bond and defects by the straight beam method. Clad thickness will be measured in accordance with approved procedures. No seams will pass through or interfere with nozzles, and they are designed for 100 percent inspectability where required by the code. Only personnel qualified and certified in accordance with ASME Section III will perform Section III examinations.

- **Pre-Service and In-Service Examination Requirements** – The pre-service and in-service examination and acceptance criteria for of the CMT will comply with the 1998 Edition with Addenda up through and including 2000 of ASME Code, Section XI, Subsection IWB for pressure boundary welds and Subsection IWF for all other welds. Inspection personnel qualified and certified in accordance with the requirements of ASME Code, Section XI, IWA-2300 will perform the pre-service examination.

- **Weld Qualifications** – All pressure boundary welding procedures and welders qualifications will be in accordance with the ASME Code, Section III and Section IX. All non pressure boundary welding procedures and welders qualifications will be in accordance with the ASME Code, Section IX or equivalent approved standards.

Together these provide a keystone for a demonstration that the CMT will achieve a high quality, will enter service free from structurally significant defects and that the effects of through-life degradation on material properties will not have a deleterious effect on the structural reliability of the vessel.

20H.3.2 Good Design is Achieved through Compliance with ASME

In order to demonstrate that good design is achieved through compliance with ASME, evidence to substantiate the following argument is provided:

- The design has been analysed and has been shown to comply with the requirements of ASME Code, Section III for Class 1 components.

  The AP1000 CMT has been designed in accordance with the requirements of the ASME Code, Section III, Div 1 – 1998 Edition with Addenda up through and including 2000. The CMT has been assessed against the limits specified in Subsection NB and the tank supports are assessed against Subsection NF. The assessment is reported in a suite of calculation notes, as listed in the Technical Index of this report. The subsection applicable to each sub-component is summarised below.

  The design transients used in the analysis are shown in Reference 20H.9. The load cases considered include normal, upset, emergency, and faulted conditions. The external load combinations on the CMT are specified in the CMT Design Specification (Reference 20H.2);

these include nozzle external loads, seismic loads and all other loads and loading combinations. The design of the CMT has, therefore, been designed against all design basis internal and external hazards.

Reference 20H.9 summarises an ASME sizing assessment of the critical locations of the CMT showing the minimum required thickness/minimum required areas compared to the actual thickness/actual area. Adequate thickness and/or actual area are provided for all locations.

Reference 20H.9 provides the results of a thermal and structural analysis which has been undertaken using established procedures to demonstrate that for the load cases analysed all the stresses and cumulative fatigue usage factors are satisfactory and meet the appropriate limits set forth in the ASME Code, Section III. This evaluation includes:

- A basic sizing and justification of the main parts and components of the CMT.
- A dynamic seismic analysis by the response spectrum method.
- Evaluation of stresses from internal pressure, earthquake effects, dead weight and externally applied loads at significant locations of the vessel shell, manway and nozzles.

Based on the results of the assessments presented in Reference 20H.9, it can be shown the design of the CMT meets all the applicable requirements of ASME Code, Section III.

20H.3.3 Mitigation and Management of In-Service Degradation

To demonstrate that the design has taken account of in-service degradation mechanisms, evidence to substantiate the following argument is provided:

- A structured process has been applied to identify in-service degradation mechanisms.
- The design has been optimised to mitigate against the risk from in-service degradation mechanisms.

20H.3.3.1 Identification of Degradation Mechanisms

Reference 20H.10 provides a failure modes and effects analysis (FMEA), which was carried out to identify design characteristics, potential hardware failures, or human errors associated with the design and operation of the CMT that could lead to a potentially hazardous condition such as injury, fatality, or loss of equipment and product.

The FMEA resulted in the identification of potential hazards or operational problems. Potential through-life degradation mechanisms considered were:

- Thermal cycling
- Fatigue
- Brittle fracture
- Corrosion
- Failure arising from manufacturing defect

The basis of the safety case argument is mitigation against corrosion, fatigue and manufacturing defects is essentially provided by compliance with ASME material specification, design and fabrication rules. The associated in-service inspection (ISI)

requirements and the operating experience embodied within the Code mitigate against these degradation mechanisms.

20H.3.3.2 **Avoidance of Non-Ductile Failure**

Reference 20H.9 presents the calculations performed for the CMT vessel shell, CMT inlet and outlet nozzles, and manway to provide confidence that the CMT is safeguarded against non-ductile failure during normal, upset, and test conditions, as required by ASME Code.

The non-ductile failure evaluation of the CMT was performed in accordance with Appendix G of the ASME Code. The ANSYS finite element analysis code was used to obtain the temperature and stresses. The FRMECH programme, Reference 20H.12, was used to obtain the stress intensity factors. Methods of evaluating non-ductile behaviour are based on linear elastic fracture mechanics of thick sections.

The postulated flaw is assumed to be perpendicular to the direction of maximum stress. The postulated flaw for the vessel shell is typically in the hoop direction and for the CMT inlet nozzle to be perpendicular to the direction of maximum stress, which is typically the hoop direction. The regions of the manway which may be susceptible to a non-ductile failure are the centre of the manway cover, the inside surface of the manway knuckle, and the inside surface of the shell

Calculated stress intensity factors (K_I) were compared with the allowable critical values (K_{IR}). The analysis is based on the general methodology set forth in Appendix G of the ASME Code and in WRC Bulletin No. 175 (Reference 20H.11). Safety coefficients have been applied to calculated stress intensity factors K_I in accordance with Appendix G, Articles G – 2215 and G – 2400.

The analysis presented demonstrates that the AP1000 CMT satisfies the structural requirements of Section III of the ASME Code for all loading conditions specified in Reference 20H.2.

20H.3.3.3 **In-Service Inspection**

ISI provides forewarning of degradation mechanisms and this forms an important element of the safety case argument. ISI will be carried out in accordance with Section XI of the ASME Code. An inspectability assessment of the CMT has been carried out. This assessment (Reference 20H.13) provides evidence that the design of the CMT has been optimised to permit ISI, including consideration of the examination requirements for the CMT using different techniques, the inspection coverage, limitations and access conditions at each location. A summary of the ISI requirements is shown in Table 20H-4.

20H.4 Strength of the Safety Case

The CMT is classified as a Standard Class 1 component. The safety argument in Section 20H.3 demonstrates how CMT structural integrity is established based on extensive quality assurance measures in design, manufacture, materials, testing, and qualified inspection. The strength of the safety case is based on achievement of integrity and that the CMT has been deterministically justified in accordance with ASME Code, Section III. The arguments presented are considered to provide a cogent basis to substantiate reliability claims commensurate with the Standard Class 1 classification of the CMT.

To substantiate this assertion this report provides a structured argument supported by suitable and sufficient evidence to achieve this, three key elements namely; Quality of Build,

Good Design and mitigation and management of in-service degradation have shown how this will be achieved.

Quality of Build has been demonstrated by compliance with ASME Code, Section III. Material specification control has been achieved in accordance with Section II of ASME Code, NDE in accordance with ASME Code, Section III with adequate fracture toughness demonstrated by compliance with the ASME Code.

Good design has been demonstrated by providing evidence that design transients including normal, upset, emergency and faulted conditions have been analysed and loadings shown to be within the allowable limits of ASME Code, Section III, Div 1 – 1998 Edition with Addenda up through and including 2000.

The approach to mitigation and management of in-service degradation has been demonstrated by identifying all design characteristics, degradation mechanisms and potential hazards that could lead to injury, fatality or loss of operation of the CMT. ISI will also provide forewarning of degradation with inspection and maintenance carried out at appropriate intervals.

20H.5 Index of Technical Reports

Table 20H-5 provides a list of technical references supporting the safety case and the function of each document within the safety case.

20H.6 Review of Open Issues

There are no open issues for the CMT that affect the basis of the safety case arguments presented in support of generic design assessment (GDA).

20H.7 Conclusions

This report presents arguments that support the claim that the structural reliability of the CMT is commensurate with the consequences of gross failure. To evaluate this, the CMT has been classified in accordance with the procedure for structural integrity classification specified in Reference 20H.1.

The main element of the safety case argument is that the CMT has been designed in accordance with the high standards of the ASME Code as applicable to ASME Class 1 components. This includes tight controls on material properties, manufacturing processes, design, testing, inspection and installation such that there is a high level of confidence in the quality of the CMT and that it will enter service free from significant flaws that could affect the integrity of the CMT over its lifetime. Section 20H.5 of this report identifies the detailed specifications and analyses that provide the evidence to support this argument. In addition, an FMEA was performed to identify potential threats to the structural integrity of the CMT through its design life. Appropriate measures have been incorporated into the design and inspection requirements to mitigate against these threats.

Based on the arguments presented, together with the referenced supporting evidence, it is considered that the structural reliability of the CMT has been justified to a standard commensurate with the consequences of its gross failure.

20H.8 References

20H.1 Westinghouse Report UKP-GW-GLR-004, Rev. 3, "UK AP1000 Structural Integrity Classification," January 2017.

20H.2 Westinghouse Report APP-MT01-Z0-100, Rev. 9, "Design Specification for AP1000 Core Makeup Tank for System PXS," August 2016.

20H.3 ASME Boiler and Pressure Vessel Code Section III, Division 1, "Rules for Construction of Nuclear Power Plant Components," American Society of Mechanical Engineers, 1998 Edition with Addenda up through and including 2000.

20H.4 Not used.

20H.5 ANSI N14.6, "Special Lifting Devices for Shipping Containers Weighing 10,000 Pounds (4500 kg) or More," American National Standards Institute, 1993.

20H.6 Electric Power Research Institute (EPRI), 1014986, "Pressurized Water Reactor Primary Water Chemistry Guidelines – Revision 6," 2007.

20H.7 Westinghouse Report APP-MT01-Z0-001, Rev. 3, "AP1000 Core Makeup Tank Functional Specification," July 2011.

20H.8 Not used.

20H.9 Westinghouse Report APP-MT01-Z0R-001, Rev. 5, "AP1000 Core Makeup Tank ASME Generic Design Report," October 2016.

20H.10 Westinghouse Report APP-MT01-GRA-001, Rev. 0, "AP1000 Core Makeup Tank Failure Modes and Effects Analysis," November 2009.

20H.11 WRC Bulletin No. 175, "PVRC Recommendations on Toughness Requirements for Ferritic Materials," Welding Research Council, Inc., August 1975.

20H.12 Westinghouse Letter LTR-NCE-02-25, "Software Release Letter for FRMECH, Version 2.0, on the HP-UX 11.0 System State," September 11, 2002.

20H.13 Westinghouse Report APP-MT01-VMR-001, Rev. 1, "AP1000 Component ISI Inspectability Assessment: Core Makeup Tank," May 2012.

Table 20H-1. Core Makeup Tank Pressure Boundary Materials

Component	Material
Shell	SA-533 or SA-508
Upper/Lower Head	SA-533 or SA-508
Inlet/Outlet Nozzle	SA-508
Inlet/Outlet Nozzle Safe End	SA-336
Manway	SA-508
Manway Cover	SA-533
Manway Insert	SA-240
Manway Closure Stud Bolt	SA-193
Manway Closure Nut	SA-194
Manway Spherical Washer	SA-194
Support Column	SA-671
Inlet Nozzle Diffuser	SA-312
Lifting Lug	SA-516 or SA-533
Level Tap, Sample/Level Tap, Thermowell Penetration	SA-479
Fill Tap	Bimetallic SB-166 w/ SA-479 Safe End

Table 20H-2. Core Makeup Tank Nozzle Mechanical Characteristics

Duty Qty.	Qty.	Pipe Size		Material	Location	End Configuration
Inlet Nozzle from Cold Leg	1	DN 200 (NPS 8) Sch. 160		SA-508 with Cladding(1)	Top Head in the Centre	per design drawing
Outlet Nozzle	1	DN 200 (NPS 8) Sch. 160		SA-508 with Cladding(1)	Bottom Head in the Centre	per design drawing
Thermowell Penetration	6	DN 25 (NPS 1) Sch 80		SA-479	Top Head, Bottom Head and Shell	per design drawing
Level Tap	8	DN 25 (NPS 1) Sch 80		SA-479	Shell	1" 3000# Socket Weld Coupling
Sample Taps Level Taps	2	DN 25 (NPS 1) Sch 80		SA-479	Top and Bottom Head	1" 3000# Socket Weld Coupling
Fill Tap	1	DN 25 (NPS 1) Sch 80		SB-166 with SA-478 Safe End	Shell	1" 3000# Socket Weld Coupling

Notes:

1. Inlet & Outlet Safe End Material: SA-336

Table 20H-3. Not Used

Table 20H-4. Summary Core Makeup Tank ISI Requirements(1)

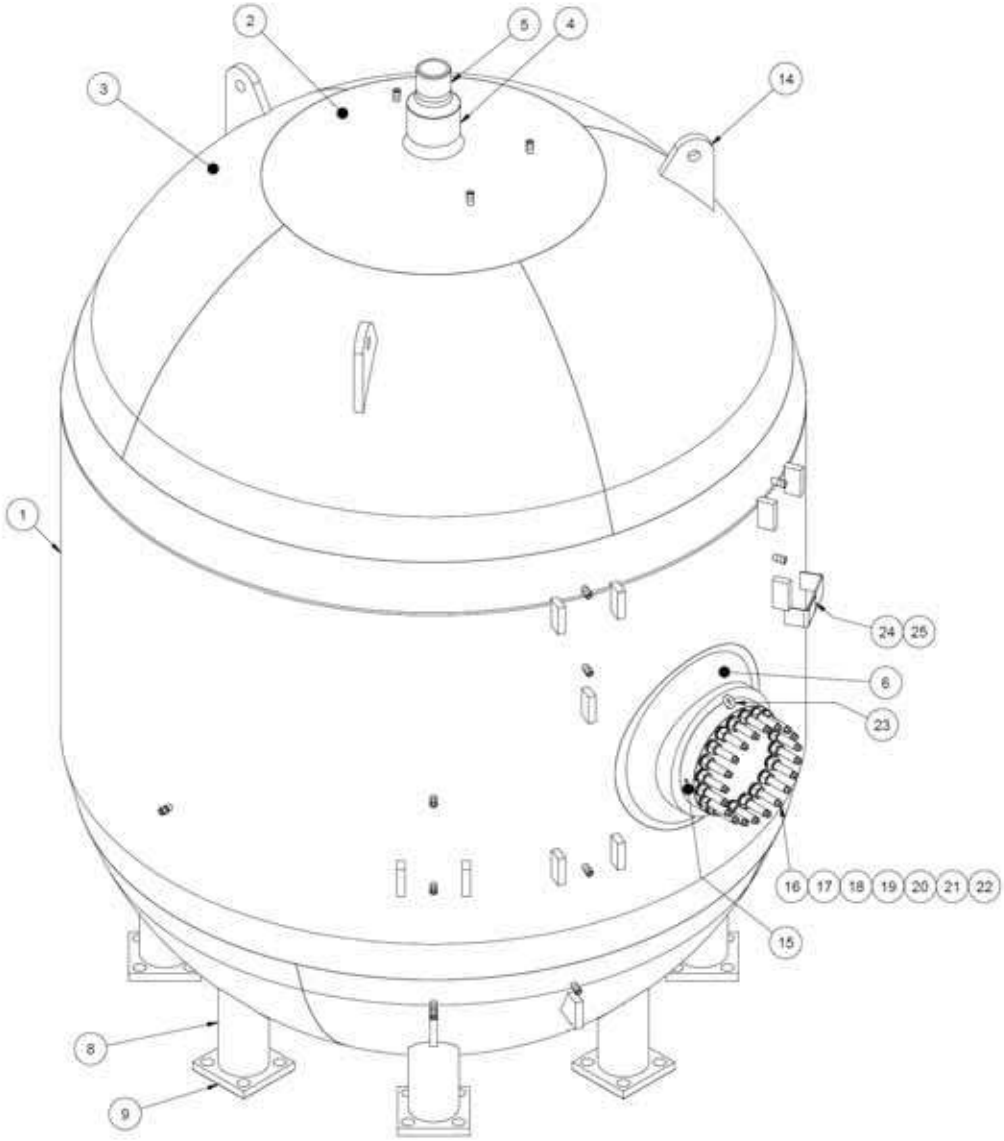
Description	Volumetric	Surface	Visual
Lower Head Transition Ring to Cylindrical Shell Circumferential Weld	X		
Upper Head Transition Ring to Cylindrical Shell Circumferential Weld	X		
Lower Head Dome to Head Transition Ring Circumferential Weld	X		
Upper Head Dome to Head Transition Ring Circumferential Weld	X		
Lower Head Transition Ring Meridional Welds(3)	X		
Upper Head Transition Ring Meridional Welds(3)	X		
Outlet Nozzle to Lower Head Dome Weld	X		
Inlet Nozzle to Lower Head Dome Weld	X		
Outlet Nozzle Inside Radius Region	[2]		[2]
Inlet Nozzle Inside Radius Region	[2]		[2]
Outlet Nozzle to Safe End Butt Weld	X	X	
Inlet Nozzle to Safe End Butt Weld	X	X	
Manway Bolts and Nuts			X
Welded Attachments (Support column to Lower Head)		X	
Pressure Retaining Boundary			X

Notes:

1. In-service inspection requirements for Class 1 tanks are not specifically designated in Table IWB-2500-1. Since the Core Makeup Tank is a Class 1 vessel the requirements identified for the pressuriser are assumed.
2. Provisions allowing for substitution of an enhanced magnification visual examination of the inside diameter (ID) surface in lieu of volumetric examination are applied.
3. Meridional welds, if applicable.

Table 20H-5. Core Makeup Tank Technical Index

Document Reference	Title	Description of Role in Safety Case
Report & Specifications		
APP-MT01-Z0-100	Design Specification for AP1000 Core Makeup Tank for System PXS	Defines the requirements for the design, materials, function, fabrication, examination, testing, cleaning, packaging, and shipping of the CMT to conform to the ASME Code, Section III.
APP-MT01-Z0-001	AP1000 Core Makeup Tank Functional Specification	Defines the functional performance and operational requirements for the CMT.
APP-MT01-Z0R-001	AP1000 Core Makeup Tank ASME Generic Design Report	Contains the detailed analyses required to demonstrate the adequacy of the structural design to sustain and meet in every respect the requirements of the Design Specification and of the ASME Code.
APP-GW-VW-001	AP1000 Design for Inspectability Program: ISI Requirements for Class 1 Components	Contains requirements and design guidance relative to ISI for ASME Class 1 components, specifically focused on the concept of design for inspectability, to ensure that adequate design and access provisions for meeting ASME Code, Section XI are considered in the overall plant design.
APP-MT01-VMR-001	AP1000 Component ISI Inspectability Assessment – Core Makeup Tank	Inspectability assessment relative to the ISI of the CMT.
APP-MT01-Z0-200	AP1000 Core Makeup Tank Fabrication Specification	Establishes the requirements for the fabrication, material, examination, testing, cleaning, packaging, preparation for shipment and quality assurance of the CMT.
APP-RCS-M1-001	Reactor Coolant System Design Transients	Defines the transients used to qualify the reactor coolant system to design requirement.
APP-GW-VLR-010	AP1000 Supplemental Fabrication and Inspection Requirements	Provides details of the AP1000 supplemental fabrication and inspection requirements.



1 Shell Barrel
2 Shell Head Crown
3 Shell Head Petal
4 Central Nozzle
5 Nozzle Safe End
6 Manway Pad
8 Support Column
9 Support Column Base
14 Vessel Lifting Lug
15 Manway Cover
16-22 Manway Closure Hardware
23 Eyebolt
24 Nameplate
25 Metallic Drive Screw

Figure 20H-1. Core Makeup Tank

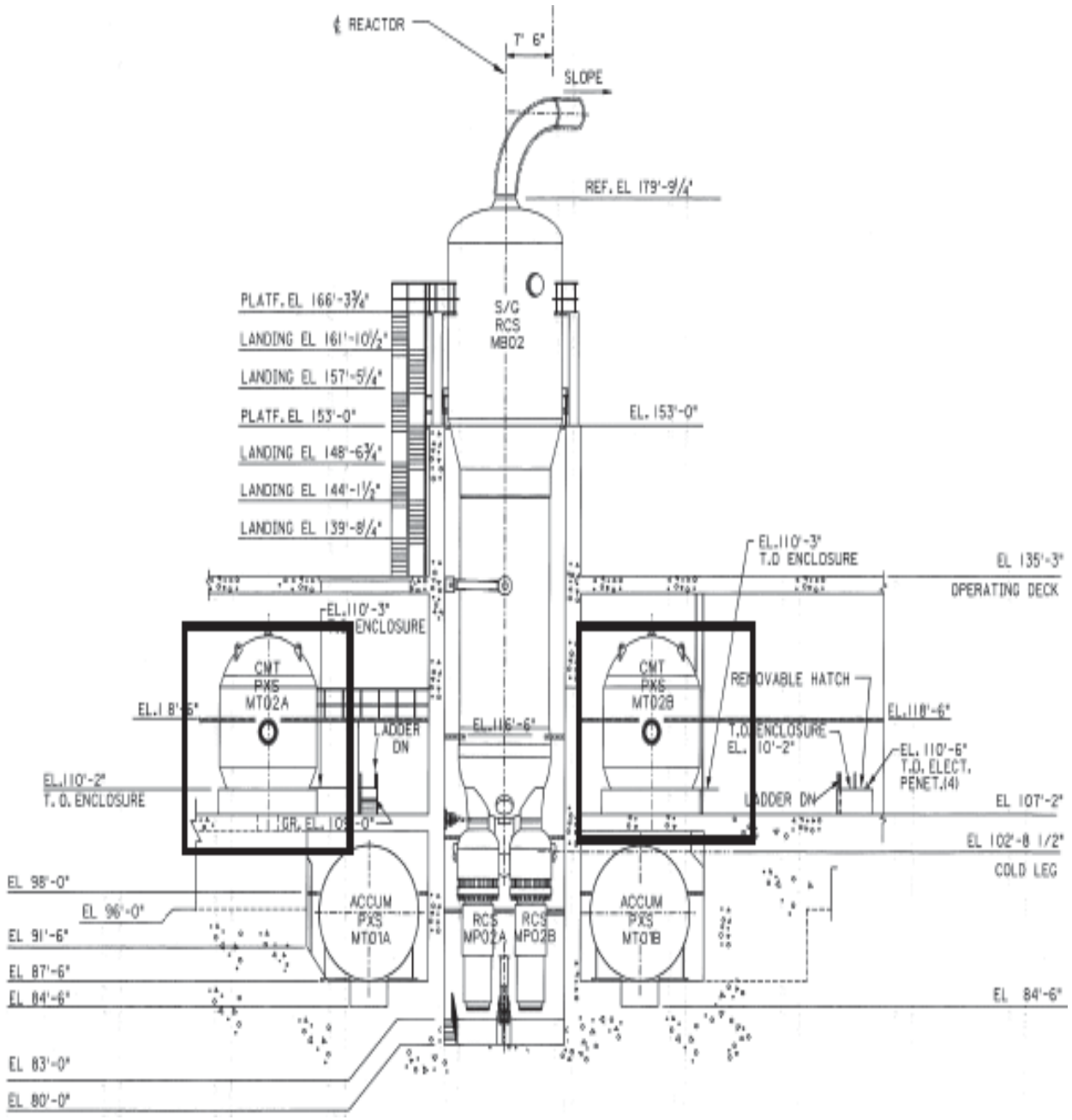


Figure 20H-2. Core Makeup Tank Elevation

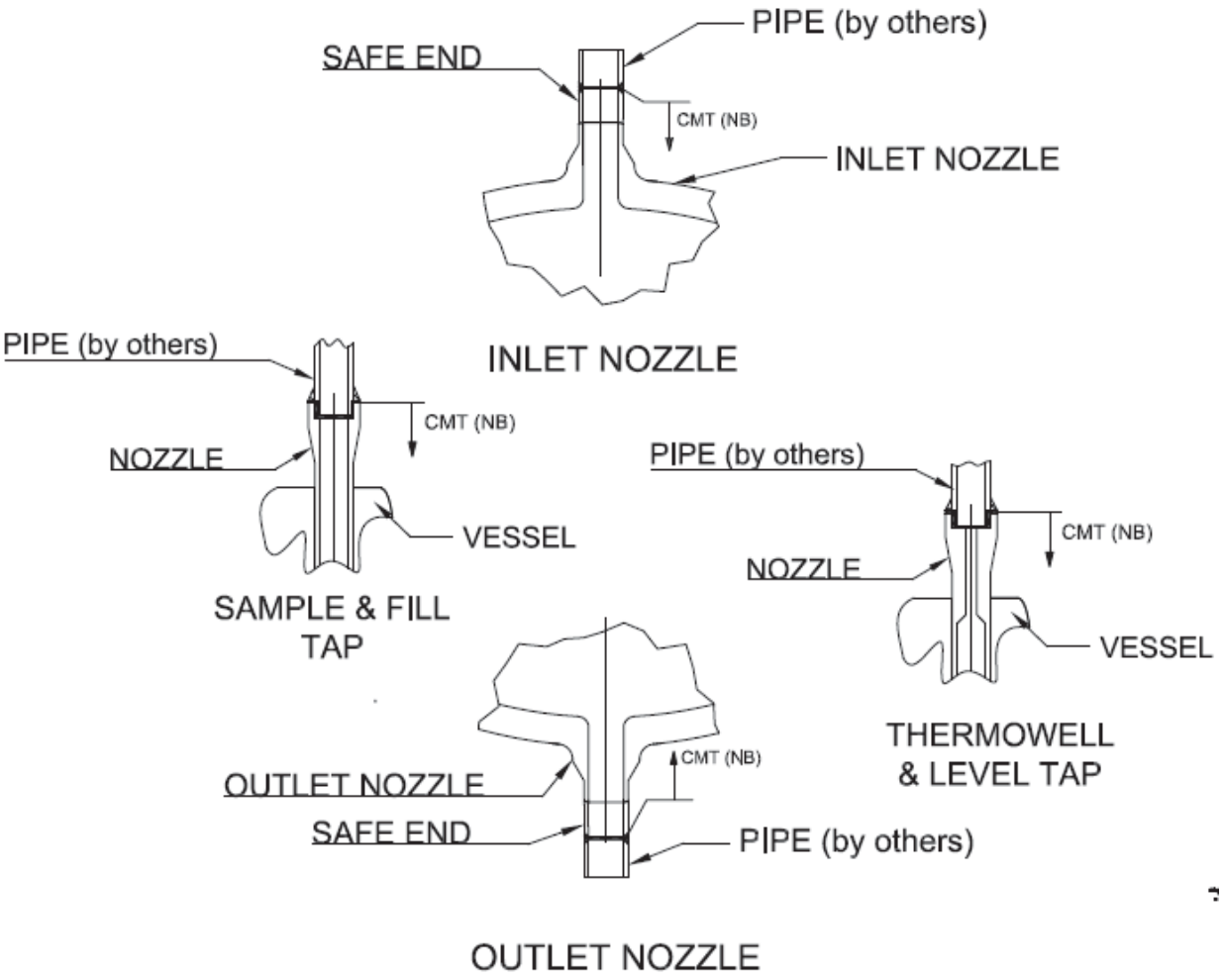


Figure 20H-3. Core Makeup Tank Nozzle Jurisdictional Boundary

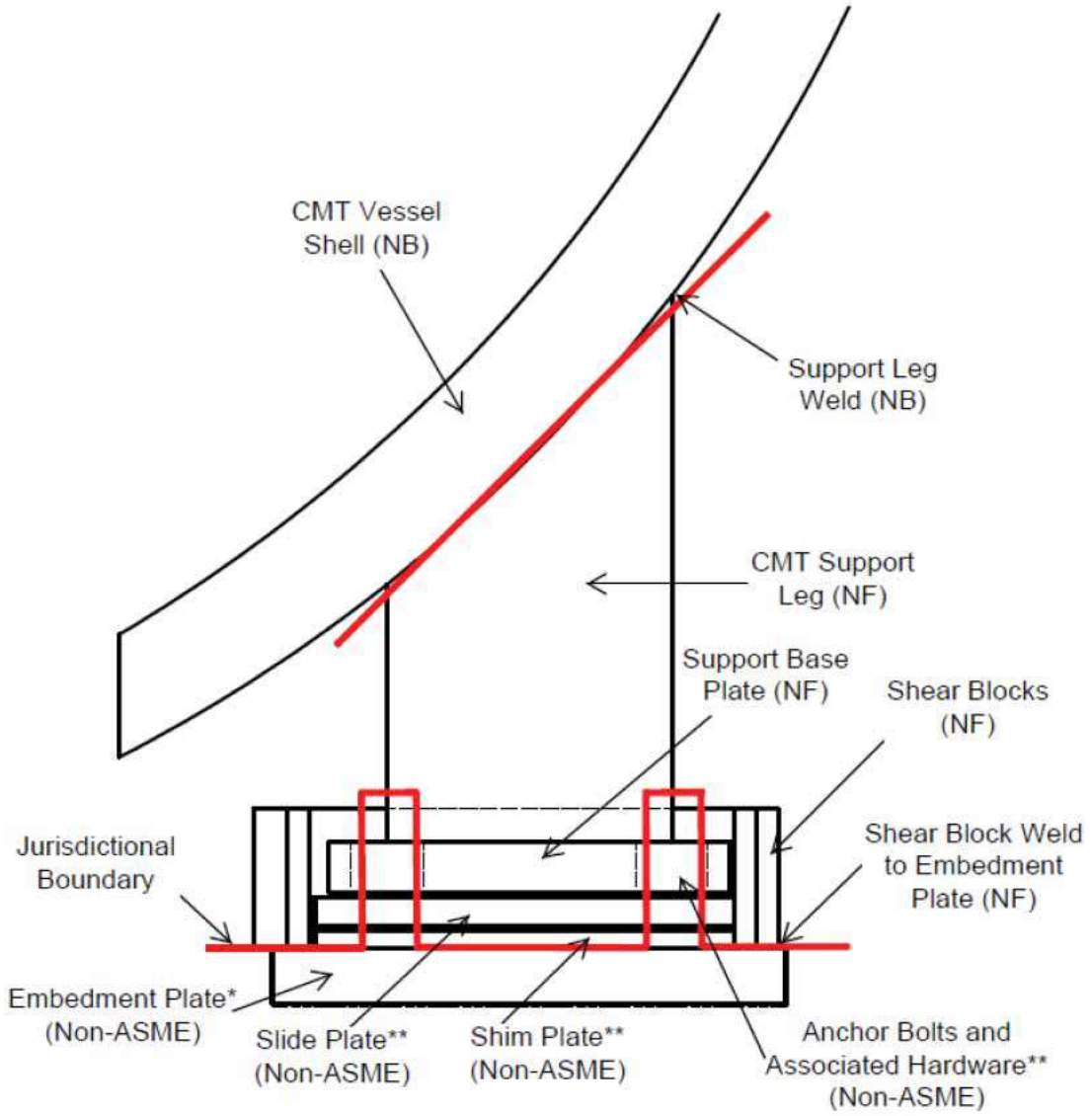


Figure 20H-4. Core Makeup Tank Support Jurisdictional Boundary

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS AND ACRONYMS

ASME	American Society of Mechanical Engineers
CMT	core makeup tank
CSR	Component Safety Report
DVI	direct vessel injection
FMEA	failure modes and effects analysis
GDA	generic design assessment
ISI	in-service inspection
LOCA	loss-of-coolant accident
NDE	nondestructive examination
PXS	passive core cooling system
RCS	reactor coolant system
SFR	safety functional requirement
SSC	system, structure, or component
UK	United Kingdom

APPENDIX 20I
ACCUMULATOR COMPONENT SAFETY REPORT

20I.1 Introduction

This is the component safety report (CSR) for the accumulator as introduced in Section 20.2. The safety argument herein substantiates the structural integrity of the accumulator to a degree of rigour commensurate with the consequences of gross structural failure. The safety argument is supported by a suite of documentation outlined in Section 20I.5 that supports the design, manufacture, installation, and operation of the accumulator.

20I.1.1 Scope

This CSR presents arguments to support the claim that the nuclear and radiological risks potentially arising from gross structural failure of the accumulator are tolerable for the design lifetime objective of 60 years. Conventional hazards to personnel safety are outside the scope of this Appendix 20I.

20I.1.2 Objectives

The safety claims made for the AP1000 plant design establish that AP1000 plant risk remains both tolerable and as low as reasonably practicable (ALARP) for the design lifetime, and are substantiated by satisfying structural integrity safety design bases for all safety-significant AP1000 systems, structures, or components (SSCs). The safety design bases, applied across the operational, process and lifecycle scope of the safety case, embody the technical scope of the safety case: if these can be maintained at all times, the plant will be acceptably safe. Specific safety functional requirements (SFRs) for each particular component are developed from the structural integrity safety design bases, and correspond to the functions that need to be maintained to provide assurance of nuclear and radiological safety. The SFRs applicable to the accumulator are identified in Section 20I.2.1.

The other objectives of this CSR are: i) to support the nuclear safety claims made for the AP1000 accumulator design and ii) to present arguments that support the claim that the structural reliability of the accumulator is commensurate with its consequences of failure. That is, where failure is intolerable, the probability of gross failure should be shown to be so low that such failure can be discounted, or where failure does not lead to intolerable offsite consequences, the target reliability is linked to the consequences in accordance with the methodology described in the AP1000 United Kingdom (UK) Structural Integrity Classification document (Reference 20I.1). This is discussed in Section 20I.2.2.

20I.1.3 Interface with Other Safety Case Documents

The safety argument presented in this report is supported by a dossier of technical specification and design analyses listed in the Technical Index (Section 20I.5). Each is specifically identified in the relevant section of the structured safety argument.

20I.1.4 Accumulator Description

20I.1.4.1 Overview

The accumulators (two), as shown in Figure 20I-1, are components of the passive core cooling system (PXS). They are located inside the containment on the floor just below the core make-up tanks. The basic function of the accumulator is to provide core cooling in the event of a large loss-of-coolant accident (LOCA) by delivering a high flow of borated water to the reactor vessel. The accumulator tanks are pressurised with nitrogen gas maintained at approximately 700 psig (4.826 MPa gauge). When the reactor coolant system (RCS) pressure falls below the accumulator pressure, check valves open and borated water is forced into the RCS by the gas pressure.

20I.1.4.2 Description

Details of the accumulator design can be found in the design specification (Reference 20I.2). The two accumulators are spherical tanks (approximately 4.9 m (16 ft) outside diameter) made of low alloy steel and clad on the internal surfaces with stainless steel. They are located inside the containment on the floor just below the core makeup tanks (CMTs). The accumulator is constructed from a top and bottom head welded to an intermediate shell section. The accumulator tank is designed with a skirt type support having a flanged interface for bolting the accumulator tank to the building structure. The accumulators are AP1000 Equipment Class C and are designed to meet seismic Category I requirements. Claims, arguments and evidence related to the designation of the accumulators as AP1000 plant Class C equipment are presented in Reference 20I.3. Therein, it is concluded that due to the similar construction requirements, the costs of volumetric inspection, and the fact that increased inspections would have no significant benefit on the reliability of the accumulator sub-system to function, it is ALARP to retain the accumulator AP1000 plant Class C classification as is because the cost on increasing the safety classification to AP1000 plant Class B is grossly disproportionate to the safety benefit.

The pressure retaining parts of the accumulator tank are qualified to American Society of Mechanical Engineers (ASME) Boiler and Pressure Vessel Code (Code), 1998 Edition with Addenda up through and including 2000, Section III for Class 3 components. The skirt support is qualified per the criteria of Subsection NF of the ASME code.

20I.1.4.2.1 Materials

Materials used in the manufacture of the accumulator pressure boundaries are shown in Table 20I-1. All surfaces that can become wetted during operation will be clad with stainless steel weld overlay. The nominal cladding thickness is 5.6 mm (0.22 in). The cobalt content of materials used in the construction of component surfaces which will be in contact with the primary coolant with the exception of the screws, bolts, washers, weld cladding and locking cups, are designed to be no greater than 0.05 weight percent, integrated average. The cobalt content of cladding materials are designed to be no greater than 0.05 weight percent. The cobalt content of all other welding materials is excluded from this requirement. The sulphur content of the base material and all welding materials are also controlled to prevent hot cracking.

20I.1.4.2.2 Design Temperature and Pressure

The structural design of the accumulator tank is based on the maximum steady state internal design pressure and design temperature values of 5.516 MPa gauge (800 psig) and 149°C (300°F), respectively. These values are used in conjunction with the appropriate values of

external pressure and temperature defined in Reference 20I.2. The temperature of the borated water in the accumulator is approximately equal to the containment temperature since the tanks are neither insulated nor heated. Over pressure protection is provided through an alarm and one safety relief valve. The relief valve is located outside of the accumulator tank jurisdictional boundary so that overpressure protection requirements are fully complied with and the safety relieving devices cannot be isolated from the accumulator tank during operation.

20I.1.4.2.3 Total Volume/Flowrate

The accumulators are designed to deliver a high flow of borated water to the reactor vessel in the event of a LOCA. This large flow rate is used to quickly establish core cooling following a large loss of reactor coolant system inventory.

Each accumulator tank has a minimum volume of approximately 56.6 m^3 (2,000 ft^3). The total wetted volume is approximately 48.1 m^3 (1,700 ft^3). The accumulator provides injection after the reactor coolant system pressure drops below the static accumulator pressure.

The injection line from each accumulator contains a flow-tuning orifice that provides a mechanism for the field adjustment of the injection line resistance. The orifice is used to establish the required flow rates assumed in the accumulator design.

20I.1.4.2.4 Manway

The accumulator tank has an access manway (457 mm (18 inch) nominal minimum diameter) in the shell of the tank to permit access for inspection and maintenance. The manway cover bolting is designed to facilitate the use of remotely operated stud tensioning and de-tensioning devices. The manway gasketed closure is leak tight without requirement for seal welding of the joint perimeter. The manway cover includes a lifting eye(s) to facilitate installation and removal.

20I.1.4.2.5 Nozzles

The mechanical characteristics of the accumulator tank nozzles are shown in Table 20I-2. All nozzles terminate in stainless steel material for compatibility with interfacing piping material. All nozzles are welded in accordance with Section III Subsection ND of the ASME Boiler and Pressure Vessel Code, of the 1998 Edition with Addenda up through and including 2000 and applicable Code Cases. The DN 25 (NPS 1) nozzles are welded to the weld build up on the cladding on the inside wall of the vessel.

20I.1.4.2.6 Lifting Lugs

The lifting lugs are designed in accordance with the criteria specified in ANSI N14.6-1993 (Reference 20I.4). The lifting lugs are capable of holding three times the weight of the accumulator tank including the shipping container without exceeding a combined tensile and shear stress equal to the yield strength of the lifting lug material, and will be designed to be capable of lifting five times that weight without exceeding the ultimate strength.

20I.1.4.2.7 Chemistry

The chemistry composition for the reactor coolant inside the RCS will be controlled in accordance with the well established Electric Power Research Institute guidelines for primary chemistry (Reference 20I.5) shown in Table 20A-3. The accumulator tank water may contain dissolved oxygen at a concentration equal to saturation at atmospheric pressure. Connections

are provided for remotely adjusting the level and boron concentration of the borated water in each accumulator during normal plant operation. Samples from the accumulator will be taken periodically to check the boron concentration.

20I.1.4.2.8 Pressurisation

Accumulator pressure is maintained by a supply of nitrogen gas that can be adjusted as required during normal plant operation. However, the accumulators are normally isolated from the nitrogen supply system. Gas relief valves on the accumulator protect them from over pressurisation. The accumulator can also be remotely vented if required. The liquid level and gas pressure are monitored by indicators and alarms. Accumulator water level may be adjusted either by draining or by pumping borated water from the chemical and volume control system to the accumulator. The operator can take action, as required, to meet the technical specification requirements for accumulator operability.

20I.1.5 Accumulator Function

The basic function of the accumulator is to provide safety injection to the RCS to ensure adequate core cooling during a LOCA. Full details of the functional requirements are given in the AP1000 Accumulator Functional Specification (Reference 20I.6).

The two accumulators contain borated water and a compressed nitrogen cover gas to provide rapid injection at a high flow rate in the event of a large LOCA. This high flow rate is used to quickly establish core cooling following a large LOCA. The accumulators discharge to their respective reactor vessel direct vessel injection (DVI) lines. A deflector in the reactor vessel downcomer annulus directs the flow downward to minimise core bypass flow.

During normal operation, the accumulator is isolated from the reactor coolant system by two check valves in series. When the reactor coolant system pressure falls below 700 psig, the check valves open and borated water is forced into the RCS by the gas pressure. Mechanical operation of the check valves is the only action required to open the injection path from the accumulators to the core.

The accumulator size, water volume, and nitrogen cover pressure are selected so that both of the accumulators are sufficient to recover the core cooling before significant clad melting or zirconium water reaction can occur following a large break LOCA. One accumulator is adequate during a small break LOCA where the entire contents of one accumulator can possibly be lost via the pipe break.

During large LOCAs or automatic depressurisation system operation, the accumulators rapidly inject a large volume of borated water into the reactor vessel through the same connections used by the CMT and the in-containment refuelling water storage tank injection. The accumulator injection rate is dependent on the RCS pressure transient. The accumulator injection provides for rapid re-flooding of the core during a large LOCA, which prevents excessive core fuel cladding temperatures.

The accumulators also help provide adequate core cooling during smaller LOCA events and automatic RCS depressurisation events. During small LOCAs as large as a DVI line break, the accumulators assist in keeping the core covered.

20I.1.6 Accumulator Boundaries

The physical boundaries for safety case assessment of the accumulator, are defined in Reference 20I.2, and identified below.

The equipment boundary of ASME Code jurisdiction includes all components in Figure 20I-2 and Figure 20I-3. The welds at the safe end/piping interface or the nozzle/piping interface are considered as part of the connecting piping systems. These figures show the end of the nozzle or safe end as the equipment boundary and the boundary for support.

The manway cover and attachment hardware and support skirt are included within the equipment boundary. The accumulator shell, upper and lower heads, nozzles, manway cover and bolting are designed to ASME Code, Section III, subsection ND. The accumulator vessel supports are designed to ASME Code, Section III, subsection NF.

The accumulator interfaces with other components through the following nozzles, openings, and supports:

- Flanged Support Skirt
- One (1) Outlet Nozzle
- One (1) Safety Relief Nozzle
- One (1) Nitrogen Inlet Connection
- Two (2) Pressure Taps
- One (1) PXS Test Header Connection
- One (1) Sample Tap
- Two (2) Level Measurement Nozzles

20I.2 Safety Case Requirements

The main focus of this CSR is to provide a structured safety argument, supported by suitable and sufficient evidence, to substantiate the reliability of the accumulator, commensurate with the classification of the accumulator as Standard Class 1, as outlined in Section 20I.2.2 of the report. To achieve this, the safety argument is presented as three key elements, as follows:

Claim 1: Quality of Build: High quality is achieved through good design and manufacture.

Objective: Provides evidence of good design and manufacture based on established design and manufacturing processes and use of proven materials. It provides a keystone for a demonstration of high reliability and embodies the code and plant operating experience with an objective of achieving quality of build and the avoidance of defects. (Section 20I.3.1)

Claim 2: Good Design: Good design is achieved through compliance with ASME.

Objective: Incorporates the build experience as embodied in the design codes. (Section 20I.3.2)

Claim 3: Mitigation and Management of In-service Degradation: Components are tolerant to through-life degradation over the design life of the plant.

Objective: Provides an assessment of through-life degradation mechanisms and shows that such mechanisms will not threaten integrity over a specific interval. (Section 20I.3.3)

The three elements of the safety argument are provided in Section 20I.3 and the strength of the argument is discussed in Section 20I.4.

20I.2.1 Safety Functional Requirements (SFR)

The structural integrity safety design bases for AP1000 SSCs are requirements of plant systems, some duty, some accident response, which must be maintained at all times to provide assurance of plant nuclear and radiological safety. Identification of the SFRs for the accumulator follow from the performance and safety design bases as follows:

- Deliver a large volume of borated water to the reactor vessel at a high flow rate in the event of the large LOCA.

- Provide adequate core cooling during smaller LOCA events and automatic RCS depressurisation events.

- During small LOCAs as large as a DVI LOCA, the accumulators assist in keeping the core covered with water.

Based on these, the following SFRs have been identified which reflect the overall role of the accumulator in plant safety:

- **SFR 20.8.1** The accumulator tanks pressure boundary must remain intact during standby, normal operation and under design basis faulted conditions for the design life of the plant.

- **SFR 20.8.2** The accumulator tanks are required to store borated water and a compressed nitrogen cover gas to provide rapid injection of borated makeup water to the RCS in the event of a large LOCA.

- **SFR 20.8.3** The accumulator tanks are required to deliver a large volume of borated water to the reactor vessel at a high flow rate in the event of a large LOCA in accordance with the component performance requirements.

Postulated failure modes which result in a loss of these functional requirements lead to identification of structural reliability targets commensurate with the consequences of gross failure, as determined through the process of component classification as described in Section 20I.2.2.

20I.2.2 Accumulator Structural Integrity Classification

For the UK AP1000 plant, the structural integrity classification methodology (Reference 20I.1), has been applied with the aim of determining the required level of structural reliability for each of the major plant components based on an evaluation of the direct consequences (e.g., LOCA) and indirect consequences (e.g., missiles/blast etc) of gross failure. The details of the classification for the accumulators are presented in Reference 20I.1.

The direct consequences of gross failure of the accumulator would not lead directly to unacceptable consequences. The normally closed check valves on the injection line would prevent a LOCA in the event the accumulator pressure boundary fails. If these valves did not remain shut, the resulting LOCA would be bounded by a single DVI line failure, which has been analysed within the design basis in section 9.6.5 and can be mitigated by a single accumulator. Assessment of the indirect consequences included consideration of the effects of missiles/jet/blast from disruptive failure of the accumulator tank shell. A review of the 3D model for the accumulator concludes that the risk of consequential damage is small as the accumulators are situated within protected compartments which would contain the energy arising from a disruptive failure of the shell and so is unlikely to lead to the generation of missiles that could challenge the integrity of essential systems or containment. This review considered the proximity of essential safety systems within line of sight of the accumulators. On this basis the accumulator has been categorised as a Standard Class 1 component.

20I.3 Safety Case Arguments

As discussed in Section 20I.2.2, the accumulator has been classified as a Class 1 component in accordance with Reference 20I.1. The structural integrity claim is therefore based on arguments which substantiate the claims listed in Section 20I.2. Consistency with the appropriate ASME III Code class provides the basic demonstration of fitness-for-purpose for the accumulator.

Compliance with ASME III rules for a UK Class 1 component provides the primary element in the safety case for the AP1000 accumulator tank.

20I.3.1 High Quality is Achieved through Good Design and Manufacture

In order to demonstrate that high quality is achieved through good design and manufacture, evidence to support the following claims is provided:

- The fabrication specification complies with AMSE Code requirements for Class 3 components.

- Supplementary requirements are specified to avoid defects and to ensure quality.

The reliability of the accumulator is dependent upon the achievement of good design and manufacture. The design intent is translated into a manufacturing route controlled by a Quality Assurance Programme that complies with rigorous design codes including the ASME Boiler and Vessel Pressure Code. Section 2.3 of the Accumulator Design Specification (Reference 20I.2) provides a list of the industry codes, specifications and standards applied to the component. Reference 20I.8 details supplemental fabrication and inspection requirements.

The justification of the quality of build of the accumulator and of materials is based on the following:

- **Processes Used for Manufacturing and Fabrication** – Design and fabrication of the accumulator is carried out in accordance with ASME Code, Section III, 1998 Edition with Addenda up through and including 2000 and applicable code cases as discussed in the Design Specification (Reference 20I.2).

- **Material Specifications** – The accumulator materials specifications and testing requirements have been specified in accordance with the requirements of Section II of the ASME Code as defined in the Design Specification (Reference 20I.2). Material specifications also include relevant Westinghouse Standards, ANSI/ASME/ASTM standards, US Code of Federal Regulations and US NRC Regulatory Guides as defined in Reference 20I.2. The primary coolant boundary will be fabricated from plate and/or forging material as allowed by ASME Code. Charpy V-Notch impact testing will be carried out as required by ASME Code. The stainless steel safe ends are sized to be of sufficient length to prevent damage to the transition weld during field welding. Nozzles will be buttered prior to final post weld heat treatment (PWHT). After final PWHT, the stainless steel safe end will be welded to the buttered outlet nozzle.

- **Material Test Reports** – Materials for parts within the jurisdiction of the ASME Code will have certified material test reports clearly presenting the results of all ASME Code required testing. All other materials will be designed to be certified as required by the applicable material specifications, but as a minimum by a certificate of compliance.

- **Mechanical Testing** – A hydrostatic test in accordance with ASME Code Section III Class 3 requirements will be carried out. This will be performed at a test pressure of approximately 6.9 MPa (1000 psi) and at a test temperature to be safe from brittle fracture.

- **In-Manufacture Nondestructive Examination (NDE)** – The NDE of the accumulator and its appurtenances is conducted in accordance with ASME Code, Section III (NC-2500 and NC-5000) requirements using ultrasonic examination, liquid penetrant examination, magnetic particle examination, surface examination and weld examination. These provide confidence that the required weld quality is achieved during manufacture. All clad surfaces, including nozzle and manway will be 100% ultrasonically inspected for both bond and defects by the straight beam method. Clad thickness will be measured in accordance with approved procedures. Only personnel qualified and certified in accordance with ASME Section III will perform Section III examinations.

- **Pre-Service and In-Service Examination Requirements** – The pre-service and in-service examination of the accumulator tank will comply with the ASME Code Section XI, Subsection IWD and IWF. The acceptance criteria are also per the ASME Code. Inspection personnel qualified and certified in accordance with the requirements of ASME Code, Section XI will perform the pre-service examination.

- **Weld Qualifications** – All pressure boundary welding procedures and welders' qualifications will be in accordance with the ASME Code, Section III and Section IX. All non-pressure boundary welding procedures and welders' qualifications will be in accordance with the ASME Code, Section IX or equivalent approved standards.

Together these provide a keystone for a demonstration that the accumulator will be of a high quality, that it will enter service free from structurally significant defects and that the effects of through-life degradation on material properties will not have a deleterious effect on the structural reliability of the vessel.

20I.3.2 Good Design is Achieved through Compliance with ASME

In order to demonstrate that good design is achieved through compliance with ASME, the accumulator design has been analysed and shown to comply with the requirements of ASME

Code, Section III for Class 3 components. The assessment is reported in a suite of calculation notes, as summarised in the ASME generic design report (Reference 20I.9) for the accumulator. The design transients used in the analysis are shown in the design report. The load cases considered include normal, upset, emergency and faulted conditions.

The external loads on the accumulator are specified in the Design Specification document (Reference 20I.2); these include nozzle external loads, seismic loads, and all loads and loading combinations. In addition, Reference 20I.10 provides a dynamic assessment to evaluate the response of the accumulator assembly to sloshing effects. The accumulator has therefore been designed against all design basis internal and external hazards.

The pressure boundary components of the accumulator have been shown to comply with the minimum required thickness compared to minimum drawing thickness in Reference 20I.9 as required by the ASME Code. The thickness requirements for all boundary components are satisfied.

Reference 20I.10 provides a detailed stress evaluation of the accumulator including all loads and loading combinations specified in Reference 20I.2 in accordance with the ASME Code Section III Sections ND and NF. This evaluation includes:

- A basic sizing and justification of the main parts and components of the accumulator.
- A dynamic seismic analysis by the response spectrum method.
- Evaluation of stresses from internal pressure, earthquake effects, dead weight and externally applied loads at significant locations of the spherical wall and skirt.

The thermal and structural analysis has been undertaken using established procedures to demonstrate that for the load cases analysed all the stresses and cumulative fatigue usage factors are satisfactory and meet the appropriate limits set forth in the ASME Code. Details of these calculations are presented in the ASME Design Report (Reference 20I.9), with the referenced calculation notes as detailed in the technical index.

Based on the results of the assessments presented in References 20I.9 and 20I.10, it can be shown that the design of the accumulator meets all the requirements of ASME Boiler and Vessel Code Section III Sections ND and NF.

20I.3.3 Mitigation and Management of In-Service Degradation

In order to demonstrate that the design has taken account of in-service degradation mechanisms, evidence to substantiate the following argument is provided:

- A structured process has been applied to identify in-service degradation mechanisms.
- The design has been optimised to mitigate against the risk from in-service degradation mechanisms.

20I.3.3.1 Identification of Degradation Mechanisms

Reference 20I.11 provides a failure modes and effects analysis (FMEA) which was carried out in order to identify design characteristics, potential hardware failures or human errors associated with the design and operation of the accumulator that could lead to a potentially hazardous condition such as injury, fatality, or loss of equipment and product. Potential through-life degradation mechanisms considered in the FMEA include the following:

- Brittle Fracture
- Fatigue
- Corrosion
- Failure arising from manufacturing defect

The basis of the safety case argument is that mitigation against corrosion, fatigue and manufacturing defects is essentially provided by compliance with ASME material specification, design and fabrication rules. The associated in-service inspection (ISI) requirements for ASME Class 3 components and the operating experience embodied within the code to mitigate against these degradation mechanisms.

20I.3.3.2 In-Service Inspection (ISI)

The ISI provides forewarning of failure and a means of monitoring degradation and this forms an important element of the safety case argument. ISI of the accumulator tank will comply with the 1998 Edition with Addenda up through and including 2000 of the ASME Code, Section XI, Subsection IWD.

Written instructions concerning accumulator tank inspection, maintenance, installation, operation, assembly details and disassembly details will be provided following the generic design assessment (GDA). From this information inspection of the accumulator will be carried out in accordance with an inspection plan and Refuelling and Maintenance Outage Schedules.

20I.4 Strength of the Safety Case

The accumulator is classified as a Standard Class 1 component. The safety argument in Section 20I.3 demonstrates how accumulator structural integrity is established, based on extensive quality assurance measures in design, manufacture, materials, testing and qualified inspection. The strength of the safety case is based on achievement of integrity and that the accumulator has been deterministically justified in accordance with ASME Boiler and Pressure Vessel Code Section III. In combination these elements provide a cogent argument to substantiate reliability commensurate with the classification of the accumulator.

To substantiate this assertion this report provides a structured argument based on three key elements, namely Quality of Build, Good Design and mitigation and management of in-service degradation. Quality of build and good design is based on compliance with ASME Code Section III.

Quality of Build has been demonstrated by compliance with ASME Code Section III. Material specification control has been achieved in accordance with Section II of ASME code and NDE in accordance with ASME Code, Section III.

Good design has been demonstrated by providing evidence that design transients including normal, upset, emergency and faulted conditions are within ASME Code Section III, Div 1 – 1998 Edition with Addenda up through and including 2000 limits.

Mitigation and management of in-service degradation has been demonstrated by identifying all design characteristics, degradation mechanisms and potential hazards that could lead failure of the accumulator. The ISI will also provide forewarning of degradation with an inspection plan and Refuelling and Maintenance Outage Schedules.

20I.5 Index of Technical Reports

Table 20I-4 provides a list of all technical references supporting the safety case and the function of each document within the safety case.

20I.6 Review of Open Issues

There are no open issues for the accumulator that affect the basis of the safety case arguments presented in support of the GDA Step 4.

20I.7 Conclusions

This report presents arguments that support the claim that the structural reliability of the accumulator is commensurate with the consequences of failure. To evaluate this, the accumulator has been classified in accordance with the procedure for structural integrity classification specified in Reference 20I.1. Based on this the accumulator has been evaluated as a Class 1 component.

The accumulator has been designed in accordance with the high standards of the ASME Code as applicable to ASME Class 1 components. This includes tight controls on material properties, manufacturing processes, design, testing, inspection and installation such that there is a high level of confidence in the quality of the accumulator and that it will enter service free from significant flaws that could affect the integrity of the component over its lifetime. Secondly that an FMEA has been carried out to identify potential threats to integrity through life and appropriate measures have been incorporated into the design and inspection requirements to mitigate against these threats. Taken together with the referenced evidence, these claims and arguments support the structural reliability claim for the accumulator tanks.

20I.8 References

20I.1 Westinghouse Report UKP-GW-GLR-004, Rev. 3, "UK AP1000 Structural Integrity Classification," January 2017.

20I.2 Westinghouse Report APP-MT02-Z0-101, Rev. 9, "Design Specification for AP1000 Accumulator Tank for PXS," December 2016.

20I.3 Westinghouse Report UKP-GW-GL-106, Rev. 1, "AP1000® Plant Safety Class B and C and Accumulator Design ALARP Assessment," March 2016.

20I.4 ANSI N14.6, "Special Lifting Devices for Shipping Containers Weighing 10,000 Pounds (4500 kg) or More," American National Standards Institute, 1993.

20I.5 "Pressurized Water Reactor Primary Water Chemistry Guidelines," Vols. 1 and 2, Electric Power Research Institute, Palo Alto, CA: Rev. 6., 2007, EPRI Document Number 1014986.

20I.6 Westinghouse Report APP-MT02-Z0-001, Rev. 4, "AP1000 Accumulator Tank Functional Specification," October 2009.

20I.7 Not Used.

20I.8 Westinghouse Report APP-GW-VLR-010, Rev. 2, "AP1000 Supplemental Fabrication and Inspection Requirements," January 2016.

20I.9 Westinghouse Report APP-MT02-Z0R-101, Rev. 7, "AP1000 Accumulator Tank Generic Design Report," December 2016.

20I.10 Westinghouse Report APP-MT02-Z0R-001, Rev. 7, "Detailed Analysis of AP1000 Accumulator Tank," January 2015.

20I.11 Westinghouse Report APP-MT02-GRA-001, Rev. 0, "AP1000 Accumulator Tank Failure Modes and Effects Analysis," September 2009.

Table 20I-1. Accumulator Pressure Boundary Materials

Component	Material
Upper, Lower Heads	SA-533 or SA-508
Intermediate Shell, Shell Petal	SA-533 or SA-508
Outlet Nozzle	SA-508
Outlet Nozzle Safe End	SA-336
Lifting Lugs	SA-516
Cladding	Stainless steel
Manway Cover	SA-533
Manway Insert Plate	SA-240
Manway Closure Stud	SA-193
Manway Closure Nuts, Heavy Hex Nut, Spherical Washer	SA-194
Manway Washer Set	SA-194
Manway Pad Forging	SA-508
Manway Insert Plate Screw	SA-479
Pressure Tap, Safety Relief, Connection, Level Measurement Nozzle, PXS Test Header Connection, Sample Tap	SA-182
Support Skirt	SA-516
Base Plate	SA-516

Table 20I-2. Accumulator Tank Nozzle Mechanical Characteristics

Description	Number	Size	Nozzle Material	Location/Field Interface Condition
Outlet	1	DN 200 (NPS 8)	SA-508	Bottom Head/BE
Sample Tap	1	DN 25 (NPS 1) 3000# Half Coupling	SA-182	Bottom Head/SW
PXS Test Header	1	DN 25 (NPS 1) 3000# Half Coupling	SA-182	Intermediate Shell/SW
Nitrogen Inlet	1	DN 25 (NPS 1) 3000# Half Coupling	SA-182	Upper Head/SW
Level Measurement	2	DN 80 (NPS 3) 300# Flange	SA-182	Upper Head RF
Pressure Tap	2	DN 25 (NPS 1) 3000# Half Coupling	SA-182	Upper Head/SW
Safety Relief	1	DN 25 (NPS 1) 3000# Half Coupling	SA-182	Upper Head/SW

Table 20I-3. Not Used

Table 20I-4. Accumulator Technical Index

Document Reference	Title	Description of Role in Safety Case
Report & Specifications		
APP-MT02-Z0-101	AP1000 Accumulator Design Specification	Provides the basis for the design and construction of the Accumulator to conform with the ASME Boiler and Pressure Vessel Code, Section III, "Rules for the Construction of Nuclear Facility Components" 1998 Edition with Addenda up through and including 2000 and applicable Code Cases referred to as ASME Code Section III.
APP-MT02-Z0-001	AP1000 Accumulator Functional Specification	Defines the functional performance and operational requirements for the Accumulator.
APP-MT02-Z0-201	AP1000 Accumulator Fabrication Specification	Specifies requirements for fabrication controls.
APP-MT02-Z0R-101	AP1000 Accumulator Tank Generic Design Report	Contains the detailed analyses required to demonstrate the adequacy of the structural design to sustain and meet the requirements of the ASME Code and the Design Specification.
APP-PXS-M8-002	AP1000 Accumulator Interface Control Document	Interface Control Document, defines the loading on the accumulator from interfacing systems, pipe nozzle loads etc.
APP-GW-VW-002	AP1000 Design for Inspectability Program: ISI Requirements for Class 2 and 3 Components and Core Internals Structures"	Contains requirements relative to ISI for ASME Class 2 and 3 components and Core Internal Structures, specifically focused on the concept of design for inspectability, to ensure adequate design and access provisions for meeting ASME Code, Section XI are considered in the overall plant design.
APP-GW-VLR-010	AP1000 Supplemental Fabrication and Inspection Requirements	Provides details of the AP1000 supplemental fabrication and inspection requirements.

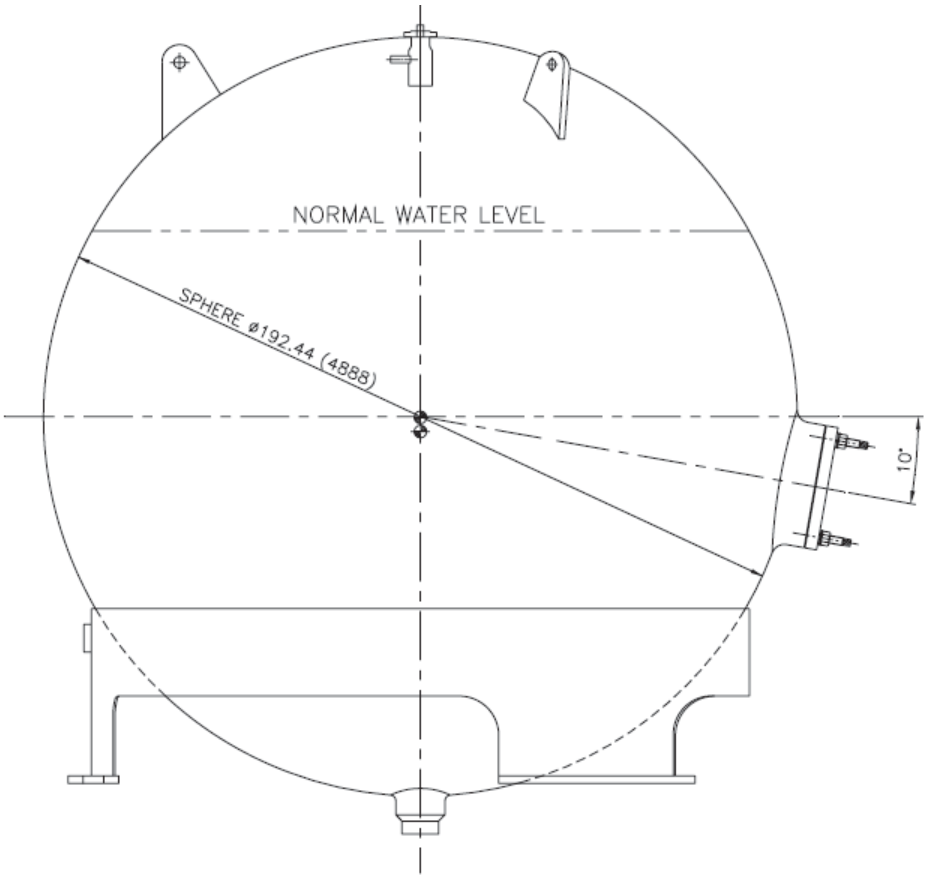


Figure 20I-1. Accumulator[1]

[1] Dimensions are nominal.

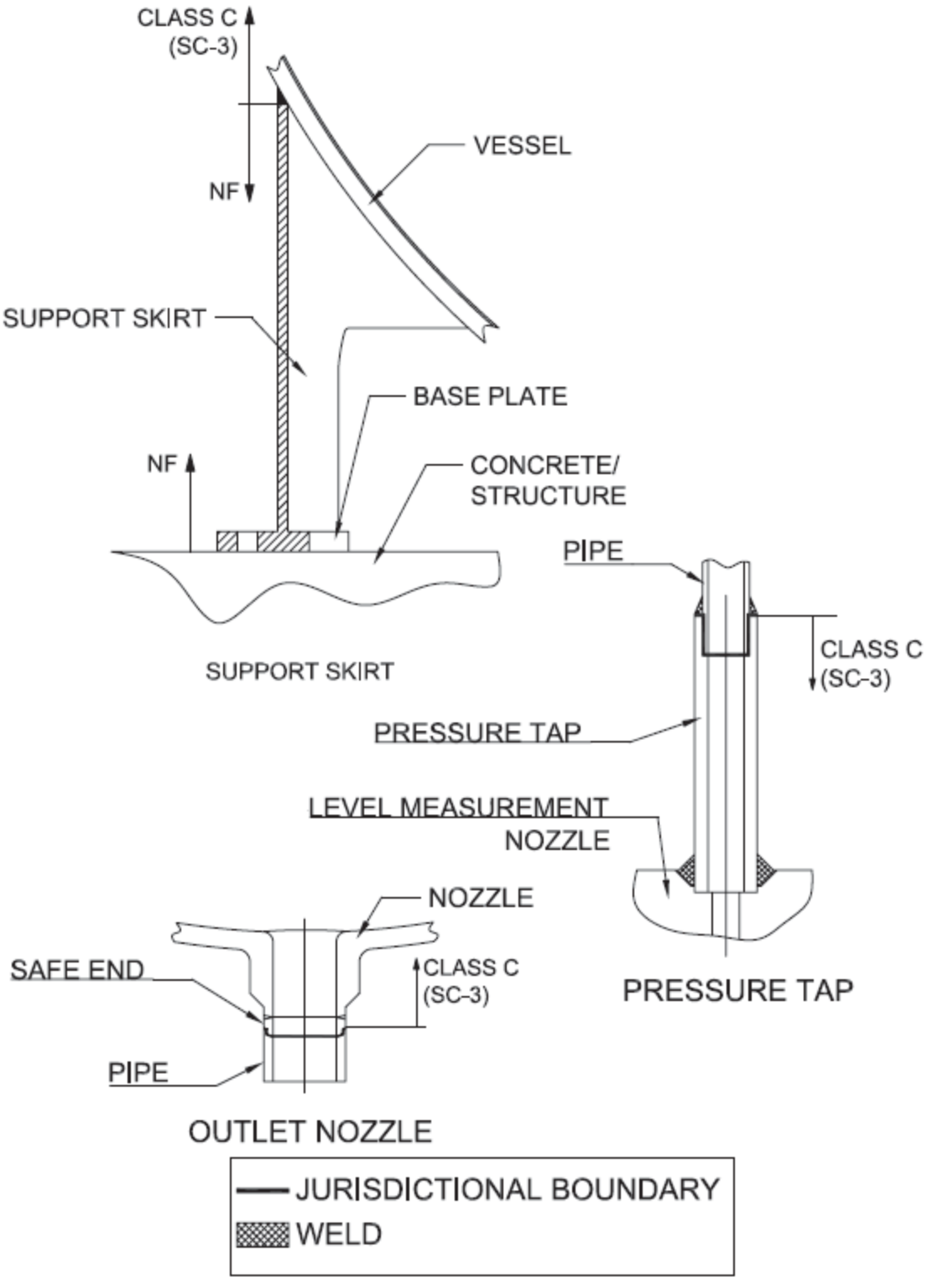


Figure 20I-2. Accumulator Equipment Boundary

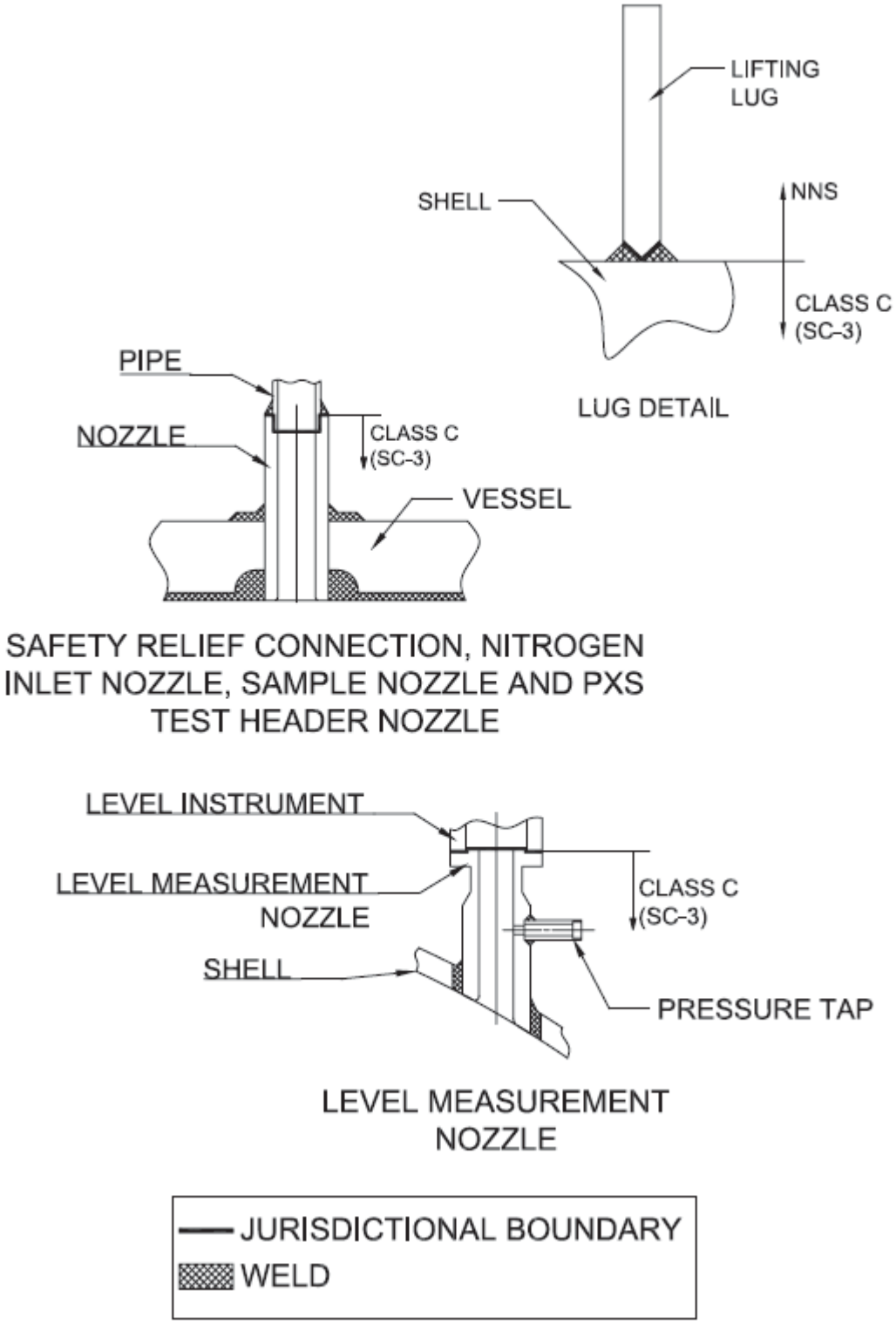


Figure 20I-3. Accumulator Equipment Boundary

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS AND ACRONYMS

ALARP	as low as reasonably practicable
ASME	American Society of Mechanical Engineers
CB	core barrel
CS	core shroud
CSR	Component Safety Report
CSS	core support structure
DVI	direct vessel injection
FIV	flow-induced vibration
FMEA	failure modes and effects analysis
GDA	generic design assessment
HFT	hot functional test
HVAP	head and vessel alignment pin
IASCC	irradiation-assisted stress corrosion cracking
IGA	instrumentation grid assembly
IGSCC	intergranular stress corrosion cracking
IITA	in-core instrument thimble assemblies
IS	internal structure
ISI	in-service inspection
LCSA	lower core support assembly
LCSP	lower core support plate
LOCA	loss-of-coolant accident
NDE	nondestructive examination
NRC	Nuclear Regulatory Commission
NSSS	nuclear steam supply system
PSI	pre-service inspection
PWR	pressurised water reactor
PWSCC	primary water stress corrosion cracking
RCCA	rod cluster control assembly
RCP	reactor coolant pump
RCS	reactor coolant system
RVCH	reactor vessel closure head
RVFS	reactor vessel flow skirt
RVI	reactor vessel internals
RXS	reactor system
SCSS	secondary core support structure
SFR	safety functional requirement
SSC	system, structure, or component
TSF	threaded structural fasteners
UCP	upper core plate
UK	United Kingdom
UNS	Unified Numbering System
USA	upper support assembly
USC	upper support column
UT	ultrasonic testing
VSP	vortex suppression plate

APPENDIX 20J
REACTOR VESSEL INTERNALS COMPONENT SAFETY REPORT

20J.1 Introduction

This is the component safety report (CSR) for the reactor vessel internals (RVI) as introduced in Section 20.2. The safety argument herein substantiates the structural integrity of the RVI (including the reactor vessel flow skirt (RVFS)) to a degree of rigour commensurate with the consequences of gross structural failure. The safety argument is supported by a suite of documentation outlined in Section 20J.5 that supports the design, material selection, manufacture, installation, operation and in-service inspection (ISI) of the RVI and RVFS.

20J.1.1 Scope

This CSR supports the claim that the nuclear and radiological risks potentially arising from gross structural failure of the RVI and RVFS are tolerably low for the design lifetime objective of 60 years. Non-nuclear hazards to personnel safety are outside the scope of this Appendix 20J.

20J.1.2 Objectives

This CSR supports nuclear safety claims that the AP1000 plant risk remains both tolerable and as low as reasonably practicable (ALARP) for the design lifetime. These claims are substantiated by satisfying structural integrity safety design bases for all safety-significant AP1000 systems, structures, or components (SSCs). The safety design bases, applied across the operational, process and lifecycle scope of the safety case, embody the technical scope of the safety case: if these can be maintained at all times, the plant will be acceptably safe. Specific safety functional requirements (SFRs) for each particular component are developed from the structural integrity safety design bases, and correspond to the functions that need to be maintained to provide assurance of nuclear and radiological safety. The SFRs applicable to the RVI and RVFS are identified in Section 20J.2.

The approaches to achieving this objective are 1) to support the nuclear safety claims made for the AP1000 RVI and RVFS design and 2) to present arguments that support the claim that the structural reliability of the component is commensurate with its consequences of failure. That is, where failure is intolerable, the probability of gross failure should be shown to be so low that failure can be discounted, or where failure does not lead to intolerable consequences, the target reliability is linked to the consequences in accordance with the methodology detailed in Reference 20J.1. This is discussed in Section 20J.2.2 below.

20J.1.3 Interface with Other Safety Case Documents

The safety argument presented in this report is supported by a dossier of technical data and analyses. These are listed in the Technical Index (Section 20J.5) and each is specifically identified in the relevant section of the structured safety argument.

20J.1.4 Reactor Vessel Internals and Flow Skirt Description

20J.1.4.1 Overview

The RVI and RVFS, contained entirely within the RV, as shown in Figure 20J-1, are part of the reactor system (RXS). The RVI are classified as either a core support structure (CSS) or an internal structure (IS). The CSS are components which provide direct support or restraint

to the core. The IS are all structures within the reactor pressure vessel other than the CSS, fuel, control assemblies, and instrumentation. The CSS and IS components are listed below.

Core Support Structure

- Upper support assembly (USA)
  - Upper support plate (USP)
  - Upper support flange and upper support skirt
  - Upper support columns (USCs)
  - Upper core plate (UCP) and clevis inserts
  - UCP fuel alignment pins
- Lower core support assembly (LCSA)
  - Core barrel (CB) cylinder
  - CB flange
  - CB outlet nozzles
  - Lower core support plate (LCSP)
  - LCSP fuel alignment pins
  - LCSP radial keys and clevis inserts
  - Alignment plates, bolts, and dowel pins
  - Threaded structural fasteners (TSFs) and pins that provide direct load-carrying capabilities of the CSS

Internal Structure

- Core shroud (CS) and top plate clevis inserts to the CS
- Instrumentation grid assembly (IGA)
- Direct vessel injection (DVI) flow deflector
- Secondary core support structure (SCSS)
- Vortex suppression plate (VSP)
- Irradiation specimen basket
- Neutron shield panels
- Head and vessel alignment pin (HVAP)
- Guide tube flange hold-down bolts
- Miscellaneous items, e.g., head-cooling nozzles, support column nozzles and guides, irradiation access plugs

- TSFs, locking caps, locking bars, pins, etc., that do not provide direct load-carrying capabilities of the CSS
- Internals hold-down spring
- Control rod guide tubes and support pins

In addition to supporting and restraining the core, the RVI provide for the controlled circulation of coolant through the core. Additional control over the coolant flow is achieved by the RVFS at the bottom of the RV, which, although not considered part of the RVI, is covered within this CSR.

20J.1.4.2 Description

The RVI, when assembled in the RV, provide the appropriate guidance, protection, alignment and support for the core and control rods to enable safe and reliable reactor operation. The lower and upper support assemblies are shown in Figure 20J-2 and Figure 20J-3, respectively. The internals are supported by the RV ledge and are restrained against upward movement by the vessel head. The lower end of the internals is restrained against rotational and/or lateral movement by four lower radial support keys that engage clevises attached to the RV.

The other key function of the internals is to control the passage of coolant through the core as well as providing a specified by-pass flow to other regions of the RVI and RV, such as the RV closure head (RVCH) plenum, outer CS and the control rod drive mechanism regions, in order to maintain the appropriate component operating conditions. The RVFS, which provides additional control over coolant flow in the lower RV plenum beneath the lower RVI, is an upright perforated circular cylinder, as detailed in Figure 20J-4. The RVFS is attached by full penetrating welds to eight support blocks on the RV shell.

The RVI and RVFS are both designed for a service life of 60 years.

Materials used in the manufacture of the RVI and RVFS sub components are given in Table 20J-1.

20J.1.5 Reactor Vessel Internals and Flow Skirt Function

20J.1.5.1 Upper Support Assembly

The USA (Figure 20J-3) provides the vertical restraint, lateral restraint, and lateral alignment to the top of the core through its main components: the USA, USCs, the UCP, and the interface with the RV. The assembly also supports the IS, such as the IGA, and supports the reactor control rod guide tubes. The USA, which is supported on its outer edge by the RVCH and the hold-down spring compression, transfers the loading of the upper support assembly to the RV. Keyways are located in the outer edges of the subassembly to align the USA to the RV and lower core support assembly during initial installation of these assemblies at the nuclear plant site and during subsequent refuelling operations. There are penetrations in the subassembly for the spray nozzles that allow limited flow into the RV upper head area. Flow holes are incorporated in the USP to allow for draining the upper head region during depressurisation accidents.

Upper Support Columns

The primary function of USC is to transfer vertical and lateral reaction loads to the USA. These columns are attached to the bottom side of the USA and form the plenum between the USA and the UCP. The USC also serve as guidance and support members for the in-core instrument thimble assemblies (IITAs).

Upper Core Plate

The UCP, which is attached to the bottom of the USC, forms the upper boundary of the core cavity. It transfers core loads to the upper support columns, and when in place within the RV, compresses the fuel assembly springs, creating the core preload. The plate is perforated to allow coolant flow while maintaining an acceptable velocity profile. It contains the upper fuel alignment pins that engage the top of the fuel assemblies. The upper-core periphery to lower core periphery alignment is provided through keyways in the outer edges of the UCP. The keyways contain customised inserts that provide the required alignment plate engagement gaps. In addition, this keyway and insert system limits any torsional rotation or translation of the UCP.

20J.1.5.2 Lower Core Support Assembly

The LCSA (Figure 20J-2) is the major core support assembly. The functions of this assembly are as follows:

- Support the core and the attached IS
- Transfer the loads from the bottom of the core, attached IS, and other design loadings to the RV
- Provide restraint and alignment of the core
- Provide directional and metered control of reactor coolant flow through the core
- Provide sufficient neutron shielding with the CSS and neutron panels for the RV

Each fuel assembly that forms the core is placed within the CS assembly and is rested on the LCSP. The LCSP contains the fuel alignment pins that locate the bottom of the fuel assembly nozzles. The LCSP has perforations to provide relatively equal flow to each assembly and to limit the flow jet velocity entering the fuel assemblies. The LCSA transmits the loading to the RV through the RV ledge and the lower radial supports, and potentially through the outlet nozzles. The LCSP has an access port that allows access to the lower radial supports with the lower RVI installed in the RV, enabling customisation of the lower radial support clevis inserts.

Rotational Support System

The rotational support system consists of keys that are attached to the rim of the LCSP. These keys engage clevis inserts that are bolted to the RV core support blocks. This system restricts the lower end of the CB from rotational and/or translational movement, and provides a load path for LCSP horizontal loadings, while allowing for radial and axial thermal displacements of the CB and LCSP.

Core Barrel Alignment Plate Assemblies

The CB alignment plates ensure alignment of the UCP and CS top support plate is maintained under lateral load conditions. There are four alignment plate assemblies attached to the CB at the same elevation as the UCP and the same angular orientation as the four inlet nozzles. The alignment plates are attached to the CB with dowel pins and hex cap screws. To assist in the radial positioning of the alignment plate relative to the CB, the alignment plate sits in a radial recess machined into the CB to match the radius of the outside surface of the alignment plate.

Core Barrel Outlet Nozzles

The CB outlet nozzles provide the passageway for the reactor coolant from the core to the RV outlet nozzle projection. The radial gap size between the CB outlet nozzles and RV outlet nozzles is controlled to restrict the amount of bypass flow.

20J.1.5.3 **Internal Structures**

Head and Vessel Alignment Pins

The head and vessel alignment pins attach to and extend above and below the flange of the LCSA. The portions of the pins extending below the flange engage pockets in the RV to provide alignment of the LCSA to the RV. The portions of the pins extending above the flange engage the upper support assembly and extend into pockets provided in the RVCH, thereby ensuring alignment of all the assemblies. Minimal clearance is maintained between the pins and the engagement pockets to ensure functional alignment and facilitate assembly.

Reactor Control Rod Guide Tubes

The reactor control rod guide tubes perform the following functions:

- Provide a straight, low-friction path for control rod insertion and withdrawal from the fuel assemblies in the core.
- Provide protection for withdrawn control rods from possible damage due to loads imposed by reactor coolant flow and/or other mechanical/vibratory loading.
- Provide storage for the control rod drive shafts during removal of the upper CSS from the vessel. The guide tubes also perform the function of removing all the uncoupled drive rods from the vessel, when the RVI are removed for refuelling.
- Allow coolant flow exiting the fuel assemblies to pass into the outlet plenum without causing significant loads on the control rods, or maldistributions in the core outlet flow pattern.
- Are removable for repair or replacement (if damaged) without affecting the upper support assembly.

Irradiation Specimen Baskets

The irradiation specimen baskets, which are attached to the outside of the CB, support and restrain the irradiation specimens. There are eight surveillance capsules, excluded from the RVI scope of supply, which will be field-installed. Capsule exposure lead factors relative to the RV are designed to the appropriate range for reactor operation. At specific intervals during the design life of the reactor, a specimen will be removed from the specimen basket and material samples will be tested to determine the current cumulative effects on the RV. The external geometry of the specimen baskets will minimise undesirable flow phenomena in the downcomer annulus, such as flow vortices and flow-induced vibration (FIV).

Secondary Core Support Structure

A SCSS is provided in the plenum area between the bottom of the CB subassembly and the bottom of the RV. (Note that this assembly is an internal structure even though the core support nomenclature is used.) The function of the secondary core support is to perform the following after a postulated failure and downward movement of the CB subassembly:

- Absorb a portion of the energy generated to limit the dynamic force imposed on the RV.
- Transmit the vertical load of the core to the RV.
- Limit the displacement to prevent withdrawal of the control rods from the core.
- Limit the displacement to prevent loss-of-alignment of the core with the UCP, so that the control rods can be inserted into the reactor.

Instrumentation Grid Assembly

The IGA is designed to prevent excessive vibration of the IITA, which contains the fixed in-core flux detectors and core-exit thermocouples. The IGA provides a path from the QuickLoc instrument nozzles through USCs and the USA to the top of the fuel assemblies. The pathway protects and guides the IITAs during initial installation, reactor operation, and withdrawal/insertion during outages.

Lower Plenum Vortex Suppression Plate

The lower plenum vortex suppression plate is positioned in the vessel lower plenum to suppress the formation of any unsteady flow vortices formed in the reactor coolant flow. The vortex suppression plate is supported by columns that are attached to bottom of the LCSP.

Internals Hold-Down Spring

The RVI hold-down spring is a circumferential spring located between the flanges of the upper and lower CSS flanges when they are assembled in the RV. This spring provides a preload to limit axial movement of the upper and lower core support assemblies during reactor operation. The preload of the hold-down spring is provided when the RVCH is properly secured by tensioning of RVCH studs.

Core Shroud

The CS assembly is located inside the CB and above the LCSP. This assembly forms the lateral periphery of the core and through the dimensional control of the cavity, i.e., the gap between the fuel assemblies and the CS, provides directional and controlled flow of the

reactor coolant through the core. The arrangement of the CS provides a transition from the cylinder-like CB to the fuel assemblies. The CS allows cooling water (i.e., bypass) to flow through the cavity between the CB and the CS lateral periphery panels while still providing sufficient material to perform the neutron reflection and radiation shielding functions.

Neutron Shielding

Neutron shielding is provided over the active core elevations on the outside of the CB by the neutron shield panels. This shielding is in the form of strategically located panels. The shielding protects the RV from detrimental radiation effects by limiting total exposure.

Direct Vessel Injection Deflector

The function of the DVI deflector is to prevent cold water from the DVI nozzle from impinging directly on the CB and to direct the water downward.

20J.1.5.4 Reactor Vessel Flow Skirt

The RVFS (Figure 20J-4) aides in the development and maintainability of an acceptable core inlet flow distribution, ensures the RV pressure drop limit is not exceeded and minimises the risk of developing undesirable flow phenomena (e.g., unstable flow vortices in the lower head) considering the full range of expected flow rates.

20J.1.6 Reactor Vessel Internals Boundaries

The physical boundaries for safety case assessment of the RVI and RVFS are shown in Reference 20J.2 and Reference 20J.3, and are identified below:

- The interfaces of the RVI with the RV occur at the internals support ledge, the outlet and DVI nozzle internal projections and the core support blocks for the internals radial support keys.

- The interface of the RVFS with the RV is at the RVFS attachment weld.

- The internals and fuel assembly have interfaces between the UCP and the fuel hold-down springs or core components and fuel alignment pins at the fuel assembly top nozzles and the LCSP at the fuel assemble bottom nozzles and fuel alignment pins at the fuel assembly bottom nozzles.

- The CSS-to-IS boundaries at:

  – USP at the intermediate flange of the lower guide tube flange and hold-down bolts
  – LCSP at the CS bottom plate
  – CB flange and upper support flange at the head and vessel alignment pins
  – CB flange and upper support flange at the RVI hold-down spring
  – CB flange at the upper head flow nozzles
  – LCSP at the secondary core support columns and fasteners
  – UCP at the guide tube support pins
  – IGA Guide studs to USP top surface
  – IGA at the top surface of the USP and inside diameter of the USCs
  – USC instrumentation adapter to USC base
  – CB cylinder at the DVI deflector
  – CB cylinder at the CS ring bands
  – CB alignment plates at the CS top plate

- CB cylinder at neutron shield panels
- CB cylinder at the irradiation specimen baskets
- USP female threads in the flange at Roto-Lock inserts male threads
- CB female threads in the flange at Roto-Lock inserts male threads

20J.2 Safety Case Requirements

The main focus of this CSR is to provide a structured safety argument, supported by suitable and sufficient evidence, to substantiate the structural reliability of the RVI and RVFS commensurate with the structural integrity classification, as outlined in Section 20J.2.2. The RVI have been classified as Standard Class 1 according to the procedure adopted in Reference 20J.1. To substantiate this, the safety argument is presented as three key elements, as follows:

Claim 1: **Quality of Build: High quality is achieved through good design and manufacture.**

Objective: Provides evidence of good design and manufacture based on established design and manufacturing processes and use of proven materials. It provides a keystone for a demonstration of high reliability and embodies the code and plant operating experience with objective of achieving quality of build and the avoidance of defects (Section 20J.3.1).

Claim 2: **Good Design: Good design is achieved through compliance with American Society of Mechanical Engineers (ASME).**

Objective: Incorporates the build experience as embodied in the design codes (Section 20J.3.2).

Claim 3: **Mitigation and Management of In-service Degradation: Components are tolerant to through-life degradation over the design life of the plant.**

Objective: Provides an assessment of through-life degradation mechanisms and show that such mechanisms will not threaten integrity over a specific interval (Section 20J.3.3).

The safety argument is tailored according to the structural reliability claims derived from a process of component classification, with the purpose of demonstrating that component structural reliability is commensurate with the consequences of gross failure.

The three elements of the safety argument are provided in Section 20J.3 and the strength of the argument is discussed in Section 20J.4.

20J.2.1 Safety Functional Requirements

The safety design bases are requirements of plant systems, some duty and some accident response, which must be maintained at all times to provide assurance of plant nuclear and radiological safety. Identification of the SFRs for the RVI and RVFS follow from the performance and safety design bases allocated in Reference 20J.2 and 20J.3, as follows:

- Support, orient, and guide the core components, namely the fuel assemblies and control rod assemblies.
- Direct the main coolant flow to and from the fuel assemblies.

- Absorb control rod dynamic loads, fuel assembly loads, and other loads, and transmit these loads to the RV.
- Support IITA within the RV.
- Convey cooling water to the core for a postulated loss-of-coolant accident (LOCA).
- Provide protection for the RV against excessive irradiation exposure from the core.
- Inhibit undesirable flow phenomena (e.g., FIV, unstable flow vortices in the lower head and flow jetting into the core).
- Not permit the RV pressure drop limit to be exceeded.
- Position and support RV irradiation specimen baskets

Based on these, the following SFRs, identified in Table 20-1, reflect the overall role of the RVI and RVFS in plant safety:

- **SFR 20.10.1** The RVI are required to support, orient and guide the core components, namely the IITA, fuel assemblies and rod cluster control assemblies (RCCAs) during standby, normal operation and under design basis faulted conditions for the design life of the plant.
- **SFR 20.10.2** The RVI and RVFS are required to inhibit undesirable flow phenomena and to direct the main coolant flow to and from the fuel assemblies and convey cooling water to the core for a postulated LOCA. Furthermore, the RVI and RVFS are required to maintain the RV pressure drop within specified limits.
- **SFR 20.10.3** The RVI are required to absorb control rod dynamic loads, fuel assembly loads, and other loads, and transmit these loads to the RV.
- **SFR 20.10.4** The RVI are required to provide protection for the RV against excessive irradiation exposure from the core.
- **SFR 20.10.5** The RVI are required to position and support the RV irradiation specimen baskets.

Postulated failure modes which result in a loss of these functional requirements lead to identification of structural reliability targets commensurate with the consequences of gross failure, as determined through the process of component classification as described in Section 20J.2.2.

20J.2.2 Reactor Vessel Internals Structural Integrity Classification

The structural integrity classification methodology described in Section 20.5 and further in Reference 20J.1 has been applied with the aim of determining the required level of structural reliability for each of the major plant components based on an evaluation of the direct (e.g., reactivity insurgence or disruption of flow) and indirect (loose articles) consequences of gross failure. The details of the classification for the RVI classification are presented in Reference 20J.1.

This concludes that the direct consequences of gross failure of the upper RVI would be the potential for either disruption to internal flow leading to fuel damage or an inability to insert control rods. As the upper RVI are supported by an independent flange to the core barrel and have their supporting structure sandwiched between the (spring loaded) UCP and RVCH, there will be no significant displacement as a result of a failure of an USA circumferential weld. To similar effect, failure of a core barrel circumferential weld will only result in an allowable vertical displacement of the lower RVI and the core on account of the SCSS and radial clevis supports. Consequently, coolant flow and control rod insertion will be retained. Additionally, the safety evaluation described in Chapter 9 demonstrates that even with the highest worth control rod assembly stuck in the fully withdrawn position, the necessary shutdown margin (with combined use of chemical shimming) is maintained during long-term xenon decay and plant cooldown, thus accounting for any local failures of the RCCA guides. On this basis, the RVI have been categorised as Standard Class 1 components.

20J.3 Safety Case Arguments

The RVI have been classified as Standard Class 1 components in accordance with Reference 20J.1 as discussed in Section 20J.2.2. The structural integrity claim is therefore based on arguments which substantiate the classification in Section 20J.2.

Consistency with ASME Boiler & Pressure Vessel (ASME Code), Section III, Subsection NG provides the basic demonstration of fitness-for-purpose for the RVI. Based on this, a satisfactory structural reliability can be claimed on account of the quality requirements, material selection, manufacturing control, stress limits, and inspection requirements associated with compliance to ASME Code, Section III, Subsection NG, as well as accounting for known degradation mechanisms.

Compliance with ASME Code therefore provides the primary element in the safety case for the AP1000 RVI.

20J.3.1 High Quality Is Achieved through Good Design and Manufacture

In order to demonstrate that high quality is achieved through good design and manufacture, evidence to support the following claims is provided:

- The fabrication specification complies with ASME Code, Subsection NG, requirements.
- Supplementary requirements are specified to avoid defects and to ensure quality.

The reliability of the RVI is dependent upon the design quality. The design intent is translated into a manufacturing route which is controlled by a Quality Assurance Programme which complies with rigorous design codes including the ASME Code. The RVI Design Specification (Reference 20J.2) and the RVFS Design Specification (Reference 20J.3) provide lists of the industry codes, specification and standards applied to the components.

The justification of the quality of build of the RVI and of materials used includes:

- All materials comply with the applicable requirements of the design and construction codes and standards including requirements of ASME Code, 1998 Edition with Addenda up through and including 2000 Addenda. The materials used in the AP1000 will be selected from materials proven in-service in pressurised water reactors (PWRs). Proven materials are those with the same nominal composition and subsequent processing steps (e.g., heat treatment, fabrication, and installation) and same exposure conditions (e.g., stress levels, water chemistry environment, temperature, or radiation fluence) as those

used successfully in existing PWRs. Only if it can be demonstrated that they have been proven to be appropriate in similar components subject to equivalent operating environmental conditions and loadings will materials potentially susceptible to degradation mechanisms in PWR environments be permitted. Maximum limits are set on the cobalt level in RVI and waterside components to minimise plant radiation levels.

- A heat treatment, for dimensional stability or relaxation of residual stresses, will be applied to CSSs and IS that undergo bending, welding, or re-straightening. Stabilisation and residual stress heat treatment requirements are specified in Reference 20J.6 and will be noted on the design drawings, as applicable. Locking cups and caps are generally annealed after machining. The annealing process to be performed will be noted on the applicable design drawing.

- Welding procedure specifications for fabrication will comply with the requirements of Section IX, Welding and Brazing Qualifications, and Section III, of the ASME Code. Specific welding requirements include (References 20J.2 and 20J.7):

  – All welders, including tack welders, will be qualified and identified for each weld joint.

  – Welding of stainless steel materials will be in accordance with the United States Nuclear Regulatory Commission (NRC) Regulatory Guide 1.44, “Control of the Use of Sensitized Stainless Steel” (Reference 20J.14).

  – In addition to the delta ferrite requirements, the requirements of US NRC Regulatory Guide 1.31 (Reference 20J.15), will be applied. Ferrite content will be determined on undiluted weld deposits.

- Interpass temperatures will be limited to 350°F (176°C) on assemblies whose constituent parts are joined by welding and to 800°F (426°C) during hardsurfacing of stainless steel and nickel based alloys that contain carbon lower than 0.03 weight percent.

- In general, austenitic stainless steels will be limited to temperature below 800°F (427°C) during the fabrication process, except instantaneously and locally by welding and thermal cutting.

- Each pass will be cleaned by stainless steel wire brushing or other mechanical means. Stainless steel brushes must be new or previously used only on stainless or nickel-based materials.

- In cases of limited accessibility a performance qualification will include testing of the welder in accordance with US NRC Regulatory Guide 1.71, ‘Welder Qualification for Areas of Limited Accessibility’ (Reference 20J.16), the test will simulate the most restrictive production weld for access by a welder and requalification is required for production welds considered more restrictive.

- Fabricators are permitted two attempts at repairing a defect after final inspection. If the repair is not successful after the second attempt the fabricator is required to submit a non-conformance report.

- Tack welds that will be incorporated into the final weld will be deposited with a contour suitable for fusion with the root pass.

- Special welder qualification is required for locking bar welds and will include making several typical locking bar welds in the production position which will be evaluated by visual examination and macro-examination to show complete fusion and free of cracks.

- All fasteners internal to the RV will be designed such that the fastener is positively locked and the head, shank, and threaded portions will be captured should the fastener fail. Moreover, the use of high strength fasteners in the RVI susceptible to intergranular stress corrosion cracking (IGSCC) has been avoided and wherever possible joint crevices will be vented in order to minimise the potential of crevice corrosion effects.

- A special cleaning procedure, as detailed in Reference 20J.8, is required for the RVI due to the complex design of the completed assembly.

- Nondestructive examination (NDE) during manufacture, as a minimum, complies with the requirements of the ASME Code, Section III, Subsection NG.

- Pre-service inspection (PSI) of the RVI is in accordance with ASME Code, Section XI, using the visual inspection method VT-3.

- Qualification of personnel, procedures, and equipment will be in accordance with ASME Code, Section XI.

Together these provide a keystone for a demonstration that the internals are well designed, will enter service free from structurally significant defects and that the effects of through-life degradation on material properties will not have a deleterious effect on their structural reliability.

20J.3.2 **Good Design Is Achieved through Compliance with ASME**

In order to demonstrate that good design is achieved through compliance with ASME, evidence to substantiate the following argument is provided:

- The design has been analysed and has been shown to comply with the requirements of ASME Code, Section III for Class 1 components.

The RVI CSS (Reference 20J.2) and RVFS (Reference 20J.3) design specifications provide the basis for their construction to conform to the rules set forth in the ASME Code, Section III, Subsection NG, 1998 Edition with Addenda up through and including 2000 Addenda. The RVI IS will be constructed to the same requirements as the CSS. Moreover, the IS will be constructed such that they do not adversely affect the integrity of the CSS. Critical RVI design features have been identified and analysed or tested to demonstrate their conformance to code, or otherwise, requirements, including fatigue, are met. The results of these assessments are documented in the design reports for the RVI and RVFS, References 20J.17 and 20J.18, respectively.

The design transients used in the analyses are summarised in Table 20-22. The load cases considered include normal, upset, emergency and faulted conditions.

The various loadings to which the RVI and RVFS are subjected are presented in Reference 20J.2 and Reference 20J.3, respectively. The loads include any loads incurred during transportation, handling and installation, the deadweight, buoyant forces, differential pressure, hydraulic lift and drag forces, flow and reactor coolant pump (RCP) induced vibrations, spring forces, thermal loads (including those due to radiation (gamma) heating),

seismic and LOCA loads. Also, the RVI and RVFS will be capable of satisfying all functional requirements under normal, upset, emergency, faulted, and test operating conditions.

The gap criteria required to ensure the structural integrity and flow requirements (including bypass flow) of the RVI and RVFS are met are detailed in Reference 20J.2 and the functional deflection and displacement limits of the RVI are provided in Reference 20J.2. In addition, the guide tubes are designed beyond the requirements of the ASME Code in order to satisfy the Westinghouse specified control rod drop time. Retention of these dimensional limits is confirmed by analysis demonstrating compliance to ASME Code, Section III, Subsection NG.

The RVI SCSS mitigates the effect of the postulated core drop event. Analysis demonstrates that the SCSS satisfies the following requirements:

- The SCSS limits the load exerted on the RV during the postulated core drop event.
- The distortion of the lower internals is limited. This ensures the ability to insert the control rods and maintain the core in a configuration to be cooled.
- The design of the SCSS is such that, during the postulated core drop event, the contact area between SCSS and the RV precludes yielding of the RV cladding.
- With the exception of a postulated core drop event, the gap between the SCSS and RV is retained sufficient to preclude contact between them for all normal, upset, emergency, faulted, and test operating conditions.
- Fuel assemblies will not disengage the UCP fuel alignment pins during a postulated core drop event.
- The gap between the SCSS and the RV is retained sufficient to preclude contact between the bottom surface of the LCSP and RVFS for normal, upset, emergency, faulted, and test operating conditions, including a postulated core drop event.

The thermal and structural analysis has been undertaken using established procedures to demonstrate that for the load cases analysed all the stresses and cumulative fatigue usage factors are satisfactory and meet the appropriate limits set forth in the ASME Code, Section III, Subsection NG. Details of these calculations are presented in the calculation notes as detailed in the technical index (Section 20J.5).

Pre-operational tests at elevated pressure and temperature are referred to as hot functional tests. The hot functional tests (HFT) are part of a comprehensive reliability test of the RVI designed to meet the guidance of U.S. NRC Regulatory Guide 1.20 (Reference 20J.13) and are part of the pre-operational testing. Transient loadings and operating conditions for HFT and pre-operational testing are accounted for in the design transients identified in Table 20-22. The duration of the HFT is defined such that each critical component will have been subjected to at least 10^6 cycles of vibration prior to final inspection of the RVI. The steady-state portion of the HFT will be performed at the no-load temperature and at a flow rate maintained between the thermal design flow and maximum design flow rates. The core may not be present during HFT.

An internals vibration measurement programme is to be conducted during the HFT on the first AP1000 plant. During HFT, the AP1000 internals are subjected to operational system

flow conditions that are similar to those imposed on previous 3XL three-loop designs. Data are calculated over the ranges of HFT temperatures and during startup, shutdown, and steady-state operation of various combinations of RCPs. The duration of the hot functional flow testing will be the same as that for the previous design. Pre- and post-test inspections will be conducted to confirm that the AP1000 internals experience no excessive motion or wear. The test results will be evaluated in terms of comparison to existing plants of similar RVI design as well as to provide confirmation of the analytical models.

20J.3.3 Mitigation and Management of In-Service Degradation

In order to demonstrate that the design has taken account of in-service degradation mechanisms, evidence to substantiate the following arguments is provided:

- A structured process has been applied to identify in-service degradation mechanisms.
- The design has been optimised to mitigate against the risk from in-service degradation mechanisms.

20J.3.3.1 Identification of Degradation Mechanisms

References 20J.2, 20J.3, 20J.7, 20J.9, and 20J.11 identify design characteristics, potential hardware failures or human errors associated with the design and operation of the RVI and RVFS that could lead to a potentially hazardous condition such as inability to insert a control rod assembly or restricted flow of coolant to the core.

The following potential hazards or operational problems have been identified:

- IGSCC
- Primary water stress corrosion cracking (PWSCC)
- Irradiation-assisted stress corrosion cracking (IASCC)
- Irradiation swelling
- Stress Relaxation
- General corrosion
- Crevice corrosion
- Fatigue
- Brittle fracture
- Failure arising from manufacturing defect
- Galling
- Wear

The basis of the safety case argument is that mitigation against corrosion, fatigue, brittle fracture and manufacturing defects is essentially provided by compliance with ASME design and fabrication rules, the use of proven materials together with the associated ISI requirements and the operating experience embodied within the code as well as other plant experience to mitigate against these degradation mechanisms.

It was determined in the RVI and RVFS failure modes and effects analysis (FMEA) studies (References 20J.9 and 20J.10, respectively) that there is sufficient mitigation in place to offset the potential hazards identified within the report, where the majority of hazards are derived to have a minimal expectation of failure occurrence.

20J.3.3.2 **Avoidance of Primary Water Stress Corrosion Cracking**

Materials known to be susceptible to PWSCC are forbidden and Alloy 600 (Unified Numbering System (UNS) N06600) will not be used for wetted environments with sustained temperatures above 400°F (204.4°C).

20J.3.3.3 **Avoidance of Inter Granular Stress Corrosion Cracking**

In addition to the close control over the reducing coolant chemistry, the stainless steel structural and weld material chemistry and delta-ferrite number (FN) will be controlled to minimise sensitisation to prevent IGSCC. Material processing and RVI material sensitisation is minimised by high quality fabrication and will not adversely affect material IGSCC resistance. As a minimum, the guidance of Regulatory Guide 1.44 (Reference 20J.14) is followed. If, during the course of fabrication, stainless steel is inadvertently exposed to the sensitisation temperature range, the material will be tested according to a process specification, following the guidelines of American Society for Testing and Materials A262, to verify that it is not susceptible to intergranular attack. Testing is not required for the following:

- Weld metal with a ferrite content of 5 percent or more
- Material with a carbon content of 0.03 percent or less
- Material exposed to special processing, provided the processing is properly controlled to develop a uniform product and adequate documentation exists of service experience and/or test data to demonstrate that the processing will not result in increased susceptibility to intergranular attack.

Material not verified to be non-susceptible to intergranular attack will be subject to re-solution annealing and water-quenching or will be rejected.

20J.3.3.4 **Avoidance of Irradiation Induced Degradation**

The irradiation exposure and/or strain limits for the RVI, including fasteners, is demonstrated based on applicable data from operating nuclear plants and/or materials test reactors. The following approaches will be considered:

- All CSS have been evaluated for radiation swelling and IASCC based on the projected peak fluence at the end-of-life for the design basis of the plant (Reference 20J.11).
- Available data for radiation relaxation have been applied where they are significant; for example fasteners.
- Heating resulting from the absorption of gamma ray energy, i.e., gamma heating, is accounted for in the evaluation of RVI components.

20J.3.3.5 **Avoidance of Wear and Galling**

Anti-galling materials and chrome plating will be used where appropriate (i.e., potential wear locations). The core inlet flow distribution will be sufficiently uniform to limit the vibration-induced fuel rod wear. This is accomplished by the core design parameters and compliance with all applicable normal operation and transient events. The RVI hold-down spring maintains a sufficient compressive preload during Level A and Level B operations to minimise sliding, wear, and vibration under all normal operating conditions, but the average

bearing stress between the RV ledge/CB flange and RV head/upper support assembly flange during Level A conditions is limited in order to prevent galling which could result from radial differential expansion between the RV and RVI at these interfaces. The guide tubes, which can suffer wear degradation, will be replaceable and subject to an appropriate ISI schedule, to be determined.

20J.3.3.6 In-Service Inspection

ISI provides forewarning of failure and a means of monitoring degradation and this forms an important element of the safety case argument. ISI is carried out in accordance with Section XI of the ASME Code. The CSS requires visual examination (VT-3 – general mechanical and structural condition) of all accessible surfaces. The visual examinations must be performed at each inspection interval, typically defined as 10 years.

The only requirement to satisfy the above mentioned examination is that the core internals structures be removed from the RV. Current ASME Code requirements do not specify what particular features of the core support and internal structures need to be examined. However, future ASME Code requirements may be more specific and as such the RVI have been designed to accommodate such examinations wherever practical. Areas that may be specified in the future for inspection and their anticipated examination requirements are included in Table 20J-2.

Features that will increase examination reliability and facilitate the inspection process for the internals include properly conditioned welds and easy remote access to the examination surfaces. For ultrasonic testing (UT) of bolting, the bolts should provide sufficient surface area for such examinations. The use of external hex head bolts is a design configuration that has proven to be amenable for such examinations in current plant designs.

Written instructions concerning RVI inspection, maintenance, installation, operation, assembly details and disassembly details will be provided following the generic design assessment (GDA).

20J.4 Strength of the Safety Case

The RVI has been classified as a Standard Class 1 component according to Reference 20J.1. The safety argument in Section 20J.3 demonstrates how the internals structural integrity is established based on extensive quality assurance measures in design, manufacture, materials, testing and qualified inspection. The strength of the safety case is based on the assurance of integrity and that the RVI and RVFS have been deterministically justified in accordance with ASME Code, Subsection NG. Additional arguments provide evidence to demonstrate that the internals are tolerant to through life degradation and this conclusion will be supported by inspection. In combination these elements provide a cogent argument to substantiate reliability commensurate with the Class 1 classification of Reference 20J.1 for the RVI.

To substantiate this claim, this report provides a structured argument supported by suitable and sufficient evidence. To achieve this, three key elements, namely Quality of Build, Good Design, and Mitigation and Management of In-Service Degradation have shown how this will be achieved.

Quality of Build and material selection has been demonstrated by compliance with ASME Code Section III, Subsection NG.

Good design has been demonstrated by providing evidence, including a summary of the results from referenced calculation notes, that design transients including normal, upset,

emergency and faulted conditions are within allowable limits specified in the ASME Code Section III, Subsection NG.

Mitigation and management of in-service degradation has been demonstrated by identifying all design characteristics, degradation mechanisms and potential hazards that could lead to loss of integrity of the RVI. ISI will also provide forewarning of degradation with engineering maintenance and inspection schedules carried out at appropriate intervals.

20J.5 Index of Technical Reports

Table 20J-3 provides a list of the relevant technical references of the RVI and RVFS, supporting the safety case and the function of each document within the safety case.

20J.6 Review of Open Issues

The design of the reactor internals has been finalised and the ASME Design Report has been issued. There are no open issues for the RVI or RVFS that affect the basis of the safety case arguments presented in support of GDA Step 4.

20J.7 Conclusions

This CSR for the United Kingdom (UK) AP1000 plant RVI and RVFS presents the safety arguments to show how the SFRs are maintained for these components. This report presents arguments that support the claim that the structural reliability of the RVI is commensurate with the consequences of failure. To evaluate this, the RVI has been classified in accordance with the procedure for structural integrity classification specified in Reference 20J.1.

The main elements of the safety case argument are firstly that the component has been designed in accordance with the high standards of the ASME Code, Subsection NG. This includes tight controls on material properties, manufacturing processes, design, testing, inspection, and installation such that there is a high level of confidence in the quality of the component and that it will enter service free from significant flaws that could affect the integrity of the component over its lifetime. Secondly, that measures to prevent and forewarn of any potential in-service degradation, such as selection of proven materials and specialised fabrication procedures to avoid IGSCC and the application of ISI at appropriate time intervals, are specified that will mitigate against the mechanisms identified that could threaten the integrity of the component through-life.

Based on the arguments presented together with the referenced supporting evidence, it is considered that the structural reliability of the RVI and RVFS has been justified to a standard commensurate with its consequences of gross failure.

20J.8 References

20J.1 Westinghouse Report UKP-GW-GLR-004, Rev. 3, “UK AP1000 Structural Integrity Classification,” January 2017.

20J.2 Westinghouse Report APP-MI01-Z0-101, Rev. 10, “AP1000 Reactor Vessel Internals Design Specification,” September 2016.

20J.3 Westinghouse Report APP-MI01-Z0-370, Rev. 4, “Design Specification for AP1000 Reactor Vessel Flow Skirt Shop Order MI01 for System RXS,” June 2015.

20J.4 Not used.

20J.5 R. Bullough, F.M. Burdekin, O.J.V. Chapman, V.R. Green, D.P.G. Lidbury, J.N. Swingler, and R. Wilson, "The Demonstration of Incredibility of Failure in Structural Integrity Safety Cases," *International Journal of Pressure Vessels and Piping* 78, pages 539-552, 2001.

20J.6 Westinghouse Report APP-GW-Z0-601, Rev. 4, "Heat Treatment of Stainless Steel for Dimensional Stability," December 2012.

20J.7 Westinghouse Report APP-MI01-Z0-600, Rev. 3, "AP1000 Reactor Internals Fabrication Requirements," January 2016.

20J.8 Westinghouse Report APP-GW-Z0-602, Rev. 3, "AP1000 Cleaning and Cleanliness Requirements of Equipment for Use in Nuclear Supply and Associated Systems," March 2013.

20J.9 Westinghouse Report APP-MI01-GRA-001, Rev. 1, "AP1000 Reactor Vessel Internals Failure Modes and Effects Analysis," March 2012.

20J.10 Westinghouse Report APP-MI01-GRA-002, Rev. 1, "Reactor Vessel Flow Skirt Failure Modes and Effects Analysis," July 2013.

20J.11 Westinghouse Report APP-MI01-Z0-001, Rev. 4, "AP1000 Reactor Vessel Internals Functional Specification," June 2011.

20J.12 Not used.

20J.13 US NRC Regulatory Guide 1.20, Rev. 2, "Comprehensive Vibration Assessment Program for Reactor Internals During Preoperational and Initial Startup Testing," 1976.

20J.14 US NRC Regulatory Guide 1.44, Rev. 0, "Control of the Use of Sensitized Stainless Steel," May 1973.

20J.15 US NRC Regulatory Guide 1.31, Rev. 3, "Control of Ferrite Content in Stainless Steel Weld Metal," April 1978.

20J.16 US NRC Regulatory Guide 1.71, Rev. 0, "Welder Qualification for Areas of Limited Accessibility," December 1973.

20J.17 Westinghouse Report APP-MI01-S3R-002, Rev 5, "AP1000 Generic Reactor Vessel Internals (RVI) Summary Design Report," October 2016.

20J.18 Westinghouse Report APP-MI01-S3C-340, Rev. 2, "AP1000 Reactor Vessel Flow Skirt Structural Qualification," June 2015.

Table 20J-1. Reactor Vessel Internals and Reactor Vessel Flow Skirt Materials

Component	Material
Irradiation Specimen Access Plug Spring	AMS 5698G[1]
Head and Vessel Alignment Pins[2]	ASME SA-182
Lower Core Support Plate Access Plug	
Core Barrel Nozzle	
Lower Radial Support Key	
Lower Guide Tube Support Pin Nut	ASME SA-193
Irradiation Specimen Basket Dowel Pin	
Upper Core Plate Insert Dowel Pin	
Core Shroud Clevis Insert Dowel Pin	
Reinforcement Pad External Hex Cap Screw	
Lower Guide Tube Support Pin	
Upper Core Plate Fuel Alignment Pin	
Core Shroud Clevis Insert Socket Head Cap Screw	
Head and Vessel Alignment Pin External Hex Cap Screw	
Irradiation Specimen Basket Socket Head Cap Screw	
Lower Core Plate Fuel Alignment Pin	
Lower Core Support Plate Access Plug External Hex Cap Screw	
Secondary Core Support Column External Hex Cap Screws and External Head Cap Screws	
Irradiation Specimen Access Plug Dowel Pin	
Guide Tube Special Plate Socket Head Cap Screw	

Table 20J-1. Reactor Vessel Internals and Reactor Vessel Flow Skirt Materials (cont.)

Component	Material
DVI Deflector Support Pins (Support)	ASME SA-193
DVI Deflector Support Pins ((Pin)-Lock)	
Upper Core Plate Insert Socket Head Cap Screw	
Upper Guide Tube Anti-Rotation Stud Nut	ASME SA-194
Lower Guide Tube C-Tube(2)	ASME SA-213
Core Shroud Half Ring Segment	ASME SA-240
Core Shroud Lower C-Panels	
Core Shroud Lower W-Panels	
Core Shroud Rib	
Core Shroud Ring Brace	
Core Shroud Upper C-Panels	
Core Shroud Upper W-Panels	
Core Shroud Vertical Plate	
Core Shroud Top Plate(2)	
Core Shroud Bottom Plate(2)	
Core Shroud Clevis Inserts(2)	
Irradiation Specimen Basket Protection Guide	
Lower Core Plate Fuel Alignment Pin Lock Washer	
Lower Core Barrel	
Middle Core Barrel	
Upper Core Barrel	
Reinforcement Pad	
Alignment Plate(2)	
Lower Neutron Shield Panel	
Middle Neutron Shield Panel	
Upper Neutron Shield Panel	
Direct Vessel Injection Flow Deflector(2)	

Table 20J-1. Reactor Vessel Internals and Reactor Vessel Flow Skirt Materials (cont.)

Component	Material
Secondary Core Support Base Plate(2)	ASME SA-240
Vortex Suppression Plate(2)	
Upper Core Plate Insert(2)	
Upper Support Skirt(2)	
Lower Guide Tube Bottom Flange(2)	
Lower Guide Tube Enclosure Half	
Lower Guide Tube Guide Plate (Lower)(2)	
Lower Guide Tube Intermediate Guide Plate(2)	
Lower Guide Tube Special Guide Plate(2)	
Lower Guide Tube Top Flange(2)	
Upper Guide Tube Flange(2)	
Upper Guide Tube Guide Plate(2)	
Upper Guide Tube Housing (Top) Plate(2)	
Upper Core Plate(2)	
Core Barrel Flange	ASME SA-336
Lower Core Support Plate	
Upper Support Flange	
Upper Support Plate	
Upper Guide Tube Enclosure(2)	ASME SA-358
Upper Support Column Body(2)	ASME SA-376

Table 20J-1. Reactor Vessel Internals and Reactor Vessel Flow Skirt Materials (cont.)

Component	Material
Core Barrel Flow Nozzle	ASME SA-479
Flow Nozzle Plug	
Guide Tube Positioning Dowel	
Head and Vessel Alignment Pin Dowel Pin	
Irradiation Specimen Access Plug (Body)	
Irradiation Specimen Basket Plug	
Irradiation Specimen Basket Double Base(2)	
Irradiation Specimen Basket Triple Base(2)	
Irradiation Specimen Basket Cap(2)	
Lower Core Support Plate Access Port Plug Locating Pin	
Lower Guide Tube Sheath Half	
Reinforcement Pad Locking Bar	
Upper Core Plate Fuel Alignment Pin Nut	
Upper Guide Tube Anti-Rotation Stud	
Upper Guide Tube Enclosure Pin	
Upper Support Column Extension	
Upper Support Column Nut	
Upper Support Column Base(2)	
Upper Support Column Top(2)	
Secondary Core Support Butt Column(2)	
Secondary Core Support Column(2)	
Secondary Core Support Energy Absorber(2)	
Secondary Core Support Guide Post(2)	
Secondary Core Support Housing(2)	
Neutron Shield Panel Spacer Pad(2)	

Table 20J-1. Reactor Vessel Internals and Reactor Vessel Flow Skirt Materials (cont.)

Component	Material
Upper Support Column Hold-Down Socket Head Cap Screw	ASME SA-479 and applicable Code cases
Neutron Shield Panel Socket Head Cap Screws	
Guide Tube Hold-Down Bolts(2)	
Core Shroud Threaded Stud	
Core Shroud Dowel Pin	
Core Shroud Nut	
Reinforcement Pad Dowel Pins	
Neutron Shield Panel Dowel Pin	
Lower Radial Support Clevis Insert	ASME SB-166, UNS N06690
Lower Radial Support Clevis Insert External Hex Cap Screw	ASME SB-637 and applicable Code cases
Lower Radial Support Clevis Insert Dowel Pin	
Hold-Down Spring	Modified Type 403 or 415 and applicable Code cases
Reactor Vessel Flow Skirt Assembly	ASME SB-168, UNS N06690

Notes:

1. This specification is also known as SAE AMS 5698G, "Nickel Alloy, Corrosion and Heat-Resistant, Wire 72Ni – 15.5Cr – 0.95Cb – 2.5Ti – 0.70Al – 7.0Fe No. 1 Temper, Precipitation Hardenable – UNS N07750."
2. Alternate materials may be substituted in compliance with ASME Code rules.

Table 20J-2. Potential Inspection Requirements

Component	Examination Requirement
Upper Support Assemble	
Support Assembly Exterior	VT-3
Support Flange	VT-3
TSF and Locking Devices	VT-3 or UT
Alignment Keys	VT-3
Alignment Surfaces (Interface)	VT-3
Support Flange Circumferential Welds (Accessible)	VT-3 or UT
Hold Down Device	VT-3
Lower Core Support Assemble	
Support Assembly Interior	VT-3
CB Flange	VT-3
Alignment Keys – Pins and Keyways	VT-3
Core Baffle	VT-3
Alignment Surfaces	VT-3
CB Flange Circumferential Weld (Accessible)	VT-3 or UT
CB in Core Beltline Region	VT-3
TSF and Locking Devices (Accessible)	VT-3 or UT
Reactor Vessel Internal Structures	
Flow Distribution Devices	VT-3
Thermal Shield Supports	VT-3
Lower Lateral Restraints	VT-3
Instrument Support Structure	VT-3

Table 20J-3. Reactor Vessel Internals and Reactor Vessel Flow Skirt Technical Index

Document Reference	Title	Description of Role in Safety Case
Generic RVI and RVFS Documents		
APP-RXS-M8-020	AP1000 Nuclear Steam Supply System (NSSS)/Core Design Interface Documents	NSSS/core design interface documents.
APP-RXS-M8-001	RXS Interface Control Document	Interface control document.
APP-GW-M1-001	Mechanical Design Criteria	Provides mechanical design criteria.
APP-RCS-M1-001	Reactor Coolant System (RCS) Design Transients	Detail derivation of RCS design transients.
APP-MI01-Z0-600	AP1000 RVI Fabrication Specification	Presents requirements and special procedures for fabrications of the RVI.
APP-MI01-Z0-601	AP1000 Identification of Parts (Reactor Internals)	Presents the requirements for permanent and temporary marking methods for identification of parts for core support and internals structures.
APP-GW-VLR-002	Technical Requirements of Stainless Steels, Nickel-Base Alloys, Carbon and Low Alloy Steels, and Welding Materials for the AP1000	Provides technical requirements for stainless steels, nickel-base alloys, carbon and low alloy steels, and welding materials.
APP-MI01-Z0-602	AP1000 Hard Surfacing with Cobalt-Chromium Alloy (Reactor Internals)	Provides details of hard surfacing reactor internal components with cobalt-chromium alloy.
APP-MI01-Z0-604	AP1000 Storage and Protection Requirements for Materials, Parts, and Assemblies of Reactor Internals	Presents the storage and protection requirements for materials, parts, and assemblies of reactor internals.
APP-GW-Z0-602	AP1000 Cleaning and Cleanliness Requirements of Equipment for Use in Nuclear Supply and Associated Systems	Presents cleaning and cleanliness requirements of equipment for use in nuclear supply and associated systems.

Table 20J-3. Reactor Vessel Internals and Reactor Vessel Flow Skirt Technical Index (cont.)

Document Reference	Title	Description of Role in Safety Case
Generic RVI and RVFS Documents (cont.)		
APP-GW-VH-001	AP1000 Site Receiving, Inspection, and Storage Requirements for System Materials and Equipment	Provides details of site receiving, inspection, and storage requirements for system materials and equipment.
APP-GW-VH-002	AP1000 Packing and Packaging Components and Spare Parts for Shipment	Provides details of packing and packaging components and spare parts for shipment.
APP-GW-G1-003	AP1000 Seismic Design Criteria	Seismic design criteria.
APP-GW-Z0-606	Requirements for Pressure Sensitive Tapes for Use on Unheated Austenitic Stainless Steel Reactor Components and Systems	Provides details of requirements for pressure sensitive tapes for use on unheated austenitic stainless steel reactor components and systems.
APP-MI01-GRA-001	AP1000 Reactor Vessel Flow Skirt Failure Modes and Effects Analysis (FMEA)	Identifies design characteristics, potential hardware failures or human errors associated with the design and operation of the AP1000 RVI that could lead to a potentially hazardous condition such as injury, fatality, or loss of equipment and product.
RVI Documents		
APP-MI01-Z0-101	AP1000 RVI Design Specification	Provides the basis for the design and construction of the RVI to conform to the ASME Code.
APP-MI01-Z0-001	AP1000 RVI Functional Specification	Defines the functional performance and operational requirements for RVI.
APP-MI01-S3R-002	AP1000 RVI Summary Design Report	A summary of the structural analyses demonstrating compliance with ASME Code, Section III, Subsection NG.
APY-GW-GLR-035	Consistency of RV Core Support Materials Relative to Known Issues of IASCC and Void Swelling for the AP1000 Plant	Demonstrates that the CSS will not be subject to degradation by IASCC or void swelling.

Table 20J-3. Reactor Vessel Internals and Reactor Vessel Flow Skirt Technical Index (cont.)

Document Reference	Title	Description of Role in Safety Case
APP-GW-VW-002	AP1000 Design for Inspectability Program: ISI Requirements for Class 2 and 3 Components and Core Internals Structures	Presents details of the design considerations for ISI of RVI.
APP-MI01-T2I-001	AP1000 Reactor Internals Vibrational Check-Out Functional Test Inspection Data	Provides locations that need to be inspected pre- and post-hot functional testing.
WCAP-16687-P	AP1000 Reactor Internals Expected and Acceptable Responses During Preoperational Vibration Measurement Program	Lists the expected frequencies during preoperational testing.

Table 20J-3. Reactor Vessel Internals and Reactor Vessel Flow Skirt Technical Index (cont.)

No	Document Reference	Title	Description of Role in Safety Case
RVI Documents (cont.)			
25	APP-GW-Z0-603	Bright Annealing of Chromium Nickel Stainless Steels	Provides specification for bright annealing of chromium nickel stainless steels.
26	APP-GW-Z0-607	Determination of Surface Chloride & Fluoride Contamination on Stainless Steel Materials	Provides acceptable method for determination of surface chloride and fluoride contamination on stainless steel materials.
27	APP-GW-Z0-625	Electrodeposited Hard Chrome Plating for Corrosion and Wear Resistance	Provides specification for electrodeposited hard chrome plating for corrosion and wear resistance.
28	APP-GW-VLR-010	AP1000 Supplemental Fabrication and Inspection Requirements	Provides supplemental fabrication and inspection requirements.
29	APP-VL51-Z0-210	Material and Process Specification for SB-637 UNSN07718 Bars, Forging, and Forging Stock for Spring Applications	Provides details of material and process specification for SB-637 UNSN07718 bars, forging, and forging stock for spring applications.
30	APP-VL52-Z0-061	AP1000 RV Material Specification for SB-166 UNS N06690 Rod and Bar (Section III-NB)	Provides details of RV material specification for SB-166 UNS N06690 rod and bar (Section III-NB).
31	APP-VL01-Z0-010	Material Specification for Lubricant, Colloidal Graphite in Isopropanol	Provides the material specification for lubricant, colloidal graphite in isopropanol.

Table 20J-3. Reactor Vessel Internals and Reactor Vessel Flow Skirt Technical Index (cont.)

No	Document Reference	Title	Description of Role in Safety Case
RVFS Documents			
32	APP-MI01-GRA-002	AP1000 Reactor Vessel Flow Skirt Failure Modes and Effects Analysis (FMEA)	Identifies design characteristics, potential hardware failures or human errors associated with the design and operation of the AP1000 RVFS that could lead to a potentially hazardous condition such as injury, fatality, or loss of equipment and product.
33	APP-MI01-Z0-370	AP1000 RVFS Design Specification	Provides the basis for the design and construction of the RVFS to conform with the ASME Code.
34	APP-MI01-S3C-340	AP1000 Reactor Vessel Flow Skirt Structural Qualification	Quantification of the structural integrity of the RVFS assembly using loadings consistent with that of APP-MI01-Z0-370 demonstrating compliance with ASME Code, Section III, Subsection NG.
35	APP-VL52-Z0-013	Material Specification for SB-168, UNS N06690, Alloy 690 Plate, Sheet and Strip	Material Specification for SB-168, UNS N06690, Alloy 690 Plate, Sheet and Strip.

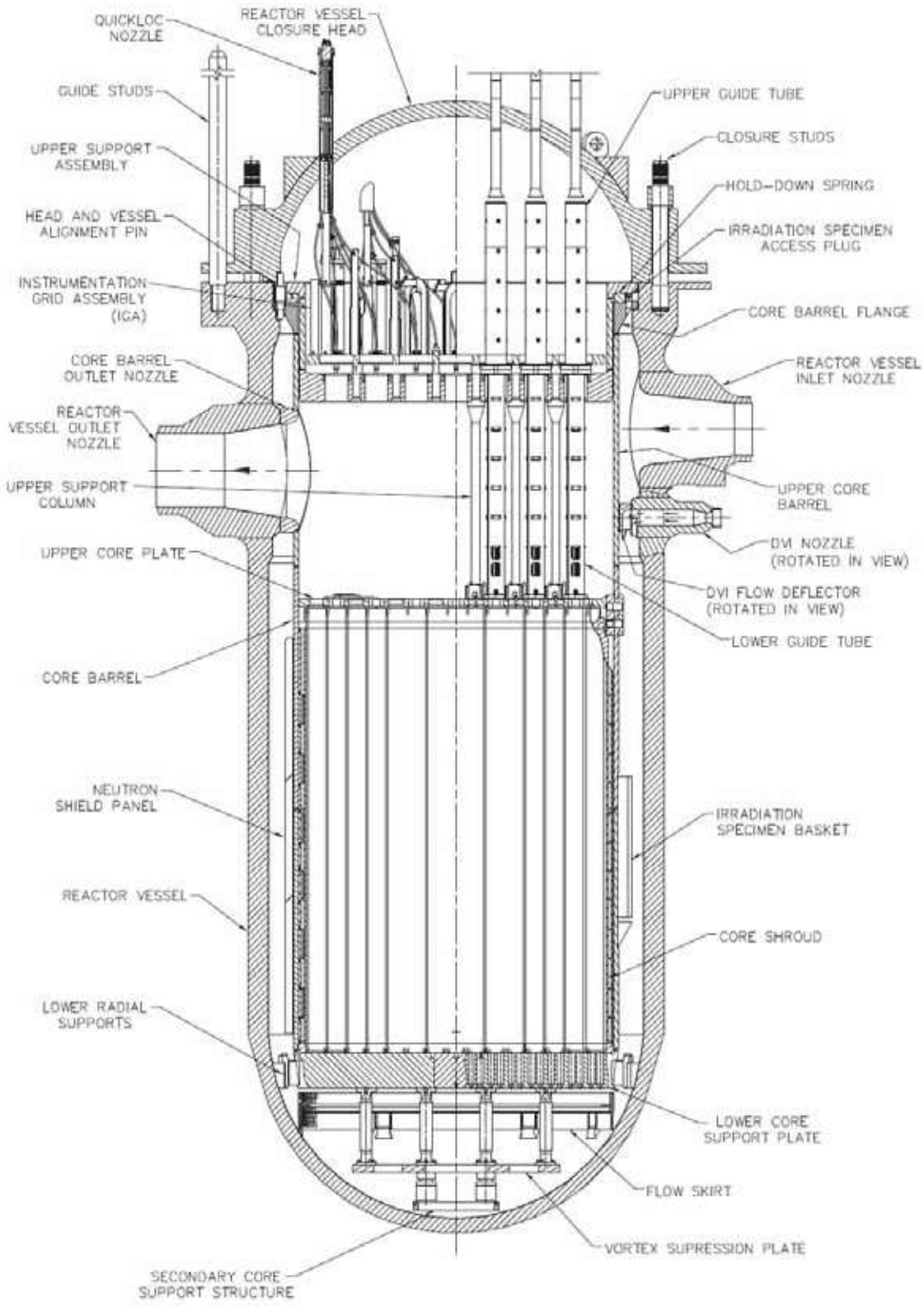


Figure 20J-1. Reactor Vessel and Internals

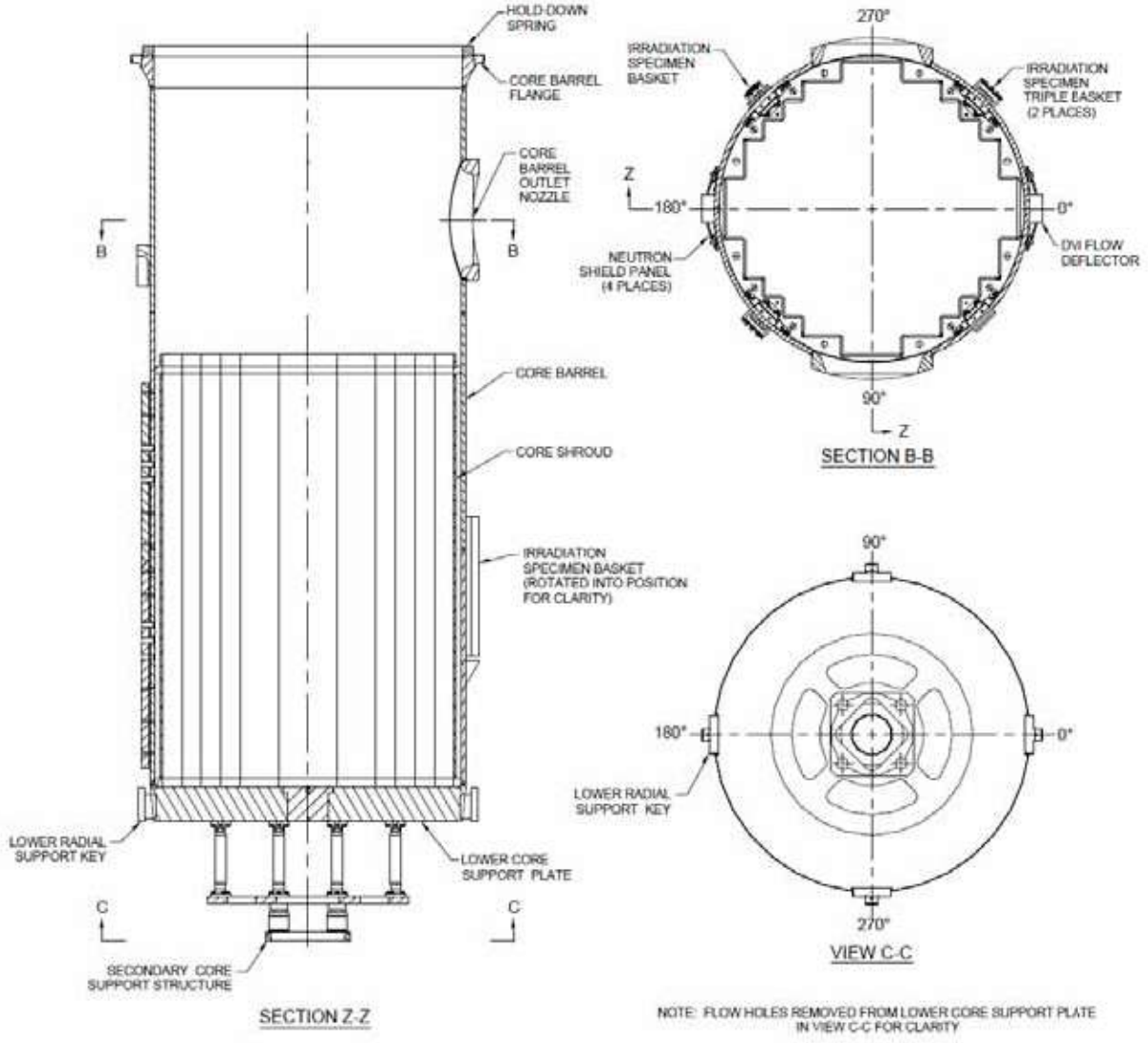


Figure 20J-2. Lower Core Support Assembly

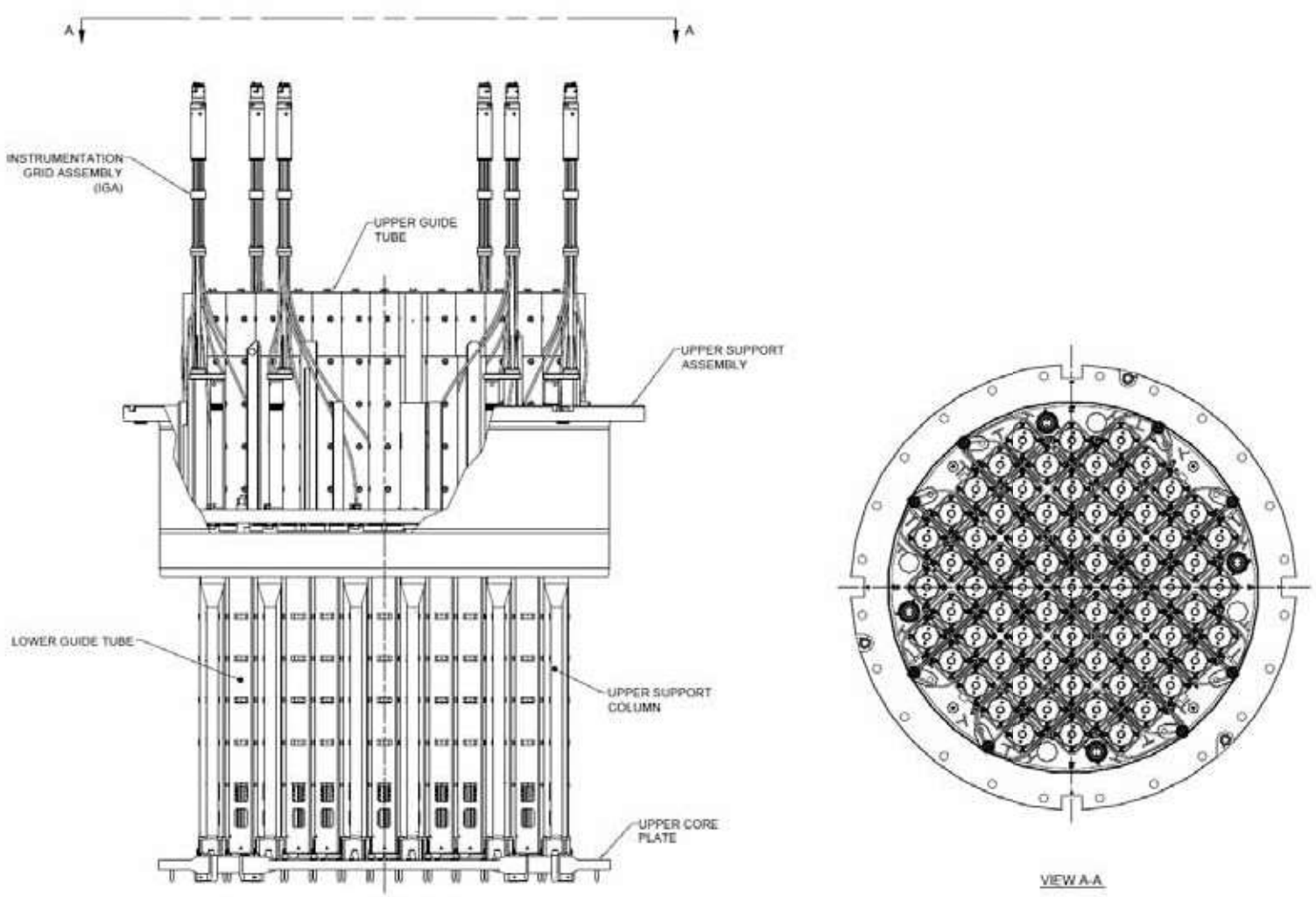


Figure 20J-3. Upper Support Assembly

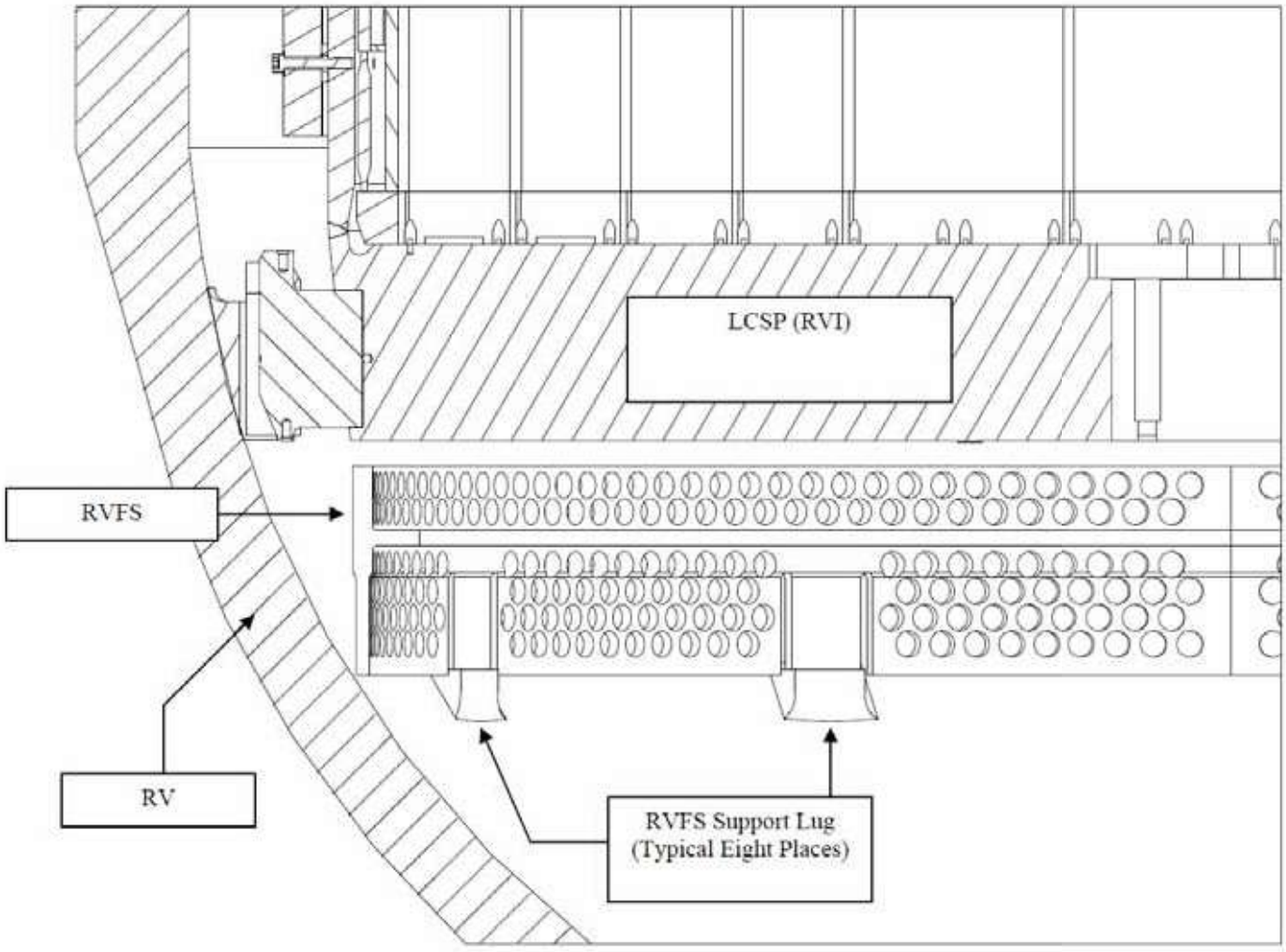


Figure 20J-4. Reactor Vessel Flow Skirt Detail

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS AND ACRONYMS

ACI	American Concrete Institute
ADS	automatic depressurisation system
ALARP	as low as reasonably practicable
ASME	American Society of Mechanical Engineers
CSR	Component Safety Report
CV	containment vessel
DBA	design basis accident
FTT	fuel transfer tube
GDA	generic design assessment
HI	high integrity
HSS	highest safety significance
LOCA	loss-of-coolant accident
MC	metal containment
MSLB	main steam line break
NACE	National Association of Corrosion Engineers
NDE	nondestructive examination
NPS	nominal pipe size
NRC	Nuclear Regulatory Commission
PCS	passive containment cooling system
PWHT	post weld heat treatment
RCS	reactor coolant system
SFR	safety functional requirement
SG	steam generator
SSC	system, structure, or component
SSE	safe shutdown earthquake
UK	United Kingdom
US	United States
VCS	containment recirculation cooling system
VFS	containment air filtration system
VWS	central chilled water system

APPENDIX 20K
CONTAINMENT VESSEL COMPONENT SAFETY REPORT

20K.1 Introduction

This is the component safety report (CSR) for the containment vessel (CV) as introduced in Section 20.2. The safety argument herein substantiates the structural integrity of the CV to a degree of rigour commensurate with the consequences of gross structural failure. The safety argument is supported by a suite of documentation outlined in Section 20K.5 that supports the design, fabrication, construction, inspection, and operation of the CV.

20K.1.1 Scope

The CV acts as a secondary pressure containment boundary in the unlikely event of a demand caused by a breach of the primary or secondary system pressure boundary within containment, actuation of the automatic depressurisation system (ADS) valves, or long-term operation of the passive residual heat removal heat exchanger. This CSR presents arguments to support the claim that the nuclear and radiological risks potentially arising from structural failure of the CV for the entire design lifetime objective of 60 years are tolerably low. Conventional hazards to personnel safety are outside the scope of this Appendix 20K.

20K.1.2 Objectives

This CSR supports the claim the AP1000 plant risk remains both tolerable and as low as reasonably practicable (ALARP) for the design lifetime. These claims are substantiated by satisfying structural integrity safety design bases for all safety-significant AP1000 systems, structures, or components (SSCs). The safety design bases, applied across the operational, process and lifecycle scope of the safety case, embody the technical scope of the safety case: if these can be maintained at all times, the plant will be acceptably safe. Specific safety functional requirements (SFRs) for each particular component are developed from the structural integrity safety design bases, and correspond to the functions that need to be maintained to provide assurance of nuclear and radiological safety. The SFRs applicable to the CV are identified in Section 20K.2.

20K.1.3 Interface With Other Safety Case Documents

The safety argument presented in this report is supported by a dossier of technical data and analyses, which are listed in the Technical Index (Section 20K.5). Where applicable, the supporting documents are identified in the relevant section of the structured safety argument.

20K.1.4 Containment Vessel Description

20K.1.4.1 Functional Overview

The containment building is defined as the CV and the structures contained within the CV. The containment building is an integral part of the overall containment system with the functions of containing the release of airborne radioactivity following postulated design basis accidents (DBAs) and, along with the shield building, of providing shielding for the reactor core and the reactor coolant system (RCS) during normal operations. The CV is an integral element of the passive protection systems since it contains the coolant inventory within the containment thereby allowing passive recirculation of the cooling water during DBA.

The CV is also an integral part of the passive containment cooling system (PCS). The CV facilitates core residual heat removal during postulated loss-of-coolant accident (LOCA) or main steam line break (MSLB) accident events where steam generator (SG) heat removal is not available or is insufficient. The CV provides the heat transfer interface with the surrounding atmosphere, which acts as the heat sink. The rate of cooling can be increased by pouring water onto the outside of the CV steel shell during accident conditions as described herein. Cooling is required to remove sufficient energy to prevent the containment from exceeding its design pressure and temperature following postulated DBAs.

To provide these functions, the CV is designed to provide a leak tight barrier against the uncontrolled release of radioactivity to the environment, to ensure that the coolant inventory is maintained within the containment in the event of a LOCA, and to assure that the containment design conditions are not exceeded for as long as postulated accident conditions and their aftermath require.

The CV also acts as a support for the polar crane, which is supported by a girder that is welded around the circumference of the CV inner surface. Other less significant items are also attached to the inner surface. Justification for the polar crane and girder is covered in Chapter 17.

The CV is an AP1000 Class C (United Kingdom (UK) Safety Class 1) component and serves as the final barrier for preventing the release of radioactive material from the AP1000 plant. The CV must be able to withstand the effects of natural phenomena such as earthquakes, tornadoes and floods, as well as airplane crash, without loss of capability to perform its safety function. It is therefore also classified as seismic Category I. The structural integrity classification of the CV is discussed in Section 20K.2.2.

20K.1.4.2 Design Description

The CV is a cylindrical welded steel vessel with elliptical upper and lower heads. Figure 20K-1 shows the general outline and major dimensions of the CV structure including the locations of the major penetrations, the crane girder and the stiffeners.

The CV is supported by embedding the lower portion in concrete below the 100 m elevation on the outside and the 102.184 m (107.17 ft) elevation on the inside. The 100 m level is the nominal vertical datum for the UK design; this corresponds to the United States (US) nominal vertical datum of 100 feet, and is the ground level elevation.

The CV is an independent, free-standing structure above elevation 100 m. Vertical and lateral loads on the CV and internal structures are transferred to the basemat below the CV by shear studs, friction, and bearing. The shear studs are not required for design basis loads; they provide additional margin for earthquakes beyond the safe shutdown earthquake (SSE).

The containment, shield and auxiliary buildings are structurally integrated on a common basemat which is embedded below the finished plant grade level. The CV is surrounded by a seismic Category I shield building, which provides shielding for the CV and the radioactive systems and components located in the containment building and also provides protection from external hazards.

Seals are provided at the surface of the concrete inside and outside of the CV so that moisture is not trapped next to the steel just below the top of the concrete. The seals accommodate radial growth of the CV due to pressurisation and heatup.

A seismic Category I polar crane is provided within the CV and its bridge is sized for lifting the steam generator. The crane is supported on a stiffened ring girder, fabricated from steel plates, which is welded to the CV. Figure 20K-1 shows the elevation of the crane girder. Figure 20K-3 shows the girder's general arrangement and basic fabrication details.

A stainless steel downspout and gutter arrangement is attached to the inside of the CV to collect steam condensate inside containment during containment pressurisation events and return it to the in-containment refuelling water storage tank. The gutter loads on the CV shell are negligible.

The CV supports most of the containment air baffle, where panels are attached to the outside of the CV to direct air flow along the CV outside surface for passive containment cooling. The air baffle permits inspection of the exterior surface of the CV.

Materials used in the construction of the CV, as specified in Reference 20K.3, meet the requirements of the American Society of Mechanical Engineers (ASME) Section III, Article NE-2000 and the additional requirements summarised in Table 20K-1.

The thickness of the heads is approximately 41.3 mm (1.625 in). The heads are ellipsoidal with a major diameter of about 39.624 m (130 ft) and a height of about 11.468 m (37.6 ft), based on inside surface dimensions. The plate thickness for the head is constant, and is established by the stresses in the knuckle. As a result, the pressure stresses in the regions away from the knuckle are well below the allowable stress, providing margin in the unlikely event of corrosion in this region. The thickness of the lower head is the same as that of the upper head. There is no reduction in shell thickness even though essentially the entirety of the lower head is embedded in concrete.

The wall thickness in most of the cylinder is approximately 44.4 mm (1.75 inches). The wall thickness of the lowest course of the cylindrical shell is increased to approximately 47.6 mm (1.875 inches) to provide margin in the event of corrosion in the embedment transition region. For the current AP1000 under construction in China and the US, the axial welds in the thickened cylindrical first course are post-weld heat treated (PWHT), with all other seam welds being left in the as-welded condition in accordance with ASME for SA-738 for the CV wall thicknesses. ASME Code Case N-841 (Reference 20K.14) has been approved to extend the PWHT exemption from 44.4 mm (1.75 inches) to 60.3 mm (2.375 inches).

As discussed in Reference 20K.13, the following arguments are made regarding the merits of PWHT:

- Fracture analysis has demonstrated significant tolerance to fracture even when a generous allowance is made for the presence of weld residual stress.
- Flaw growth of any undetected flaws is considered to be negligible due to the mild service conditions of the CV.
- SA-738 Grade B has demonstrated excellent fracture toughness properties.
- PWHT is likely to increase the tolerable flaw size from 33% to 60% of the shell thickness.
- UT is expected to provide reliable detection of flaws 10% to 20% of the shell thickness.
- PWHT may reduce the physical strength and/or the fracture toughness of the CV material.
- There is a risk of producing reheat cracking associated with PWHT.

- Local PWHT presents a risk of introducing unquantified residual stress into the structure:
    - Prediction of these stresses is anticipated to be challenging.
    - Controlling local PWHT process on a large scale represents a significant challenge.
    - There is a risk of introducing local distortion that may reduce the buckling capacity of the CV shell.

Based on this discussion regarding the benefits and risks associated with local PWHT, and the margin demonstrated between the reliable detection of UT and the relatively large tolerable flaw size, even when considering a generous weld residual stress, Westinghouse considers the decision not to perform PWHT on the majority of the CV shell welds to be ALARP.

The containment atmosphere during normal operating conditions is maintained within prescribed pressure, temperature, and humidity limits by means of the containment recirculation cooling system (VCS), and the central chilled water system (VWS). The recirculation system cooling coils are provided with chilled water to provide sufficient temperature control. The containment air filtration system (VFS) supply and exhaust subsystem can be utilised to purge the containment air for pressure control. Periodic inspection and maintenance are performed to verify functional capability.

Certain design basis events and credible inadvertent systems actuation have the potential to result in ambient external pressure exceeding the internal CV pressure. For the design external pressure, a conservatively large magnitude of 1.2E-2 MPa (1.7 psi) differential pressure is used, which bounds the external pressure at which the vacuum relief system actuates to mitigate the external pressure. The vacuum relief subsystem is part of the VFS, which is described in section 6.9.1.2 and section 23.3. Evaluation of the design external pressure load is performed in accordance with ASME Code, Section III, Subsection NE.

Containment pressure is monitored by redundant Class 1E pressure transmitters, principally as an indication of increased leakage or a high energy line break. Similarly, the containment average temperature is monitored using temperature instrumentation at the inlet to the containment fan cooler as an indication of increased leakage or a high energy line break. The VFS provides intermittent venting of air into and out of the containment to maintain the containment temperature and pressure within their normal range during normal plant operation as described in Section 23.3.

20K.1.4.2.1 Penetrations

Two equipment hatches are provided. One is at the operating floor elevation (110.744 m, 135.25 ft) with an inside diameter of about 4.9 m (16 ft). The other is at floor elevation (102.184 m, 107.1 ft) to permit grade-level access into the containment, with an inside diameter of about 4.9 m (16 ft). The hatches consist of a cylindrical sleeve with a pressure seated dished head bolted on the inside of the CV (Figure 20K-5). The containment internal pressure acts on the convex face of the dished head and the head is in compression. The flanged joint has double gasketed compression seals with an annular space that may be pressurised for leak testing the seals. Each of the two equipment hatches is provided with an electrically powered hoist and with a set of hardware, tools, equipment and a self-contained power source for moving the hatch from its open position and moving it to its closed position.

Two personnel airlocks are provided, each located adjacent to each of the equipment hatches (Figure 20K-4). Each personnel airlock barrel has about a 3.0 m (9.8 ft) diameter and a door at each end. The airlocks are long enough to provide a specified clear distance unimpaired by the swing of the doors within the airlock. The airlocks extend radially outward from the CV through the shield building, and are supported entirely by the CV. The doors have double-gasketed, pressure-seated seals. The doors are mechanically interlocked to prevent simultaneous opening of both doors and to allow one door to be completely closed before the second door can be opened. The interlock can be bypassed by using special tools and procedures, as during outages.

The mechanical penetrations consist of the fuel transfer tube (FTT) penetration, main steam, main feedwater, startup feedwater, steam generator blowdown, and normal residual heat removal penetration and other mechanical penetrations. Design requirements for the mechanical penetrations are as follows:

- Design and construction of the process piping follow ASME Code, Section III, Subsection NC. Design and construction of the remaining portions follow ASME Code, Section III, Subsection NE. The boundary of jurisdiction is according to ASME Code, Section III, Subsection NE.

- Penetrations are designed to maintain containment integrity under design basis accident conditions, including pressure, temperature, and radiation.

- Guard pipes are designed for pipe rupture protection.

- Bellows are stainless steel or nickel alloy and are designed to accommodate displacements between the piping and the containment vessel. These displacements include thermal growth of the main steam and feedwater piping during plant operation, relative seismic movements, and containment accident and testing conditions. Cover plates are provided to protect the bellows from foreign objects during construction and operation. These cover plates are removable to permit in-service inspection.

Figure 20K-6, sheet 1 shows typical details for the main steam penetration. The main steam penetration includes bellows to minimize piping loads applied to the containment vessel and a guardpipe to protect the bellows and to prevent overpressurisation of the containment annulus in a postulated pipe rupture event. Similar details are used for the feedwater penetration. The bellows form a part of the containment pressure boundary for these penetrations. The main steam and feedwater penetrations are combined into a common 95 mm (3-3/4-inch)-thick insert plate. The main steam penetration has an inside sleeve diameter of approximately 1448 mm (57 inches). The feedwater penetration has an inside sleeve diameter of approximately 965 mm (38 inches). The insert plates for the main steam and feedwater penetrations are shown in Figure 20K-6, Sheet 7. The insert plate also includes the penetration for the DN 150 (NPS 6) startup feedwater pipe. The insert plate is designed in accordance with ASME Code, Section III, Subsection NE-3330.

Figure 20K-6, sheet 2 shows typical details for the startup feedwater penetration. The startup feedwater penetration includes a guardpipe to prevent overpressurisation of the containment annulus in a postulated pipe rupture event. Similar details are used for the steam generator blowdown penetration.

Figure 20K-6, sheet 3 shows typical details for the normal residual heat removal penetration. The normal residual heat removal penetration and other mechanical penetrations below elevation 102.184 m (107’-2”) (where there is concrete inside the containment vessel) have flued heads integral with the process piping and welded to the containment sleeve. The welds

are accessible for in-service inspection. The containment sleeve is separated from the concrete by compressible material.

Figure 20K-6, sheet 5 shows typical details for the FTT penetration. The FTT penetration is provided to transfer fuel between the containment and the fuel handling area of the auxiliary building. The FTT is welded to the penetration sleeve. The containment boundary is a double-gasketed blind flange at the refuelling canal end. The FTT is fitted with expansion bellows that are not a part of the containment boundary. Rather, they are water seals during refuelling operations and accommodate differential movement between the CV, containment internal structures, and the auxiliary building.

Figure 20K-6, sheet 4 shows representative details for the other mechanical penetrations. These consist of a sleeve welded to containment with flued head welded to the sleeve (detail A), a sleeve welded to containment with the process pipe welded directly to the sleeve and in direct contact with the process fluid (detail B), a sleeve welded to containment with process pipe passing through the sleeve (detail C), and a sleeve welded to a thicker insert plate welded to containment with sleeve welded to pipe and in contact with process fluid (detail D). Flued heads are used for stainless piping greater than DN 50 (NPS 2) and for piping with high operating temperatures. The type of weld connecting the sleeve to pipe may vary.

Figure 20K-6, Sheet 6 shows a typical DN 450 (NPS 18) diameter electrical penetration. The electrical penetration assemblies consist of conductor modules (or medium voltage cable modules in a similar penetration) passing through a bulkhead attached to the containment nozzle. Electrical design of these penetrations is described in section 18.6.5.

Electrical penetrations are designed to maintain containment integrity under DBA conditions, including pressure, temperature, humidity and radiation. Double barriers permit testing of each assembly to verify that containment integrity is maintained. Design and testing is according to IEEE Standard 317-83 and IEEE Standard 323-74.

20K.1.5 Containment Vessel Boundaries

The CV is essentially defined by its pressure boundary functions including the portion embedded in concrete. The design boundaries for the CV are in accordance with the boundaries of jurisdiction as listed in ASME Code, Section III. In addition, the following interface boundaries are defined to clearly establish locations where the containment is in contact with non-vessel structures:

- All pressure retaining materials up to, but excluding, the non-pressure-retaining attachments such as the air baffle supports. This includes the stiffening function of the polar crane ring girder and two other stiffening rings in the event of the external pressure exceeding that within the CV.

- Pressure retaining containment penetrations. Refer to Reference 20K.3 where each penetration's boundary limit is defined.

- The welds between the CV wall and the pipework and electrical penetrations. The pipework and penetration components including bellows and guard pipes are justified separately.

- The welds between the CV wall and the mechanical FTT penetration. The penetrations and hatches themselves are mechanical components and are justified in Chapter 17.

The CV is supported by the Nuclear Island concrete structures in which the bottom ellipsoidal head is embedded. Shear studs welded to the bottom head provide additional seismic margin against overturning and uplift of the containment internal structures and the CV. These shear studs are considered non-structural attachments as defined by ASME Section III, Subsection NE. Shear studs will not be attached to CV weld locations. The CV bottom head has been designed for the ultimate stud load. The containment internal structures are supported within the bottom ellipsoidal head and transmit loads through the CV bottom head into the Nuclear Island basemat.

20K.2 Safety Case Requirements

The CV will prevent leakage, under all conditions of specified design loading that may occur during its lifetime. Section 20K.3.2 summarises the specified design load combinations used to design the CV.

The main focus of this CSR is to provide a structured safety argument, supported by suitable and sufficient evidence, to substantiate the classification of the CV as a Standard Class 1 type component, as outlined in Section 20K.2.2. To achieve this, the safety argument is presented as three key elements, as follows:

Claim 1: **Quality of Build: High quality is achieved through good design and manufacture.**

Objective: Provides evidence of good design and manufacture based on established practices and track record. It provides a keystone for a demonstration of appropriate reliability and embodies the code and plant operating experience with the objective of achieving quality of build and the avoidance of defects (Section 20K.3.1).

Claim 2: **Good Design: Good design is achieved through compliance with ASME.**

Objective: Incorporates the build experience as embodied in the design codes (Section 20K.3.2).

Claim 3: **Mitigation and Management of In-service Degradation: Components are tolerant to through-life degradation over the design life of the plant.**

Objective: Provides an assessment of through-life degradation mechanisms and show that such mechanisms will not threaten integrity over a specific interval. It is also established that potential degradation mechanisms are understood and that the inspection and maintenance programme will detect degradation before it affects the performance requirements (Section 20K.3.3).

The safety argument is tailored according to the structural reliability claims derived from a process of component classification, with the purpose of demonstrating that component structural reliability is commensurate with the consequences of gross failure.

The three elements of the safety argument are provided in Section 20K.3 and the strength of the argument is discussed in Section 20K.4.

20K.2.1 Safety Functional Requirements

Safety design bases are identified for each of the AP1000 SSCs. These include duty functions and design basis accident response requirements of plant systems, which must be maintained at all times or upon demand as appropriate to provide assurance of plant nuclear and

radiological safety. Structural integrity safety functional requirements for the CV were identified from the performance and safety design bases, as follows:

- The CV is an integral part of the containment system, which forms a structure that encloses the nuclear power system or that may be connected to other containment items and which is designed to provide a pressure containing barrier for the primary purpose of containing, within leakage limits, or of channelling, for containment or for controlled disposal, radioactive or hazardous effluents released from the system.

- The CV is also part of the PCS whose function is to provide the safety grade ultimate heat sink for the removal of the reactor coolant system normal heat, core decay heat, and decay heat associated with accident sources.

- The CV supports the polar crane girder which in turn supports the polar crane. The CV also supports the majority of the containment air baffle on the exterior surface of the cylinder. The containment air baffle is a functional component of the PCS which promotes heat removal during postulated accidents.

Based on these, the following Safety Function Requirements have been identified which reflect the overall role of the component in plant safety:

- **20.9.1** **Standby function**:

  The CV is required to provide a leak tight barrier against the uncontrolled release of radioactivity to the environment under postulated accident conditions for the design life of the plant, to assure that the containment design conditions important to safety are not exceeded for as long as postulated accident conditions require and to retain coolant inventory in the event of a LOCA.

- **20.9.2** **Duty function**:

  The CV is required, along with the shield building, to provide shielding for the reactor core and the reactor coolant system during normal operations.

- **20.9.3** **Standby function**:

  The CV is required to facilitate core residual heat removal during postulated LOCA or MSLB accident events where SG heat removal is not available or is insufficient.

- **20.9.4** **Duty (normal)/Standby (faulted)**:

  The CV is required to act as a support for the polar crane at all times, including normal and faulted conditions, including seismic events.

Postulated failure modes which result in a loss of these functional requirements lead to identification of structural reliability targets commensurate with the consequences of gross failure, as determined through the process of component classification as described in Section 20K.2.2 below.

20K.2.2 Containment Vessel Structural Integrity Classification

For the AP1000 plant, a structural integrity classification methodology, Reference 20K.1, has been applied to pressurised components with the aim of determining the required level of structural reliability for each of the major plant components based on an evaluation of the direct (e.g., LOCA) and indirect (e.g., missiles/pipe whip, etc.) consequences of gross failure. The CV is not specifically covered by the structural integrity classification methodology because it is not normally pressurised. The CV provides a pressure boundary function on demand in the event of a fault of another component. In accordance with the UK AP1000 classification of SSCs described in Section 5.2, the CV is a Class 1 component because the CV is the final barrier for maintaining nuclear safety upon demand. Failure of the CV has the potential for radioactivity release to the environment during post-accident conditions. Recognising the important role that the CV has in the performance of the AP1000 passive protection systems, it is necessary to provide assurance of adequate structural reliability commensurate with the frequency of demand. The structural integrity classification methodology is not specifically applicable to the CV. A review against the methodology determined the CV would not merit classification as a high integrity (HI) or highest safety significance (HSS) component. However, for the purpose of assuring adequate structural reliability, the structural integrity of the CV is evaluated as if it were a Standard Class 1 component.

20K.3 Safety Case Arguments

Consistent with other Class 1 components, the basis of the structural integrity claim is centred on arguments and evidence to substantiate the claims listed in Section 20K.2.

Claim 1: High quality is achieved through good design and manufacture (Section 20K.3.1).

Claim 2: Good design is achieved through compliance with the ASME Code (Section 20K.3.2).

Claim 3: Components are tolerant to through-life degradation over the design life of the plant (Section 20K.3.3).

Consistency with the ASME Code, Section III for Class MC (metal containment) components provides the basic demonstration of fitness-for-purpose for the CV and forms the primary element in the safety case for the AP1000 CV.

20K.3.1 High Quality Is Achieved through Good Design and Manufacture

The reliability of the CV is dependent upon the quality of the design and the fabrication. The design intent is translated into a manufacturing plan which is controlled by a Quality Assurance Programme compliant with rigorous design codes including the ASME Code. The CV Design Specification (Reference 20K.3) provides a list of the industry codes, specification and standards applied to the CV.

The argument to support the achievement of high quality is supported by the following supplemental arguments:

- **Design and Fabrication in Accordance with ASME Code, Section III**: The CV is classified as UK AP1000 Class 1. Design and fabrication of the CV is carried out in accordance with ASME Code, Section III requirements. Fabrication and installation of the CV including forming, welding qualification, and heat treatment will meet the

requirements of ASME Code, Section III Article NE-4000 and the additional requirements specified in the Design Specification (Reference 20K.3).

- **Material Specifications**: The CV materials and testing requirements have been specified in accordance with the requirements of NE-2000 of the ASME Code. The basic containment material is SA-738, Grade B, carbon steel plate. The material fracture toughness has been selected to satisfy the lowest service metal temperature requirement of -28°C (-18°F). This temperature is established by analysis for the portion of the CV exposed to the environment when the minimum ambient air temperature is -40°C (-40°F).

Carbon steel plate for the personnel airlock is to conform to SA-516 Grade 70. Carbon steel forgings are to conform to ASME SA-350, Grade LF2. Stainless steel forgings are to conform to ASME SA-182 Gr. F304L.

- **Supplemental Requirements**: The procurement specification for the SA-738, grade B, plate includes supplemental requirements S1, Vacuum Treatment and S20, Maximum Carbon Equivalent for Weldability (Reference 20K.4). Welding will be carried out in accordance with the ASME Code, Section III and Section IX for all safety class, seismic Category I components as described in Reference 20K.3. Thermal post weld heat treatment of welds for plates exceeding 44 mm (1.75") thickness is required in accordance with the ASME Code (see Table NE-4622.7(b)-1). Although ASME Code Case N-841 (Reference 20K.14) has been approved to extend the PWHT exemption from 44.4 mm (1.75 inches) to 60.3 mm (2.375 inches), PWHT will still be performed on plates in this thickness range, thus providing additional margin. Tolerances are as specified by the ASME Code, except that the difference between the maximum and minimum diameter at any cross-section will not exceed 0.5 percent of the nominal diameter of the CV. The diameter at any cross-section will not deviate more than 0.25 percent of the nominal diameter. Out of plumb will not exceed 0.25 percent, measured between tangent lines after making allowance for out of roundness as specified.

- **Avoidance of non-Ductile Failure**: As a minimum requirement, impact testing will be as specified in Section III of the ASME Code, Paragraph NE-2300 as applicable to demonstrate material ductility. Charpy V-notch specimens will be used for all impact testing. Weld test plates will be made and impact tested in accordance with Subsection NE of Section III of the ASME Code as described in Reference 20K.3.

- **Quality Control**: The quality control programme involving welding procedures, erection tolerances, and nondestructive examination (NDE) of shop and field-fabricated welds conforms to Subsections NE-4000 and NE-5000 of the ASME Code. In particular, NDE of shop and field-fabricated welds will conform to Subsection NE-5000 of the ASME Code using radiographic examination, ultrasonic examination, penetrant examination, magnetic particle examination, and surface examination as appropriate.

- Radiography, as required by the ASME Code, is capable of detecting and length sizing structurally significant planar and volumetric flaws. However this method does not provide a through-wall size for a planar flaw. UT would provide this additional dimension and could also serve to enhance the detectability of smaller and tilted/skewed planar flaws. Therefore this RT requirement will be augmented or replaced with UT. The design specification for the CV in the UK will require that UT be used in addition to or in-lieu of RT for plants constructed in the UK. Westinghouse will petition the ASME Boiler & Pressure Vessel Code to extend Code Case N-659-2 that allows UT in lieu of RT, to NE welds in metal containments. If UT is allowed in lieu of RT, a performance

demonstration would be required, as dictated by N-659-2. This performance demonstration needs to consider the specific fracture assessments to determine the flaw matrix for the qualification block(s).

The CV is designed to permit construction using large subassemblies, each of which will be subjected to NDE as will the final assembly welds. These subassemblies consist of the two heads and three or more ring sections. The intention is that these will be assembled in an area near the final installed location in the nuclear island, using plates fabricated in a shop facility.

Personnel performing NDE will be qualified and certified using a written practice prepared in accordance with ANSI/ASNT CP-189, Standard for Qualification and Certification of NDE Personnel (Reference 20K.9).

- **Testing and Examination**: Testing is in accordance with ASME NE-6000. Pre-service examination is in accordance with ASME Article IWE-2200. This is a 10% overpressure pneumatic test (Reference 20K.3).

Together, these arguments provide a basis for a demonstration that the CV will achieve a high quality of design and fabrication, will enter service free from significant structural defects and that the effects of through-life degradation on material properties will not have a deleterious effect on the structural reliability of the CV. The outcome of the materials testing including fracture toughness testing, NDE and CV pressure testing will provide supporting evidence on a case-by-case basis in due course.

20K.3.2 Good Design Is Achieved through Compliance with ASME

The CV is designed and constructed according to the 2001 Edition of the ASME Code, Section III, Subsection NE, Metal Containment, including the 2002 Addenda. Stability of the CV is evaluated using ASME Code, Case N-284-1, Metal Containment Shell Buckling Design Methods, Class MC, Section III, Division 1, as published in the 2001 Code Cases, 2001 Edition, July 1, 2001. Full ASME Code compliance has been demonstrated.

20K.3.2.1 Load and Load Combinations

The design and analysis procedures for the CV are according to the requirements of the ASME Code, Section III, Subsection NE. Loading conditions are derived from an assessment of applicable normal and abnormal operating conditions, as well as from those identified from the consideration of internal and external hazards, as discussed in Chapters 9, 11, and 12. These hazards are often conveniently classified as basic (dead load, live load), operational (pressure, temperature), natural (seismic, wind, tornado), and man-made (blast, impact, dropped load). Reference 20K.3 details the load combinations and which ASME Service Levels apply to the various loads and combinations. A summary of the load combinations analysed for qualification of the CV design to the ASME Code is provided in Table 20K-4.

The numerical analysis methods are summarised in Table 20K-3. The overall CV was modelled as an axisymmetric shell and analysed using the ANSYS computer programme (Reference 20K.8). Dynamic analyses of the axisymmetric model were performed to obtain frequencies and mode shapes. These were used to confirm the adequacy of the CV seismic stick model as input to the Nuclear Island model.

Stress analyses were performed for each of the following loads:

- Dead load
- Internal and external pressure
- Thermal
- Seismic
- Polar crane wheel loads
- Wind and tornado loads

DBAs produce the bounding containment internal pressures and temperatures and are discussed in section 20K.3.2.2.

The personnel airlocks and equipment hatches are modelled in ANSYS using in a 3-D shell finite element model of the containment to consider the effect of the penetrations and their quasi-static response due to a seismic event. Static analyses are performed using the finite element model for internal pressure, dead load (including the polar crane in the parked position), thermal loads and seismic loads. Stresses are evaluated against the stress intensity criteria of ASME Code, Section III, Subsection NE for the load combinations described in Table 20K-4.

20K.3.2.2 Design Basis Accident Conditions

The containment system is designed such that for all pipe break sizes, up to and including the double-ended severance of a reactor coolant pipe or secondary side pipe, the containment peak pressure and temperature remain below the design limits. Hence, Code compliance is assured in the worst operational accident case. As described in Section 9D, the containment analyses are performed taking into account single failures that maximise stresses on the CV. A summary of the results of the containment analysis is presented in Table 9D.1-1.

The results of the containment analysis indicate that the peak pressure and peak temperature are not coincident. However, the temperature refers to the containment atmosphere and lasts for a short duration such that the CV metal does not exceed its design limit. Also, the passive containment cooling system is cooling the CV metal during this event.

The peak stresses experienced by the CV during a DBA were quantified by using an ANSYS finite element model as shown in Figures 9 through 18 of Reference 20K.2. The peak stresses were found to be fairly localised near the hoop stiffeners and the knuckle region of the top head. Reference 20K.2 gives a more extensive description of the stress analyses.

The bottom head is fully embedded in the concrete base at elevation 100 m, the nominal vertical datum for the UK design. This results in the generation of localised stresses at this location under thermal and pressure loading associated with the DBA due to restrained radial movement. The CV design includes a Service Level A combination in which the CV above elevation 102.184 m (107.16 ft) is specified at the design temperature of 149°C (300°F) and the portion of the embedded CV (and concrete) below elevation 100 m (100 ft) is specified at a temperature of 21°C (70°F). The temperature profile for the CV is linear between these elevations. Containment shell buckling in this region is evaluated against the criteria of ASME Code Case N-284-1. Code Case N-284-1 is also used for the evaluation of the CV upper head and equipment hatches.

Conservative design basis static, dynamic and transient natural and man-made loads have been defined and appropriately combined for design and substantiation purposes. The conditions considered include normal, upset (accident), emergency and faulted conditions.

As discussed in section 20K.1.4.2.1, mechanical penetrations for the large-diameter high-energy main steam and feedwater piping include expansion bellows that are part of the containment boundary. The piping and flued head have large pressure capability. The response of expansion bellows to severe pressure and deformations is described in NUREG/CR-5561 (Reference 20K.5). The bellows can withstand large pressure loading but may tear once the containment vessel deflection becomes large, beyond design conditions. Testing reported in NUREG/CR-6154 (Reference 20K.10) has shown that the bellows remain leaktight even when subjected to large deflections sufficient to fully compress the bellows. Such large deflections of the containment vessel would not occur in response to design basis events. The containment penetration bellows are designed for a pressure of 0.60 MPa (87 psig) at design temperature within Service Level C limits, concurrent with the relative displacements imposed on the bellows when the containment vessel is pressurised to these magnitudes.

20K.3.2.3 Thermal Loads

Thermal stresses have been considered in the design and evaluation of the CV at Service Levels A, C and D both with and without design pressure for the temperature conditions specified in Table 20K-5.

The CV has been designed for the temperatures given in Table 20K-5. These are metal temperatures. The thermal gradient through the wall is negligible as the CV shell is relatively thin, any effects will be secondary and the margins to gross failure are generous. Two cases are specified: one corresponding to normal operation in extreme cold weather, which maximises the temperature differences at the crane girder, the insulated enclosure (upper equipment hatch and personnel airlock) and the external stiffener, and one corresponding to the DBA condition in hot weather which maximises the temperature difference at the embedment. A step change in temperature has been assumed for normal operation at elevation 109.677 m (131.75 ft) (except in the insulated enclosure region), at the interface between the crane girder and the shell, and the internal stiffener and the shell. Analyses close to the embedment for the DBA considered a temperature profile that decreases linearly between elevations 102.184 m (107.16 ft) and 100 m (100 ft). The temperature of the concrete structures is assumed to remain at 21°C (70°F).

20K.3.2.4 Seismic Loading

Safe shutdown following a SSE requires the use of safety significant systems to bring the site to a safe state without the need for operator action. A SSE is defined as the maximum potential vibratory ground acceleration for safe shutdown without loss of plant capability to perform safety functions and is taken as the design basis earthquake for the purpose of this assessment. The design intent is for the CV to remain elastic under postulated earthquake loading.

The CV is a seismic Category I structure. The overarching claim for seismic hazards is that there will be no loss of key safety functions in a credible seismic event. To support these claims, it is argued that a generic envelope for site seismology has been defined for the AP1000 design and that a SSE has been defined that generally bounds the UK design basis. Chapter 16 present a generic seismic justification for the AP1000 design.

The peak horizontal ground acceleration of the SSE has been established as 0.30g for the AP1000 design. The vertical peak ground acceleration is conservatively assumed to equal the horizontal value of 0.30g; UK practice is to scale the horizontal spectra by two thirds.

Both horizontal and vertical design response spectra are based on the US NRC Regulatory Guide 1.60 (Reference 20K.7) spectra augmented at the higher frequencies.

A fixed-base ANSYS interaction model for the nuclear island is described within Section 16.8. This has predicted the dominant modes and frequencies in three orthogonal directions; direction Z denotes the vertical direction. The results from the ANSYS shell model for the various load cases were factored and combined as shown in Table 4 of Reference 20K.15. The stress results from the design basis seismic load show an axial compression and a tangential shear at the base of the cylindrical portion of the CV, which were evaluated in accordance with ASME Code Case N-284-1, Revision 1 and shown to be compliant.

20K.3.2.5 Wind Loading

Chapter 4 details the wind and tornado derivation and loadings used in the AP1000 design. The portions of the CV which will be exposed above grade prior to the construction of the shield building were designed for the wind loads on the projected area of the circular shape in accordance with the American Society of Civil Engineers code: ASCE 7-98 (Reference 20K.6). A basic wind speed of 31.3 m/s was used to calculate the wind load during construction. This bounds any wind loading experienced once the shield building has been constructed.

The shield building is justified for the design basis wind and therefore protects the CV from the direct effects of wind loading including wind-borne missiles. Nevertheless, the CV has been evaluated and found to be acceptable for design wind and tornado, which induce a reduction in atmospheric pressure external to the CV and non-uniform pressures assumed to occur at the same time.

20K.3.2.6 Conservatism in Material Property Data

The CV is designed using SA-738, Grade B material, which has a stated specified minimum yield of 415 MPa (60 ksi) and an ultimate capacity 585 MPa (85 ksi). Test data for materials having similar chemical properties were reviewed by Westinghouse. In a sample of 122 tests for thicknesses equalling or exceeding 38.1 mm (1.5 in) and less than 44.4 mm (1.75 in), the actual yield had a mean value of 476 MPa (69 ksi), with a standard deviation of 23 MPa (3 ksi). This results in an actual yield about 15 percent higher than the minimum yield. This additional capacity has not been claimed in the design of the CV or in the internal pressure ultimate capacity analysis results presented in Table 20K-6. Membrane yield of the cylinder is predicted to occur at an internal pressure of 1.23 MPa (178 psi) gauge.

Ultimate capacity analyses were also performed that displayed a generous margin to gross yield and ductile behaviour beyond yield. A series of stress and buckling ultimate limit analyses that were carried out to determine the maximum internal pressure capacity at a fixed 38°C (100°F). The results are based on the minimum ASME–specified material properties and are presented in Table 20K-6. Reasonable margins beyond the design pressure of 0.407 MPa (59 psi) were predicted with no brittle failure modes. The pressure related to gross hoop yield of the cylindrical shell was a predicted ultimate internal pressure of 1.069 MPa (155 psi). A temperature compensation at 204°C (400°F) using the tables given for material properties in the ASME Code reduced the yield stress by 17% and the pressure capacity corresponding to shell gross yield reduced from 1.069 to 0.889 MPa (155 to 129 psi) gauge.

20K.3.2.7 Fracture Assessment Above and Beyond ASME

Fracture analysis of the CV above and beyond the requirements of ASME has been performed to demonstrate that it will provide an adequate barrier to large release in the event that it is called on to do so (Reference 20K.13). The analysis examines the flaw tolerance associated with PCS flow actuation following an initiating event in which containment has been pressurized. Conservative loadings and stresses are applied to reflect the worst case thermal shock event. The combined stress used envelopes all credible defect locations and orientations. The flaw location is chosen at the top of the containment vessel to maximise the temperature difference between the PCS flow and the containment metal. The orientation of the postulated flaw is assumed to be along the direction of the weld as the welding process is unlikely to produce transverse flaws. Flaws transverse to the weld are likely contained within the weld and thus will be small enough as to not challenge the structural integrity of the CV.

The flaw tolerance is determined by postulating a range of flaw sizes and determining the conditions where the applied stress intensity factor is equal to a fracture toughness that is conservatively assumed. The results of the analysis demonstrate that for a relatively long flaw, which has a length equal to ten times the depth, the criteria are met with a flaw depth that is 33% of the wall thickness. For an elongated flaw, with length equal to 1000 times the depth, a depth of 25% of the wall thickness is shown to be acceptable.

Ultrasonic inspection will be used to detect possible flaws in the CV as it has a higher reliability for detecting, characterizing and sizing planar defects with reliable detection rates for defects 10% - 20% of the weld thickness and is roughly equal to radiographic inspection for the detection of volumetric defects. UT inspection of 100% of the welds will be performed during manufacture.

Based on the above, there is confidence that the flaws which were determined to be tolerable are larger than those that can be detected with the chosen inspection technique such that the CV will enter service free from defects of structural significance.

20K.3.3 Mitigation and Management of In-Service Degradation

20K.3.3.1 Corrosion

Reasonable and appropriate steps as described below have been implemented in the design of the CV to minimise the level of surface corrosion which, in conjunction with the inspection regime summarised in section 20K.3.3.2, provides a robust justification for the 60 year design life.

There is no specific Code requirement for corrosion allowance. The wall thickness in most of the cylinder is 44.4 mm, which is a standard US off-the-shelf plate thickness (1.75 in).

The wall thickness of the lowest course of the cylindrical shell, which interfaces with the CV interior concrete, is approximately 47.6 mm (1.875 inches) to provide margin to compensate for corrosion in the concrete embedment transition region. The 44.4 mm (1.75 in) walls of the CV have a nominal additional allowance against the ASME overall sizing thickness which, although it has not been designed as a corrosion allowance, is available to offset minor corrosion. Note that the ASME sizing thickness is for the entirety of the CV shell. Locations of postulated localised degradation that result in shell thickness well below the sizing thickness are tolerable with respect to structural integrity and the functions of containing radioactivity and providing shielding.

The National Association of Corrosion Engineers (NACE) Corrosion Engineer's Reference Book (Reference 20K.11) provides a single face corrosion rate of 0.1-0.3 mm/year for carbon steel in a "quiet seawater" environment. At the higher corrosion rate of 0.3 mm/year it will take more than 12 years to erode through the sizing allowance in the thickened region for single face corrosion and more than 6 years for double face corrosion. At the same rate, it will take two years to erode the nominal sizing allowance elsewhere for single face corrosion. Owing to the differing internal and external environments above the concrete embedment, it is not reasonable to presume that corrosion will occur simultaneously on both faces in the same region. Note, however, that the margins to gross failure beyond the design basis are generous and that a ductile response is expected as described in section 20K.3.2.6.

The AP1000 CV is coated with an inorganic zinc coating to an elevation of at least 30.4 cm (12 in) below the top surface of the concrete inside and outside of the CV. Electrical and mechanical penetrations are generally coated with inorganic zinc coating. The outside of the CV shell is coated to a distance of 30.4 cm (12 in) beyond the penetration blockout in the concrete where applicable. This coating provides an effective barrier to both oxygen and water which reduces the rate of corrosion to negligible levels in the treated area. Outside of these coating requirements, surface treatment (other than cleaning or wetting) of the lower portions of the bottom head prior to concrete embedment is not required.

Loss of material due to corrosion in inaccessible areas is considered not to be significant because the following conditions will be satisfied:

- Concrete will meet the requirements of American Concrete Institute (ACI) 318-08 (Building Code Requirements for Structural Concrete and Commentary) or ACI 349-06 (Code Requirements for Nuclear Safety-Related Concrete Structures and Commentary) enhanced by the guidance of ACI 201.2R-01 (Guide to Durable Concrete) on durability for the containment concrete in contact with the embedded containment shell or liner.

- The concrete will be inspected and monitored to ensure that it is free of penetrating cracks that could provide a path for water seepage to the surface of the containment shell.

- The moisture barrier (concrete seal), at the junction where the shell becomes embedded, is subject to aging management activities in accordance with ASME Code, Section XI, Subsection IWE requirements. The concrete seals will be visually inspected periodically as required by the ASME Code and will be repaired if necessary. The corrosion allowance does not claim benefit from the seal between the CV wall and the concrete.

Borated water spills and water ponding on the containment concrete floor are uncommon and when detected will be cleaned up in a timely manner.

The air baffle promotes air flow over the external surface of the CV under all conditions. This is specifically designed to aid in the evaporation of any moisture. The CV internal atmosphere is humidity controlled.

Considering the steel embedded in the concrete, the design philosophy is that there will be no significant corrosion because there will be no oxygen present in the unlikely event that water is present, and there will be an alkaline environment that will impede corrosion.

The approach for localised corrosion is that if corrosion were to occur, localised thinning will not result in a structural or containment concern provided that there is sufficient material surrounding the localised thin area and there remains sufficient wall thickness at the thinned region to withstand the pressure and maintain containment.

The inside containment surface from approximately elevation 102.2 m (107 ft) to 110 m (33 ft) (i.e., approximately the operating deck level) is coated with an epoxy topcoat to facilitate cleaning of the coated CV.

20K.3.3.2 Testing and In-Service Inspection

The AP1000 has a 60-year design life. It must be demonstrated that the structural integrity of the CV is maintained throughout the design life such that the component continues to deliver it functions. Assurance in this respect is provided by minimising the degradation as discussed in section 20K.3.3.1 and by implementing a suitable in-service inspection and maintenance strategy.

The following design and in-service inspection aspects have been considered and incorporated to mitigate the effects of corrosion of the AP1000 CV:

- The concrete seals provided at the top surfaces of the concrete along the CV shell/concrete interface inside and outside containment will be visually inspected in accordance with ASME Code Section XI.

- In-service inspection (Visual Examination) of the exposed surfaces of the CV is required approximately every 40 months in accordance with ASME Code Section XI. Note that both the inside and outside steel surfaces are accessible for inspection. Any degradation will be detectable by evidence of bubbling, flaking or peeling of the inorganic zinc coating.

- The presence of the inorganic zinc coating reduces the corrosion rate to negligible levels; hence, the 40 month interval is considered reasonable. Also, as discussed in section 20K.3.2.6, the margins to gross failure are generous and a ductile response is expected.

- Containment leak testing is performed approximately every 40 months. Testing of the CV and the pipe assemblies forming the pressure boundary within the CV will be according to the provisions of NE-6000 and NC-6000, respectively. The expansion bellows have a test enclosure to allow leak testing the flexible bellows external to the containment atmosphere.

20K.4 Strength of the Safety Case

The CV is classified as an AP1000 Standard Class 1 component. As such, the strength of the safety case is based on the achievement and maintenance of integrity. The CV has been deterministically justified in accordance with the ASME Code for Class MC components. The safety argument in Section 20K.3 demonstrates how CV structural integrity is established based on extensive quality assurance measures in design, fabrication, manufacture, materials, testing and qualified inspection. Additional arguments show that the design of the CV considers all recognised loads and load combinations applicable to the UK and provide evidence to demonstrate that acceptable margins to failure (gross yield) have been achieved, and that ductile response beyond yield is expected. Further arguments provide evidence to demonstrate that the CV is sufficiently tolerant to credible through-life degradation; this conclusion is supported by start-of-life inspection of the whole assembly and regular through-life inspection of the region above the concrete embedment. In combination, these elements provide a cogent argument to substantiate integrity commensurate with the classification of the CV for the 60 year design life.

20K.5 Index of Technical Reports

Table 20K-7 provides a list of technical references supporting the safety arguments within this CSR.

20K.6 Review of Open Issues

The Technical Index for this CSR will be updated before generic design assessment (GDA) closeout to reflect a representative set of calculations supporting the claims in this report. There are no additional open issues for the CV that affect the GDA.

20K.7 Conclusions

The CV acts as a secondary pressure containment boundary on demand in the unlikely event of a breach of the primary or secondary system pressure boundary component within containment or actuation of the ADS valves. The CV is also an integral part of the AP1000 pressure protection systems. The CV is an integral part of the PCS, which, together with the passive core cooling system, provides heat removal during postulated accidents by containing, cooling and recirculating the coolant inventory. To provide these functions, the CV provides a leak tight barrier against the uncontrolled release of radioactivity to the environment and assures that the containment design conditions important to safety are not exceeded for as long as postulated accident conditions require.

The CV is classified in accordance with the UK AP1000 Classification of SSCs as a Class 1 component because the CV is the principal means for maintaining nuclear safety upon demand. Although it is not normally pressurised, a review against the methodology presented in Reference 20K.1 determined the CV should be evaluated as a Standard Class 1 component. For such components, the main elements of the safety case argument are:

- Firstly, that the component has been designed in accordance with the high standards of the ASME Code as applicable to Class MC structures. This includes appropriate controls on material properties, manufacturing processes, design, testing, inspection and installation such that there is a high level of confidence in the quality of the component and that it will enter service free from significant flaws that could affect the integrity of the component over its lifetime.

- Secondly, that the design considers all credible loads and load combinations and complies with the appropriate requirements of the applicable ASME Code. This has been demonstrably achieved for the AP1000 CV with sufficient margins to failure (gross yield) and ductile response beyond yield.

- Thirdly, that measures to prevent, detect or forewarn of in-service degradation, such as the application of the inorganic zinc coating and implementation of a suitable in-service inspection regime, are specified which will mitigate the mechanisms identified which could threaten the integrity of the component through life. Such measures have been identified for the CV.

Based on the arguments presented, together with the referenced supporting evidence, the structural reliability of the CV has been justified to a standard commensurate with the consequences of its gross failure.

20K.8 References

20K.1 Westinghouse Report UKP-GW-GLR-004, Rev. 3, "AP1000 UK Structural Integrity Classification," January 2017.

20K.2 Westinghouse Report APP-MV50-S2C-002, Rev. 1, "Design of Containment Vessel for Internal and External Pressure," April 2010.

20K.3 Westinghouse Report APP-MV50-Z0-001, Rev. 9, "AP1000 Containment Vessel Design Specification," August 2015.

20K.4 Westinghouse Report APP-GW-VLR-010, Rev. 2, "AP1000 Supplemental Fabrication and Inspection Requirements," January 2016.

20K.5 U.S. Nuclear Regulatory Commission NUREG/CR-5561, "Analysis of bellows expansion joints in the Sequoyah containment," 1991.

20K.6 ASCE 7-98, American Society of Civil Engineers, "Minimum Design Loads for Buildings and Other Structures."

20K.7 US Nuclear Regulatory Commission, Regulatory Guide 1.60, Rev. 1, "Design Response Spectra for Seismic Design of Nuclear Power Plants," December 1973.

20K.8 ANSYS Inc., ANSYS Engineering Analysis User's Manual, Releases up to and including ANSYS 5.7.

20K.9 The American Society for Nondestructive Testing, "ASNT Standard for Qualification and Certification of Nondestructive Testing Personnel," ANSI/ASNT CP-189.

20K.10 US Nuclear Regulatory Commission, NUREG/CR-6154, "Experimental Results from Containment Piping Bellows Subjected to Severe Accident Conditions," 1994.

20K.11 National Association of Corrosion Engineers, "Corrosion Engineer's Reference Book," 3rd Edition, NACE International, 2002.

20K.12 American Concrete Institute, "Code Requirements for Nuclear Safety Related Structures," ACI-349-01, 2001.

20K.13 Westinghouse Report UKP-MV50-S2C-036, Rev. 0, "AP1000 Containment Vessel Flaw Tolerance Evaluation," October 2016.

20K.14 ASME Code Case N-841, "Exemptions to Mandatory PWHT of SA-738 Grade B for Class MC Applications."

20K.15 Westinghouse Report APP-GW-C1-001, Rev. 3, "AP1000 Civil/Structural Design Criteria," February 2015.

Table 20K-1. Containment Vessel Materials (Reference 20K.3)

Component	Material
Pressure boundary	ASME SA-738, Grade B carbon steel plate
Equipment hatch	ASME SA-738
Personnel airlock	ASME SA-516
Carbon steel forgings	ASME SA-350
Stainless steel forgings	ASME SA-182
Carbon steel pipe penetration sleeves	ASME SA-333 or ASME SA-738
Non-carbon steel pipe penetrations	ASME SA-312
Carbon steel bolting	ASME SA-193 Impact tested in accordance with ASME SA-320
Carbon steel nuts	ASME SA-194 Impact tested in accordance with ASME SA-320
Welding materials	Supplier selected to conform to ASME requirements

Table 20K-2. General Design Characteristics (Reference 20K.3)

Condition	Parameter
General Design Characteristics	Nominal Inside Diameter: 39.624 metres (130 ft) Nominal Inside Height: 65.634 metres (215.33 ft) Design Code: ASME III, Division 1, Subsection NE Material: SA-738, Grade B; also conforming to the requirements of specification SA-1 and SA-20 Design Pressure (internal): 0.407 MPa (59 psi) (gauge) at the internal design temperature Design Temperature (internal): 149°C (300°F) Design External Pressure: 0.012 MPa (1.7 psi) design differential at 21°C (70°F) Long Term Accident Pressure: 0.16 MPa (23 psi) (gauge) Long Term Accident Temperature: 110°C (230°F)
Normal Operation	Internal temperature = 10°C to 49°C (50°F to 120°F) External temperature = -40°C to 46°C (-40°F to 115°F) Internal Pressure = -1.4 kPa to +6.9 kPa (-0.2 psig to 1 psig) Humidity = 0 to 100% Radiation[1] = 4.5×10^{-1} rad/hr Gamma Dose Rate 2.4×10^{5} rads-air 60 year Gamma Dose
Abnormal Operation (short term = 4 hrs.)	Internal Temperature = 10°C to 66°C (50°F to 150°F) Pressure = atmospheric Humidity = 100% Radiation[1] = 4.5×10^{-1} rad/hr Gamma Dose Rate 2.4×10^{5} rads-air 60 year Gamma Dose
Abnormal Operation (long term = 30 days)	Internal Temperature = 10°C to 121°C (50°F to 250°F) Pressure = 124 kPa (18 psig) Humidity = 100% Radiation[1] = 4.5×10^{-1} rad/hr Gamma Dose Rate 2.4×10^{5} rads-air 60 year Gamma Dose
Accident	Internal Peak Temperature = 216.7°C (422°F) Maximum vessel temperature = 149°C (300°F) Pressure = 407 kPa (59.0 psig) Humidity = 100% Radiation[1] = 1.2×10^{6} rads-air/hr Peak Gamma Dose Rate 6.7×10^{6} rads-air/hr Peak Beta Dose Rate

Note:

1. Location of radiation measurement is outside RCS loop compartment walls.

Table 20K-3. Summary of Containment Vessel Models and Analysis Methods

Model	Analysis Method	Program	Purpose
Axisymmetric shell	Modal analysis	ANSYS	To calculate frequencies and mode shapes for comparison against stick model
Lumped mass stick model	Modal analysis	ANSYS	To create equivalent stick model for use in nuclear island seismic analyses
Axisymmetric shell	Static analyses using Fourier harmonic loads	ANSYS	To calculate containment vessel shell stresses
Axisymmetric shell	Nonlinear bifurcation	BOSOR5	To calculate buckling capacity close to base under thermal loads To calculate pressure capacity of top head
Finite element shell	Linear bifurcation	ANSYS	To study local effect of large penetrations and embedment on buckling capacity for axial and external pressure loads
Finite element shell	Modal analysis	ANSYS	To calculate frequencies and mode shapes for local effects of equipment hatches and personnel airlocks
Finite element shell	Static analyses	ANSYS	To calculate local shell stress in vicinity of the equipment hatches and personnel airlocks

Table 20K-4. Load Combinations and Service Limits for Containment Vessel (Reference 20K.3)

Load Description	Service Limit Design Cases[1,2]										
	Const	**Test**	**Des1**	**Des2**	**A1**	**A2**	**A3**	**C1**	**C2**	**D1**	**D2**
Dead, D	X	X	X	X	X	X	X	X	X	X	X
Live, L	X	X	X	X	X	X	X	X	X	X	X
Wind[(5)], W	X						X				
SS earthquake, E_s								X		X	X
Tornado, W_t									X		
Test pressure, P_t		X									
Test temperature, T_t		X									
Operating pressure, P_o							X		X		
Design pressure, P_d			X			X		X			X
Design external pressure, P_e				X	X					X	
Normal reaction, R_o				X	X		X		X	X	
Normal thermal[(4)], T_o				X	X		(3)		(3)	X	
Accident thermal reactions, R_a			X			X		X			X
Accident thermal, T_a			X			X		X			X
Accident pipe reactions, Y_r											X
Jet impingement, Y_j											X
Pipe impact, Y_m											X

Notes:

1. Service limit levels are per ASME-NE.
2. Where any load reduces the effects of other loads, that load is to be taken as zero, unless it can be demonstrated that the load is always present or occurs simultaneously with the other loads.
3. Temperature of vessel is 21°C (70°F).
4. Temperature distribution for normal operation in cold weather.
5. Wind load for the construction load combination is based on a 31.29 m/s (70 mph) wind. Wind load for the Service Level A load combination is analysed as a reduction in external pressure.

Table 20K-5. Containment Vessel Metal Temperatures (Reference 20K.3)

Location	Case 1 Metal Temperatures °C (°F) Normal Operation in Cold Weather of -40°C (-40°F) Ambient.	Case 2 Metal Temperatures °C (°F) Design Basis Accident in Hot Weather of 46°C (115°F) Ambient.
Vessel shell above elevation 109.677 m (131 ft – 9 in)	-28[1] (-18.5)	149 (300)
Crane girder and inner stiffener[2]	21 (70)	149 (300)
Upper equipment hatch and upper personnel airlock insulated enclosure region.	See Figure 10 of Reference 20K.3.	149 (300)
Outer stiffener at elevation 109.677 m (131 ft – 9 in) [3]	-28 (-18.5)	149 (300)
Vessel shell at elevation 109.677 m (131 ft – 9 in) to 102.184 m (107 ft-2 in)[2]	21 (70)	149 (300)
Vessel shell from elevation 102.184 m (107 ft-2 in) to elevation 100 m (100 ft) (Linear Profile)	21 (70)	149 to 21 (300 to 70)
Vessel embedded below elevation 100 m (100 ft)	21 (70)	21 (70)

Notes:

1. For Case 1, -28°C (-18.5°F) is conservative and bounding.
2. These components are conservatively assumed to be at the CV inside air temperature. For the crane girder and inner stiffener, there is a step change at the CV shell to the CV shell temperature.
3. Outer stiffener is assumed to be at the CV shell temperature above the stiffener, except that all outer stiffener gussets inside or outside of the insulated enclosure are at 21°C (70°F).

Table 20K-6. Containment Vessel Pressure Capabilities

Containment Element		Pressure Capability (SI units)				
		Deterministic Severe Accident Capacity[1]			Maximum Pressure Capability[2]	
Temperature		37.78°C	148.89°C	204.44°C	37.78°C	204.44°C
Cylinder		0.931 MPa gauge	0.807 MPa gauge	0.772 MPa gauge	1.069 MPa gauge	0.889 MPa gauge
Ellipsoidal Head		0.717 MPa gauge	0.627 MPa gauge	0.600 MPa gauge	1.200 MPa gauge	0.993 MPa gauge
16-foot equipment hatch	F.S. = 1.67	0.869 MPa gauge	0.834 MPa gauge	0.814 MPa gauge	1.448 MPa gauge	1.365 MPa gauge
	F.S. = 2.50	0.579 MPa gauge	0.558 MPa gauge	0.545 MPa gauge		
Personnel airlocks[3]		>1.124 MP a gauge	>1.124 MPa gauge	>1.124 MPa gauge	>2.068 MPa gauge	>2.068 MPa gauge

Containment Element		Pressure Capability (US customary units)				
		Deterministic Severe Accident Capacity[1]			Maximum Pressure Capability[2]	
Temperature		100°F	300°F	400°F	100°F	400°F
Cylinder		135 psig	117 psig	112 psig	155 psig	129 psig
Ellipsoidal Head		104 psig	91 psig	87 psig	174 psig	144 psig
4.9 m equipment hatch	F.S. = 1.67	126 psig	121 psig	118 psig	210 psig	198 psig
	F.S. = 2.50	84 psig	81 psig	79 psig		
Personnel airlocks[3]		>163 psig	> 163 psig	>163 psig	>300 psig	>300 psig

Notes:

1. The buckling capacity for internal pressure of the ellipsoidal head is taken as 60 % of the critical buckling pressure calculated by nonlinear analyses; the buckling capacity at higher temperatures is calculated by reducing the capacity at 37.78°C (100°F) by the ratio of yield at 37.78°C (100°F) to yield at the higher temperature. Evaluations of the equipment hatch covers are shown both for ASME paragraph NE-3222 (F.S. = 2.50) and Code Case N-284-1 (F.S. = 1.67). Evaluations of the other elements are according to ASME Service Level C.
2. The estimated maximum pressure capability is based on minimum specified material properties.
3. The capacities of the personnel airlocks are estimated from test results.

Table 20K-7. Containment Vessel Technical Index

Document Reference	Title	Description
General Documents		
APP-GW-C1-001	Civil/Structural Design Criteria	Presents the general requirements and guidelines to be used in the design of structures for the AP1000 plant.
APP-GW-G1-003	Seismic Design Criteria	Defines the seismic design criteria that will be used for the AP1000 plant.
APP-CNS-M3-001	AP1000 Containment System – System Specification Document	Identifies the specific design requirements for the Containment System and documents the method of satisfactorily meeting those requirements.
APP-MV50-Z0-001	Containment Vessel Design Specification	Specifies the complete design, furnishing and fabrication, delivery, unloading and hauling, storing, site fabrication of large subassemblies, erection, shop prime coat painting, field coating, epoxy top coating, testing, and inspection of the containment vessel.
APP-EY01-Z0-001	Electrical Penetration Assemblies	Covers the technical and general requirements for the design, fabrication, welding and related testing of the electrical penetration assemblies.
APP-FT01-Z0-001	AP1000 Fuel Transfer Tube, ASME Boiler and Pressure Vessel Code Section III, Subsection NE, Class MC	Establishes the requirements for the design, material, fabrication, examination, testing, cleaning, packaging, preparation for shipment, quality assurance, inspection and delivery of the fuel transfer tube.
APP-ML10-Z0-002	Containment Piping Penetrations with Flued Heads Design Specification	Covers the design, fabrication, testing, inspection, examination, certification, cleaning, painting, finishing, packaging and delivery of the flued heads for containment vessel mechanical penetration assemblies.
APP-ML10-Z0-004	AP1000 CV – MS and FW Bellows Expansion Joints Design Specification	Covers the design, fabrication, testing, inspection, examination, ASME Code stamping, certification, cleaning, coating, finishing, packaging and delivery of universal expansion joints for the containment vessel main steam and feedwater mechanical penetrations.
APP-MV50-Z0-002	AP1000 Containment Vessel Equipment Hatch	Covers the complete design, furnishing and fabrication, shop prime coat painting, shop finish painting, testing, inspection, ASME Code stamping and delivery of equipment hatches.

Table 20K-7. Containment Vessel Technical Index (cont.)

Document Reference	Title	Description
General Documents		
APP-MV50-Z0-003	AP1000 Personnel Airlocks	Covers the complete design, furnishing and fabrication, shop prime coat painting, shop finish painting, testing, inspection, ASME Code stamping and delivery of personnel airlocks.
APP-MT05-Z0-001	AP1000 PCS Water Distribution Weirs System	Establishes the basis for the materials, design, furnishing and fabrication, inspection, shop prime coat painting, packing, preparation for shipment, storing, installation of the weirs located on the CV upper head.
APP-CC01-Z0-026	Design Specification for Safety Related Mixing and Delivering Concrete, Westinghouse Safety Class C "Nuclear Safety Related"	Covers the technical and quality assurance requirements associated with the furnishing of all materials, labor, equipment (except as otherwise noted), and services required for receiving and stockpiling material, batching, mixing and transporting the required nuclear safety related concrete and grout to the delivery point.
APP-GW-Z0-602	AP1000 Cleaning and Cleanliness Requirements of Equipment for use in Nuclear Supply and Associated Systems	Defines the general cleaning requirements for components in the AP1000 plant during fabrication of components and installation of equipment.
APP-GW-Z0-604	Application of Protective Coatings to Systems, Structures and Components for the AP1000 Reactor Plant	Provides direction for surface preparation, coating procurement and application of protective coating work to be performed for the CV.
UKP-MV50-S2C-036	AP1000® Containment Vessel Top Head Fracture Analysis due to PCS Flow Actuation	Documents an investigation of the fracture behaviour of the CV top head in the event of PCS water flow.
APP-1000-S2C-056	Nuclear Island Seismic Floor Response Spectra	Develops enveloping design floor response spectra for use in analyses for piping and equipment design.
APP-MV50-GEC-001	Verification of AP1000 Containment Vessel not Requiring Analysis for Cyclic Service Report	Documents an analysis demonstrating the CV meets the conditions of ASME Code, Section III, Subsection NE, Paragraph NE-3221.5(d) excepting the CV from analysis for cyclic service.

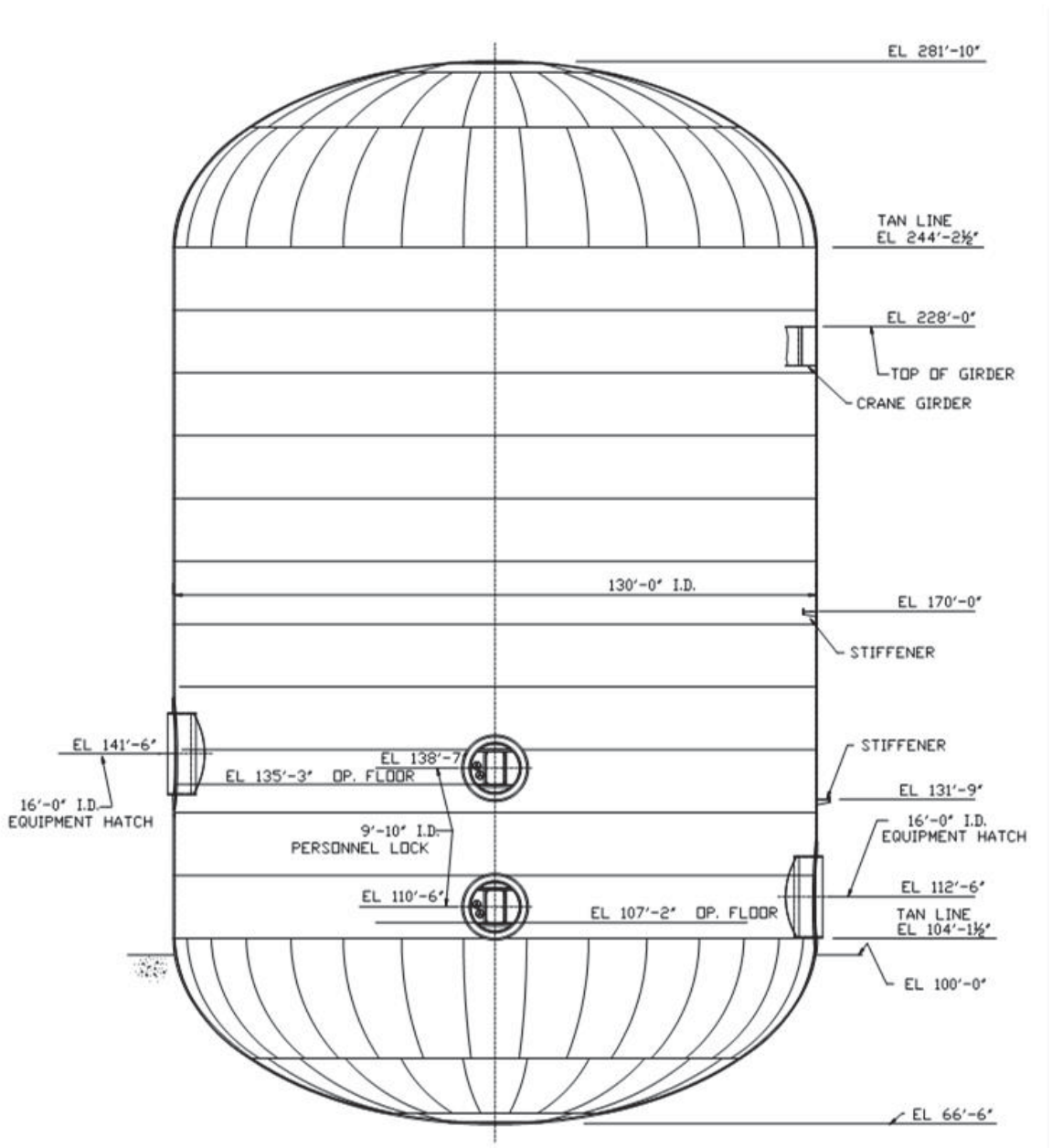


Figure 20K-1. Containment Vessel General Outline*

*Note: Course layout, plate/insert plate geometry, and weld seams are shown for illustrative purposes only. Final, constructed layout may differ.

Figure 20K-2. Not Used.

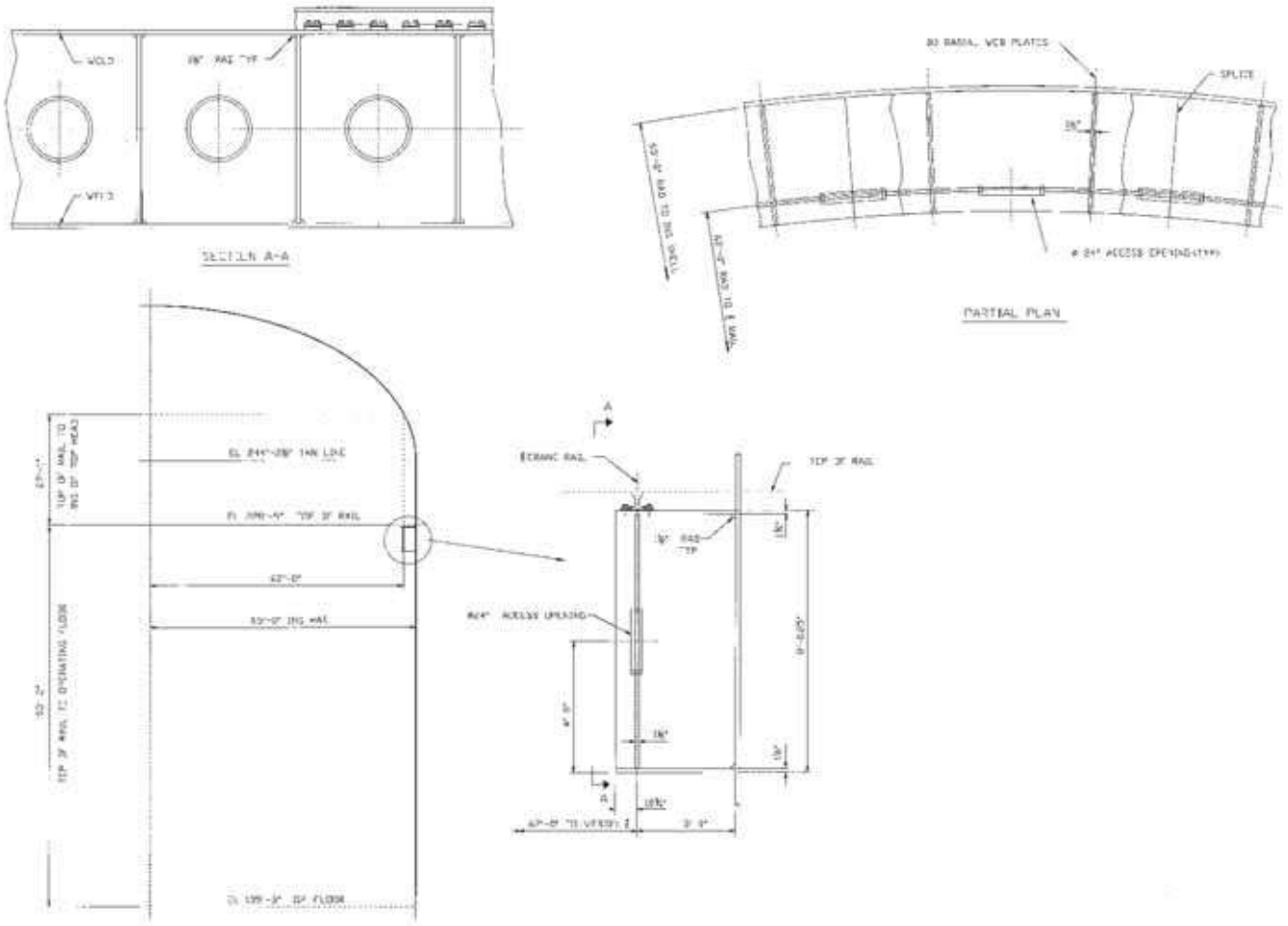


Figure 20K-3. Polar Crane Support Structure

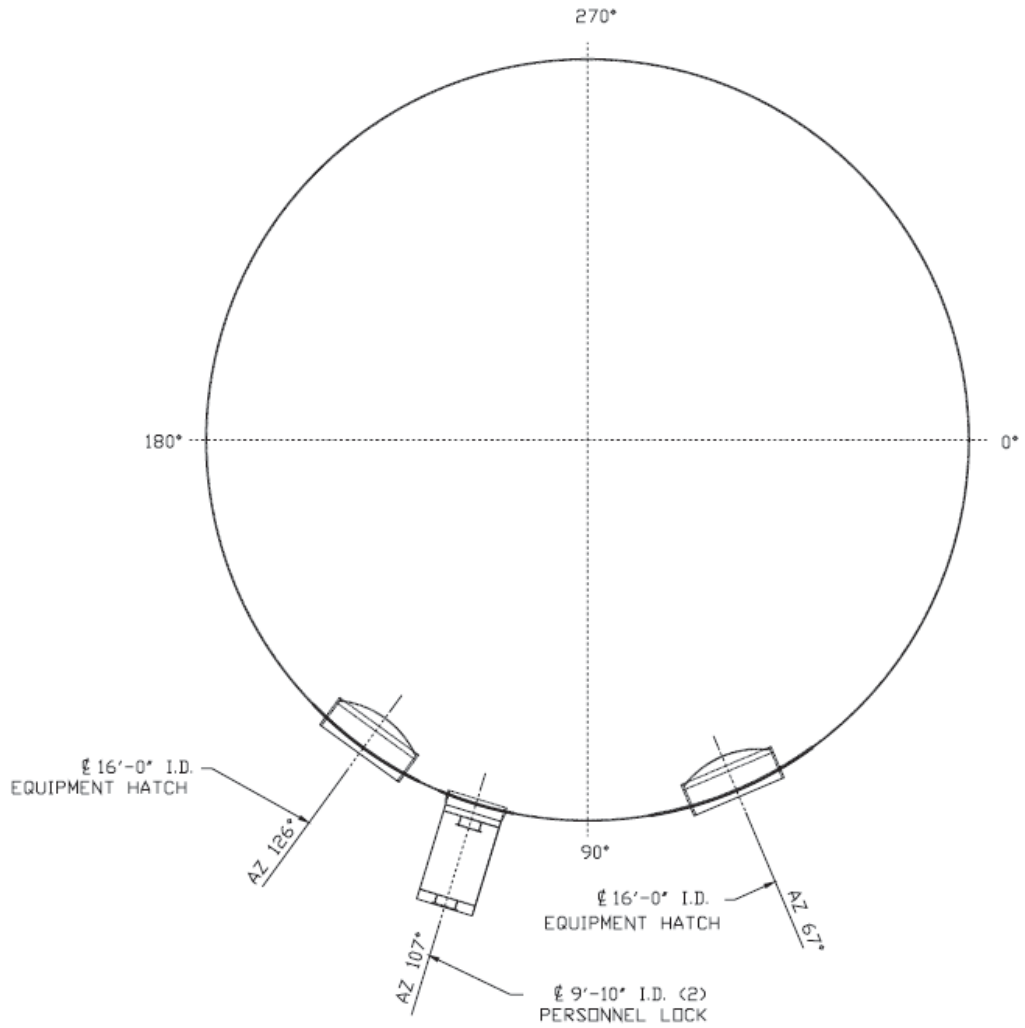


Figure 20K-4. Orientation of Major Penetrations

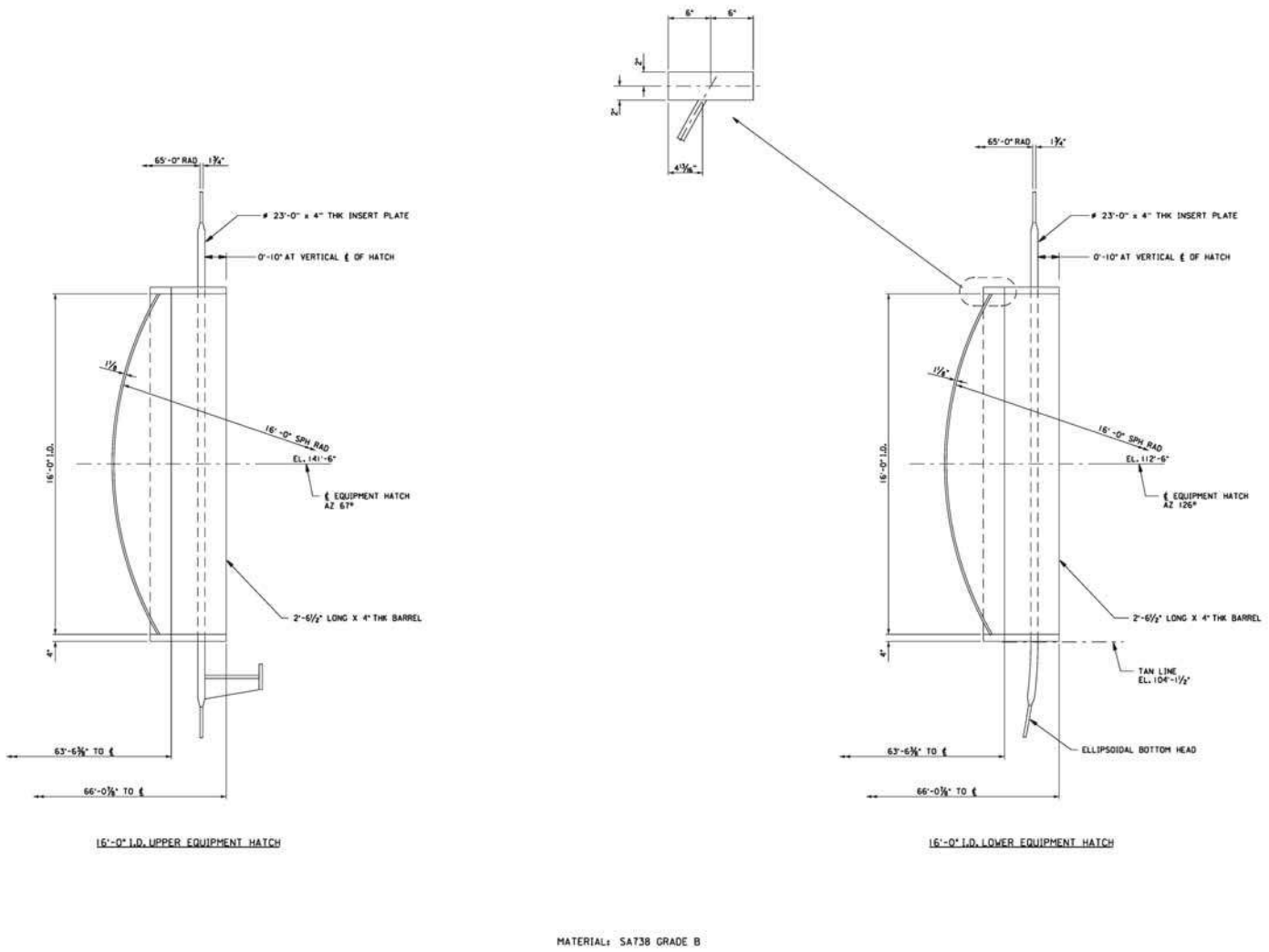


Figure 20K-5. Equipment Hatches

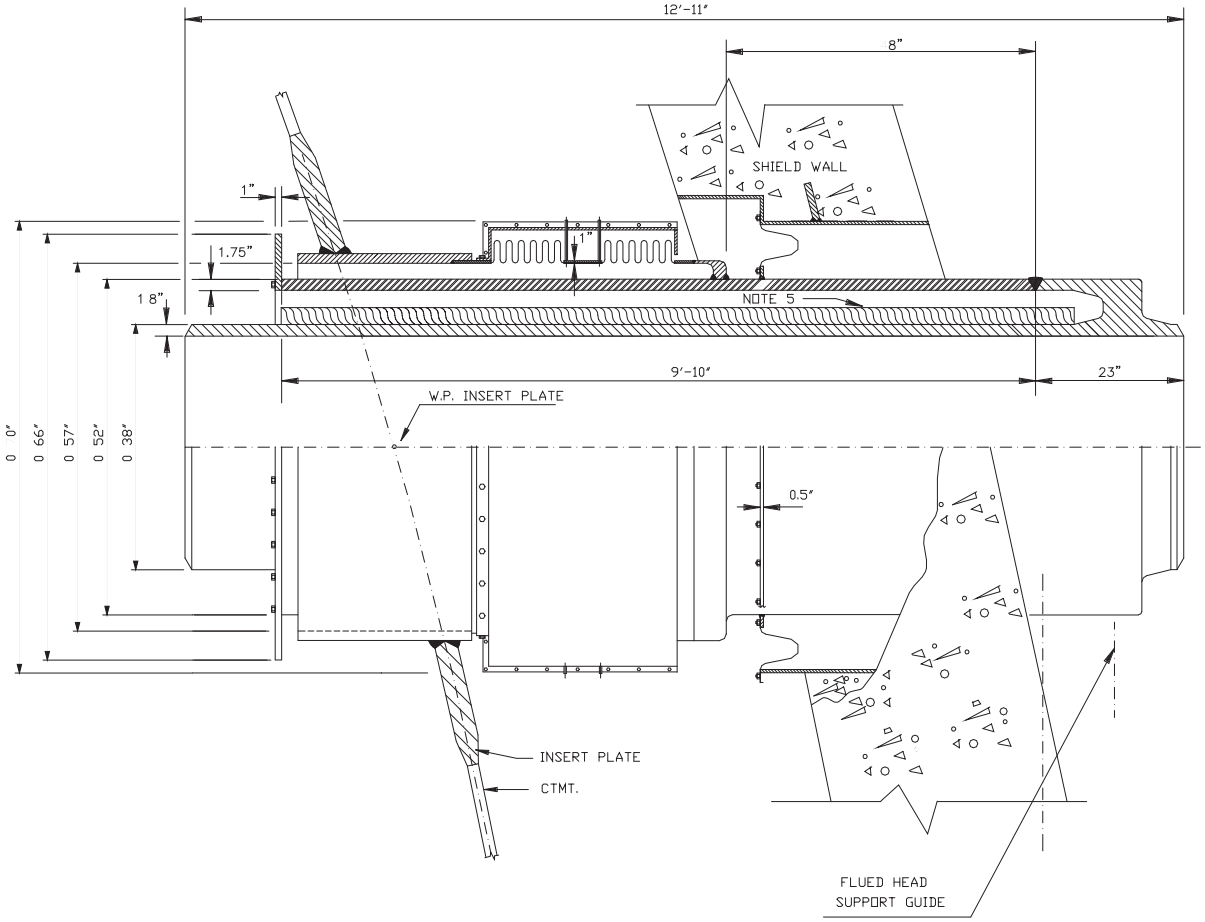


Figure 20K-6. Containment Penetrations (Sheet 1 of 7) – Main Steam

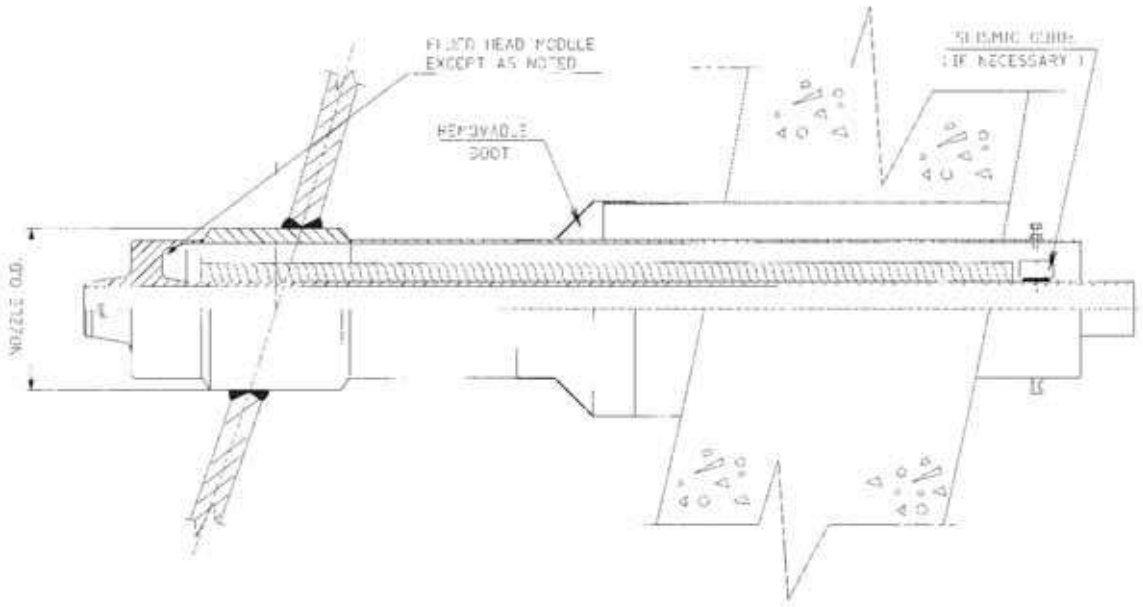


Figure 20K-6. Containment Penetrations (Sheet 2 of 7) – Startup Feedwater

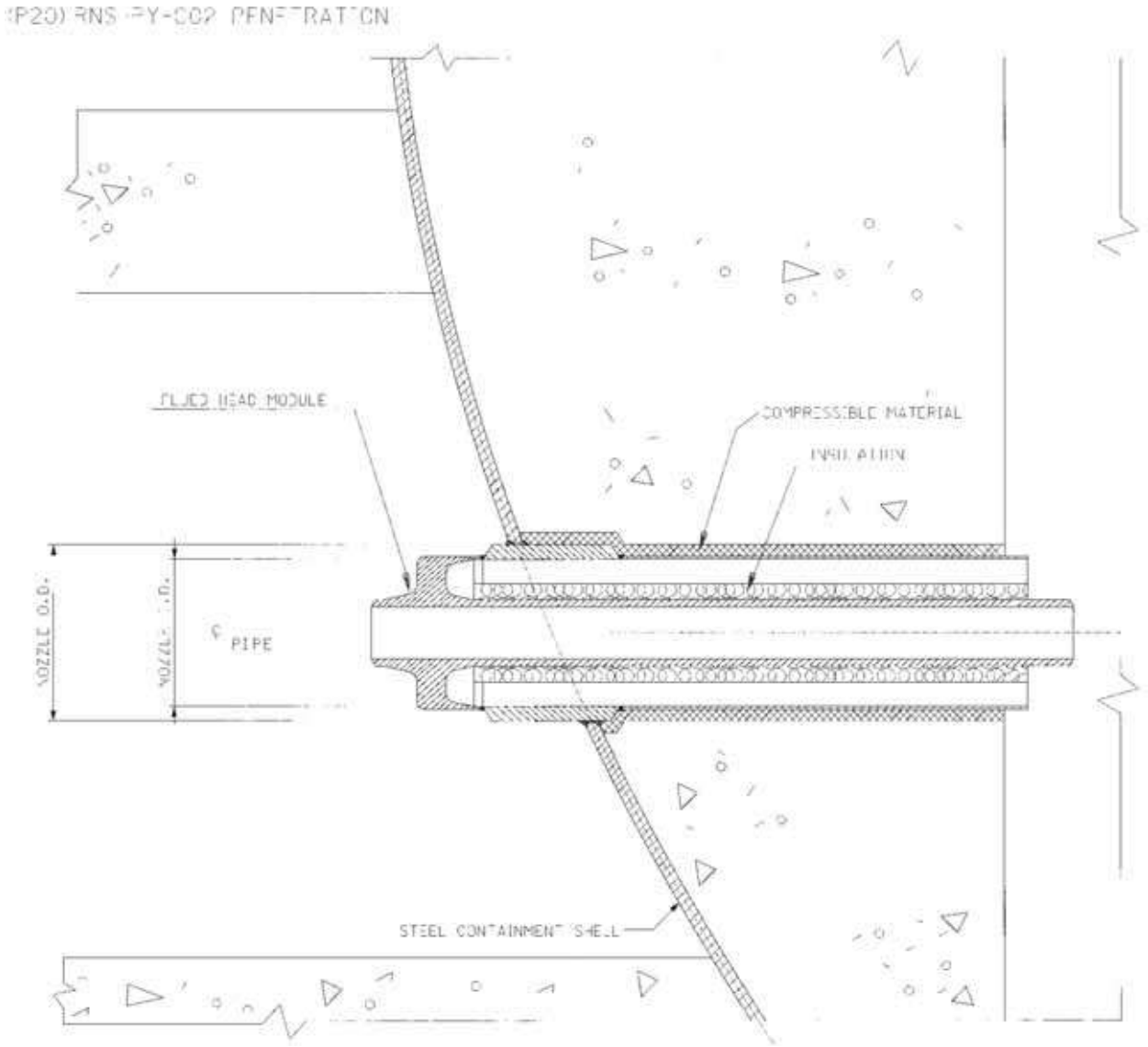


Figure 20K-6. Containment Penetrations (Sheet 3 of 7) – Normal RHR Piping

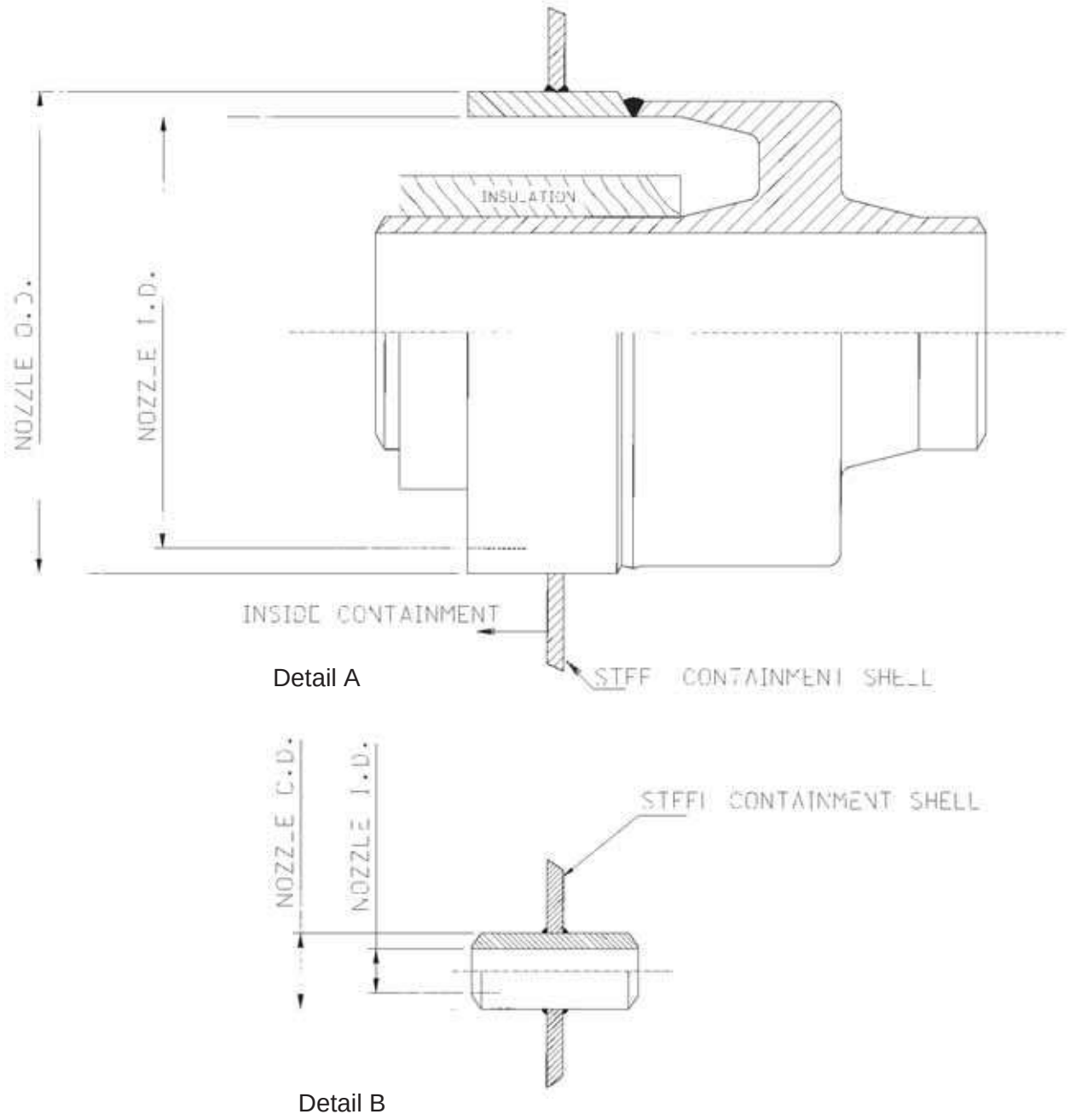


Figure 20K-6. Containment Penetrations (Sheet 4 of 7)

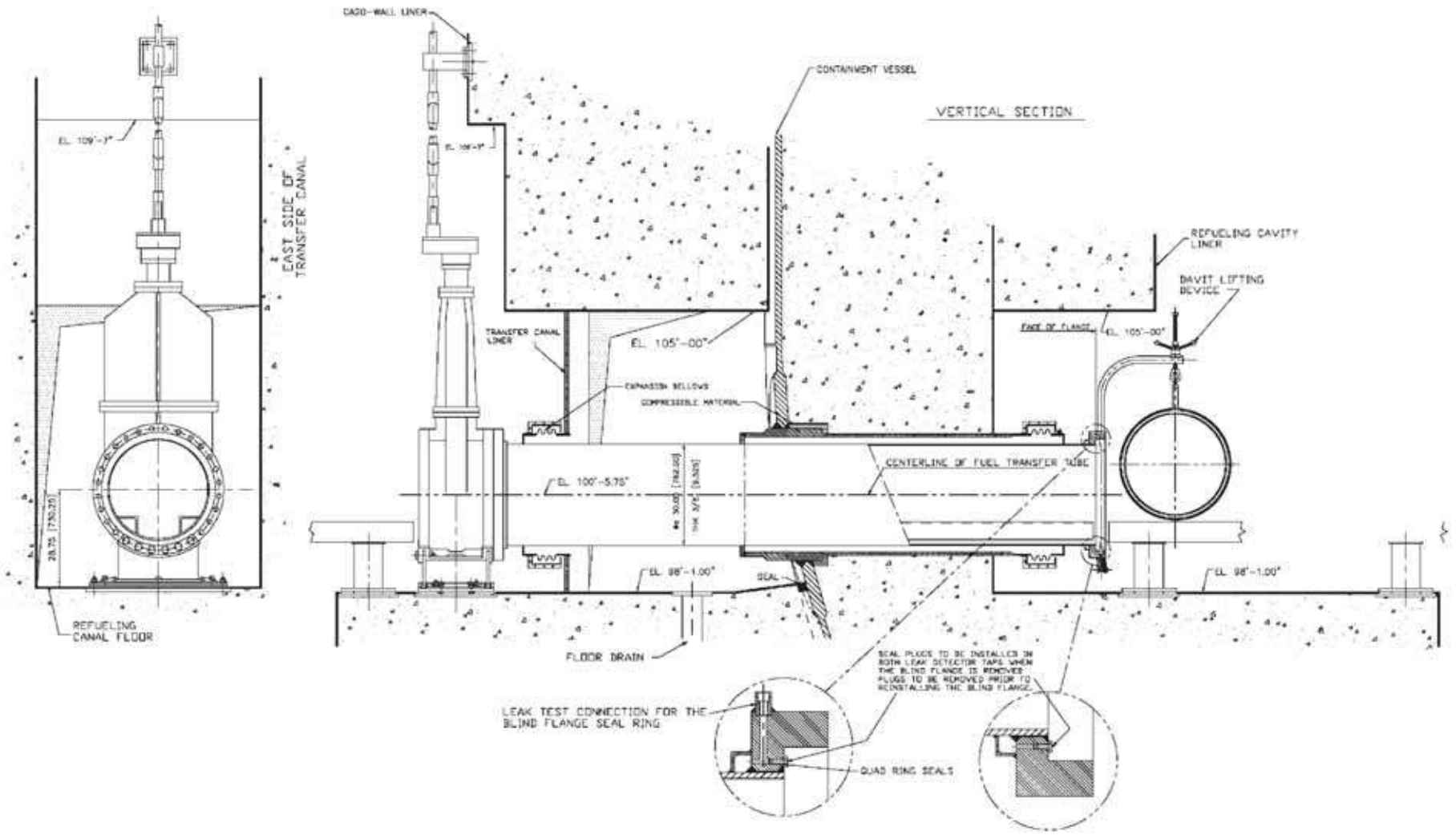


Figure 20K-6. Containment Penetrations (Sheet 5 of 7) – Fuel Transfer Penetration

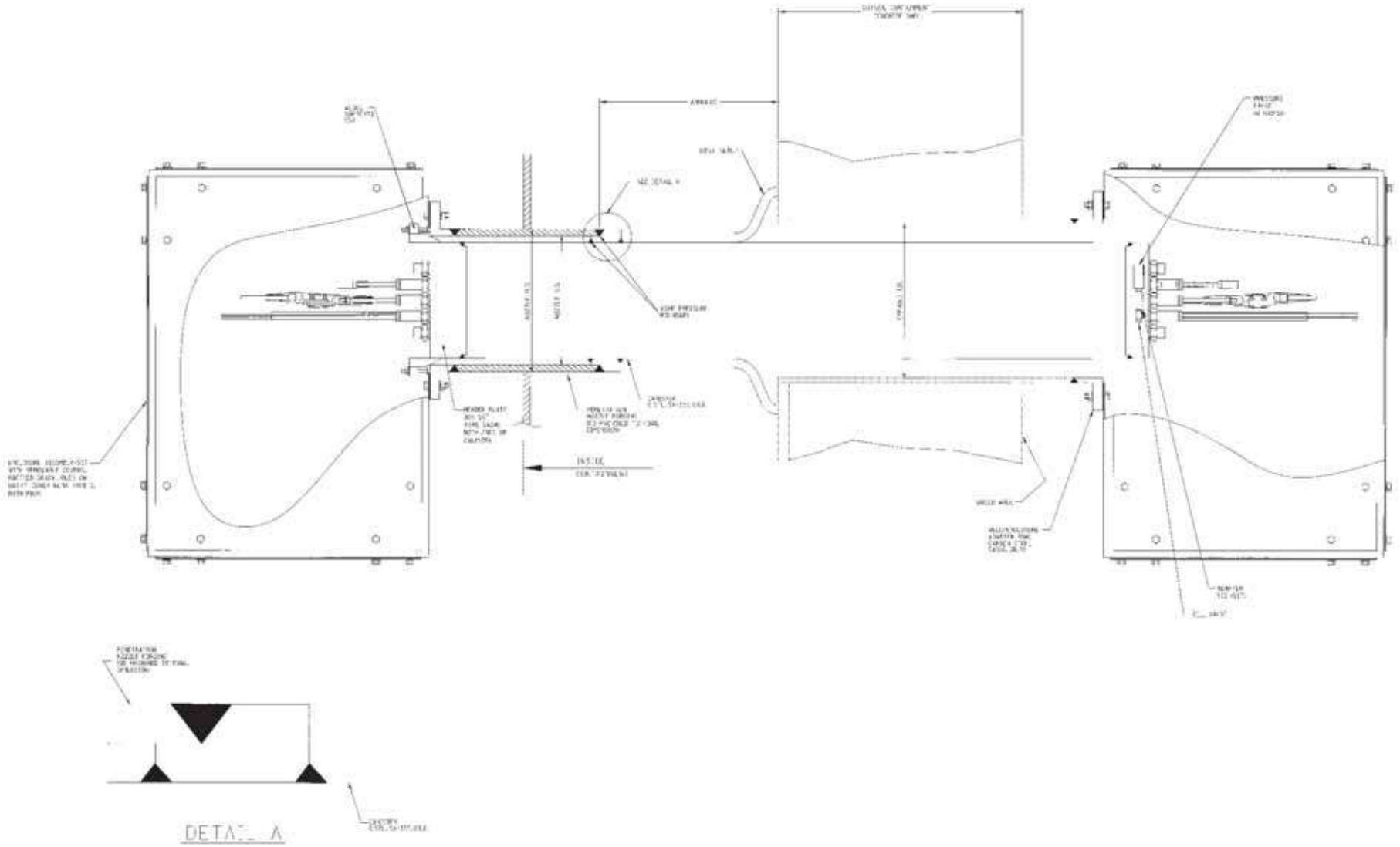


Figure 20K-6. Containment Penetrations (Sheet 6 of 7) – Typical Electrical Penetration

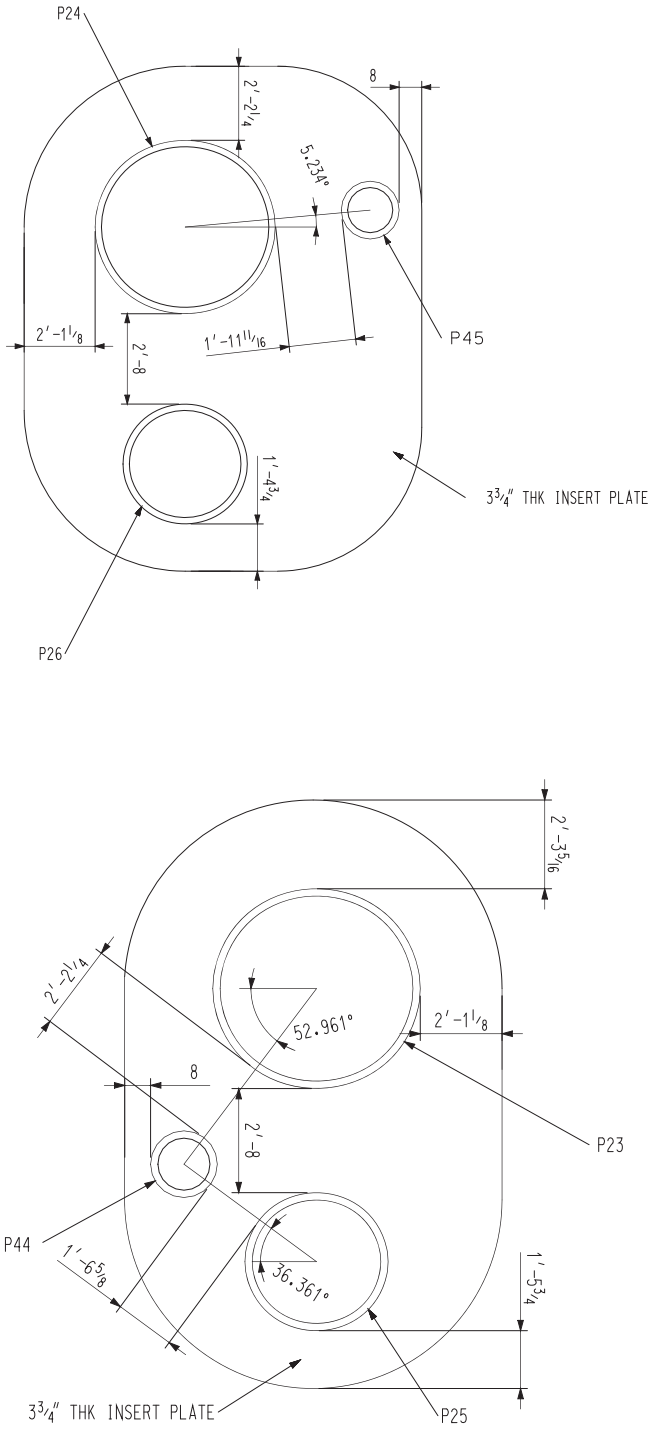


Figure 20K-6. Containment Penetrations (Sheet 7 of 7) – Steam and Feedwater Line Insert Plates

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS, ACRONYMS, AND TRADEMARKS

ac	alternating current
ADS	automatic depressurisation system
AISI	American Iron and Steel Institute
ALARP	as low as reasonably practicable
AO	axial offset
AOA	axial offset anomaly
ASS	auxiliary steam supply system
ASTM	American Society for Testing and Materials
AVT	all-volatile treatment
BA	burnable absorber
BAST	boric acid storage tank
BDS	steam generator blowdown system
BSL	basic safety level
CAS	compressed air system
CASS	cast austenitic stainless steel
CCS	component cooling water system
CDS	condensate system
CERT	constant extension rate test
CF	cartridge filtration
CFS	turbine island chemical feed system
CGR	crack growth rate
CILC	crud-induced localised corrosion
CIPS	crud-induced power shift
CLP	cask loading pit
CMT	core makeup tank
CORS	catalytic oxygen reduction unit
CPS	condensate polishing system
CRDM	control rod drive mechanism
CST	condensate storage tank
CVS	chemical and volume control system
CWS	circulating water system
dc	direct current
DCPD	direct current potential difference
DTS	demineralised water treatment system
DVI	direct vessel injection
DWS	demineralised water transfer and storage system
DWST	demineralised water storage tank
ECP	electrochemical potential
EDI	electrodeionisation
EDS	standby electrical supply system
EHT	effluent holdup tank
EPRI	Electric Power Research Institute
FAC	flow-assisted corrosion
GE-GRC	General Electric-Global Research Center
HAZ	heat-affected zone
HDPE	high-density polyethylene
HFT	hot functional testing

LIST OF ABBREVIATIONS ACRONYMS, AND TRADEMARKS (cont.)

HP	high pressure
HT	high-temperature
HVAC	heating, ventilation, and air conditioning
HX	heat exchanger
ID	inside diameter
IGA	intergranular attack
IGSCC	intergranular stress corrosion cracking
IRWST	in-containment refuelling water storage tank
LAS	low-alloy steel
LOCA	loss-of-coolant accident
LWR	light water reactor
MA	mill-annealed
MB	non-regenerable mixed bed exchanger
MCR	main control room
MRP	Materials Reliability Programme
MSR	moisture separator reheater
MSS	main steam system
NUREG	Nuclear Regulatory Commission technical report designation
OD	outside diameter
ODSCC	outer diameter stress corrosion cracking
ORE	occupational radiation exposure
ORP	oxidation reduction potential
PAD	performance and analysis design
PAR	passive autocatalytic recombiner
PCCAWST	passive containment cooling ancillary water storage tank
PCCWST	passive containment cooling water storage tank
PCI	pellet-clad interaction
PCS	passive containment cooling system
PCSR	Pre-Construction Safety Report
PGS	plant gas system
pH_T	pH at temperature
PRHR	passive residual heat removal
PSS	primary sampling system
PWR	pressurised water reactor
PWSCC	primary water stress corrosion cracking
PXS	passive core cooling system
RCDT	reactor coolant drain tank
RCP	reactor coolant pump
RCPB	reactor coolant pressure boundary
RCS	reactor coolant system
RMCS	reactor makeup control system
RNS	normal residual heat removal system
RO	reverse osmosis
RPV	reactor pressure vessel
RTD	resistance temperature detectors
RVI	reactor vessel internals
RWS	raw water system
SCC	stress corrosion cracking
SFAIRP	so far as is reasonably practicable

LIST OF ABBREVIATIONS ACRONYMS, AND TRADEMARKS (cont.)

SFP	spent fuel pool
SFS	spent fuel pool cooling system
SG	steam generator
SGS	steam generator system
SGTR	steam generator tube rupture
SSD	system specification document
SSRT	slow strain rate tensile test
SSS	secondary sampling system
STP	standard temperature and pressure
SWS	service water system
Tech Spec	Technical Specification
TGSCC	transgranular stress corrosion cracking
TSP	trisodium phosphate
TT	thermally treated
TTS	top of tube sheet
UV	ultraviolet germicidal irradiation
VFD	variable frequency drive
VLS	containment hydrogen control system
WGS	gaseous radwaste system
WLS	liquid radwaste system
WSS	solid radwaste system
WWS	waste water system
ZIRLO	zirconium alloy

TRADEMARKS

Inconel is a registered trademark of Special Metals Corporation.

Metamic is a registered trademark of Metamic, LLC.

Stellite is a registered trademark of Deloro Stellite Company.

21 REACTOR CHEMISTRY

21.1 Introduction

This chapter describes the application of chemical controls and treatments in the AP1000 plant design. It provides outline descriptions for a number of systems in the AP1000 design that contain fluids essential to their functions, including heat transfer and control of core reactivity. The quality of these fluids and their interactions with system components and materials can have a substantial impact on the reliable and safe operation of the individual systems. Chemical additives are employed to optimise the performance of the fluids and minimise potential negative effects such as corrosion of materials of construction. Chemical additives are also used to mitigate the impact of various accident and fault conditions.

The AP1000 plant is designed to operate safely within the Electric Power Research Institute (EPRI) chemistry guidelines (References 21.2, 21.3, and 21.4), AP1000 plant-specific chemistry operating specifications, and the AP1000 Chemistry Manual guidance (References 21.5 and 21.6) as discussed in the rest of this chapter. The EPRI guidelines are developed and continually updated from accumulated industry-wide research and pressurised water reactor (PWR) operating experience. As such, these guidelines provide an authoritative best-practice operations envelope for the AP1000 plant subject to the modifications necessary to address unique AP1000 design features. The effects of these unique AP1000 design features are addressed in the AP1000 Chemistry Manual and in Westinghouse supplement to the EPRI chemistry guidelines; however, the detailed operational chemistry control strategy will be the responsibility of the plant operator, who may choose to vary and optimise the operating parameters within the bounds of the plant- and site-specific operating safety case. Limits and conditions for chemistry are described in Section 5.6.

21.2 Objectives

The chemistry of important systems in the AP1000 plant is described in this chapter. This description includes chemistry control, its impact on reactor safety, and the factors influencing its specification.

21.3 Approach

The chemistry functions in the AP1000 plant are dealt with under three headings: primary system, secondary system, and auxiliary systems. The essential safety requirements of the chemistry in each system are identified. The various physical systems and their design basis functions are described briefly. The technical background to the main chemistry functions are discussed in each case to provide an understanding of the main issues involved. This approach also provides evidence to justify arguments that the safety functions of the chemistry have been met. Compliance with the chemistry safety requirements is demonstrated for each operational mode of the AP1000 plant. This includes a description of the chemistry strategy and the standards that are applied.

The chemical aspects of accident scenarios, the potential hazards and the hazard mitigation measures, are then discussed. Arguments are presented detailing how the chemistry strategy in such situations supports the overall safety claims of the plant.

21.4 Safety Requirements

The AP1000 design is much simpler than previous PWR designs and enhances safety by virtue of the reduced number of components and provides economic benefits through simplified construction and reduced operation costs. The design utilises passive safety systems that rely on simple natural processes. The safety of the design is based on adherence to a number of inviolate principles given in Chapter 1.

Adherence to these principles is achieved by defining what safety function is required during normal modes of operation and in response to design basis events. This chapter discusses the reactor chemistry and chemistry control systems that support these functions, for example, by aiding control of core reactivity; ensuring the integrity of the pressure boundary; and optimising the quantities, distribution, and containment of radioactive materials.

21.5 Primary Circuit

This section describes the systems used to maintain and monitor the chemical properties of primary reactor coolant. The interfacing systems whose performance depends on the maintenance of the chemical environment are described in Section 21.7.

The following systems are covered:

- Primary circuit
- Primary sampling system (PSS)
- Chemical and volume control system (CVS)

21.5.1 Description of the Primary Circuit

The primary circuit comprises the reactor core and coolant system, including the reactor pressure vessel (RPV), steam generators (SGs), pressuriser, cold and hot leg pipework, and reactor coolant pumps (RCPs). A description of the major components of the primary circuit is given in Sections 6.4 and 6.5.

The boundary of the system, for the purposes of assessing chemistry influences on containment of radioactive material, can be taken as the limits of the reactor coolant pressure boundary. This includes the vessels, piping, pumps, and valves that are part of the reactor coolant system (RCS); or that are connected to it up to and including the following:

- The outermost containment isolation valve in system piping that penetrates the containment. The second of two valves closed during normal operation in system piping that does not penetrate containment.

- The RCS overpressure protection valves. The RCS pressure boundary provides a barrier against the release of radioactivity generated within the reactor and is designed to provide a high degree of integrity throughout the operation of the plant.

The RCS is also served by a number of auxiliary systems, including the passive core cooling system (PXS), normal residual heat removal system (RNS), steam generator system (SGS), PSS, liquid radwaste system (WLS), and component cooling water system (CCS).

21.5.2 Functions of the Primary Circuit Related to Chemistry

The primary circuit design basis functions related to chemistry are as follows:

- The RCS provides the water used as the core neutron moderator and reflector conserving thermal neutrons and improving neutron economy. The RCS also provides the water used as a solvent for the neutron absorber used in chemical shim reactivity control (boric acid).
- The RCS maintains the homogeneity of the soluble neutron poison absorber concentration and the rate of change of the coolant temperature so that uncontrolled reactivity changes do not occur.
- The pressuriser maintains the system pressure during operation and limits pressure transients. During the reduction or increase of plant load, the pressuriser accommodates volume changes in the reactor coolant.
- The SGs provide steam of the required quality to the turbine. The tubes and tube sheet boundary prevent the transfer of radioactivity generated within the core to the secondary system.
- The RCS contains the coolant under operating temperature and pressure conditions and limits leakage (and activity release) to the containment atmosphere.
- The RCS contains a solution of boric acid, lithium hydroxide (LiOH), and zinc; and is dosed with dissolved hydrogen. This solution is circulated at a flow rate and temperature consistent with achieving the reactor core thermal and hydraulic performance.
- The RPV head is connected to the head vent system.
- The pressuriser surge line and each loop spray line connected with the RCS are instrumented with resistance temperature detectors (RTDs) attached to the pipe to detect thermal stratification.

21.5.3 Primary Circuit Chemistry Safety Requirements

The safety requirements of the primary circuit chemistry are as follows:

- The primary circuit chemistry aids the control of reactivity of the core to within operating limits.
- The primary circuit chemistry assists in maintaining the integrity of the primary circuit and the fuel cladding.
- The primary circuit chemistry aims to minimise the slow buildup of radioactivity outside the core region by minimising the transport of corrosion products.

To achieve these safety requirements, a coolant chemistry control strategy aimed at maintaining chemical conditions in the primary circuit within specified ranges is adopted. This involves the monitoring and control of a number of chemistry parameters. A summary of the control parameters is given in the following sections, together with specified ranges (included or referred) and a brief justification for the adopted control. Most of the information given relates to operation in mode 1 (power operation). Further details of chemistry control during other operating modes are given in Section 21.8. Further arguments and evidence are given in later sections. A description of the control and monitoring of chemistry parameters through use of the PSS and CVS is given in Sections 21.5.7 and 21.5.8.

The AP1000 plant reactor coolant water chemistry specification is given in the AP1000 Chemistry Manual (Reference 21.5, Chapter 4). This chapter of the AP1000 Chemistry Manual and its references provide guidance for reactor coolant power operation control and diagnostic parameters. For control parameters, EPRI provides specific guidance on action levels, which are summarised in the AP1000 Chemistry Manual. However, it is noted that operating plants normally operate with site-specific administrative limits well below the EPRI action level guidelines and Westinghouse expects each plant to create site-specific administrative guidelines as a basis for operation. Safety limits for each parameter defined by the designers are also included in Table 21-5 for the parameters identified and discussed below.

21.5.4 Reactivity Control and Fuel Performance

21.5.4.1 Use of Boron

Safety Requirements

Boron (in the form of boric acid) dissolved in primary coolant is varied to control reactivity changes due to fuel burnup. The dissolved boron can also compensate for xenon burnout reactivity changes and maintain the reactor in the cold shutdown condition. Dissolved boron is used to establish the required shutdown margin under normal and accident conditions where a cooldown to ambient temperature is required.

During power operation, the AP1000 plant controls normal fluctuations in reactivity by the use of grey rods and not by adjustments in boron concentration as is the case with conventional PWRs. If load following is practiced, this is also done using grey rods. Please see Chapter 22 for further details, along with the safety evaluation performed for the PSS where these AP1000 plant differences are discussed in the context of boron monitoring requirements (Reference 21.72). Refer to Table 21-5 for safety limits applicable to boron in the primary circuit.

Technical Basis

Boron dissolved in the primary water is used as a chemical reactivity shim to regulate fission through absorption of neutrons. ^{10}B is an absorber of thermal neutrons, with the added advantage that the product is a transitory high-energy form of ^{11}B, which rapidly decays into ^{7}Li, with the emission of an alpha particle. ^{7}Li is already present in the coolant as a normal additive.

The concentration of boron within the primary water is varied throughout the operating range by the use of the CVS to control reactivity changes that occur relatively slowly, including the effects of burnup; fission product poisoning, including xenon and samarium; burnable absorber (BA) depletion; and the cold-to-operating temperature moderator change.

Boron concentration in the coolant is adjusted to allow maintenance of the desired control rod position, i.e., above the control rod insertion limits, to maintain the shutdown margin (see Section 22.6.2.12 for further details). Boron concentration in the coolant is adjusted to allow maintenance of the desired control rod positions and/or to maintain the reactor coolant average temperature in the operating band. Control rods are inserted or withdrawn to control or, as appropriate, to induce, relatively rapid reactivity changes.

Method of Control

The boron is added and removed in the form of a solution of boric acid mixed with demineralised water to the required concentration. The programmed pressurised level is maintained by removing coolant through the CVS letdown line if required. A dedicated tank is provided for boric acid supply via the CVS. The boron concentration is varied throughout a fuel cycle to maintain control rod position. The concentration of boron is varied during normal operations only to control reactivity changes that occur relatively slowly,principally to accomodate the effects of fuel burnup. The boron storage and dosing system are described in Section 21.5.8.3.

Other sources of water input to the RCS are also borated to avoid inadvertent dilutions, which could constitute an increases in reactivity. This includes the core makeup tanks (CMTs), accumulators, and in-containment refuelling water storage tank (IRWST). These other sources of water input are described in Section 21.7.3.1 under the PXS.

Monitoring

The boron concentration is monitored in accordance with the AP1000 plant Technical Specification (Tech Spec) (Reference 21.74) by grab-sampling through the PSS. During periods when reactivity may be changing more rapidly, such as startup or shutdowns, boron analysis will be performed much more frequently to ensure that large mismatches in boron concentration do not occur between different locations within the primary circuit. A boron concentration monitoring system is also provided within the PSS for monitoring and trending purposes.

Faults

Clearly, too high a concentration of boric acid will result in loss of reactivity More significantly, too low a boron concentration will result in an increase in core reactivity and potential loss of control. A number of automatic and manual systems are in place to deal with boron dilution faults. Analyses of effects and consequences in the following situations are given: refuelling, cold shutdown, safe shutdown, hot standby, startup, and full power operation. The impact of loss of external power as a consequence of a turbine trip is also considered. The description of the plant response when the reactor is in automatic and manual rod control, is discussed in Section 9.4.6.

Inadvertent dilution during refuelling is prevented by administrative controls that lock specified valves in the CVS during refuelling operations. This isolates the RCS and prevents any nonborated water from entering the system. In other scenarios, the rate of dilution is low enough to allow time for detection and operator or automatic intervention. In most cases, the source range nuclear instrumentation detects the rise in neutron flux. The protection and safety monitoring system automatically initiates valve movements to terminate the dilution flow and sounds an alarm.

During startup, the reactor is in manual control and the operator withdraws the control rods and dilutes the reactor coolant with nonborated water at controlled rates until criticality is achieved. Excessive or continued dilution due to an unknown source would lead to a more rapid power escalation, which would be mitigated by an automatic reactor trip. In the event of such a trip, the demineralised water transfer and storage system (DWS) is automatically isolated and the CVS pumps are realigned to draw water from the boric acid storage tank (BAST). More information on dilution during refuelling and startup is provided in Section 9.4.6.

21.5.4.2 Crud-Induced Power Shift and Crud-Induced Localised Corrosion

Crud-induced power shift (CIPS) or axial offset anomaly (AOA) can be described as a condition in which the difference in the relative power produced in the upper and lower parts of the core deviates from predicted values by more than 3 percent (Figure 21-1). The axial offset (AO) should be close to zero early in the fuel cycle and stay close to zero for plant normal operations. In some cases, however, the AO has been found to be negative near midcycle. CIPS or AOA is more common in high-duty cores with significant subcooled nucleate boiling and has been attributed to the buildup of boron and lithium-boron compounds on fuel elements in the upper part of the core. Where such localised boiling occurs, dissolved species may precipitate as crud deposits. These deposits may contain boric acid and lithium salts.

Crud-induced localised corrosion (CILC) can result where local crud deposits thicken to the point that liquid coolant is prevented from reaching the cladding surface so that only a steam layer forms near the cladding surface. The reduced heat transfer through the steam leads to an increased surface temperature and consequently higher oxidation rates, which can result in cladding failures.

Corrosion product transport management can aid in the mitigation of CIPS and CILC. Measures taken include material choices, surface finish, and better chemistry control (e.g., pH programme selection, adherence to latest industry guidance). Also, shutdown and restart strategies that optimise corrosion product removal are managed within the constraints of the outage schedule requirements. Crud formation and deposition are discussed in Section 21.5.10 in addition to chemistry practices that aid in mitigation. Nickel-rich crud, which has been associated with the occurrence of CIPS, is more difficult to remove by the current outage chemistry practices. However, outage chemistry regime is not meant to decontaminate the primary system, as the main goal is to prepare the system for opening it to the atmosphere for refuelling.

The AP1000 plant incorporates systems designed to minimise the risk of CIPS and CILC. Zinc addition is employed to lower the system corrosion rate and consequently aids in the mitigation of CIPS and CILC, along with the other systems used for maintenance of primary circuit integrity described in Section 21.5.5. Section 22.7.3 describes the AP1000 plant

specific analyses and consideration that have been performed on the overall risk and minimisation of CIPS and CILC.

21.5.5 Maintenance of Primary Circuit Integrity (Chemistry Control)

The maintenance of primary circuit integrity is achieved by controlling primary coolant chemistry in all reactor operating modes to minimise the risk of corrosion of the primary circuit, the core materials, or the fuel cladding. In practice this involves the following:

- Providing a high-quality demineralised water supply free from contaminants for coolant makeup and cleanup via the demineralised water treatment system (DTS) and CVS, respectively
- Controlling the pH at temperature (pH_T) (coordinated with the boric acid concentration) to within target limits (refer to Section 21.5.5.2 below).
- Maintaining low potential in the makeup water by deoxygenation via the DWS
- Removing oxidising species by dosing with controlled amount of hydrogen sufficient to maintain a hydrogen residual and low electrochemical potential
- Dosing with zinc to lower oxidation rates and to minimise corrosion product buildup on fuel (resulting in lower risk for CIPS and CILC)

Chemistry control is achieved largely through the CVS, which controls the following:

- Chemical additions to the coolant
- Maintenance of the reactor coolant lithium and boron concentration through dilution, addition, or demineralisation
- Purification of the coolant

Monitoring is achieved by chemical analysis of grab samples from the PSS. Additionally, online measurements for oxygen and hydrogen can be taken. The hydrogen concentration range selected for the AP1000 plant is consistent with current operating experience. The major components of the primary circuit are described briefly in Section 21.5.1 and the design basis functions are given in Section 21.5.2. For more detail, see Chapter 6. The functions of the CVS, in terms of maintaining chemical composition and removing any impurities, are presented in Section 21.5.8. A detailed consideration of the corrosion issues, the relevant chemistry factors, and the technical background to justify the primary circuit chemistry specification is given in Section 21.5.9. Emerging corrosion issues are further discussed in Section 21.5.9.

21.5.5.1 Contaminants

Safety Requirements

A number of chemical species, such as chloride, sulphate, fluoride, and silica are known to have detrimental contributions to corrosion of primary circuit materials and therefore, over time, to threaten the integrity of the primary circuit and fuel cladding. Refer to Table 21-5 for safety limits applicable to contaminants in the primary circuit.

Technical Basis

Chloride and sulphate can initiate pitting or crevice corrosion of stainless steels and nickel alloys (Reference 21.8). Chloride can also cause stress corrosion cracking (SCC) of stainless steels in oxygenated conditions and sulphate can enhance the susceptibility of stainless steels and nickel alloys to SCC in deaerated conditions. Fluoride can have effects similar to chloride. Aluminium, calcium, and magnesium can form oxides and silicates in primary coolant. Zeolite minerals in particular could cause densification of crud deposits and increase the risk of CILC.

Method of Control

In practice, the chloride, fluoride, and sulphate concentrations are maintained as low as reasonably possible and maximum concentrations are given in the primary coolant specification. Boric acid and raw demineralised water are both sources of contaminants. The boric acid used for chemical shim is specified as 99.9-percent purity with low levels of specified impurities (Reference 21.5). The maximum chloride, fluoride, and sulphate concentrations are specified for the BAST and primary makeup water (per the Westinghouse supplemental guidelines) (Reference 21.6).

The AP1000 plant design does not use Boraflex racking material (identified as a silica source) or recycle boric acid, therefore, silica levels are expected to be low. The primary coolant specification limits calcium, aluminium, and magnesium concentrations to low levels and silica to 1 ppm in accordance with the Westinghouse supplemental guidelines. The Westinghouse supplemental guidelines for the AP1000 plant (Reference 21.6) also limit aluminium, calcium, and magnesium to low concentrations in primary makeup water (20, 5, and 5 ppb, respectively). Since elevated silica and hardness elements in boric acid storage tank can result from impurities in makeup water and boric acid additions, limits are also placed on these species in the BAST. Silica limits for the BAST are set at [ ] ppb (Reference 21.6).

Control of contaminant species in the primary coolant is achieved by the use of high-purity makeup water from the DWS and continual cleanup of the coolant by the CVS demineralisers and filters.

Monitoring

Contaminant concentrations in the primary coolant are monitored by analysis of grab samples taken via the PSS. Chapter 4 of Reference 21.5 describes the guidance and requirements for the frequency of contaminant analysis.

Faults

Deviations above the specified limits will increase the risk of SCC and will lead to higher general corrosion rates in the long term; however, these processes are relatively slow so that a small excursion for a short period is unlikely to have any serious effect. In addition, owing to the relatively slow turnover of primary coolant, contaminated makeup water will take some time to significantly alter the composition of primary coolant; therefore, grab sampling of primary coolant is sufficient to allow adequate monitoring.

21.5.5.2 pH Control with Lithium Hydroxide

Safety Requirements

The primary coolant pH_T strongly influences the corrosion processes that affect the primary circuit and fuel cladding integrity. pH_T also significantly impacts crud production and mobilisation around the primary circuit. Alkaline conditions (high pH) minimise the general corrosion rates of primary circuit materials and lead to a lower primary circuit crud inventory, therefore reducing the risk of CIPS and CILC. Additionally, the formation of tritium is minimised through the use of ^{7}Li and the overall amount of Li minimises the amount of fuel clad degradation. Refer to Table 21-5 for safety limits applicable to pH control in the primary circuit.

Technical Basis

EPRI guidelines discuss possible pH control strategies and the Westinghouse supplemental guidelines for the AP1000 plant (Reference 21.6) specify a pH_T (the pH at operating temperature) range of [ ] during power operation. This range is supported by plant experience of crud production (Reference 21.2) and by laboratory corrosion testing. Section 21.5.9 gives further details of environmental effects on corrosion rates and Section 21.5.10 discusses crud production. The actual pH_T control adopted in the plant is the responsibility of individual operators and will be optimised within this range. Expected pH levels and associated lithium concentrations for different types of pH control programs are provided in Section 4.3.6 of Reference 21.5.

Method of Control

Lithium (in the form of LiOH) is added as the pH control agent. This is coordinated with boric acid concentration to achieve the desired pH_T. The concentrations of lithium and boron are determined by analysis of grab samples of the primary coolant. Tests using cladding material have indicated that high concentrations of lithium can lead to excessive corrosion of fuel cladding. In view of this concern, the primary coolant lithium concentration is limited to a maximum of [ ], in accordance with the fuel vendor (Westinghouse) warranty and recommendations (Reference 21.6), with a safety limit of [ ] (refer to Table 21-5). More recent work has suggested that the lithium concentrations required to significantly affect oxidation of the cladding material are much higher than those expected under normal power operation, in the presence of boric acid (21.2). As increased crud formation due to operating at lower pH is likely to have a significant effect on cladding life, options for operating at higher lithium concentrations are being investigated.

LiOH enriched to 99.9 percent in the ^{7}Li isotope is used. This particular isotope is specified because ^{6}Li will form tritium under neutron irradiation and there is a requirement to avoid the elevated primary circuit radioactivity that tritium imparts. ^{7}Li is much less likely to form tritium in these conditions.

Limiting the lithium concentration will result in an initial phase at the start of the fuel cycle where pH_T may be at the lower end of the operating band. As the boron concentration is decreased throughout the fuel cycle, to compensate for fuel burnup, the pH_T may increase to the maximum of the range. After this point, LiOH concentration will be coordinated with that of boric acid to maintain the target pH_T, reducing steadily until the end of the fuel cycle. Figure 21-2 illustrates an example of pH control profile. Boron-induced offset anomaly model calculations for the AP1000 design predict that primary coolant pH_T will not drop below [ ] during a fuel cycle (Reference 21.77).

Control of lithium in the primary coolant is achieved through the use of the CVS makeup pumps with the chemical addition tank for addition, and through the intermittent use of the cation demineraliser and letdown in the CVS for removal.

Monitoring

Grab samples will be taken from the hot leg and pressuriser liquid space, along with the downstream CVS demineralisers sample location to enable monitoring of boron and lithium concentrations and calculation of the pH_T. Deviations from the target pH_T are likely to be gradual and small, and the impacts of small changes from the target pH_T on corrosion and crud production are relatively slow, so that regular monitoring is adequate for timely adjustment. EPRI guidelines recommend a specified routine for sampling of boron, lithium, and pH_T during power operation (Reference 21.2). Changes to pH_T are achieved by dosing makeup water with additional LiOH or removing lithium in the CVS. Strategies for managing pH_T in conjunction with periodic boron reductions are discussed in the 'Technical Basis' and 'Control' sections above.

Faults

Operating outside the recommended pH_T range increases the risk of corrosion damage to the primary circuit and fuel and leads to greater oxidation of primary circuit materials and a consequent increase in primary circuit activity. Primary coolant dilution, similar to that described for boron, can affect the coolant pH_T. In such cases, the changes in reactivity would trigger alarms as for boron dilution. Errors in chemical analysis and dosing or inadvertent lithium removal could result in unintended pH_T changes. In these cases, pH_T calculations based on normal sampling would detect the changes in adequate time to avoid any significant impact. Control of pH_T during shutdown and startup is more important to avoid the possibility of crud bursts. This is discussed in Section 21.8.

21.5.5.3 Removal of Oxidising Species by Dosing with Controlled Levels of Hydrogen

Safety Requirements

Even low concentrations of oxygen have a strong impact on electrochemical potential, which has a significant effect on the susceptibility of primary circuit materials to SCC. Oxygen also affects the oxidation rate of primary plant materials (see Section 21.5.9.2), and therefore leads to increased crud in the primary circuit. A further effect of increased oxygen is increased oxidation rate of fuel cladding.

During operations typical sources of oxygen in the coolant are from radiolysis in the core, and from any oxygen in the makeup source from the boric acid storage tank. Control of oxygen concentration in the reactor coolant system is provided by injecting hydrogen from the CVS.

Refer to Table 21-5 for safety limits applicable to oxidising species and hydrogen control in the primary circuit.

Technical Basis

If the hydrogen concentrations were to become too low, there would be a rise in the electrochemical potential and a consequent increase in general corrosion rates. This in turn would lead to an increase in primary circuit crud levels. In addition, the increased electrochemical potential would increase the probability of SCC of stainless steels.

Hydrogen influences the susceptibility of nickel alloys to primary water stress corrosion cracking (PWSCC). The optimum hydrogen concentration is still the subject of research. Alloy 690 and its weld materials (Alloys 52 and 152) are highly resistant to PWSCC and no cases have been reported in the field. Laboratory testing of Alloy 600 has demonstrated an effect of hydrogen on SCC crack growth rates (CGRs), which indicates a maximum CGR at a hydrogen concentration equivalent to a potential close to the Ni/NiO transition. In addition, work with Alloy 600 has suggested a minimum crack initiation rate in primary circuit conditions with a hydrogen concentration of 30 cc (standard temperature and pressure (STP))/kg H_2O [1]. This has led to the following two proposed alternative strategies for hydrogen control in PWR primary water:

- Adoption of a very low hydrogen concentration (around 5 cc/kg H_2O)
- A very high hydrogen concentration

Both these strategies are aimed at avoiding the hydrogen concentration for peak CGRs. Whilst the majority of reported lab data relate to Alloy 600, it should be noted that this material is not used for pressure boundary components in contact with primary coolant in the AP1000 design (Chapter 20). Instead, the AP1000 design uses only Alloy 690. No PWSCC initiation data are available for Alloy 690 under normal conditions and data relating CGRs to hydrogen concentration are so far inconclusive. Therefore, the AP1000 design specifies a hydrogen concentration range of 25 to 50 cc/kg H_2O as operational limits, with the safety limits provided in Table 21-5. This is a prudent choice given the lack of a firm consensus regarding the effect of alternative hydrogen concentrations on the PWSCC performance of Alloy 690 and current operating experience.

Method of Control

In view of the deleterious effects of high oxygen levels, the concentrations in the primary coolant are maintained at very low levels during power operation, and target maximum levels to be achieved at certain stages of startup are specified. In addition, makeup water is limited to a maximum oxygen concentration of 100 ppb (Reference 21.6).

It should be appreciated that oxygen (and other oxidising species) are generated by the radiolytic degradation of water in the core during power operation. Hydrogen is, therefore, added to the primary coolant to ensure the removal of oxidising water degradation products and the maintenance of a low electrochemical potential. Hydrogen is injected into the primary coolant via the CVS. This hydrogen addition controls general oxidation of circuit materials and fuel cladding, and also suppresses PWSCC of primary circuit materials. The maximum oxygen concentration in primary coolant during power operation with hydrogen dosing is specified as 5 ppb.

Hydrogen gas is provided to the hydrogen injection package, located in the turbine hall, by a regulated supply from high-pressure storage bottles within the plant gas system (PGS) which are located outside in the plant yard. The hydrogen injection system consists primarily of piping, valves, and instrumentation. There are two parallel flow paths: one for continuous addition of hydrogen during power operation, and one for batch additions of hydrogen during startup and restart when it is desirable to change the hydrogen concentration in the coolant quickly. Each line has a control valve and flow transmitter to provide operators with system parameters and control capabilities.

1. An abbreviated version of this unit, cc/kg H_2O, will be used in the rest of the chapter.

The hydrogen injection point is downstream of the CVS regenerative heat exchanger shell side outlet line. Any undissolved hydrogen enters the RCS on the suction side of reactor coolant pumps 1A and 1B, which provide the adequate source of mixing aside from the mixing that occurs from the hydrogen injection package to the RCS.

The criteria the hydrogen injection system is designed for includes:

- Maximum Allowable Injection – the maximum rate at which hydrogen can be added and still absorb into the coolant shall be significantly larger than the required injection rate for all operating modes.
- Startup – bringing the concentration up from [ ] cc (STP)/kg of H_2O/kg in 8 hours and then from [ ]cc (STP)/kg of H_2O /kg within 24 hours of reaching criticality.
- Normal Power Operation – maintaining a concentration of [ ] cc (STP)/kg of H_2O
- Transients – maintaining a concentration of [ ] cc (STP)/kg of H_2O as water is added/removed from the RCS.

These design criteria for the hydrogen injection system are demonstrated and substantiated within Reference 21.73.

Additional measures to maintain low potentials (and low oxygen levels) are employed during startup. The procedures invoked include the following:

- Dosing with hydrazine (a powerful reducing agent)

- On first fill, evacuating the air-filled circuit prior to adding water (vacuum filling) to prevent oxygen in trapped air from dissolving in the water

Monitoring

Dissolved hydrogen concentration is monitored by grab sampling at least three times daily during power operation in order to adequately monitor hydrogen injection. More frequent sampling may be necessary during operations that may significantly impact hydrogen concentration (e.g., during plant transients or exchanges of coolant during boration or dilution) or periods of hydrogen instability (Reference 21.6).

Additionally, the primary sampling system (PSS) contains hydrogen and oxygen on-line monitors within the grab sample panel to continuously monitor trends of hydrogen and oxygen in the coolant.

The appropriateness of these means of monitoring is justified in Reference 21.72.

Faults

The injection of hydrogen into the primary coolant means that equipment failures lead to an immediate change in dosing rate. Considering a control band of [ ] cc/kg, the regular analysis of the primary coolant proposed by Westinghouse supplemental guidelines (three times daily) (Reference 21.6) ensures that changes will be detected before they are significant.

Considerations for faults that lead to unintended concentration changes within the reactor coolant system are discussed and substantiated within Reference 21.73.

21.5.5.4 Zinc

Safety Requirements

Zinc (in the form of zinc acetate) is to be added to the primary circuit to control crud production and primary circuit activity. Zinc helps to stabilise oxides on primary circuit materials and decreases the degree of deposition of ^{58}Co in the corrosion film. These two effects lead to a lower crud inventory in the primary circuit, resulting in improved fuel performance and lower circuit radioactivity.

The justification for the incorporation of zinc addition into the AP1000 plant design is based on laboratory studies and operating experience, particularly at plants which have injected zinc from the beginning of plant life or immediately following SG replacement. The addition of zinc minimises the risk of PWSCC in susceptible materials, and reduces ongoing corrosion in the primary circuit. Lower corrosion release, in turn, reduces the risk of CIPS/CILC, and also minimises plant dose rates. Hence, zinc injection in the AP1000 plant follows the as low as reasonably practicable (ALARP) principle.

It is noted that the elevated levels of zinc within the primary circuit may cause zinc oxide or zinc silicate to deposit within crud on the core and increase fuel cladding corrosion due to the solubility limit of zinc. Thus, the concentration of zinc is controlled to maintain the benefits of the dose reduction from zinc, while limiting the potential for fuel cladding corrosion.

Refer to Table 21-5 for safety limits applicable to zinc control in the primary circuit.

Technical Basis

The current target concentration for zinc in AP1000 plants during power operation is [ ] ppb with an operating band of ± [ ] ppb around the target (Reference 21.6). The target zinc concentration chosen will decrease ongoing corrosion rates for RCS materials and lower the corrosion products released to the coolant, resulting in a reduction in fuel crud deposits. The recommended target concentration also remains well below the solubility limit for zinc, providing operating margin for any unexpected increases in zinc concentration. Similar target concentrations in operating plants have been successful in reducing plant dose rates and mitigating PWSCC in susceptible materials as described in Reference 21.2. The target zinc concentration is appropriate for high boiling duty plants based on current operating experience.

Zinc acetate is available as either natural or depleted zinc. “Natural” zinc acetate has the natural mix of zinc isotopes that contains 48.6 percent ^{64}Zn, which can be activated in the neutron flux to generate ^{65}Zn (1.1-MeV gamma emitter with a 243.8-day half-life). “Depleted” zinc acetate typically contains less than 1 percent ^{64}Zn and its use would therefore result in comparatively lower plant dose rates than the application of natural zinc. For this reason, most, if not all, plants worldwide currently use depleted zinc. Although either may be used, it is recommended that depleted zinc be used in the AP1000 plants to maintain dose rates ALARP (Reference 21.5).

Method of Addition

Zinc acetate solution is injected into the RCS (via the CVS) from the zinc injection package addition tank via a positive displacement pump located in the turbine building. Injection of zinc acetate solution is continuous at a low flow rate. Grab samples are taken for zinc analysis periodically during power operation. This is sufficient to allow timely adjustment to maintain the zinc concentration within the target limits given the slow dosing rate. The dosing system can be calibrated during hot functional testing (HFT) when there is no risk to the fuel.

Monitoring and Faults

One caution associated with adding zinc to a PWR is the possibility of zinc oxide or zinc silicate depositing within the crud on the core if the boiling concentration process within the crud were to cause the zinc concentration to exceed the solubility limit. Such deposition could decrease heat transfer through porous crud, potentially increasing fuel cladding corrosion. Maintaining the zinc concentration within the targeted limits eliminates this concern for the AP1000 plant. Zinc addition rates will be calibrated during HFT when there is no fuel present, and regular monitoring of addition rates and coolant concentrations will be used during power operation to maintain a steady-state target concentration. Note also that short-term transients above the targeted value are not expected to be detrimental to the fuel (refer to Reference 21.6 for additional information), and zinc injection will be secured as needed to allow for cleanup in the case of an inadvertent overfeed.

21.5.5.5 Conductivity

Safety Requirements

Conductivity measurements give a rapid, although nonspecific, indication of changes in primary coolant chemistry and are therefore an important monitoring tool.

Refer to Table 21-5 for safety limits applicable to conductivity in the primary circuit.

Technical Basis

The conductivity of the coolant depends on all of the ionic chemical species present and is therefore a nonspecific measurement that varies throughout the fuel cycle. The relatively large concentration of boric acid and LiOH will account for most of the conductivity because the other ionic species (primarily zinc and impurities) will be present in orders of magnitude less concentration.

Monitoring

Conductivity is monitored (typically as a diagnostic parameter) to provide rapid indication of problems or ingress of species that could only be specifically analysed by more time-consuming methods, and to assess for consistency with boron and lithium measurements.

21.5.6 Design for the Minimisation of Buildup of Primary Circuit Radioactivity

Primary circuit activity is largely due to activated crud that has deposited throughout the primary circuit. The AP1000 plant design is optimised to reduce crud production ALARP while also maintaining primary circuit integrity and reactivity control. Refer to Reference 21.80 for additional details.

The crud control function is achieved by chemical monitoring and regulation via the CVS and PSS. While further details of the operational and shutdown chemistry control are described in Section 21.5.10.3, the control of crud transport is achieved by the following:

- Minimising the concentration of oxidising species
- Deaerating makeup water via the catalytic oxidation reduction system (CORS)
- Hydrogen addition via the CVS
- Maintaining pH_T within the range [ ]
- Controlling chemical conditions during shutdown and startup to avoid crud bursts and maximise removal of species which are subject to radiological activation.
- Adding zinc to the coolant to promote the formation of passive oxides and decrease the content of radionuclides in the crud, both during normal operation and as a part of HFT during commissioning
- Appropriate material selection for systems, equipment, and components to minimize corrosion and degradation, preventing additional corrosion product formation

21.5.6.1 Construction and Commissioning

A number of measures have been adopted during the construction and commissioning of the AP1000 plant to minimise the production of crud and hence circuit activity. These measures include specification of low-cobalt primary circuit construction materials, surface finishes to reduce corrosion, HFT with zinc, and cleaning procedures. Additional details are given in Section 21.10.

Primary circuit materials are specified and selected to minimise primary circuit activity. Low cobalt levels are specified for all materials in contact with primary coolant as far as practicable. Exceptions to this are some valve seats and components in the control rod drive mechanism (CRDM), RCPs, and reactor vessel internals (RVI), which are specified as a high-cobalt alloy, Stellite™, for its wear resistance. Steps are being taken to identify and qualify a low-cobalt alternative but the current choice is considered to be consistent with ALARP goals as alternatives wear faster and generate more crud.

21.5.6.2 Suspended Solids

Safety Requirements

Primary circuit activity outside of the core is largely due to mobilised deposits and corrosion products. Monitoring suspended particulate or colloidal material in the primary coolant gives information regarding the degree of solid transport around the circuit.

Refer to Table 21-5 for safety limits applicable to suspended solids in the primary circuit.

Technical Basis

Filtration of coolant in the CVS helps to control the level of suspended material. The levels of suspended solids in the primary coolant are, therefore, typically very low; however, monitoring is recommended under EPRI and Westinghouse supplemental guidelines to detect problems that lead to crud movement around the circuit. Too high a level of suspended material could lead to problems due to deposition on the fuel, possibly leading to CIPS/CILC and increased primary circuit activity.

Control

A diagnostic limit of [ ] ppb of suspended solids is specified in the Westinghouse supplemental guidelines (Reference 21.6), and grab sampling is carried out on a regular basis to allow identification of trends.

21.5.6.3 Other Radionuclides

Safety Requirements and Technical Basis

Safety limits on the RCS and secondary side specific activities are specified in the plant technical specifications for consistency with the plant's offsite dose analyses in the event of postulated fault conditions.

Refer to Reference 21.74 for details on these limits.

Monitoring and Control

The recommended types of monitoring in the primary circuit and secondary coolant (principally measurement for dose-equivalent iodine) are described in Section 12 of Reference 21.5.

21.5.7 Primary Sampling System

The PSS is a manually operated system, including two liquid sample lines; one containment atmosphere sample line; and one containment return line penetrating the containment, which is accessed through one of the three ovation stations. The PSS allows access for obtaining representative samples of fluids from the RCS and various primary auxiliary system process sources for analysis. This sampling process is performed during HFT, startup, shutdown, and power plant operations. It provides information to operators, enabling timely actions to maintain the chemical conditions needed to meet the primary coolant chemistry safety requirements.

The PSS performs the following functions:

- Provides a central location to collect both liquid and gaseous samples in normal operation mode
- Provides for local grab samples during normal operation mode
- Provides samples of the RCS, containment sump, and containment atmosphere for analysis during post-accident and accident recovery phases

The PSS provides the means to sample the primary system under various system conditions for analysis. Local sample points (not within the scope of the PSS) are provided at various process points of the auxiliary systems for taking samples for analysis. All PSS samples are

collected at the grab sampling unit and provides capability to collect samples in the radiochemistry laboratory.

During normal operation, the PSS provides a central location outside of containment to obtain representative samples of fluids in the RCS, auxiliary primary systems process streams, and the containment atmosphere for analysis.

The results of the sample analyses are used to perform the following functions:

- Monitor core reactivity
- Monitor fuel rod integrity
- Evaluate ion exchanger (demineraliser) and filter performance
- Specify chemical additions to the various systems
- Maintain acceptable hydrogen levels in the RCS
- Detect radioactive material leakage

During the post-accident and accident recovery phases the PSS provides the capability to sample from the RCS hot legs, the WLS containment sump, and the containment atmosphere. The collection of these samples allows for the analysis of reactor coolant for boron, containment atmosphere for hydrogen and fission products, and containment sump water for pH.

More information on the PSS is provided within Section 6.4.4. Further details of the overall system design and sampling procedures are given in the system specification document (SSD) for the PSS (Reference 21.13).

The PSS consists of two separate portions: liquid sampling and gas sampling. These are detailed separately below.

21.5.7.1 Liquid Sampling

For liquid sampling, the PSS provides a sample header that has two dedicated sample header lines for use of RCS based samples and a separate sample line that is dedicate for only the use of the PXS samples.

The PSS sample lines utilises proper piping and tubing to promote the integrity of connections to high-energy systems. Additionally, 10 mm DN (3/8-inch NPD) orifices are fitted in the sample lines originating directly from the RCS pressure boundary to limit reactor coolant loss to less than CVS makeup capacity (Section 6.4.2).

A delay coil of tubing is installed inside containment to provide at least 60 seconds of transit time for the sampling fluid to exit the containment from the RCS hot leg. The 60-second delay is provided for N-16 decay in order to lower radioactivity levels and potential personnel exposure from the sample fluid prior to exiting containment.

The grab sample panel used for collecting samples utilises proper valve orientation and design to promote quick sample collection with minimum radiation exposure. Prior to the collection of liquid samples, the lines are first purged with source liquid to ensure that representative samples are obtained. Sample representativeness is also further ensured through the segregation of the RCS based samples and the PXS samples within the sample header. The purging and excess sample flow is sent to the WLS Effluent Holdup Tanks (EHTs) for waste processing. The sampling lines are fitted with radiological and temperature-

monitoring equipment such that in the event of an excessive temperature or radiation level, the proper outside containment isolation valve is closed and an alarm informs the operator. The continuous sample line also provides for the capability to obtain corrosion product sampling using capillary lines to a filter for laboratory analysis.

21.5.7.2 Gas Sampling

The PSS collects gaseous samples from the containment atmosphere. This is achieved using an ejector as the motive force for sample collection.

Gaseous sampling is conducted in the sample room in the auxiliary building. Like the liquid sampling system, gas sampling can also be manually operated with extension stems on the valves. Unlike the liquid sampling capabilities, only grab samples are collected for the gas sampling. The lines are purged prior to sample collection to provide representative samples. The purged gas returns to containment. The sampling line is fitted with radiological-monitoring equipment such that in the event of an excessive radiation level, the outside containment isolation valve is closed and an alarm informs the operator of this event.

Containment atmosphere samples can be used as a backup to the containment hydrogen control system (VLS) hydrogen analysers. Reactor coolant pressure boundary (RCPB) leakage is detected with the containment atmosphere radiation monitoring skid, which continuously monitors for airborne noble gases and ^{18}F particulates.

21.5.7.3 Post-Accident Sampling Capabilities

Post-accident sampling sources and measurement procedures that may be performed with the PSS are listed in Reference 21.13, Table 2-1.

The PSS in post-accident conditions is used for sampling the conditions in containment; the PSS has the capability to obtain liquid reactor water samples for boron analysis post-accident and for reactor coolant for boron, containment atmosphere for hydrogen and fission products, and the containment sump water for pH. The primary means for sampling of the containment atmosphere for hydrogen analysis is performed by the hydrogen analysers of the VLS and is not part of the PSS post-accident sampling capabilities. Containment atmosphere samples for radionuclide analysis, however, can be obtained following an accident using the PSS. Samples collected during post-accident conditions will be returned to the containment rather than the WLS, which is the location for sample volume during normal liquid sampling operations.

Refer to Reference 21.72 for justification for the appropriateness of the post-accident sampling capabilities of the AP1000 plant PSS.

21.5.8 Chemical and Volume Control System

The CVS consists of regenerative and letdown heat exchangers (HXs), demineralisers and filters, makeup pumps, and tanks; and associated valves, piping, and instrumentation. It provides performs chemistry control during normal operations and defence in depth support to the safety requirements of the primary coolant chemistry by providing the means to control the coolant composition in terms of boron concentration for reactivity control, pH, dissolved hydrogen concentration for oxygen control, zinc dosing, and removal of contaminant species.

In addition to the chemistry control functions the CVS performs the following safety functions:

- Containment isolation
- Preservation of the reactor coolant pressure boundary
- Reactor coolant system inventory control and makeup
- Borated makeup to auxiliary equipment
- Pressuriser auxiliary spray
- Reactor coolant system degassing prior to shutdown

More discussion on the CVS and the evidence for the system capability to support the safety functions described above is discussed within Section 6.4.2. Demonstration of the adequacy of the CVS to perform its normal operation and defence in depth functions and incorporate relevant good practice has been provided (refer to Reference 21.78).

The ability for the CVS to provide chemistry control for the reactor coolant is described within the rest of this section.

21.5.8.1 Chemical and Radioactivity Control through Purification

The CVS removes radioactive corrosion products, ionic fission products, ionic impurities, and fission gases from the RCS to maintain low RCS activity levels. The CVS purification capability considers occupational radiation exposure (ORE) to support ALARP goals.

The CVS is designed to maintain the RCS activity level at less than the Tech Spec limit (Reference 21.74) for normal operations with design basis fuel defects. The purification rate is based on minimising occupational radiation exposure and providing access to the RCS equipment. Justification for the capability of the current mixed bed demineralizer sizing and flow capacity to support this function was provided in Reference 21.78.

The normal CVS purification loop is inside the containment and operates at RCS pressure, utilising the developed head of the RCPs as the motive force for the purification flow. During power operations, fluid is continuously circulated through the CVS from the discharge of one of the RCPs. The flow then passes through the regenerative HX where it is cooled by the returning CVS flow, and is further cooled by component cooling water in the letdown HX. This two-stage cooling achieves a final temperature that is compatible with the demineraliser resins, which would be degraded if exposed to excessive temperatures. The purification fluid flows through a mixed bed demineraliser, and optionally through a cation bed demineraliser, before finally flowing through a filter designed to trap resin fines emanating from the demineraliser. The flow from the filter returns to the suction side of an RCP after being reheated in the regenerative HX.

The mixed bed demineralisers are provided in the purification loop to remove ionic corrosion products, ionic impurities, and certain ionic fission products; they also remove zinc. In addition, the demineralisers act as filters. One mixed bed is normally in service, with a second demineraliser acting as a backup in case the bed in service should become exhausted during operation. Each demineraliser and filter is sized to provide a minimum of one fuel cycle of service without change out.

The mixed bed demineraliser in service can be supplemented by intermittent use of the cation bed demineraliser. The cation bed demineraliser is used during power operation for removal of excess lithium, both for pH control and for removal of lithium generated from neutron activation of boron. The cation bed can also provide additional purification in the event of fuel defects.

During plant shutdowns when the RCPs are stopped, the RNS provides the motive force for the CVS purification. Purification flow from the RNS HX is routed directly through the normal CVS purification loop. Boron changes and dissolved gas control are still possible by operating the CVS in a semiclosed loop arrangement.

21.5.8.2 Chemical Shim and Chemical Control

The CVS provides the means to vary the boron concentration in the RCS. The system also controls the RCS chemistry for the purpose of limiting corrosion and enhancing core heat transfer, as discussed further in the ensuing subsections.

Small reactivity changes (due to load following, for example) are achieved via control rod movements. This avoids frequent boron concentration changes, as used in current operating PWRs, and the consequent production of additional liquid waste through repeated dilution and boration.

The concentration of boron in the RCS is adjusted with the aim of achieving the desired control rod position with core depletion. The CVS has the capacity to accommodate a cold shutdown followed by a return to power at the end of core life and also (as an independent case) to borate the plant to cold shutdown immediately following return to power from refuelling.

Boric acid is made up in batches by dissolving solid boric acid (as a crystalline solid) in demineralised water at elevated temperature in the boric acid batching tank to a final concentration of 2.5 wt% boric acid (equivalent to approximately 4375 ppm boron).

Changes in RCS boron levels are controlled by a main control room (MCR) operator by interfacing with the reactor makeup control system (RMCS). In normal operation, the RMCS allows the operator to add makeup while maintaining the coolant boric acid concentration. Boration is achieved by aligning the suction side of the makeup pumps to the BAST via a three-way valve. When dilution of the dissolved boron levels is desired, the three-way valve is operated to align the pumps with the demineralised water supply. Towards the end of fuel life, the boron concentration in the primary coolant is low and precise dilution by this process becomes increasingly difficult. In this case the operators may optionally use flow through the standby mixed bed demineraliser to deborate the coolant. The second demineraliser will not be borated as it is reserved for end of cycle boration.

21.5.8.3 pH Control

Lithium is used to control the pH_T of the RCS. The required concentration of lithium is varied with boric acid concentration to achieve target pH_T, according to the pH_T control strategy adopted for the plant and within the lithium concentration limit. The concentration of the ^6Li isotope is minimised to limit the formation of tritium, which contributes to primary circuit radioactivity. The concentration of ^6Li is controlled by the isotopic specification for a high percent of ^7LiOH as discussed in Section 21.5.5.2.

21.5.8.4 Oxygen Control

The CVS maintains the proper conditions in the RCS to minimise corrosion of the fuel cladding and primary surfaces. During plant heatup, hydrazine is added to the reactor coolant (including the pressuriser) to scavenge dissolved oxygen. As discussed in Section 21.5.9.3, hydrogen is dissolved in the reactor coolant to minimise the levels of dissolved oxygen. The CVS is capable of maintaining the concentration of dissolved hydrogen in the RCS at a

minimum of 25 cc/kg H_2O hydrogen required during power operation, assuming anticipated operating losses. Hydrogen makeup is supplied to the RCS by CVS piping and is described in more detail within Reference 21.14 and Reference 21.73.

During plant startup from cold shutdown, the CVS introduces hydrazine into the RCS via the chemical addition tank. The solution is used only for oxygen control at low RCS temperatures during startup from cold shutdown conditions. At other times during plant operation, hydrogen is used for oxygen control.

21.5.9 Maintenance of Primary Circuit Integrity (Materials)

A second major function of primary circuit chemistry is controlling the corrosion of materials exposed to the primary coolant, including structural components and fuel cladding. This section describes the principal materials used in the primary circuit, the potential mechanisms of corrosion, the influence of primary coolant chemistry parameters, and chemistry control strategies employed to minimise corrosion.

21.5.9.1 Materials

The AP1000 plant, like all PWRs, operates at temperatures that can accelerate corrosion of materials; therefore, materials with proven ability to operate in these conditions have been selected. A brief summary is provided of these materials, their applications, and material fabrication techniques that could potentially alter a material's corrosion resistance.

Primary System Materials of Construction

The RPV is constructed from low-alloy steel (LAS). It is clad on its internal (wetted) face with austenitic stainless steel for corrosion resistance. Vessel head penetrations, including CRDM housings and vent pipes, are constructed from Alloy 690. All primary circuit components in contact with the primary coolant are constructed from, or clad with, austenitic stainless steels (with some exceptions where justified). SG tubes and passive residual heat removal (PRHR) HX tubes are manufactured using thermally treated (TT) Alloy 690 (Alloy 690TT). RCP piping and the surge line are made from austenitic stainless steels. Valve components are made from austenitic stainless steels but valve seals and stems may be constructed from Alloy 718, Type 630, or Type 316 steel. Based upon lessons learned from the previous generation of nuclear power plants, Alloy 600 is not used in the AP1000 plant primary circuit except in small quantities in the RCPs, and is not used for pressure boundary components in contact with primary coolant. Details of primary circuit materials are given in Chapter 20.

The major core support materials for the reactor internals are Type 304, 304L, 304LN, or 304H stainless steels. For threaded structural fasteners, the material used is strain-hardened Type 316 stainless steel, and for the clevis insert-to-vessel bolts, either Alloy 718 or Alloy 750. The remaining internal parts not fabricated from Type 304, 304L, 304LN, or 304H stainless steels typically include wear surfaces such as hard facings on the radial keys, clevis inserts, alignment pins (Stellite-6 or low-cobalt hard faces), dowel pins (Type 316), hold-down springs (Type 403 stainless steel (modified) or 415), clevis inserts (Alloy 690), and irradiation specimen springs (Alloy 750). Instrument guide assembly materials that are not Type 304, 304L, 304LN, or 304H stainless steel are the guide bushings and guide stud tip (UNS S21800) and the instrument guide tube spring (Alloy 718). The use of cast austenitic stainless steel (CASS) is minimised in the AP1000 reactor internals. If used, CASS will be limited in both carbon (low carbon grade: L grade) and ferrite content and will be evaluated in terms of thermal aging effects.

Moreover, compatible weld materials are used throughout, including Alloys 52, 52M, and 152 for Alloy 690. For austenitic stainless steels, the weld materials are Types 308, 308L, 309, 309L, 316, and 316L.

In addition, susceptibility to irradiation-assisted SCC or void swelling in reactor internals identified in the current PWR fleet are being addressed in reactor internals Material Reliability Programmes (MRPs). The selection of materials for the AP1000 plant reactor internals considers information developed by these programmes. Decidedly, Ni-Cr-Fe Alloy 600 is not used in the AP1000 plant reactor internals.

Fuel Cladding and Fuel Assemblies

Fuel cladding and fuel assembly intermediate support grids are made from zirconium alloy (ZIRLO™). ZIRLO, an advanced zirconium-based alloy used in the AP1000 plant, has equal or better corrosion resistance than Zircaloy-4 (Reference 21.15). Controls on fuel fabrication specify maximum moisture levels to preclude clad hydriding. In addition, the top, bottom, and protective grids of the fuel assemblies are made of nickel-chromium-iron (Ni-Cr-Fe) alloy (Alloy 718). Control and grey rod cladding are made from cold-worked Type 304L stainless steel.

Sensitisation and Cold Working

Sensitisation and cold working can change a material's resistance to different corrosion mechanisms. The approach used in developing the AP1000 plant to minimise the impact of sensitised or cold-worked materials is described below.

Sensitisation may occur when stainless steel is subjected to certain combinations of temperature and exposure time that precipitate chromium carbides at the grain boundaries, resulting in a chromium-depleted layer adjacent to the grains that provides a path of lower corrosion resistance along the grain boundaries. Therefore, sensitised stainless steel is more susceptible to intergranular stress corrosion cracking (IGSCC). Also, the chemistry of the reactor coolant is controlled to prevent the intrusion of aggressive species; testing has shown that, even with sensitised materials, IGSCC of stainless steel should not occur in the reducing- and low-chloride conditions of PWR primary coolant (Section 21.5.9.2). Nevertheless, sensitisation is avoided to further minimise the risk. Low carbon grades are applied wherever possible in the AP1000 plant. The AP1000 plant uses austenitic stainless steels in the solution-annealed and water-quenched condition to avoid introducing sensitised material. An example of using materials that avoid the potential for sensitisation is the single-piece forging technology implemented for the "hot leg with side nozzles" (and cold legs), which eliminated welds and in-service inspections.

In addition, welding processes are controlled to prevent sensitisation, and any other processes that may result in sensitisation during manufacture are avoided. Testing is carried out on any stainless-steel components where sensitisation through processing is suspected, and any sensitised material is heat-treated or rejected. Materials having a carbon content greater than 0.03 wt% receive a suitable intergranular corrosion test (practice E American Society for Testing and Materials (ASTM) A262-70 (Chapter 20). This confirms that the welding procedures used for the manufacture of components in the primary pressure boundary and the reactor internals do not result in the sensitisation of heat-affected zones (HAZs). The delta ferrite content of weld materials is specified as 5 to 16 FN for Mo-containing material, and 5 to 20 FN for other materials. Weld procedures are controlled to avoid hot cracking in stainless-steel welds.

The use of cold-worked stainless steels is restricted to small components such as pins, fasteners, and cladding of control and grey rods; and is avoided in pressure boundary components by selecting raw materials and controlling manufacturing processes to avoid or minimise residual cold work and the resultant elevated yield stresses that may predispose the material to SCC. Solution heat-treated materials are normally used and reheating in the range of 426.7 to 815.6°C (800° to 1500°F) is avoided. Pressure boundary parts and components made of stainless steel do not have specified minimum yield strength greater than 620.53 MPa (90 ksi).

21.5.9.2 Degradation Mechanisms

Oxidation

General corrosion (oxidation) of primary circuit materials can occur in high temperature (HT) aqueous environments and at a uniform rate over the entire surface area of a material. The rate of general corrosion depends on a number of factors, including material, metallurgical condition and history, surface finish, temperature, pH, oxygen concentration, electrochemical potential, and the concentration of aggressive species such as chloride and sulphate. Thus, Westinghouse has chosen materials such as Alloy 690 and ZIRLO with proven performance in PWR chemistry environments.

The primary system materials of construction that come into contact with reactor coolant include Alloy 690 and austenitic stainless steels. Alloy 690 has been selected, in part, due to its low general oxidation rate in PWR primary coolant conditions as compared with previous-generation high-nickel alloys, such as Alloy 600. The SG tubing is made of Alloy 690, which is the largest application of this material in the AP1000 plant. In addition, the AP1000 pressure vessel steel is clad with austenitic stainless steel on its inner (wetted) face to provide a corrosion-resistant barrier. This is more effective than an unclad vessel since stainless steels form a relatively protective surface oxide in HT water. Also, RCS pressure boundary materials, as noted in Section 21.5.9.1, are made of materials that have demonstrated resistance to oxidation in AP1000 plant primary water chemistry.

In addition to Alloy 690 and stainless steels, zirconium alloys are used in the primary system as cladding for the fuel. Oxidation of zirconium alloys can depend on the alloy microstructure and distribution of minor alloying elements. Fuel cladding oxidation rates are related to the temperature of the metal-oxide interface. When a surface oxide layer accumulates on the zirconium alloy surface, it imposes an additional barrier to the conduction of heat through the clad (i.e., it has a partially insulating effect). As a result, a thickening surface oxide results in a steadily increasing interface temperature and an accelerating corrosion rate at the interface so that the corrosion rate increases throughout the fuel life. An additional exacerbating effect is the deposition of corrosion products (crud) from other parts of the primary circuit. This takes the form of nickel ferrites, nickel oxide, and nickel metal. A further concern is that hydrogen produced by the corrosion reaction can penetrate the zirconium alloy and cause embrittlement of the material.

ZIRLO is used as the fuel cladding material in the AP1000 plant. ZIRLO has been developed by Westinghouse to replace the formerly used Zircaloy-4 alloy. While ZIRLO has been demonstrated to have mechanical properties comparable with Zircaloy-4 (Reference 21.15), both operational experience in the North Anna PWR and trials in the BR-3 test reactor have demonstrated that the levels of oxidation are considerably lower for ZIRLO as compared with Zircaloy-4 (Reference 21.15).

The lower oxidation of ZIRLO mitigates the potential of excessive thinning of the clad wall or exceeding the thermal limits of the ZIRLO cladding. Furthermore, results have indicated that ZIRLO and Zircaloy-4 have comparable hydrogen pickup at an equivalent level of oxidation; therefore, the potential for hydrogen inventory impairing the mechanical performance of the cladding will be mitigated by the lower levels of oxidation for ZIRLO.

During transitions between normal operation and shutdown conditions, the AP1000 plant water chemistry is controlled to ensure that proper redox conditions of the reactor coolant are maintained. For full-power operations, the reactor water is maintained at alkaline-reducing conditions. During shutdown, the reactor water chemistry transitions from alkaline-reducing to acid-reducing and then to acid-oxidising chemistry conditions. During startup, the reactor water chemistry is returned to acid-reducing and then to alkaline-reducing to resume full-power operation. This general control strategy has a proven history in the industry and improves plant performance and reliability by reducing the formation of particulate corrosion products from general corrosion of austenitic stainless steels and Alloy 690. The AP1000 plant has included this proven chemistry strategy to obtain the same plant performance and reliability. Additional details on overall chemistry operations are provided in Section 21.8.

The EPRI guidelines (Reference 21.2), which generally provide input to the primary water chemistry control programme for the AP1000 plant (Reference 21.5), also consider the chemistry to control the oxidation of zirconium alloys, including ZIRLO. First, a maximum lithium concentration (as determined by the fuel vendor) is imposed by the EPRI guidelines for input to Reference 21.5; additional information on lithium limits is provided in Section 21.5.9.3. These guidelines impose and ensure a reducing chemistry around the primary circuit that facilitates the effective performance of ZIRLO in terms of levels of oxidation and associated hydrogen pickup.

Pitting and Crevice Corrosion

Pitting and crevice corrosion are a common, localised corrosion mechanism of stainless steels that rely on a thin protective oxide layer for their corrosion resistance. Disruption of this layer by aggressive chemical species such as chloride ions, leads to local activation and self-propagating local attack, which can result in pitting or crevice corrosion. The attack is initiated in solutions containing contaminant species such as chloride and sulphate in oxidising conditions. At ambient temperatures, relatively high concentrations of these species (>100 ppm) are required for pitting or crevice corrosion to occur. Attack occurs more readily at higher temperatures with low pH conditions at low electrochemical potential (ECP) than in PWR primary coolant. To mitigate pitting and crevice corrosion of stainless steels, the AP1000 plant chemistry is controlled to much lower impurity levels and at an alkaline pH during full-power operation, compared to that required during shutdown.

Stress Corrosion Cracking

SCC is a notable form of localised corrosion and can lead to premature failure of engineered components, often leading to leaks. A variety of factors are involved, but SCC only occurs given certain combinations of material, stress, and chemical environment. PWR materials of construction, such as Alloy 600, have previously experienced SCC. Therefore, the potential for SCC to occur has been extensively studied in stainless steels and nickel alloys in a variety of environments, including light water reactor (LWR) primary coolants (Reference 21.17). In addition, SCC in zirconium alloys has also been studied in LWR primary coolants. The selection of AP1000 plant primary system materials, such as Alloy 690, stainless steels, and

zirconium alloys, as well as the development of AP1000 plant primary water chemistry requirements have applied this operating experience and testing results.

The AP1000 plant primary coolant chemistry specification is designed to minimise the risk of SCC of primary circuit materials by controlling levels of contaminants, oxygen, hydrogen, $pH_{T,}$ and electrochemical potential in accordance with the recommendations of the EPRI guidelines (Reference 21.2). During full-power operations, the chemistry of the primary coolant is maintained at alkaline-reducing conditions with a low levels of impurities, particularly fluoride, chloride, and sulphate, to mitigate the occurrence of SCC. Combined with the selection of resistant materials and correct manufacturing processes, this design implements a mitigation strategy based on the best industry-wide understanding of PWSCC. A brief discussion follows on the impact of metallurgical properties, interaction with the chemical environment, fabrication methods, and design. Further details of PWSCC mitigation measures involving materials and construction methods are given in Section 21.10.

Alloy 690

The AP1000 plant has benefited from the study of SCC in Alloy 600 and the subsequent development of Alloy 690, which is more resistant to SCC than Alloy 600. Analysis of data from a range of laboratory test programmes on SCC of cold-worked Alloy 600 exposed to simulated PWR primary coolant indicated that the dominant factors were more frequently material and stress rather than chemistry effects (Reference 21.18). Laboratory CGR testing has demonstrated that SCC also occurs in cold-worked Alloy 690 materials; however, most Alloy 690 materials appear to be highly resistant (Reference 21.17), and CGRs are substantially lower than the most susceptible heats of Alloy 600. SCC of Alloy 690 has been observed on cold-worked material when stressed in susceptible orientations, including TT heats. It should be emphasised that all the information to date on PWSCC of thick-walled Alloy 690 relates only to laboratory tests for crack growth in heavily and unidirectionally cold-worked material. The mechanism by which this sometimes induces susceptibility is the subject of both research and speculation but is presently unclear. The Alloy 690 weld metals (Alloys 152 and 52) are also being studied but are currently thought to be highly resistant to the effect of simulated primary water (or other HT water and steam environments) on crack growth, even from pre-existing defects. Finally, no evidence has yet been obtained of crack initiation occurring through PWSCC in Alloys 690, 152, and 52, either in laboratory testing or in nearly 20 years of operation in the field under primary water conditions; therefore, Alloy 690 has been chosen for the AP1000 plant.

Austenitic Stainless Steels

Austenitic stainless steel, another material of construction in the AP1000 plant primary circuit, has been previously linked to SCC in other PWR primary circuits. The industry then studied SCC in stainless steels and determined a number of factors, including material manufacturing methods and environmental conditions that influence SCC. For example, cold work has also been shown to increase the susceptibility of stainless steels to SCC. Also, particular forms of SCC in austenitic stainless steels have been associated with specific environmental conditions. Environmental conditions for SCC have been defined in a number of studies (Reference 21.19), and electrochemical potential, pH, and impurities (chloride and sulphate, notably), are all known to influence susceptibility to SCC.

The combined effect of environmental conditions (oxygen and chloride concentration) on the susceptibility of stainless steels to SCC in various metallurgical conditions has been examined and is shown in Figure 21-3. In deoxygenated HT good-quality PWR primary

water at low potential, IGSCC of nonsensitised stainless steels is not generally thought to occur. Transgranular SCC (TGSCC) of solution-annealed stainless steel is most common in the presence of chloride, although some degree of oxygenation is required.

Also, many cases of SCC of stainless steels in operating plants have been attributed to the development of local aggressive conditions. Occluded regions of the plant where exchange with the bulk primary coolant is low can retain oxygen or contaminants such as chloride following startup. This leads to an HT environment that is not representative of the majority of the primary circuit: it is mainly within such local environments that SCC occurs.

In recent years, increasing attention has been directed to the possible SCC susceptibility of cold-worked stainless steels under normal chemistry conditions in the primary circuit. In a 2007 EPRI presentation (Reference 21.20), around 140 events of stainless steel field cracking were described in a variety of PWR components. Of these, about 15 percent were ascribed to the effects of cold work (leading to hardness > 300 HV) during exposure to flowing primary water without contaminants (Figure 21-4). None of these were associated with thermal sensitisation, although the observed SCC was predominantly intergranular.

In addition to environmental interactions, cold-worked areas of nonsensitised austenitic stainless-steel components (e.g., pressuriser heater sleeves) in French PWRs have experienced a limited of number of cases of IGSCC, and widespread research into this topic is ongoing in France (References 21.20, 21.21, and 21.22). In general, the material condition and the loading parameters have been found to control cracking susceptibility, with the exact primary water chemistry, at most, a secondary factor (Reference 21.23). A higher propensity to cracking was noted, however, in an unusually high pH environment representing the conditions that might arise following actual leakage through a pressuriser heater sleeve.

Thus, for stainless steels, IGSCC in the AP1000 plant is mitigated by the use of low-carbon materials and control of welding procedures (see Section 21.5.9.1) to eliminate the risk of sensitisation. Maintaining low oxygen and halogen concentrations effectively mitigates IGSCC in sensitised stainless steels and this, combined with control of manufacturing procedures to minimise cold work, also helps to minimise the risk of TGSCC.

Fuel Cladding

With respect to fuel and clad chemical interaction, it is postulated that the fission product iodine is the corrosive agent for SCC. Out-of-pile tests have shown that in the presence of high clad tensile stresses, large concentrations of iodine can chemically attack the ZIRLO tubing and may lead to eventual clad cracking by pellet-clad interaction (PCI) SCC. Extensive post-irradiation examination has produced no evidence that this mechanism has been operative in Westinghouse commercial PWR fuel. A Westinghouse model (see Section 22.4) has been developed to evaluate the risk of PCI and has been applied to ZIRLO clad fuel for the AP1000 plant. The model is based on data from the Westinghouse performance and analysis design (PAD) model (Reference 21.16) and power ramp test results using ZIRLO rodlets irradiated in Vandellos II and Belleville reactors. The model predicts a comfortable margin for PCI at the end of a fuel cycle.

AP1000 Design Features

In addition to chemistry control and material selection, improved design concepts in the AP1000 plant have reduced the susceptibility of components to SCC. A number of cases of SCC related to canopy seal welds have been reported. The CRDM lower canopy seal weld is eliminated in the AP1000 plant, and there are no spare penetrations with threaded and canopy seal-welded head adapter plugs and capped latch housing joints. A single-piece forging is used for the "hot leg with side nozzles" (and for the cold legs) to eliminate welds and in-service inspections. Also, the AP1000 plant reactor vessel head uses cold leg cooling to reduce the temperature of the head. The lower temperature of the materials in the head in turn reduces the susceptibility of SCC in the reactor vessel head.

Another design feature of the AP1000 plant that mitigates SCC is the addition of zinc acetate to the primary coolant. Laboratory data and plant operating experience related to Alloy 600 PWSCC mitigation with zinc are well documented (Reference 21.37). Benefits have been demonstrated even in plants with low zinc concentrations (e.g., 5 ppb). Although there has been no evidence of cracking of Alloy 690TT in operating PWRs to date, zinc injection is still expected to be beneficial in reducing the susceptibility of AP1000 plant materials to SCC.

Corrosion of Low-Alloy Steels due to Primary Coolant Leakage

A particular concern in PWRs arises from the leakage of borated primary coolant from joints such as gasketed flanges and its impingement on carbon and LAS components (e.g., flange studs). Solid boric acid at room temperature and dilute, deaerated boric acid solutions regardless of temperature have little effect on carbon steels and LASs; but as the boric acid concentrates, corrosion rates of up to about 1 mm per year (1 mm/a) may be reached. Aerated solutions can be much more aggressive, with the attack increasing with acid concentration. Note that as hot coolant escapes to the environment, its boric acid content (which may be nominally 2000 ppm or more as elemental boron) concentrates by evaporation. At temperatures near 100°C (212°F), which are attained by surfaces impacted by coolant flashing to steam, corrosion rates can reach approximately 250 mm/a (Reference 21.24).

In some situations, flow effects can exacerbate the attack: e.g., they are implicated in the corrosion of PWR pressure-vessel steel by borated coolant leaking through cracked penetrations in the RPV head (Reference 21.25). At the Davis Besse PWR in 2002, such corrosion had threatened the integrity of the vessel. The sequence of events that can lead to cavity formation next to a nozzle was postulated to consist of three phases: initially, slow seepage of coolant into the external annulus (crevice) in the head would be accompanied by low corrosion rates; next, when the crevice had opened enough and the crack had lengthened to give substantial leak rates, an evaporating coolant jet would accelerate the attack through flow effects; finally, leakage into a cavity would create a turbulent evaporating pool, extending the attack sideways.

An extensive testing programme sponsored by EPRI is investigating the phases of boric acid attack at Davis Besse and its implications for possible leakage at either top or bottom RPV heads in other PWRs. The second phase, which experienced substantial flow effects, was simulated with laboratory experiments in which a flashing jet of borated coolant was directed onto a heated sample of pressure-vessel steel and the damage assessed in terms of system parameters, notably, coolant chemistry and flow rate (Reference 21.26). Volumetric (or massive) metal loss was correlated with volumetric coolant flow and seemed to behave differently from metal penetration, which was correlated with jet velocity.

The miniature scallops in the damage craters that formed around (but some distance away from) the points of jet impact provided indications of flow-assisted corrosion (FAC). Metal loss rates attained about 3 cc/a at a flow rate of 200 mL/min with a boric acid concentration equivalent to 1500 ppm (B) and $pH_{300°C}$ of 6.9 adjusted with lithium; the rate depended on the volumetric flow in the jet raised to the power 0.84. Under the same chemistry conditions, the penetration rate reached 200 mm/a at a jet velocity of 140 m/s and the two were correlated via the velocity raised to the power 4.3. It was notable that neither $pH_{300°C}$ nor the boron concentration was the controlling chemistry parameter; rather, it was the ratio of (B)/(Li) (Figure 21-6).

Leakage at RPV head penetrations is not expected for the AP1000 plant, owing to better materials and improved design, so the above mentioned chemistry effects are unlikely to play any direct role with regard to ensuring component structural integrity. They illustrate, however, the complexity of assessing the aggressiveness of concentrated primary coolant toward carbon and LASs if it were to escape from the circuit.

21.5.9.3 Environmental Factors Influencing Degradation

It is necessary to consider several parameters of the solution chemistry to assess whether environmentally assisted cracking or other corrosion mechanisms are likely to occur. These parameters include the following:

- pH
- Electrochemical potential
- Contaminant species, such as chlorides, fluorides, and sulphates
- Dissolved hydrogen
- Boron
- Lithium
- Zinc
- Temperature

Some of these parameters, such as contaminants, are controlled to ALARP. Other chemicals, such as dissolved hydrogen, boron, lithium, and zinc are added to the coolant to control the environmental conditions that influence corrosion. The pH and electrochemical potential are directly influenced by the control of these chemical parameters. Also, system temperature, which is largely independent of the above variables, impacts corrosion rates but is determined by plant operations. The impact of each of these parameters on corrosion is discussed below.

Effect of pH

In general terms, an alkaline pH environment promotes passivation and low general corrosion rates as well as reduced incidence of localised corrosion in a variety of steels and nickel alloys in aqueous environments. In PWRs, the target pH_T control is generally achieved by coordinating the concentration of lithium with the required boron concentration for reactivity control and within the constraints of the maximum acceptable lithium concentration.

Westinghouse guidelines recommend operating to an elevated pH_T to control the development of CIPS and CILC, within a maximum lithium concentration of [ ] ppm (Reference 21.6). The upper limit of the lithium concentration is determined based on the corrosion resistance of ZIRLO. pH_T has a strong effect on crud deposition on fuel, which subsequently affects fuel cladding corrosion.

Crud buildup on fuel cladding is greater at lower pH_T but higher cladding corrosion rates can occur at higher pH where subcooled boiling occurs. The Westinghouse supplement (Reference 21.6) suggests a pH at temperature (core average temperature, pH_T) of greater than [ ] to limit corrosion and crud buildup. More recently, target pH_T values of up to 7.4 have been adopted. Corrosion rates for both stainless steels and nickel alloys are known to decrease as the pH_T is raised from [ ] (Reference 21.29). This reduces crud release rates and there has been an increasing trend of operating PWR plants at elevated pH_T, up to pH_T [ ] (Reference 21.6).

In addition to general corrosion rates, pH also affects SCC. In austenitic stainless steels, alkaline pH also lowers the incidence of SCC initiation (Reference 21.27). Figure 21-7 shows the results of susceptibility tests on sensitised Type 304 stainless steel at constant load in aerated sodium sulphate solutions at 300°C (572°F). The minimum electrochemical potential for SCC susceptibility was similar over the $pH_{300°C}$ range 2 to 5.6. SCC was also noted at higher pH although the mechanism was different (Reference 21.19). Constant extension rate tests (CERTs) of sensitised Type 304 stainless-steel samples in solutions using a variety of pH buffers (which have the effect of limiting the variation of pH) indicated that crack initiation was suppressed at a pH of greater than 7 (Reference 21.28). This work was conducted at low temperature, but the effect could be assumed to apply under PWR conditions; although as the pH neutral point changes with temperature, the broad pH effects may be the same. A study of CGRs using sensitised Type 304 in oxygenated NaOH solutions at pH 5.6 to 10 (Reference 21.27) found a tenfold reduction in CGR at pH 9 (Figure 21-8). A further study concluded that pH_T over the range of 5.7 to 7.8 had no significant effect on CGRs of Alloy 600, Inconel™ X-750, or cold-worked Type 304 stainless steel tested under PWR conditions (Reference 21.2). Additional details on SCC are provided in Section 21.5.9.2.

Therefore, the AP1000 plant water chemistry maintains an alkaline pH_T of [ ] during operation (Reference 21.6). The alkaline pH_T reduces the amount of general corrosion that occurs and mitigates the probability of SCC occurring. Additional details on PWR pH control strategies are available in EPRI PWR Primary Water Chemistry Guidelines (Reference 21.2).

Electrochemical Potential

The ECP has been shown in laboratory studies to strongly influence the susceptibility of stainless steels to SCC. If the ECP is reduced below a critical value, IGSCC does not occur; however, the value of the critical potential is influenced by material and environmental factors, including sensitisation, temperature, and concentrations of contaminant species such as chloride or sulphate ions. The threshold potential for TGSCC of solution-annealed stainless steels in deaerated solutions is more positive than that for IGSCC of sensitised material. That is, for plants such as PWRs that normally operate at low ECP, slow rises in the ECP due to fault conditions could induce IGSCC degradation before TGSCC degradation.

It has been shown that there is equivalence between oxygen content in HT water and applied ECP in deaerated water in slow strain rate tensile (SSRT) tests. Low concentrations of oxygen have a great influence on ECP because of the change in cathodic reaction from water reduction to oxygen reduction. The presence of small amounts of oxygen in water can significantly increase general and localised corrosion rates (Figure 21-7). SCC susceptibility of stainless steels and nickel alloys increases rapidly with increasing oxygen concentration, especially in the presence of contaminants such as chloride and sulphate.

Increased general corrosion can lead to higher crud levels and circuit activity. Hydrogen added to the primary coolant reduces the ECP, removes oxygen generated in the core, and eliminates oxygen introduced via makeup water.

Contaminant Species

A number of chemical species are known to influence corrosion of primary circuit materials. Fluoride, chloride, and sulphate are directly associated with the degradation of primary circuit materials and have been designated as control parameters, which require corrective actions if control limits are exceeded. Aluminium, calcium, magnesium, and silica are not directly associated with degradation of primary circuit materials and are designated as diagnostic parameters. The AP1000 plant controls the impact of these contaminant species by limiting their concentration in the primary circuit through the application of the AP1000 Chemistry Manual, EPRI Guidelines, and the Westinghouse supplemental guidelines (References 21.5, 21.2, and 21.6); however, a brief introduction on the basis for control is provided.

Fluoride, chloride, and sulphate have a demonstrated direct impact on the degradation of primary circuit materials. Chloride can induce SCC of stainless steels in oxygenated conditions and can enhance localised corrosion at higher concentrations. Sulphate can also accelerate localised corrosion and is known to influence initiation of SCC under deoxygenated conditions. SCC of Alloy 600 at two plants was attributed to the presence of reduced sulphur species; IGA of sensitised Alloy 600 was related to ingress of large amounts of ion exchange resin, which gave rise to high sulphate concentrations (greater than 20 ppm). The effect of fluoride is less well understood but is known to influence SCC of Alloy 600 and the corrosion of zirconium. The work of Whyte and Picone (Reference 21.33), however, indicated that sensitised stainless steels were susceptible to fluoride-induced SCC but only at concentrations of at least 10 ppm. No SCC was found where boric acid was present in the test environment. Therefore, the concentrations of chloride, sulphate, and fluoride anions in the AP1000 plant primary coolant are controlled to levels that have proven material performance in the field (References 21.2 and 21.6).

Aluminium, calcium, and magnesium can form oxides and silicates in the primary coolant. As the solubilities of these salts have a negative temperature coefficient (i.e., solubility decreases as the temperature is increased), it is expected that they could deposit on fuel cladding and possibly lead to enhanced corrosion. Zeolite minerals in particular could cause densification of crud deposits.

In many current operating PWRs, silica is present in the spent fuel pool (SFP) water in relatively high concentrations because of the use of Boraflex in the fuel racks and can enter the primary coolant during refuelling operations or from recycled boric acid. Silica solubility is relatively high in primary coolant conditions and deposits are unlikely. It is possible, however, that high concentrations of silica will precipitate low concentrations of zeolites with aluminium, calcium, or magnesium. Thermodynamic calculations suggest that calcium and magnesium borates will precipitate preferentially over silicates except when boric acid concentrations are low at the end of cycle, so that is unlikely to present a real problem. In practice, aluminium, magnesium, and calcium are controlled at low levels, and plants operating with high silica levels (greater than 1 ppm) have reported no problems. Crud deposit analyses have revealed silicon contents of 2 to 5 percent but low levels of zeolite-forming elements. EPRI guidelines (Reference 21.2) recommend minimising silica ingress and maintaining a control level related to aluminium, magnesium, and calcium concentrations. Westinghouse supplemental guidelines (Reference 21.6) specify limits for these contaminants. The AP1000 design does not use Boraflex fuel racking or boron

recycling, so silica contamination of the primary coolant is expected to be below the 1-ppm limit.

Dissolved Hydrogen

Hydrogen is added to the primary circuit in the AP1000 plant as well as other PWRs to maintain reducing conditions (low ECP). The low potential reduces oxidation rates and reduces the incidence of SCC of stainless steels and nickel alloys. Specifically, dissolved hydrogen reacts with any dissolved oxygen to form water, as shown below.

$$2H_2 + O_2 \leftrightarrow 2H_2O$$

To ensure that the low potential is maintained, the hydrogen concentration is maintained from 25 to 50 cc/kg H_2O to ensure that any oxygen that might be introduced into the primary circuit reacts with hydrogen to form water. Also, the hydrogen residual ensures that the radiolytic decomposition of water does not favour the production of oxygen. While benefit is achieved by adding hydrogen to maintain reducing conditions in the primary circuit to reduce both general oxidation and localised corrosion in the AP1000 primary circuit, the potential impact of hydrogen on primary circuit materials of construction is discussed briefly.

While Alloy 600 has ostensibly been replaced by Alloy 690 in the AP1000 plant, previous experimental work on Alloy 600 is provided to allow for comparison with Alloy 690. Experimental work suggested that higher hydrogen concentrations increased the susceptibility of mill-annealed (MA) Alloy 600 to SCC in HT water; however, CGR tests on Alloy 600 specimens, in which the hydrogen fugacity was changed in steps from 20 through 40 to 80 cc/kg H_2O (Reference 21.30), showed a slight reduction in CGR at higher hydrogen concentrations. Tests on Alloy 182 weld material indicated a clear reduction in CGR at higher hydrogen levels.

Studies of PWSCC carried out at General Electric-Global Research Center (GE-GRC) as part of the EPRI MRP investigated CGRs of Alloy 600 and 182/82 weld metals under good-quality PWR coolant conditions. A peak rate was identified at ECPs equivalent to the Ni/NiO transition potential, which is close to the H_2/H_2O transition potential. In practice, the corrosion potential in deaerated water is controlled by the hydrogen activity, which can be used to drive the potential either above or below the Ni/NiO potential. Operating at hydrogen activities away from the Ni/NiO boundary will minimise CGRs. In theory, the CGR, relative to the peak rate at the Ni/NiO potential, could be reduced by a factor of as much as 16 for Alloy 82/182 weld materials, and up to a factor of three for Alloy 600.

This tendency for a hydrogen content at which SCC CGRs peak is seen across a range of temperatures. The hydrogen activity giving a potential corresponding to the Ni/NiO boundary increases with temperature: about 4.2 cc/kg H_2O at 290°C, 10.4 cc/kg H_2O at 325°C (554°F), and 15.3 cc/kg H_2O at 340°C (644°F). The current operating regime for PWRs (EPRI) targets H_2 at 35 cc/kg H_2O and a range of 25 to 50 cc/kg H_2O. This regime of PWR dissolved hydrogen concentration is above the concentration at which peak SCC CGRs are observed. To give an equivalent CGR, on the low hydrogen side of the peak, to that expected at 35 cc/kg H_2O, would require 7.7 cc/kg H_2O at 343°C (649°F), decreasing with temperature to 0.5 cc/kg H_2O at 290°C (554°F).

This pattern of hydrogen effect appears to be independent of temperature, stress intensity, boron or lithium concentration, or heat of alloy. If very low hydrogen levels were to be used, there would be concerns that radiolytically produced oxygen could locally raise the ECP due

to lack of hydrogen in the water. That, in turn, would raise concerns of increased general corrosion and SCC. The chosen hydrogen content has therefore been specified to avoid localised regions of high potential and to avoid peak susceptibility to SCC.

Also, PWSCC initiation studies of Alloy 600 have shown a minimum initiation rate at a hydrogen concentration of 30 cc/kg H_2O (Reference 21.32). Data from Bettis (Reference 21.17) demonstrated a loss of the mitigation effect of low hydrogen at high stress intensity values, but this was reversed at low stress intensity values.

In comparison, recent CGR tests performed on Alloy 690 materials showed a higher CGR at 50 cc/kg H_2O hydrogen concentration compared with tests at 23 cc/kg H_2O. Also, this work used cold-worked materials previously shown to be highly susceptible (Reference 21.31). Since 1989, when Alloy 690 tubing was used in the first PWR SG, there has not been any reported impact of hydrogen concentration on SCC of Alloy 690. Thus, the amount of cold-working in PWR components has not been significant enough to produce SCC in the field. Since no clear evidence of SCC initiation in Alloy 690 under PWR conditions has been produced, the influence of hydrogen on initiation, if any, is unknown, and work is continuing to determine the mechanism of possible SCC of Alloy 690. Thus both laboratory data and operational experience to date have not shown any apparent impact on SCC of Alloy 690 from dissolved hydrogen in primary circuit environments.

However, there is currently much debate regarding the optimum hydrogen concentrations in PWR primary coolant, mostly centred on the susceptibility of nickel alloys to SCC. Most of the existing data have been generated using Alloy 600, and the CGR data support a rise in hydrogen concentration. There is an argument for extrapolating this finding to other nickel alloys, such as Alloy 690. Some Alloy 690 test data appear to contradict the trend for Alloy 600 but work is still ongoing. Also, EPRI is considering increasing the existing range for hydrogen concentration specified in the existing guidelines (Reference 21.2). The specification of hydrogen concentration in the AP1000 plant (Reference 21.5) agrees with the current EPRI guidelines. Given the impact of hydrogen on Alloy 600 and the laboratory and operational experience of hydrogen concentration on Alloy 690, the current guidelines' value is a reasonable position that ensures that reducing conditions are maintained to minimise general corrosion and localised corrosion mechanisms, such as SCC and pitting, and also minimises any other potential detrimental impacts from hydrogen (Reference 21.2).

SCC performance of Alloy 690 and its weld materials is discussed in more detail in Section 21.5.9.2.

Boron

Andresen studied the effect of boron on CGRs of Alloy 600 in PWR water and found no effect (Reference 21.30). An EPRI-sponsored study of the effects of various chemistry parameters on CGRs of Alloy 600 nickel alloy concluded that boric acid at concentrations from 60 to 3200 ppm had no significant effect on CGRs (Reference 21.34). This is expected to hold true for the Alloy 690 used in the AP1000 plant as well.

Also, boric acid could potentially attack the RPV mild steel where primary coolant leaks onto the outer surface of the vessel and evaporates. Boric acid attack of mild steel surfaces is not expected in the AP1000 plant and is discussed in detail in Section 21.5.9.2.

Lithium

Lithium is added to the primary circuit to increase the pH_T and establish alkaline conditions, which reduces the rate of general corrosion and localised corrosion mechanisms, such as SCC; it is discussed in Section 21.5.9.2. While the concentration of lithium must be balanced with the boric acid concentration required for reactivity control, lithium addition for the AP1000 plant is limited to a maximum concentration of [ ] ppm. However, lithium concentration itself may impact primary circuit materials and is controlled within the AP1000 plant to minimise any potential unfavourable impacts.

A number of studies (Reference 21.36) have looked at the effect of lithium concentration on the initiation rate of PWSCC in Alloy 600. Tests of reversed u-bend samples of MA and TT Alloy 600 in primary coolant containing from 2 to 6.5 ppm lithium suggested a minimum propensity for PWSCC at 3.5 ppm lithium. The pH_T varied, however, with lithium concentration from 6.9 to 7.4 and the minimum initiation rate corresponded to a pH of 7.1. Statistical analysis of other data has indicated a tendency for increased initiation rate with increasing lithium concentration but the effect is considered to be small. Also, Andresen studied the effect of lithium on CGRs of Alloy 600 in simulated PWR primary coolant and found nothing significant (Reference 21.34).Early studies of the effect of lithium on CGRs of Alloy 600 specimens, monitored by direct current potential difference (DCPD), showed some increase in SCC propagation rates with increased lithium concentration. A further study showed an inconsistent relationship between CGRs and lithium. Recent DCPD testing of an Alloy 600 fracture mechanics specimen, in which the lithium concentration was reduced in a single step from 4.3 to 2.2 ppm and with the CGR continually monitored during the period, showed no effect on CGR, although pH_T and conductivity changed (Reference 21.30).

Moreover, plant experience up to 2003, during which lithium concentrations were increased from 2.2 to 3.5 ppm, showed no detectable increase in PWSCC occurrence in either Alloy 600 or 690 SG tubes. Similarly, no effect on PWSCC of Alloy 690 is expected. Therefore, based on both experimental and operational experience of both Alloys 600 and 690, the application of lithium in the design of the AP1000 plant is within industry experience and has been demonstrated to have a small, acceptable effect on the SCC of Alloys 600 and 690.

Zirconium alloys used for fuel cladding have also been evaluated. Experimental work has shown that elevated lithium concentrations can lead to higher corrosion rates on zirconium alloys. Tests indicated a two- to six fold increase at 70 ppm lithium and a smaller but measurable effect at 7 ppm. Local subcooled boiling in crevices could produce high local concentrations of LiOH, giving high corrosion rates. Analysis of cladding oxide thicknesses from plants employing coordinated chemistry (2.2 ppm lithium) with others using enhanced lithium chemistry (up to 3.5 ppm) suggest that the oxide thickness is increased in the latter case by 10 to 15 percent. Loop tests using electrically heated rods showed little effect of 10 ppm lithium on Zircaloy with a thin oxide but enhancement of up to two times at very high oxide void fractions; however, the effect has been shown to be reduced in the presence of high concentrations of boric acid. As the lithium concentration in PWRs is related to that of boric acid, the practical influence of lithium on cladding corrosion may be small and only significant where a large degree of subcooled boiling or boiling within pores occurs. The AP1000 design is aimed at avoiding departure from nucleate boiling and minimising crud production, which will mitigate this possibility.

Zinc

Zinc can be incorporated into primary circuit oxides on stainless steels and nickel alloys. Oxides of these materials grown in the presence of zinc in the primary coolant grow more slowly and tend to be thinner than they would be in the absence of zinc dosing and have been associated with reduced rates of corrosion in austenitic stainless steels and in Alloy 600. Zinc has also been shown to reduce the risk of initiation of SCC in Alloy 600 (Reference 21.37). Additional details on zinc addition are available in Sections 21.5.5.4 and 21.5.9.2.

Temperature

Temperature affects both general oxidation and susceptibility to the probability of SCC occurring. Increasing temperature has been shown to increase SCC CGRs of cold-worked Alloys 600 and 690 but the temperature dependence appears to be stronger in the former case.

Figure 21-9 shows the relationship among SCC of stainless steels, potential, and temperature (Reference 21.35).

21.5.10 Chemistry Controls for the Minimisation of Primary Circuit Activity

21.5.10.1 Safety Requirements

Deposition of activated material on out-of-core surfaces leads to increasing circuit radioactivity and consequently higher dose rates for operators. Primary coolant chemistry is controlled to minimise the production, mobilisation, and deposition of activated material and thus minimise primary circuit activity. While details of the various chemistry parameters controlled on the primary side are provided in Section 21.5.5, the chemistry controls for the minimisation of primary circuit activity are discussed in the following subsections. See Section 21.5.6 for information on AP1000 plant design features that aid in controlling the buildup of primary circuit activity.

21.5.10.2 Technical Basis

Primary circuit radioactivity is produced from a combination of fission products leaking from fuel, tramp uranium impurities on the cladding, activated coolant additives (boron and lithium), activated impurities (e.g., nitrogen), and structural materials that have become activated. Materials exposed to core radiation fields become activated over time and form a number of radionuclides. Much of this material will be generated and remain on the reactor core. Corrosion processes generate species that can be transported in the primary coolant. Where these are generated within the core, they will include radionuclides that can then be transported to and deposit on other parts of the primary circuit. In addition, material generated out of core can be deposited in the core, become activated, and then be transferred to other parts of the circuit. Over time, an inventory of deposited active material crud builds up in the primary circuit and increases radioactivity throughout the system, contributing to operator dose during maintenance and refuelling activities. In addition, local crud deposits on the fuel may increase the cladding corrosion (CILC), potentially resulting in fuel rod failure. Excessive crud deposition on the fuel may also increase the risk for CIPS (see Section 21.5.4.2).

In primary coolant, nickel alloys and stainless steels oxidise at a low rate. The nickel alloys form a surface layer comprising a nickel/iron/chromium spinel. Stainless steels form a protective chromium-rich oxide. An outer crud layer, largely consisting of nickel ferrite, is formed from material crystallising from solution and the base material. Analysis of SG tubing primary-side oxide has revealed that the crud layer consists mostly of nickel ferrite ($NiFe_2O_4$) and nickel metal crud deposits on fuel have been analysed as non-stoichiometric nickel ferrites ($Ni_xFe_{3-x}O_4$), nickel oxide, and nickel metal. A small amount of cobalt is also present. In cores experiencing significant boiling, the nickel content of the crud can be elevated and is believed to represent large amounts of nickel oxide. The nickel can be activated in the core to ^{58}Co, which contributes a large part of primary circuit activity. Other radionuclides can be incorporated into the crud by substitution into the crystal lattice, including ^{60}Co from activated ^{59}Co.

The production of fuel crud is a function of the release of precursor species by primary circuit material oxidation. This is balanced by removal of these species through deposition in other parts of the circuit and by the purification system in the CVS. Alloy 690 has exhibited a lower oxidation rate than Alloy 600 in tests and this is expected to mitigate crud production in the AP1000 plant primary circuit. The deposited layer on Alloy 600 has been observed to be much thinner than the one on stainless steels; the one on Alloy 690 is less again. Zinc dosing is known to stabilise oxides on primary circuit materials to reduce overall crud production. In addition, zinc will block the deposition of circulating radio cobalt, allowing removal by the CVS and thus reducing the rate of increase in the radionuclide inventory. Zinc treatment is particularly effective if applied in the initial stages of oxide development. Zinc treatment will be applied during HFT of the AP1000 reactor to develop a stable zinc-doped oxide film, and during normal operation.

Operating chemistry, and particularly the environmental changes occurring during startup and shutdown, strongly influences corrosion product transport and inventory as well as activity distribution around the primary circuit. A number of factors, including temperature, oxygen concentration, and pH, can influence crud production through effects on oxidation of primary circuit materials and deposition and dissolution processes. In practical terms, the control of pH has been shown to be particularly important to overall crud production.

21.5.10.3 Method of Control

Oxygen

The production, dissolution, and deposition of crud are sensitive to the oxygen concentration and redox potential. The redox potential is controlled during operation by the hydrogen content of the coolant, and changes in hydrogen content or in-leakage of oxygen can alter crud production and distribution. A number of incidents have been recorded in which oxygen ingress resulted in increased crud deposits and reactor problems. In the AP1000 plant, the demineralised water system supplies the primary makeup water that is deoxygenated to ≤100 ppb so that oxygen ingress through makeup source is minimised. Maintaining a relatively low concentration of hydrogen (1 to 5 cc/kg H_2O) is sufficient to suppress radiolytically produced oxidising species from the core and the AP1000 plant chemistry specification calls for hydrogen concentration to be in the range of 25 to 50 cc/kg H_2O at power.

pH

Operating pH_T can significantly influence primary circuit crud production. Oxidation of primary circuit materials is pH-sensitive with lower corrosion rates in more alkaline conditions. Consistent with EPRI recommendations, Westinghouse requirements call for a pH_T of at least [ ] during operation at power (References 21.5 and 21.6). The AP1000 plant is designed to be operated to EPRI guidelines within a maximum lithium concentration of [ ] ppm required by Westinghouse as the fuel vendor (Reference 21.6).

Zinc

Addition of zinc to the primary coolant reduces oxidation rates of primary circuit materials, which reduces overall crud production and therefore the source term for activation of corrosion products. In addition, the incorporation of zinc in the oxide film inhibits the deposition of activated corrosion products on RCS surfaces, hence reducing radioactivity. Zinc addition is being increasingly used in PWRs throughout the world to mitigate buildup of active crud in reactors and radiation exposure to operators. Zinc will be added (as zinc acetate) to the primary coolant of the AP1000 plant at a target concentration of [ ] ppb, during power operation. The use of depleted zinc is recommended to maintain dose rates ALARP. Treatment with zinc from initial exposure to coolant at elevated temperatures, in this case during HFT, results in relatively thin oxide layers and gives the greatest benefit in terms of overall reduction of crud. While some mature plants have experienced elevated levels of radio cobalt in the coolant upon initiation of zinc injection due to the presence of oxide radio cobalt, this situation does not apply to the AP1000 plant since zinc addition will be initiated from the very beginning of the plant life.

Shutdown Operations

Chemistry control during shutdown is particularly important for reducing overall primary circuit activity and radiation exposure during an outage, and avoiding problems such as crud bursts. Westinghouse recommends the adoption of an appropriate strategy during shutdown in accordance with EPRI guidelines (Reference 21.2) and Westinghouse supplemental guidelines (Reference 21.6). Based on operating experience in cases where early reduction of pH_T prior to an outage resulted in high crud levels, EPRI recommends that a minimum coolant pH_T be maintained while at operating temperature. Although EPRI permits reduction to below this minimum pH during the 24 hours before shutdown, Westinghouse does not endorse or recommend this practice.

Shutdown chemistry is controlled to minimise radiation fields during the outage so far as is reasonably practicable (SFAIRP) by preventing particulate release and optimising corrosion product removal and cleanup. This is achieved by maintaining reducing conditions as the plant cools down and the coolant becomes more acidic. Oxidising conditions are then created in a controlled manner by introducing hydrogen peroxide, which dissolves nickel and cobalt, allowing for their effective removal by CVS purification. See Section 21.8.5 for additional recommendations on shutdown chemistry control.

21.5.11 Primary Chemistry As Low As Reasonably Practicable Goals

The design of the AP1000 plant has been optimised to ensure the safety of the primary circuit. Primary chemistry is controlled to control the reactivity of the core, ensure the integrity of primary fuel cladding and primary circuit materials, and minimise the radioactivity around the primary circuit. This is consistent with the safety claims made for the primary circuit chemistry as a whole, given in Section 21.5. The specific chemistry controls that ensure that the safety risk for the primary circuit is ALARP are summarised below:

- The injection of zinc from the beginning of plant life will result in corrosion films on primary circuit materials that are more protective, lowering corrosion rates and minimising the risk for PWSCC. This in turn will minimise the deposition of corrosion products on the fuel, resulting in lower risk for CIPS and CILC and significantly reducing primary circuit radioactivity.

- The boron concentration in the primary coolant is maintained according to the reactivity control requirements of the core as appropriate in all operational modes.

- The concentrations of contaminant species are maintained below specified levels that have been shown to minimise the risk of SCC of primary circuit materials and fuel cladding.

- The concentration of hydrogen is designed to achieve good oxygen control and thus low ECP in the primary circuit, while minimising the risk of SCC of structural materials.

- The pH_T is expected to be controlled within EPRI guidelines during power operation to minimise general corrosion and corrosion product deposition on the fuel (Reference 21.2). Within this pH range, the maximum lithium concentration is [ ] ppm to minimise the risk of unacceptable fuel cladding corrosion (Reference 21.6). While pH_T does influence the risk of corrosion failure through its effect on SCC, the impact is small within PWR power operation ranges.

Note also that in many cases, measures directed toward achieving one ALARP goal also serve to minimise the risk in another area. For example, minimising the risk for SCC avoids the need for component repairs that would result in additional worker exposure to radiation fields. Similarly, controls that ensure fuel integrity and minimise crud deposition on the fuel directly affect the radiation sources associated with fission products and corrosion products, thus minimising worker dose. Therefore, the overall strategy above is considered to reduce the risks to fuel and primary circuit integrity and primary circuit radioactivity to levels that are ALARP.

21.6 Secondary Circuit

This section describes the systems used to maintain and monitor the chemical properties of the secondary circuit, as well as the expected operational controls on chemistry parameters and design safety limits.

The following systems are covered:

- Secondary circuit
- Secondary sampling system (SSS)

- Steam generator blowdown system (BDS)

21.6.1 Description of the Secondary Circuit

The secondary circuit removes heat from the primary coolant in the SGs and converts it to electrical power in the turbine generators. The steam generated in the two SGs is supplied to the high pressure (HP) turbine by the main steam system (MSS). After expansion through the HP turbine, the steam passes through the two moisture separator reheaters (MSRs) and is then admitted to the three low-pressure turbines. A portion of the steam is extracted from the HP and low-pressure turbines for seven stages of feedwater heating. Further details of the system are given in Chapter 6 and in the AP1000 Chemistry Manual (Reference 21.5, Chapter 5).

Exhaust steam from the low-pressure turbines is condensed and is partially deaerated in the main condenser. The heat rejected in the main condenser is removed by the circulating water system (CWS). The condensate pumps take suction from the condenser hot well and deliver the condensate through four stages of low-pressure closed feedwater heaters to the fifth stage, open deaerating heater. Condensate then flows to the suction of each feedwater booster pump and is discharged to the suction of each main feedwater pump. The feedwater booster pumps are horizontal, centrifugal pumps located upstream of the main feedwater pumps. Each feedwater booster pump takes suction from the deaerator storage tank and pumps forward to its associated main feedwater pump. An electric motor drives both the booster pump and the main feedwater pump. The booster pump is driven by one end of the motor shaft and the main pump is driven by the other end through a mechanical speed increaser. The booster pump, operating at a lower speed than the main feedwater pump, boosts the pressure of feedwater from the deaerator to meet the net positive suction head requirements of the main feedwater pump. The feedwater pumps discharge the feedwater through two stages of HP feedwater heating to the two SGs.

21.6.2 Functions of the Secondary Circuit

The functions of the secondary circuit are as follows:

- Transfer of heat from the primary circuit
- Production of steam for the turbines
- Disposition of any radioactive material that enters from the primary circuit because of leaks

21.6.3 Secondary Circuit Chemistry Safety Requirements

The safety requirement of secondary circuit chemistry is to control corrosion of secondary circuit materials, control oxygen and contaminant levels in the secondary circuit, and thus maintain the integrity of the secondary circuit and the primary and secondary interface at the SG tubes and support heat removal functionality of the SGs.

The secondary circuit chemistry regime and administrative limits are specified by the plant operator. Westinghouse endorses the adoption of EPRI guidelines and the AP1000 plant is designed to operate safely within them. The AP1000 Chemistry Manual (Reference 21.5, Chapter 5) provides secondary chemistry guidance to operators based on EPRI guidelines (Reference 21.4) and appropriate safety limits for operation of the secondary circuit plant.

These safety limits are summarized in Table 21-6. Any description of secondary chemistry operating parameters or strategies given herein is based on current options discussed in Reference 21.5, Chapter 5.

The secondary chemistry achieves its safety objectives by maintaining an environment compatible with circuit materials, i.e., all-volatile treatment (AVT) alkalinity and low ECP conditions, while minimising the concentrations of contaminant species. This especially relates to halides, sulphate, and low melting-point metals. An AVT chemistry is adopted to minimise the risk of sludge accumulation and hence localised corrosion of SGs and to enhance chemical control in the condenser.

21.6.4 Corrosion Control

Another major function of secondary circuit chemistry is controlling the corrosion of materials exposed to the secondary coolant, including structural components. This section describes the potential mechanisms of corrosion, the principal materials used in the secondary circuit, and the influence of secondary coolant chemistry.

21.6.4.1 Deterioration Mechanisms

Relevant deterioration mechanisms are briefly described in this section together with some simplified statements of the mitigation measures used in the AP1000 plant in each case. Corrosion control is achieved largely through a combination of SG design, materials selection, and chemistry control. Further details of chemical and materials mitigation measures are discussed in Sections 21.6.4.2 and 21.6.4.3.

Many of the material degradation issues of concern in the primary circuit, including SCC, also apply to the secondary side. However, the environment of the secondary circuit operates at lower temperature and much lower pressure than the primary circuit and comprises a two-phase system. Therefore, the secondary circuit is subject to several additional corrosion mechanisms relative to the primary system. Localised boiling flux in flow occluded regions (e.g., crevices) within the SG may concentrate dissolved impurities, resulting in sufficiently high impurity concentration and regions of elevated superheat that result in localised corrosion. In addition, various materials of construction are encountered so that SCC, general corrosion, and FAC are all potential corrosion mechanisms in the secondary circuit. Other deterioration mechanisms such as pitting and wear of SG tubes have been observed in the operating plants.

Oxidation

General corrosion (oxidation) of the pipework, low-alloy components in SGs, and turbine materials does occur because of the higher ECP in the secondary circuit and the presence of considerable amounts of low-alloy and carbon steels. Control of general corrosion is achieved by employing an AVT treatment for chemistry control in the secondary circuit and control of dissolved oxygen.

The AP1000 plant uses AVT chemistry control to create alkaline conditions in combination with a reduced oxygen environment to minimise ECP and thus mitigate the impact of general corrosion. In addition, the conditions established by AVT chemistry control promote the formation of a stable oxide layer on the steel surface, a key factor in minimising the general oxidation of ferrous materials and subsequent deposition of corrosion products on SG surfaces.

Both pH control additives and oxygen scavengers (e.g., hydrazine) are considered a part of AVT chemistry and are added to control the chemistry of both the liquid and two-phase regions of the secondary circuit. The volatility of these feedwater additives allows for simultaneous control in both liquid and two-phase regions from the same additives. For pH control, volatile additives, such as ammonia, amines, or a combination thereof, have been adopted to establish an alkaline environment to reduce the amount of general corrosion without contributing to the impurity concentration in crevices. For oxygen control, the AP1000 design specifies the addition of hydrazine, a volatile oxygen scavenger used as part of the overall AVT chemistry control strategy.

Pitting

Pitting is a form of localised corrosion characterised by the appearance of a cavity in the material and has been observed in the secondary side of operating PWR SGs. An active pit can quickly result in localised through-wall corrosion or provide an initiation site for SCC. Pitting observed on turbine blades and discs has generally been attributed to defects in the materials. Pitting on the SGs is seen on stainless steels exposed to acidic oxidising conditions, particularly in the presence of copper, chlorides, and to a lesser extent, fluorides. Alloy 600MA tubes have also been reported to show evidence of pitting, especially in acid-oxidising conditions in the presence of copper, chloride, or sulphate (Reference 21.4).

Along with the use of advanced alloys, the AP1000 plant mitigates pitting through strict control of chemistry including compliance with EPRI guidance. AVT chemistry is used to maintain alkaline conditions and control of oxygen concentration within the secondary circuit. Also, since chloride and sulphates have been associated with pitting in some PWR applications, vigilance in the control of contaminant levels is required. However, it should be noted that plants with observed pitting on SG tubing correlated with introductions of brackish water or seawater from the cooling system or from copper from the balance of plant components. The AP1000 design has greatly reduced the known culprits of pitting by using titanium condenser tubing, which is has demonstrated less susceptibility to corrosion; and eliminating copper or copper alloy components within the secondary circuit. The AP1000 design along with AVT chemistry coupled with rigorous operational impurity and maintenance foreign material exclusion control of the secondary systems reduces the likelihood of pitting corrosion.

Stress Corrosion Cracking

Many cases of field-related SCC on the secondary side of A600MA SG tubes have been reported and the causes have been extensively investigated. Varieties of environments leading to aggressive SCC degradation of SG tubes have been identified in the laboratory, and testing programmes have been refined to evaluate material performance in both isothermal and heat transfer environments, such as model boiler testing. Identification of aggressive corrosive conditions has facilitated laboratory testing, resulting in qualification of advanced materials for SG tubing.

As repair methodologies progressed beyond tube plugging to include sleeving of degraded SG tubing, advanced materials were used as the sleeve tubing of choice; these were sometimes further tailored to provide resistance to the field-observed SG specific corrosion environment. The most common materials for the >100,000 sleeves installed worldwide were either A600TT or A690TT. A clad tubing material with A625 on the outside diameter (OD) and A690TT on the inside diameter (ID) was also installed into field service (Reference 21.40). The clad tubing was chosen to give pitting resistance on the OD and PWSCC resistance on the ID. Field NDE of the sleeve materials showed good corrosion resistance in general and provided additional service experience for these materials.

The observation of caustic related SCC and intergranular attack (IGA) in the 1980s (Reference 21.41) spurred laboratory development work on SG tubing materials and a very extensive database was developed by Westinghouse and other research and development efforts worldwide. Many extremes of environments involving testing parameters of solution chemistry, deposit chemistry, temperature, stress level, material type and condition, heat transfer, flow conditions, crevice design, and so forth were evaluated. The database grew to such an extensive size and varied quality of information that citing of individual experiments could not be considered representative of the available data.

A reasonable attempt to interpret this large laboratory-based data set involved the creation of improvement factors that allowed the performance of one material tested in an environment to be compared to the result for a different material or material condition tested in the same or a similar environment (Reference 21.42). A600MA became the reference material as the base for comparisons. The overall comparative results for the performance of A690TT versus A600MA overwhelmingly favours A690TT for outside diameter stress corrosion cracking (ODSCC) as well as PWSCC. As an example, caustic environment improvement factors for A690TT compared with A600MA generally range from 2 to >200 based on material considerations alone (Reference 21.43).

Although the laboratory-generated materials improvement factors show benefit, the requirement of producing useful laboratory data in a relatively short exposure time results in laboratory conditions that are generally very aggressive and may be accelerated by using increased temperature, very high stress levels, and/or unusually aggressive chemical environments. These conditions are not likely to be experienced for sustained periods of time in actual operational experience and result in improvement factors that are overly conservative. Therefore, the better measure of field performance is field performance itself and A690TT SG tubing material, which in 2011 has been in commercial SG service for more than two decades, is presently generating an exceptional record.

An extensive evaluation of United States' experience with A690TT SG tubes in commercial PWRs has been compiled and published as a Nuclear Regulatory Commission technical report designation (NUREG) document (Reference 21.44). At the time of data compilation at the end of 2004, A690TT had been in service in replacement SGs since 1989.

The NUREG reports that of the 577,070 A690TT tubes placed in service, no corrosion failures had occurred and only 0.06 percent of the tubes had been removed from service for all other reasons including mechanical wear and pre-service plugging.

A more recent report (Reference 21.45) updates this continuing service exposure, confirming that as of October 2010, service-induced corrosion degradation has not been observed in A690TT SG tubing.

The performance record generated by the operation of A690TT SG tubing continues even under some corrosion-promoting conditions where the SG tubes are being subjected to non-design configurations as a result of denting occurring at the tube sheet region. In a recent SG operating experience summary, it was reported that top of tube sheet (TTS) denting at Almaraz 1 and 2 and at ASCO 1 and 2 had resulted in circumferential cracking of the Incoloy 800 SG tubing. Similarly the Belleville 2 A600TT tubing was degraded with circumferential cracking at the TTS as a result of denting. The Ginna instance of TTS denting has not resulted in cracking of the A690TT SG tubing material as of the last (2008) inspection (Reference 21.46).

It should be noted that the physical deformation caused by denting of SG tubing, which occurs under operational conditions, represents a highly unusual condition that has not been extensively tested with A690TT.

As result of the inherent A690TT material performance, coupled with secondary-side design and manufacturing and operations advances, such as redesigned support structures with corrosion-resistant materials, full-depth hydraulic expansion in the tube sheet crevices, and improved chemistry operations, continuing corrosion-free performance is expected to lead to higher improvement factor values as operational experience accumulates (Reference 21.45). These results support the appropriateness of the current AP1000 plant design recommendations for secondary circuit chemistry.

Crevice Corrosion and Denting

Particular features of secondary-side SG environments are the accumulation of sludge on the tube sheet, deposit buildup on the tubes, and corrosion in crevices formed between the tubes and tube sheet or tube support plate. In-situ formation of iron oxide within these crevices adjacent to tubing can result in denting. The localised stress gradient induced by the denting can lead to SCC of the tube. Such instances of SCC attributed to denting have been observed in operating plants. Denting occurs when elemental iron is oxidised in a geometrically restricted region (deep crevice or shallow crevice beneath a sludge pile), and the oxide formed from the corroded iron occupies more volume (Pilling-Bedworth Ratio), resulting in a localised force exerted on the tubing. In addition, the geometrically restricted region can produce crevices where local boiling leads to concentration of solutes and the formation of local shifts in pH. Contaminants, such as chloride, can become concentrated in crevices and form localised acidic or alkaline conditions. The original problem was mitigated in earlier plants by changing chemistry environments in the areas of concentration, boric acid soaks, and boric acid addition to neutralise the concentrated solutions.

Several features in the AP1000 plant SG minimise crevice areas and the deposition of contaminants from the secondary-side flow. The AP1000 SGs have stainless-steel tube support plate material for improved corrosion resistance and broached trefoil hole design with the flow area adjacent to the tube to reduce the risk of deposition. Also, the potential crevice between the tube-to-tube-sheet interface has been removed by full-depth hydraulic expansion. The length of the expansion is carefully controlled to minimise the occurrence of an overexpanded condition above the tube sheet and to minimise the extent of unexpanded tube at the top of the tube sheet. Thus, the AP1000 design has included design elements that provide improved ability to avoid or minimise the potential for crevice corrosion and denting. Chapter 15 of the AP1000 Chemistry Manual provides further guidance to identify and mitigate excessive sludge accumulation on the TTS.

Flow-Assisted Corrosion

FAC is an extension of a general corrosion process. FAC occurs through disruption of the normally protective oxide layer on the material surface under flow, leading to localised thinning of the oxide and subsequent increased corrosion rates. Under sufficient reducing conditions, the magnetite oxide layer at the oxide-water interface is dissolved. The material corrodes as it tries to re-establish the oxide under flow. FAC has been observed in all PWR secondary circuits to varying extents, and the AP1000 plant has used both design and operational recommendations to reduce the areas susceptible to FAC.

FAC has a parabolic relationship with temperature. FAC rates are typically highest at temperatures between 120 and 205°C (248°F and 478.4°F) because of the increased solubility of $Fe(OH)_2$ in that temperature range and are therefore a concern for the regions of the secondary circuit that operate in this range. Carbon steels and LASs are particularly susceptible, as are any materials that form a protective iron oxide (magnetite) layer. In addition, design and operational factors, such as piping geometry, materials of construction, stream velocity, and steam quality, also strongly influence FAC rates and material susceptibility. For example, moisture content in steam lines is minimised in the AP1000 plant through the use of condensate drains, chevrons, and reheat; the pipe system is designed to minimise abrupt changes in flow. Also, metal loss rates are strongly influenced by a number of chemistry factors, including pH control dissolved oxygen concentration and lack of copper alloys in the BOP. For chemistry control in particular, oxygen content and pH are controlled to reduce the risk of FAC on susceptible materials.

Material loss decreases with increasing pH of at least up to 10 (measured at 25°C (77°F). Studies have shown that FAC rates decrease by a factor of 25 if the pH_T increases from 6.7 to 7.1 (Reference 21.47). The pH in PWR secondary circuits is controlled by dosing with a pH control chemical, such as ammonia or an amine.

Oxygen has also been shown to have an effect on rates of metal loss due to FAC at operating temperatures. Very low concentrations of oxygen (<2 ppb, depending on temperature and flow conditions) result in increased rates of metal loss (Reference 21.48). At Seabrook, it was found that reducing the condensate dissolved oxygen concentration to 0.7 ppb increased the iron concentration to above 25 ppb; however, increasing the oxygen concentration to 2 to 3 ppb decreased the iron content to 5 to 6 ppb (Reference 21.49). This effect of increased oxygen content is interpreted as being due to the consequent upward shift in ECP providing a more stable passive oxide layer. Typically, plants aim to control condensate-dissolved oxygen to more than 2 but less than 10 ppb. In addition, materials for the AP1000 plant secondary circuit have been selected to minimise FAC and subsequent corrosion transport to the SG. In particular, copper alloys, which require low pH control regimes that are more susceptible to FAC, are prohibited for components that are in contact with feedwater, steam, or condensate. Material selection for MSRs, condenser tubes, and feedwater heaters is consistent with the recommendations given in EPRI NP-2294 (Reference 21.50). FAC-resistant materials employed include chromium alloy (ASTM A335 Grade P-11 or equivalent) and austenitic stainless steels. Where carbon steel is used, an additional thinning allowance of 2 mm is applied.

Chemical control measures (Section 21.6.4.3 below), material selection (Section 21.6.4.2 below), and design features have been employed in the AP1000 plant to reduce the material loss as a result of FAC. In addition, lower FAC reduces the quantity of corrosion products transported throughout the secondary circuit, which in turn reduces SG sludge accumulation. Excess SG sludge accumulation has been associated with increased potential for SG tubing degradation and reduced SG thermal and hydraulic performance.

Turbine Corrosion

Turbine blades and discs can suffer from pitting, corrosion fatigue, and SCC. The incidence appears to be related to oxygen ingress and condenser leaks. While the chemical environment could impact corrosion, the cause of turbine blade and disc corrosion has been attributed to defects in the materials and not chemistry. Current EPRI guidance, which is endorsed for the secondary system of the AP1000 plant and an ALARP approach to secondary chemistry, has demonstrated success in reducing or eliminating instances of turbine blade corrosion.

21.6.4.2 Materials

Secondary circuit materials are selected to be resistant to the various corrosion mechanisms that they are likely to encounter. EPRI NP-2294, the EPRI SG handbook, and the URD document (References 21.41, 21.50, and 21.51) provide material recommendations to overcome the various corrosion problems. AP1000 plant secondary-side material selections comply with these recommendations. The safety limits selected in Table 21-6 are principally related to the material selection process (refer to Reference 21.76). The following is a brief discussion on the materials used throughout the AP1000 plant secondary circuit.

The MSR tubes are made from a ferritic stainless steel. The chevrons are composed of stainless steel and the shell is constructed from carbon steel with chrome steel or stainless-steel overlays and impingement plates. The condenser shell is made from carbon steel with impingement plates to protect against erosion. The condenser tube sheet is made from titanium-cladded carbon steel and the tubes are titanium grade 2. Feedwater heater tubes are manufactured from a ferritic stainless steel and the feedwater heater shells are made from carbon steel with stainless-steel overlays and impingement plates; the tube sheets are carbon steel, clad with stainless steel in the HP heaters. Piping is made from carbon steel, chromium-molybdenum alloy steel or stainless steel.

Wall thinning from erosion-corrosion effects does not occur in the auxiliary stainless-steel piping and tubing because Series 300 austenitic stainless materials are highly resistant to these effects. There is no record of erosion-corrosion-induced wall thinning in the stainless-steel piping of operating plants.

The SGs use Ni-Cr-Fe alloys in contact with fluids wherever erosion-corrosion or FAC could be a problem, including the nozzles on the feedwater ring and startup feedwater sparger. The tubes are made from TT Alloy 690, which has a high resistance to general corrosion and SCC. The channel head divider plate is also Alloy 690. The interior surfaces of the reactor coolant channel head, nozzles, and manways are clad with austenitic stainless steel. The primary side of the tube sheet is weld-clad with Ni-Cr-Fe alloy. The tube support plates are made of corrosion-resistant Type 405 stainless-steel alloy. Further details are given in Table 20C-2.

The main condenser is a three-shell, single-pass, multi-pressure (or single pressure if the plant uses seawater as cooling water source), spring-supported unit. Each shell is located beneath its respective low-pressure turbine. The condenser is equipped with titanium tubes. The titanium material provides good corrosion- and erosion-resistant properties. Continuous online instrumentation is utilised to detect condenser leaks by monitoring for cooling water ingress at each condenser hot well segment. Depending on the cooling water chemistry and leak rate, analysis of hot well samples often can be used to locate the particular condenser tube bundle containing the tube leak. Once the affected tube bundle has been identified, reactor power must be reduced to a level that can be supported by the unaffected cooling water train. The cooling water supply to the leaking condenser tube bundle should then be isolated and the tube side of the condenser drained for repair.

Copper and copper alloys are not used for any components in contact with secondary circuit feedwater, steam, or condensate to avoid corrosion problems. The only exceptions are the HP turbine casing and HP turbine stop and control valve bodies, which are a cast 0.5 copper-nickel-chromium steel. This material is the standard design of the turbine supplier and has been used in other operating PWRs. The addition of a very small amount of copper provides better erosion resistance for the wet steam conditions in the HP turbine. The copper is bound and is not residual surface copper.

21.6.4.3 Chemistry

The secondary circuit chemistry is integral to the successful management of circuit materials. Much effort is put into optimising the chemistry to minimise corrosion risks discussed in Section 21.6.4.1 and to maximise the system performance. The secondary water chemistry is the responsibility of plant operators. As described within Reference 21.5, Westinghouse mandates strict adherence to EPRI guidelines. Each plant is required to develop and maintain a secondary-side strategic water chemistry plan that considers plant-specific design, operating parameters, operating history, component warranty requirements, and utility-specific goals.

The secondary circuit chemistry uses AVT to control the pH and dissolved oxygen concentration and an ALARP approach for impurity concentrations maintained within EPRI guidance. The selection of pH control additive(s) with the appropriate relative volatilities ensures adequate chemistry protection in both the liquid and steam phases in the secondary circuit. To preserve the integrity of the secondary circuit and comply with EPRI guidelines, an ALARP approach to impurity control is prudent. To maintain impurities at ALARP levels, ingress of ionic impurities, such as sodium, fluoride, chloride, and sulphate, is controlled through a combination of makeup water quality and removal of secondary ionic impurities through the BDS EDI unit and the CPS. Metal impurities, such as copper and lead, are controlled through specifications applied to AP1000 plant materials of construction. These specifications have eliminated materials such as copper-alloy tubing in the main condenser in favour of titanium tubing. For both dissolved and particulate impurities, control limits have been placed on the secondary circuit to minimise the impact on the corrosion of SG and secondary-side materials. Further control of FAC and ODSCC of SG tubing is achieved through pH and oxygen control in the secondary feedwater.

The secondary-side water chemistry pH is maintained in a basic regime to minimise the amount of corrosion product transport that occurs by lowering the solubility of ferrous metal corrosion products in solution. In addition to pH control, an optimum oxidation reduction potential (ORP) is maintained through dissolved oxygen control. The combination of alkaline pH and optimised ORP in secondary feedwater provides a thermodynamic region of protective oxide stability to reduce FAC in ferrous piping while still maintaining an environment against SG tubing that provides optimum protection against ODSCC. To maintain a stable passive oxide layer, proper control of pH and ORP is crucial. The passive oxide layer in secondary piping is a thin, tightly adherent oxide layer that forms on the metal surfaces and provides an increased resistance to FAC. The AP1000 plant uses AVT pH control additives, such as ammonia, amines, or a combination thereof to control pH in both the liquid and two-phase regions of the secondary circuit. Thus, an alkaline pH can be maintained in both the liquid and two-phase regions to reduce the rate of FAC of secondary circuit materials.

Also, the amount of dissolved oxygen is directly related to the control of electrochemical corrosion potential within the SG. Elevation of dissolved oxygen concentrations in the bulk fluid increases the following:

- General corrosion rates of carbon steels
- Pitting, IGA, and ODSCC susceptibility of nickel-based and austenitic alloys
- Formation of oxidising species such as hematite or cuprite

By controlling dissolved oxygen in the SG, the formation of magnetite against the tubing surfaces is promoted, and the formation of hematite is prevented. The oxygen concentration within in the secondary circuit is controlled by a catalytic oxygen recombining system and the addition of hydrazine to scavenge and react with any dissolved oxygen. However, as noted in Section 21.6.4.2, too low of a dissolved oxygen concentration may lead to FAC. Therefore, the concentration of oxygen in the secondary circuit must be balanced to control the ECP within the SG and FAC in the rest of the secondary circuit. Additional details on oxygen control are available in the AP1000 Chemistry Manual (Reference 21.5).

Impurity ions, such as sodium, fluoride, chloride, and sulphate, are measured in most nuclear power plants because of their role in promoting several different kinds of submodes of localised corrosion within the SG and FAC in the steam drum and steam flow path. In particular, SCC and pitting are two types of corrosion that have occurred in nuclear power plants and are associated with elevated levels of particular ionic impurities. While materials now used to construct SGs, such as Alloy 690TT, are much more resistant to SCC than the original mill-annealed or Alloy 600TT, laboratory testing has demonstrated their susceptibility to SCC and pitting in sufficiently off-normal chemistry conditions (e.g., caustic solutions with high concentrations of lead).

In addition, elevated ionic impurities in the presences of excess sludge piles or crevices have demonstrated the formation of environments conducive to denting, resulting in a localised stress condition against the tubing. Hence, controlling the concentration of dissolved impurities is still prudent for adequate protection of the SG and steam flow path materials. In addition, dissolved impurities concentrate in crevices, thereby producing localised regions of elevated concentrations and superheat leading to environments conducive to localised corrosion. In the AP1000 plant, the concentration of ionic impurities is minimised by compliance with EPRI guidelines and using ALARP methods. Also, conductivity, which is an overall measure of the concentration of dissolved solids, is continuously measured in the EDI stack inlet line and in the process outlet line as a means of detecting condenser leakage into

the secondary system. Two redundant trains of two series (roughing and fine) filters are located directly upstream of the EDI nozzles in order to prevent particulate from entering the EDI modules.

For the AP1000 plant, condensate polishers can be used to purify feedwater if a condenser leak rate is sufficient to approach or exceed the administrative action levels of a plants secondary chemistry. The condensate polishers require a reduction to 30% main steam rate to provide 'full flow' polishing capability (30% power allows full flow through the condensate polishers.

Further information on secondary circuit chemistry is given in the AP1000 Chemistry Manual (Reference 21.5, Chapter 5); including a detailed description of the condensate polishing system and the capabilities provided to support secondary chemistry control (Reference 21.5, Section 5.2.1). Additional discussion of secondary circuit chemistry recommendations during shutdown and startup are provided in Section 5.5 of Reference 21.5.

21.6.5 Secondary Circuit Sampling System

The AP1000 plant SSS delivers representative samples of fluids from secondary systems to sample analyser packages. Continuous or semi-continuous online secondary chemistry monitoring detects impurity ingress and provides early diagnosis of system chemistry excursions in the plant. Secondary sampling monitors send control signals to the turbine island chemical feed system (CFS) that automatically injects chemicals into the condensate and feedwater systems to control pH and dissolved oxygen concentration. PCSR Section 6.5.16 and Reference 21.38 contains further discussion of the SSS.

Within the secondary sampling system, some sample points are continuously or semi-continuously monitored. Other sample points are selectively monitored (where a single analyser package can be used to selectively monitor multiple sample points). A complete list of sampling points is given in Table 21-3 and Table 21-4.

After being analysed, noncontaminated samples are returned to the condensate system (CDS). Sample lines containing reagents and those from sink drains are collected in the waste water system (WWS) and processed for disposal.

The SSS monitors water samples from the CDS, feedwater system, MSS, BDS, auxiliary steam supply system (ASS), condensate polishing system (CPS), and heater drains. Water quality analyses are performed on these samples to determine the necessary parameters for controlling the water chemistry.

21.6.6 Steam Generator Blowdown System

The BDS assists in maintaining acceptable secondary coolant water chemistry during normal operation and during anticipated operational occurrences of main condenser inward leakage or primary-to-secondary SG tube leakage. It does this by removing a small fraction of the bulk fluid from the SG in which the impurities have become concentrated. The BDS accepts water from each SG and processes it as described below.

The blowdown from each SG is cooled by a regenerative HX, and the pressure is reduced by blowdown flow control valves. To recover the blowdown fluid, each blowdown train has an electrodeionisation (EDI) unit that removes impurities from the blowdown flow. The blowdown fluid is processed through the EDI units and [ ] percent of the flow is discharged to the CDS (condenser hot well) for reuse. The remaining [ ] percent is

discharged to waste. If radioactivity due to SG tube leakage is detected in the blowdown flow, BDS flow is automatically diverted to the WLS for processing and disposal.

Further details about the BDS are given in the AP1000 Chemistry Manual (Reference 21.5, Chapter 5), and Section 6.5.11.

21.6.7 Condensate Polishing System

The CPS is a secondary cycle condensate cleanup system consisting of deep bed ion exchange vessels aligned to remove corrosion products, dissolved solids, suspended solids, and other impurities from the condensate system. The CPS is used principally during startup to reduce the time necessary to achieve proper secondary circuit chemistry and can be used during power operation to maintain proper secondary circuit chemistry following impurity ingresses during abnormal event(s) such as a condenser tube leak.

Selection of a system type and mode of operation is site specific depending on the CWS water quality design basis. As a result, condensate polishing systems have been installed in various configurations. For plants using fresh or brackish water as the cooling medium in the CWS, a one-third condensate flow CPS may be used such that 100% of the condensate may be processed during plant operations in Modes 2, 3, 4 and 5 (startup, hot standby, safe shutdown and cold shutdown, respectively). A full condensate flow CPS may be specified for an AP1000 plant that uses seawater as the CWS cooling medium.

Refer to Section 6.5.15 of this report for additional details on the CPS.

21.7 Auxiliary Water Systems

Like the primary and secondary circuit material selection and chemical regimes, the auxiliary systems have been designed (chemically and materially) to reduce the risk of fault conditions occurring. The fault conditions for these systems from a chemical perspective are the corrosion effects (which can result in leaks) or fouling of the pipes, which could reduce flow rates and impact the effectiveness of the system. The chemical regimes selected for these are chosen to mitigate the risk of these events occurring.

21.7.1 Component Cooling Water System

21.7.1.1 Description of the Component Cooling Water System

Section 6.11.1.1 of this report provides a detailed description of the CCS design and configuration, including its safety functions and defence in depth functions.

21.7.1.2 Component Cooling Water System Chemistry

The safety requirement of the CCS chemistry is to minimise the risk of loss of integrity of the CCS through corrosion or a loss of function through fouling.

The CCS is chemically treated for the purpose of minimising corrosion of system materials and prolonging equipment life. Component cooling water essentially consists of demineralised water, to which one or more corrosion inhibitors and pH control agents are added to protect the materials of construction in contact with the fluid. Additional chemicals may be dosed to prevent biological growths or fouling (Reference 21.5).

Westinghouse does not dictate specific chemical regimes for the CCS, but directs the utilities operating the plant to follow the EPRI guidelines (Reference 21.3), as they apply to the chemical treatment options found suitable for use in the AP1000 plant. Westinghouse has performed calculations to support the design of the CCS within the limits of the EPRI guidelines to demonstrate that materials selected operate sufficiently within the proposed chemical regime. (Reference 21.81)

The operating ranges are suggested by EPRI for water chemistry. The AP1000 proposed chemical regime is presented in the AP1000 Chemistry Manual (Reference 21.5, Chapter 6), with safety limits for the chemistry provided in the summary report of AP1000 plant chemistry characterizations (Reference 21.76, Table 5-4).

In the event of deviation from proper chemistry in the CCS coolant, appropriate chemicals are added via the chemical addition tank and mixing is achieved through a recirculation line from the pump discharge header through the operating surge tank to the pump suction line.

Corrosion Inhibitors

The EPRI guidelines for closed-loop cooling water systems recommends various chemical treatment programmes to minimise the corrosion of the CCS materials. Specific corrosion inhibitors are dependent on utility preferences. The example inhibitors suggested by the guidelines are listed in the EPRI guidelines (Reference 21.3). pH control chemicals are also added to maintain the pH in a range where corrosion is minimised and treatment chemicals are most effective. In addition, Westinghouse has stated that the AP1000 plant design should not use chromates or silicates, which are suggested as coolant treatments in the EPRI guidelines (Reference 21.3).

Faults

Operation of the CCS outside of the proposed chemistry regime will result in increased risk of fouling and corrosion rates. The long-term consequence of an increased corrosion rate in the CCS is an increased risk of leaks in the system, either between the RCS and CCS, or out of the CCS to other CCS users or the environment.

The monitoring of the flow rate, temperatures, and pressure of the CCS can be used to indicate fouling or leaks.

Leaks

In the event of a leak from the CCS, the level in the surge tank will drop as the coolant drains from the system. The surge tank will then be supplied automatically with water from the DWS.

If there is a large leak, the level will drop further, actuating a second alarm that prompts the operator to investigate the leaks visually or through investigation of flow rates across components. If the components cannot be isolated or the leak sealed, then the level will drop further, initiating a third alarm that will shut off the pumps.

A leak from the CCS into the RCS is only possible during shutdown when the RCS is depressurised. Detection would be as above and any contamination of the RCS would be detected by normal sampling prior to startup and then rectified.

Leaks of the Reactor Coolant System in the Component Cooling Water System

In the event that a significant amount of primary coolant is lost (therefore a significant transfer of active inventory), the valves on the CCS within the containment isolation section will close to prevent radiation exposure out of containment.

21.7.2 Normal Residual Heat Removal System

21.7.2.1 Description of the Normal Residual Heat Removal System

The RNS consists of two trains, each with one RNS pump, one RNS HX, and interconnecting piping and valves configured to allow redundancy of any one component or pipe section. All components in the RNS circuit are designed and built to withstand full reactor temperature and pressure. Each RNS train discharges to a separate direct vessel injection (DVI) line, which is part of the PXS (discussed in Section 21.7.3) connected directly to the RPV.

See Section 6.4.3 for a full description of the RNS circuit.

21.7.2.2 Normal Residual Heat Removal System Chemistry

The RNS chemistry serves to minimise corrosion of RNS materials to maintain the structural integrity of the system.

During operation of the RNS in cooldown mode, primary coolant will be flowing through the RNS with nominal primary coolant chemistry. Sampling may be performed using the normal residual heat removal HXs channel head drain connections. Sampling of the RCS using these connections is available at shutdown.

The RNS is constructed of the same materials as the primary circuit and will operate with primary coolant chemistry but at a lower temperature and pressure (less than 177°C (350°F) and 3.10 MPa gauge (450 psia)); it is designed to maintain the coolant temperature at approximately 52°C (125°F). Given that the coolant chemistry has been designed to operate with the RCS and RNS materials at a higher temperature (therefore at an increased corrosion rate), the RNS should be sufficiently corrosion-resistant to cope with the flow of RCS coolant. For safety limits for the RNS chemistry, refer to the safety limits provided for the primary circuit in Section 21.5.

In the event of out-of-chemistry conditions, the RNS will react in a fashion similar to the RCS, but given the lower operating temperature and short duration of operation of the RNS, the effects would be greatly reduced.

21.7.3 Passive Core Cooling System

21.7.3.1 Description of the Passive Core Cooling System

The PXS is a Class 1 system consisting of two CMTs, two accumulators, the IRWST, the PRHR HX, depressurisation spargers, and pH adjustment baskets; and associated piping, valves, instrumentation, and other related equipment.

In addition to heat removal, the PXS is used to supply coolant to the core. This is provided by the CMTs. The CMTs provide RCS makeup and boration during events not involving loss of coolant when the normal makeup system is unavailable or insufficient.

Along with the CMTs, the AP1000 design utilises two accumulators containing borated water with a compressed nitrogen cover. The accumulators can deliver a very high flow of coolant into the RCS for a short duration. They are used in conjunction with the CMTs during loss-of-coolant accident (LOCA) events to maintain sufficient cover of the fuel to provide heat extraction. Please see Section 6.6.1 for a detailed description of the PXS.

The primary function of the PXS during a safe shutdown using only Class 1 equipment is to provide a means for boration, injection, and core cooling. The PXS is capable of maintaining the desired post-accident pH conditions in the recirculation water after containment flood up. Please see Chapter 22 for details related to pH control during post-accident conditions.

Refuelling

The IRWST is sized to facilitate the flooding of the refuelling cavity with borated water for normal refuelling and the post-LOCA flooding of the containment for RCS long-term cooling mode; to support the PRHR HX operation; and to supply borated water to the SFS (Reference 21.6). Flow out of the IRWST during the injection mode includes conservative allowances for spill flow during a DVI line break. The tank is lined with stainless steel and is provided with a vented cover to avoid the ingress of debris. The boron concentration can be adjusted by the CVS and is specified between 2600 and 2900 ppm boron.

21.7.3.2 Functions of the Passive Core Cooling System

The PXS has three functions: first, to provide a decay heat removal system through the PRHR HX for use after transients that prevent normal heat removal via the SGs; second, to provide emergency core cooling following postulated events; and third, to provide borated water to the refuelling cavity from the IRWST. To accomplish this, the PXS is designed to perform the following functions:

- Emergency core decay heat removal
- RCS emergency makeup and boration
- Safety injection
- System depressurisation
- Containment pH control
- Provide a source of borated water for flooding the refuelling cavity during refuelling

21.7.3.3 Passive Core Cooling System Chemistry Safety Requirements

The PXS chemistry has the following four safety functions:

- Boration of the core in accident scenarios where loss of primary coolant occurs
- Boration of refuelling cavity water
- Maintenance of system integrity by minimising the risk of corrosion damage
- Control of fission products in containment in the event of a leak by maintaining alkaline conditions in leaked coolant

21.7.3.4 Chemistry and Materials

Those portions of the PXS in contact with reactor coolant are fabricated from or cladded with corrosion-resistant material. Sulphur, lead, copper, mercury, aluminium, antimony, arsenic, and other low melting-point elements and their alloys and compounds are restricted in their use in the construction (both as construction materials and as substances that come into contact with the construction materials) of the PRHR HX that are in contact with RCS fluid or the IRWST. Contamination of stainless steel and Ni-Cr-Fe alloys by copper, low-melting-temperature alloys, mercury, and lead is prohibited. For these portions of the PXS, refer to the general primary circuit description of safety limits provided in Section 21.5.

The PRHR HX, accumulators, and CMTs are constructed from materials specified to minimise corrosion and erosion and to provide compatibility with the operating environment, including the expected radiation level. These include austenitic stainless steels of grades derived from American Iron and Steel Institute (AISI) Type 304 for the plates and forgings of the PRHR HX, and ASTM Ni-Cr-Fe alloy N06690 for the PRHR tubing. Chapter 20 details the fabrication, installation, and manufacturing processes and procedures to minimise the sensitisation of components and corrosion of the stainless steel, along with instruction on material selection, maintenance water chemistry within the specification, and minimising residual stress in the piping, all of which can have an impact on the potential for SCC.

The CMTs are filled with cold water borated to 3500 ppm (nominal) boron as boric acid to provide the required shutdown margin in the event of a loss of coolant. The accumulators are filled with cold water borated to 2700 ppm (nominal) boron as boric acid for use in the event of a loss of coolant. The IRWST is filled with cold water borated to 2700 ppm (nominal) boron as boric acid for use in refueling and in the event of a loss of coolant. For these portions of the PXS, refer to summary report of AP1000 plant chemistry characterizations (Reference 21.76, Table 5.2) for the chemistry safety limits.

The water in all major PXS components is borated. As the temperature in the system is relatively low, it is expected that the corrosion-resistant stainless steels and nickel alloys of the system will not be at risk from corrosion.

During any event involving leakage of primary coolant into containment, the leaked coolant floods baskets of trisodium phosphate (TSP), which dissolves in the water to maintain pH within the alkaline range to stabilise water-soluble iodine species and minimise the loss of iodine to the containment atmosphere (see Section 21.9.1).

21.7.4 Passive Containment Cooling System

21.7.4.1 Description of the Passive Containment Cooling System

The passive containment cooling system (PCS) is designed to remove heat from the containment vessel and transfer it to the environment to ensure that the containment vessel does not exceed the operating temperature for the vessel in the event of a major leak in the RCS circuit and PXS becoming operational.

The PCS cools the containment vessel in two ways: directing air flow between the steel containment vessel and concrete building and passing cooling water (from the passive containment cooling water storage tank (PCCWST) at the top on the reactor building) over the external skin of the steel containment vessel. The contents of the PCS tanks are recirculated to maintain acceptable chemistry and temperature conditions. See Section 6.6.2 for a detailed description of the PCS.

21.7.4.2 Functions of the Passive Containment Cooling System

The PCS performs the following functions directly related to the fluid in the PCCWST and the PCCAWST:

- Supports containment of fission product releases by transferring heat from the containment atmosphere to the environment. The removal of containment heat maintains containment pressure within design limits, thus supporting containment integrity
- Provides a makeup source and flow path to the SFP. In the event that SFP cooling is lost; under certain circumstances (see Chapter 9) the PCCWST and the PCCAWST provide the necessary makeup to the SFP to ensure that the spent fuel is not uncovered
- Provides a seismically qualified source of fire protection water
- Recirculates the contents of the PCCWST and the PCCAWST to monitor and maintain acceptable chemistry and temperature conditions within these tanks

21.7.4.3 Passive Containment Cooling System Chemistry Safety Requirements

The only safety requirement of the PCS water chemistry is to support the maintenance of the system integrity. The PCS is filled from the DWS. The PCCWST is dosed with 50 ppm of hydrogen peroxide to control biological growth in the tank. The concentration of hydrogen peroxide is analysed weekly and the concentration of impurities (chloride, sulphate, fluoride) is checked quarterly (Reference 21.5, Chapter 9). The stainless-steel lining of the PCCWST will provide sufficient corrosion resistance at ambient temperatures given the specified water quality. Hydrogen peroxide dosing is not expected to induce a significant corrosion risk provided that the levels of impurities in the water are kept low, as specified. For the PCS, refer to summary report of AP1000 plant chemistry characterizations (Reference 21.76, Table 5.12) for the chemistry safety limits.

21.7.5 Demineralised Water Treatment System

21.7.5.1 Description of the Demineralised Water Treatment System

The DTS is responsible for providing demineralised water for use as makeup to primary, secondary, and other systems. The DTS removes impurities from the raw water system (RWS) feedwater, utilizing three main unit operations: cartridge filtration (CF), reverse osmosis (RO) and EDI to remove impurities. See Section 6.11.1.5 and the AP1000 Chemistry Manual, Chapter 3 (Reference 21.5) for further details of the DTS.

21.7.5.2 Functions of the Demineralised Water Treatment System

The DTS is required to provide water of sufficient quality and quantity to meet the needs for makeup of the primary, secondary, and other plant systems. For the AP1000 standard plant, the DTS is designed to produce a maximum treated water flow rate of 68.1 m^3/hr (360 gpm).

Chapter 3 of the AP1000 Chemistry Manual (Reference 21.5) provides details regarding the functional requirements of the DTS, as well as a listing of recommended limits for key parameters of interest that are considered action levels to take immediate corrective actions should any of the concentration levels listed be exceeded. Continuously, the actual DTS effluent operating band for the parameters listed in Chapter 3 of the AP1000 Chemistry

Manual (Reference 21.5) must be kept below the values listed to ensure consistent production of high purity water.

21.7.5.3 Operation of the Demineralised Water Treatment System

The DTS supplies demineralised water of suitable quality to the DWS for further treatment to then supply the makeup to the primary and secondary circuits. Therefore, it supports the achievement of the operating safe chemistry standards in these systems.

Two parallel treatment trains consisting of CF, RO, ultraviolet germicidal irradiation (UV), EDI, and non-regenerable mixed bed exchanger (MB) units provide flexibility for system operation under various plant conditions, and allow for the cleaning and maintenance of a single train while the other train remains available for service. Chemicals to prolong, stabilize, and optimize the performance of the DTS are added via the CFS.

The CF units act as protective devices to prevent particulate matter from entering the RO units in the case where small particulates may be present in the pretreated RWS, and also from larger particulates that may carry over from any transient upsets. The RO units reject dissolved solids (salts), small amounts of nonbiodegradable organics, and colloids through the membrane diffusion process. The product water from the RO units is then pumped through UV treatment units. The UV light breaks apart and reduces the total organic carbon molecules within the flow stream. The water then flows to the EDI unit for secondary demineralization.

EDI is a membrane process that removes ions from the RO permeate water to produce high purity water. The water passes through the EDI stacks with alternating cation and anion permeable membranes and electrode plates across which a dc voltage attracts ions. The water in the EDI is split into brine (concentrate) and dilute (permeate) flows. The brine and permeate flows are directed by spacers between the membranes. The dilute flowpath contains high-grade ion exchange resin that acts as a conduit to quickly transfer ion contaminants to the respective paired anode or cathode membrane. After treatment, the EDI product water is sent to the MB. The MB is the final treatment process prior to prior to distribution to the DWS, and removes trace ionized impurities from the EDI effluent water.

The DTS effluent is fed to the DWS for further processing, storage, and transfer to subsequent downstream plant uses. If at any point the output of the DTS is outside the operating band setpoints, a three-way motorised valve is used to direct the flow to the inlet of the CFs for reprocessing through the RO and EDI units.

The quality of the DTS effluent is monitored by online analytical instruments and analysis of grab samples to ensure that the system is functioning properly.

21.7.6 Demineralised Water Transfer and Storage System

21.7.6.1 Description of the Demineralised Water Transfer and Storage System

The design of the DWS is described in detail in Section 6.11.1.4.

The DWS receives water from the DTS and provides a reservoir of demineralised water to supply the condensate storage tank (CST) and for distribution throughout the plant.

21.7.6.2 Functions of the Demineralised Water Transfer and Storage System

Demineralised water is processed in the DWS to remove dissolved oxygen. In addition to supplying water for makeup of systems that require pure water, the demineralised water is used to sluice spent radioactive resins from the ion exchange vessels in the CVS, the SFS (described in Section 6.12.4), and the WLS (described in Section 6.12.8) to the WSS.

21.7.6.3 Demineralised Water Transfer and Storage System Chemistry Safety Requirements

The DWS water is used for makeup of primary and secondary circuits and as feed to other systems, including the SFS and CCS. The quality of the water is important in achieving the chemistry functions of these systems, therefore the DWS acts to support the functioning of other systems. The chemistry requirement of the DWS is the provision of water deoxygenated to the level required for system makeup.

21.7.6.4 Demineralised Water Transfer and Storage System Operation

The water supplied by the DTS enters the DWS and is initially stored in the demineralised water storage tank (DWST), which has a capacity of 378.5 m^3 (99,989 US gal). The tank is equipped with a level control that controls the DWS to maintain the operational level. The temperature instrumentation controls an electrical heater used to heat the water to prevent it from freezing. The DTS final mixed bed units feature ion exchange resin traps to prevent resin fines from entering the DWST and CORS units.

The DWS is also responsible for deoxygenation of the demineralised water. This is performed by using CORSs. A CORS deoxygenates the water by adding hydrogen gas from the PGS and then passing the water, rich in dissolved hydrogen, through a catalytic chamber resin bed with a catalyst that combines dissolved hydrogen and dissolved oxygen to form water. The water entering the deoxygenation process is pumped from the DWST by the demineralised water transfer pumps. The water leaving the CORS unit is either recirculated through it for further oxygen reduction via the DWST or flows onto the demineralised water distribution header.

The water in the DWS is used to supply the CST and other plant systems.

Condensate Storage Tank

The CST has a capacity of 1835.9 m^3 (485,000 US gal) and is a vertical cylindrical tank constructed of stainless steel. Level and temperature instrumentation are provided with the tank level controlled by the makeup valve. Freeze protection is supplied by immersion-type electric heaters.

The CST has a CORS unit identical to the one used on the output of the demineralised water transfer pump to maintain the condensate water oxygen level within specifications. An oxygen analyser in the CST controls the catalytic oxygen reduction unit pump.

The CST provides a sufficient supply of water to the startup feedwater system to permit 8 hours of hot standby operation, followed by an orderly plant cooldown from normal operating temperature to conditions that permit operation of the RNS over a period of approximately 6 hours. The capacity of the CST is sufficient to maintain SG cooling for at least 24 hours following the loss of normal alternating current (ac) power.

The CST is also required to supply the ASS as needed to support the auxiliary boiler. Makeup water is supplied to heating, ventilation, and air conditioning (HVAC) humidifiers, storage tanks, and to other equipment for flushing, washing, and cooling operations as required to support plant operation.

Chemical and Volume Control System

The DWS is responsible for supplying water to the CVS used for reactor makeup water and for boron dilution evolutions. The water is also necessary for sluicing the resin beds in not only the CVS but also the CPS, SFS, WLS, and WSS.

21.7.7 Service Water System

21.7.7.1 Description of the Service Water System

The service water system (SWS) is responsible for the supply of cooling water to the two HXs in the CCS, located in the turbine building. See Section 6.11.1.1 for a detailed description of the CCS. The AP1000 standard design incorporates a recirculated fresh water SWS using cooling towers as discussed herein. As an option, the SWS can be configured using seawater in a once-through system.

The SWS is split into two mechanical trains, each consisting of the following:

- Service water pump
- Cooling tower
- Strainer

The piping leading to and from the HXs is interconnected to allow cooling water from either train to flow through either or both of the CCS HXs, and to then return to either cooling tower.

21.7.7.2 Functions of the Service Water System

The SWS provides cooling to two HXs in the CCS and maintains the CCS coolant within its operating temperature range.

21.7.7.3 Service Water System Chemistry Safety Requirements

The SWS provides heat removal from the CCS, which in turn cools a number of systems, including the RCPs and SFP, supporting their operation.

The function of the SWS chemistry is to minimise the risk of loss of integrity of the SWS through corrosion or a loss of function through fouling.

21.7.7.4 Service Water System Operation

The SWS coolant water is drawn from the cooling water basin by the SWS pump, and passes through the strainer before entering the CCS HX to remove heat from the CCS coolant. The heated SWS water returns to the cooling tower for cooling before entering the cooling tower basin for recirculation around the SWS.

During normal operation, the CCS operates only one HX with the SWS supplying the operating HX with service water at a temperature below 34.17°C (94°F). In transient

conditions, the CCS uses both HXs and the SWS supplies service water to both HXs to support the CCS cooling requirements. Cooling both HXs requires that both SWS cooling trains (pump, tower, and strainers) be brought into service.

Temperatures in the system are moderate and the pressure of the SWS fluid is kept above saturation at all locations. This, along with other design features of the system arrangement and control of valves, minimises the potential for thermodynamic or transient water hammer.

SWS materials are compatible with the cooling water chemistry and chemicals are used for the control of long-term corrosion and organic fouling. Water chemistry is controlled by the turbine island CFS.

The two cooling towers are identical with a storage basin beneath. The basin stores enough water to run the cooling of a single CCS HX for 72 hours with no refilling.

21.7.7.5 Materials

Diverse materials are used in the AP1000 plant SWS. Materials of construction may include the following:

- Piping consisting mainly of carbon steel with high-density polyethylene (HDPE) in the blowdown piping.
- Pumps manufactured of carbon steel, cast steel, and stainless steel; and with bearing material selection based on supplier experience.
- Strainers with carbon steel or stainless-steel bodies and stainless-steel screens.
- Cooling towers composed of a fibreglass composite material with polyvinyl chloride or polypropylene fill.
- Fan blades of moulded fibre-reinforced polyester/fibreglass composite with a cast-iron speed reducer.
- Concrete cooling tower basins.

21.7.7.6 Service Water System Water Chemistry

Chemical treatment is used to protect the SWS against corrosion of the materials and fouling through a variety of mechanisms, including chemical and biological processes. The precise treatment regime is defined by the operator within the guidance given in the AP1000 Chemistry Manual (Reference 21.5, Chapter 7), with safety limits provided in summary report of AP1000 plant chemistry characterizations (Reference 21.76, Table 5.19).

The chemicals can be divided into six categories based upon function: biocide, algaecide, pH adjustor, corrosion inhibitor, scale inhibitor, and silt dispersant. Specific chemicals used within the system, other than the biocide, are determined by the site water conditions. The pH adjustor, corrosion inhibitor, scale inhibitor, and dispersant are metered into the system continuously or as required to maintain proper concentrations. A sodium hypochlorite treatment system is provided for use as the biocide and controls microorganisms that cause fouling. The biocide application frequency may vary with seasons. Algaecide is applied, as necessary, to control algae formation on the cooling towers.

Chemical concentrations are measured through analysis of grab samples. As example, when adding sodium hypochlorite as a biocide, the chlorine residual is measured to ensure excess chlorine is maintained in the stream to prevent microbial growth. Addition of water treatment chemicals is performed by CFS injection metering pumps and is adjusted as required.

Chemical injections are interlocked with each service water pump to prevent injection into a train when the associated service water pump is not running.

21.7.7.7 Fault Conditions

Radiation in the Service Water System

The radiation in the SWS is detected via a monitor placed in the SWS blowdown line, and provision is in place for radiological analysis of grab samples. The valves in the blowdown line should be closed by the operator to prevent release and strainer back flush should be disabled.

The presence of radioactive species in the SWS requires a double leak from the RCS into the CCS and then a second leak into the SWS from the CCS. If a high-radiation alarm in the SWS is initiated, the first step is to check the activity in the CCS. It is then necessary to determine the leak source. A sample can be taken from valves near the HXs and it is possible to isolate and switch to a standby HX.

Failure of Service Water System

In the event that the SWS completely fails, i.e., no cooling water is supplied to the CCS HXs, within minutes the CCS will overheat and enter alarm/shutdown. The shutdown of the CCS will result in the shutdown of the RCPs and consequently the reactor.

The interconnecting pipework and the interchangeability of redundant components (through the interconnecting pipes and valves) reduces the likelihood of such an event resulting from a failure of a single active component, since the SWS operates with only one processing train under normal operation.

21.7.8 Spent Fuel Pool

21.7.8.1 Description of the Spent Fuel Pool

The SFP provides storage space for spent fuel. The SFS is designed to remove decay heat generated by stored fuel assemblies from the water in the SFP. A secondary function of the SFS is clarification and purification of the water in the SFP, transfer canal, and refuelling water. See Section 6.12.4 for a detailed description of the SFP; SFP faults are discussed in Chapter 9.

21.7.8.2 Spent Fuel Pool Chemistry Requirements

The SFP and SFS chemistry safety requirements are controlling reactivity by immersion in a solution of boric acid, and maintaining integrity of the SFP, SFS, and fuel cladding by minimising corrosion. These risks of corrosion and radioactivity are described in more detail within Section 21.5. The SFP is borated to a nominal concentration of 2700 ppm of boron, which controls reactivity.

The neutron-absorbing material used in the spent fuel racks is Metamic™, which is a metal composite of Type 6061 aluminium alloy matrix with boron carbide (B_4C) reinforcement. The minimum boron carbide concentration required by the design specification of the SPF to maintain a subcritical activity level is 30.5 wt%. The specified minimum boron carbide concentration equates to a minimum ^{10}B density of 0.0304 g/cm^3.

The Metamic alloy shows sufficient dimensional and ^{10}B areal density stability under irradiation testing. This testing has been used to show that the Metamic absorber sections of the rack will not be detrimentally affected by the radiation from the spent fuel cells even for the 60-year plant life (Reference 21.70).

The aqueous environment of the pool with a nominal dissolved Boron concentration of 2,700 ppm will be slightly acidic. Elevation temperature (93°C [200°F]) corrosion rate testing of 32 wt% B_4C Metamic (Reference 21.71) for 90 days indicated that "no corrosion was observed" and there was "no significant change in ^{10}B areal density." The complete lack of any chemical changes in the tests, combined with the knowledge of the effects of temperature and pH on corrosion rate, is sufficient to show that the aqueous spent fuel pool environment, even for 60 years, will not detrimentally affect the condition of the Metamic panels. Safety limits for the chemistry in the spent fuel pool are provided in the AP1000 plant Chemistry Manual (Reference 21.5, Sections 4.3.5) and the summary report of AP1000 plant chemistry characterizations (Reference 21.76, Table 5.2). For additional information on spent fuel pool chemistry, refer also to Reference 21.82.

The function of cooling and shielding the fuel in the SFP is performed by the water in the pool.

21.7.8.3 Spent Fuel Pool Cooling

The SFS is designed to maintain the cooling water temperature below 48.89°C (120°F) with a maximum fuel cell load plus either partial or full core loads (full core 120 hours after shutdown).

SFP boiling in the event of a loss of SFP cooling is discussed in Section 9.11.

21.7.8.4 Cooling Water Purification

The SFS is designed to remove contaminants from the cooling water in the SFP, refuelling cavity, and water in the IRWST. The SFS removes radioactive corrosion products, fission ions, ionic impurities, and particulates to do the following: maintain coolant activity levels in accordance with SFP ALARP goals, to limit corrosion, and maintain cooling water clarity.

The SFP is initially filled for use with water having a nominal boron concentration of 2700 ppm. Demineralised water can be added for makeup purposes, including replacement of evaporative losses, from the DWS. Boron may be added to the SFP from the CVS. The purity of the DWS is discussed in Reference 21.5, Chapter 3; the purity of the boron is discussed in Reference 21.5, Chapter 10.

The two SFS demineralisers are of mixed bed type. The demineralisers are initially charged with a cation resin in the hydrogen form and anion resin in the hydroxide form to remove fission and corrosion products. The demineralisers will be borated during initial operation with boric acid. Each demineraliser is sized to accept the maximum purification flow from its respective cooling train. The vessels are constructed of austenitic stainless steel.

The SFS filters are situated downstream from the demineralisers and are sized to collect small particles and resin fines escaping from the demineraliser resin beds. The filter assemblies are constructed of austenitic stainless steels (all piping in the SFS is austenitic stainless steel) with replaceable filter cartridges (PCSR Section 17.9.1).

21.7.8.5 Water Transfer

The SFS is also responsible for transferring the water from the IRWST to the refuelling cavity. The water level in the refuelling cavity, fuel transfer canal, and SFP must be sufficient to allow the extraction of fuel cells from the core with at least the minimum depth of the fuel rod submerged in cooling water. The SFS is also responsible for the return of the water in the refueling cavity to the IRWST.

In some current operating PWRs, the transfer of the water from the refuelling water storage tank to the refuelling cavity is traditionally through the residual heat removal system. This flow path is a concern because the refuelling water is directed into the cold leg and through the reactor, which can mobilise loose crud from fuel surfaces and increase turbidity. Since the AP1000 design uses the SFS to transfer refuelling water, this improves the clarity of water entering the refuelling cavity. The capability to transfer water through the RNS is available in the AP1000 design.

21.8 Operational Strategies in the AP1000 Design

This section provides a summary of the operational strategies for the primary circuit, which is described in detail within Section 4.4.4 of Reference 21.5. For secondary chemistry operational strategies, please see Section 5.5 of Reference 21.5.

21.8.1 Operational Modes

The operating modes of the RCS are as follows:

- Power operation
- Startup
- Hot standby
- Safe shutdown
- Cold shutdown
- Refuelling

Each mode corresponds to any one inclusive combination of core reactivity condition, power level, average reactor coolant temperature, and RPV head closure bolt tensioning with fuel in the RPV (see Table 21-6).

21.8.2 Power Operation (Mode 1)

During operation at power, the reactor primary coolant is a solution of boric acid, maintained at a concentration appropriate to the reactivity of the core. The boric acid concentration is gradually adjusted during a fuel cycle to compensate for fuel burnup and the buildup of xenon. The pH_T is maintained in alkaline conditions by the addition of LiOH. Target pH_T varies according to the chemistry regime adopted but Westinghouse requires that pH_T be kept above [ ] to minimise general corrosion and SCC risks to fuel cladding and primary circuit materials (References 21.5 and 21.6).

The pH_T requirements also reduce crud deposition on the fuel. In addition, the lithium concentration is limited to [ ] ppm in view of concerns regarding its effects on fuel cladding corrosion. The operating chemistry parameters are defined by Westinghouse endorsement of the EPRI guidelines (Reference 21.2) as well as the supplemental chemistry guidelines (Reference 21.6). The pH_T strategy is decided by individual plants within the constraints of the EPRI guidelines and with a maximum lithium concentration of [ ] ppm (Reference 21.6). Lithium concentration is controlled by adding LiOH via the chemical addition tank and by dilution or processing the primary coolant through the cation bed in the CVS purification loop. During this time, it is expected that the sampling frequency will increase to ensure proper concentrations of lithium are provided per Reference 21.2.

Hydrogen is dissolved in the primary coolant in the concentration range of 25 to 50 cc/kg H_2O to maintain a low ECP for the control of SCC and corrosion. The hydrogen residual will also scavenge oxygen generated by radiolysis within the core. Undesirable contaminants, including chloride, sulphate, fluoride, calcium, magnesium, and aluminium, are removed by the CVS to below the target levels given in the EPRI and Westinghouse Supplemental Guidelines (References 21.2 and 21.6). In addition, silica is monitored in the reactor coolant to minimise the risk of silicate deposition on the fuel. The purification flow is provided by the RCP head and does not require operation of the CVS makeup pumps. Thus, purification is continuous during power operation.

Control of the adopted chemistry regime is achieved by analysing grab samples of the primary coolant for boron, dissolved hydrogen, lithium, zinc, and radioactivity; which is followed by the subsequent chemistry adjustments via the CVS.

Load following power variations are achieved by movement of control rods and grey rods. In the primary circuit, adjustment of dissolved boron is used to compensate for fuel burnup only and adjustments are made to keep the rod control groups within their allowable insertion limits. The boric acid blending valve can be adjusted to achieve the desired makeup concentration. Boron dilution is carried out as needed by CVS makeup with demineralised water and the excess volume is discharged to the WLS via CVS letdown.

21.8.3 Startup Chemistry Operations (Mode 5 through to Mode 1)

During startup following a normal refuelling outage, the reactor needs to be filled with coolant and brought to operating conditions in a manner that protects the core and primary circuit materials from corrosion. It is also necessary to minimise crud redistribution to avoid increases in circuit radioactivity or risks of CIPS and CILC. Strategies have been devised to achieve these aims and Westinghouse will continue to work with utilities to develop them further. The AP1000 plant will be operated to EPRI guidelines (Reference 21.2), which discuss options for chemistry control during PWR reactor startup. This section will outline the startup chemistry strategies and their impact on the safety functions of the AP1000 plant primary circuit.

Refill water quality is checked prior to filling to ensure that contaminants are within specification. The AP1000 plant specification calls for halogen concentrations to be maintained within specification regardless of system temperature. The makeup pumps are used to fill the reactor with water from the demineralised water supply and the BAST to achieve the correct starting boron concentration.

The RCS is vented via the RPV head and pressuriser. The pressuriser may be filled via the auxiliary spray line. Alternatively, the RCS can be vacuum-filled as this reduces the

RCS oxygen concentration and supports heatup. Vacuum filling will be routinely adopted in the AP1000 plant.

Hydrazine is added to the pressuriser and the bulk reactor coolant to scavenge oxygen. The reaction between oxygen and hydrazine is slow and is favoured at alkaline pH and higher temperatures. Initially, during heatup, the pH will be acidic due to the high boron concentration in the coolant but is later increased by lithium dosing according to the plant chemistry strategy. The AP1000 Chemistry Manual (Reference 21.5) calls for oxygen to be controlled during power operation and prior to operation at temperatures above 121°C (250°F) in both the RCS and the pressuriser, which is within the EPRI guidelines target.

Good operational practice suggests that hydrazine is dosed after analysis of the residual oxygen in the coolant to allow the addition of only sufficient hydrazine to scavenge the remaining oxygen. Excess hydrazine can produce ammonia, which can impact the CVS resin beds, possibly leading to a release of chloride from them (Reference 21.2).

As the solubility of nickel, cobalt, and iron is reduced as the temperature of the primary coolant increases, there is a risk of deposition of dissolved metals on the primary circuit and particularly in the core. Nickel deposition is a concern because of the eventual impact on ^{58}Co inventory and, in high-duty cores, the increased risk of CIPS. To manage this, the CVS purification flow with ion exchange demineralisation can be employed during the startup operations.

Consistent with the EPRI guidelines (Reference 21.2), the Westinghouse Supplemental Guidelines (Reference 21.6) stipulate that hydrogen should be above 15 cc/kg H_2O when the reactor is critical and between 25 and 50 cc/kg H_2O within 24 hours of the reactor reaching critical. The AP1000 reactor will be operated to EPRI guidelines.

LiOH is added to increase the pH to the alkaline range to minimise corrosion of primary circuit materials and especially to reduce the risk of SCC. Lithium addition can be delayed to extend the time in acid-reducing conditions if it is necessary to remove nickel. The RNS needs to be isolated prior to addition of lithium to prevent addition of lithium to the reactor coolant during later uses of the RNS. Lithium dosing will be coordinated to achieve a target pH_T of at least [ ] at reactor criticality. LiOH is added via the chemical mixing tank to the suction manifold of the makeup pumps. The demineralised water supply is deoxygenated to an oxygen content of less than 100 ppb but the boric acid storage tank is normally open to the atmosphere so that the filling water is not fully deoxygenated. Hydrogen injection is started and the coolant hydrogen concentration is raised to the target level.

Once the reactor is critical, the primary coolant silica concentration has been confirmed to be less than or equal to 1000 ppb and zinc injection may be initiated (Reference 21.6).

The pressuriser heaters are operated to heat the water in the pressuriser and create a steam bubble. As the bubble grows, volume is maintained and pressure controlled by diverting the coolant through letdown to the WLS. With the shutdown control rod banks withdrawn, makeup is drawn from the demineralised water supply to reduce the boric acid concentration to that required for power operation. The hydrogen and boron concentrations and water quality are confirmed by chemical analyses and then the control banks are withdrawn to raise power and control neutron flux.

21.8.4 Hot Standby (Mode 3)

Spurious reactor trips or maintenance operations can result in the reactor being held at a subcritical condition but with the ability to return to power in the time taken to withdraw the control rods. The average temperature is maintained by dumping steam to the condenser or, at a later stage, by operating the RCPs. Xenon builds up during the shutdown and increases the criticality margin. If a rapid return to power is needed, the reactor coolant may be diluted by adding demineralised water to counteract this.

21.8.5 Safe/Cold Shutdown (Mode 4 to Mode 5)

Safe/cold shutdown involves moving the plant from normal operating temperature to cold conditions in preparation for refuelling or maintenance. Safe shutdown is defined as Mode 4 operation, i.e., where the reactivity is less than 0.99 but the temperature is above 93.3°C (225.5°F). Cold shutdown, or Mode 5, is the same but the average reactor coolant temperature is less than 93.3°C (225.5°F).

A major consideration during shutdown is the effect of environmental changes on crud mobility and the removal of activity from the primary circuit. Consistent with EPRI guidelines (Reference 21.2), Westinghouse makes a number of recommendations regarding shutdown chemistry practices aimed at minimising primary circuit activity buildup (References 21.5 and 21.6). These recommendations are summarised as follows:

- Control of reactor coolant pH during shutdown. This is defined as a plant-specific control and the EPRI guidelines do not define a precise pH band; however, plant experience suggests maintaining pH_T above [ ] while at power to avoid particulate transport (Reference 21.2). It is also important to avoid increasing the alkalinity of the coolant by adding LiOH. Lithium removal via the CVS cation demineraliser will most likely begin prior to shutdown.

- Acid-reducing conditions should be established during cooldown, before the temperature falls below 200°C (417.6°F), to enable decomposition of nickel ferrites, which form a major component of crud and contain cobalt. This allows removal of nickel and radio-cobalt from the circuit. Hydrogen needs to be maintained at 15 cc/kg H_2O or better.

- Monitor coolant chemistry and maintain adequate cleanup capability. This includes assessing the resin bed capacity.

- Maximise purification flow to optimise cleanup.

- Ensure that the RNS does not adversely impact RCS chemistry when it is brought into service. Procedures prevent inadvertent addition of lithium to the RNS, however, transient oxygen, or corrosion products may be present.

- Prior to chemical degassing operations, the reactor coolant drain tank (RCDT) hydrogen content shall be reduced to ≤4 percent volume hydrogen to prevent the risk of explosive gas mixtures. A stoichiometric amount of hydrogen peroxide is added to the RCS and pressuriser to react with the residual hydrogen in the RCS. Once the RCS hydrogen concentration has been reduced to less than 5 cc/kg H_2O, the chemical degassing operations have been completed.

- Create acid-oxidising conditions by adding hydrogen peroxide to solubilise nickel and radio cobalt.

- Prior to opening the RCS, the hydrogen concentration shall be confirmed to be less than 5 cc/kg H_2O to prevent the risk from an explosive mixture.

The exact chemistry practice is determined by the plant operator and the EPRI guidelines (Reference 21.2), which state that best practice may differ from plant to plant. An assessment needs to be made in each case and reviewed to optimise shutdown chemistry.

Some aspects of RCS shutdown chemistry are not well understood and relevant aspects of crud composition and chemistry are still being studied. It is likely, therefore, that shutdown chemistry practices will be modified in the future, so it is appropriate that responsibility for applying best practice lies with the operator.

The expected shutdown sequence for the AP1000 plant is as follows:

- The WLS and gaseous radwaste system (WGS) are prepared to accept waste generated from degassing operations, required letdown, or boration.

- The purification flow is routed to the WLS via CVS letdown where the coolant is stripped of gases and returned to the makeup system. This is carried out prior to shutdown to reduce fission gas inventory to support shutdown operations for personnel access. Active hydrogen injection will be continued through shutdown and boration to ensure an adequate residual of hydrogen is maintained in the RCS.

- Lithium removal is started 24 hours prior to shutdown by placing the CVS cation demineraliser in service. The pH_T is monitored and maintained at or above [ ] while at power.

- The BAST and IRWST are sampled and analysed for quality prior to shutdown.

- Boration is carried out by adding a measured volume of boric acid solution via the makeup system and verified by chemical analysis of reactor coolant. The reactor makeup control is set to the boron concentration required for shutdown, and the makeup during depressurisation and cooldown is automatic. This produces acid-reducing conditions to aid in the solubilisation of corrosion products. Lithium removal is completed following plant shutdown.

- The pressuriser is vented to reduce the gaseous hydrogen inventory, fission gases, and noncondensable gases. RCS-dissolved hydrogen degassing can then be completed by using the degasifier in the WLS and/or chemical degassing by the addition of hydrogen peroxide.

- Hydrogen peroxide is added to produce acid-oxidising conditions, which aids solubilisation of corrosion products (particularly nickel-metal) and activated corrosion products (notably ^{58}Co).

- The RCS dissolved oxygen and hydrogen peroxide concentrations shall be maintained at greater than 2 ppm to ensure that an oxidising chemistry environment is maintained.

- Cleanup of the primary coolant continues using the CVS demineralisers to minimise refuelling cavity dose rates and support clarity of cavity water.

21.8.6 Refuelling (Mode 6)

During refuelling operations, the clarity of the refuelling cavity water can degrade because of the formation of a ferrous iron colloid that, after partial oxidation, can produce a green colouration to the cavity water. This can be sufficiently dense to impede refuelling operations. Treatment of this problem is usually oxidation with hydrogen peroxide, including monitoring RNS peroxide levels before it is put into service and treatment if necessary. The peroxide converts the ferrous iron to a ferric form, which forms a gel that settles or can easily be removed by filtration.

Fission product removal can be an issue for refuelling outages. Gaseous and volatile fission products must be reduced to low levels prior to lifting the reactor head. Hard gamma emitters will be less than 0.05 μCi/cc (total of ^{58}Co, ^{60}Co, ^{54}Mn) prior to lifting the reactor head. Reference 21.5, Chapter 4 provides more information. Iodine can exist in a number of oxidation states and the coolant chemistry may be adjusted to favour iodide and maximise demineraliser removal. Iodine concentrations in the primary coolant should be monitored prior to shutdown to enable an iodine cleanup to be carried out as part of the shutdown procedure if needed.

21.9 Accident Chemistry

A list of possible fault and accident scenarios are discussed in detail in Chapters 8 to 12. In a number of these scenarios, including LOCAs, SG tube rupture (SGTR), reactor coolant leakage, and CVS faults, chemical means are used to mitigate the impact in the event that systems, structures, and components fail to prevent fault progression to a large release to containment and to the environment. Several important chemistry control features are discussed below.

21.9.1 Control of Fission Products in Containment

Airborne particulate material and aerosols released following a severe accident are removed from the containment atmosphere by a number of passive processes, including; diffusiophoresis, thermophoresis, and sedimentation. The AP1000 design includes a manual containment spray system but this is not credited in the analysis and is designed to be used only following severe accidents should high doses be observed outside containment. A study of the relative benefits of a spray system and a number of options for providing a recirculating spray system concluded that it had no real benefits in terms of offsite dose and entailed additional risks.

Release of molecular iodine from the water within the containment is minimised by dissolving TSP in the coolant to establish and maintain an alkaline pH that stabilises iodine in solution as iodide or iodate ions. The TSP is contained in baskets inside containment that are exposed to the containment floodup water. Sufficient TSP is placed in containment to neutralise acids from all possible sources, including nitric acid formed from dissolved nitrogen in the coolant and hydrochloric acid formed from breakdown of electric cable insulation (Reference 21.62).

To conservatively estimate the TSP required, the amount of boric acid was maximised by including the maximum amounts of boric acid contained in both accumulators, both CMTs, and the IRWST. In addition, the reactor coolant is assumed to be at its maximum boric acid

concentration and the maximum concentration from the CVS BAST and SFS cask loading pit (CLP) are considered in determining the required amount of TSP. Reference 21.62 also includes the following significant conservatisms in the calculation of the dissolution time:

- Only the front surface of the basket is exposed to the water.
- The TSP granules have agglomerated into a solid block so that the surface area is simply the basket width times the height of the TSP inside.
- The dissolution rate is based on a temperature of 71.1°C (160°F) with no agitation. It was calculated that the maximum dissolution time is 2.27 hours and determined that 12,000 kg (13.2 ton) of TSP is required to obtain a pH of 7 in the containment sump water (Reference 21.62).

21.9.2 Containment Atmosphere Hydrogen Control

In accident scenarios, release of hydrogen into the containment building could occur from oxidation of fuel cladding and containment materials, with the potential for the formation of a combustible mixture of hydrogen and air. The AP1000 design incorporates two systems in containment for removing atmospheric hydrogen: passive autocatalytic recombiners (PARs) and igniters. A description of the hydrogen control system is given in Section 6.7.3.

The containment is designed to allow natural convective flow and mixing of containment air and to avoid dead spaces where hydrogen-rich pockets could develop. Containment atmospheric hydrogen concentration is monitored continually.

The PARs are designed to prevent the buildup of hydrogen during a LOCA. Two PARs are located in containment to prevent the hydrogen concentration from reaching the flammability limit of 4-percent volume. The PARs are effective in a range of hydrogen and oxygen concentrations, under wet or steaming conditions, and at room or elevated temperatures.

In the case of a severe accident, it is assumed that 100 percent of the fuel cladding reacts with water and produces a rapid rise of hydrogen in the containment. The hydrogen igniters initiate a controlled burn of hydrogen at a concentration between the lower flammability limit and 10 percent by volume to prevent the occurrence of hydrogen detonation.

A total of 66 igniters are strategically located throughout the containment. The locations are based on the evaluation of hydrogen generation sites, flow around containment, hydrogen burn physics, and potential accumulation points. The igniters are located to avoid acceleration of the flame front during the burning. The igniters are divided into two power groups with 33 igniters in each group. Power is provided to each group normally by offsite power, however, should offsite power not be available, the igniters are powered by onsite Class 2 standby diesel generators and, should they fail, by the Class 2 standby electrical supply system (EDS). The igniters are located such that one power train of igniters provides sufficient coverage to control the concentration of hydrogen throughout the containment. Please see Chapter 10 for further details.

21.9.3 Steam Generator Tube Rupture

The complete severance of a SG tube is considered unlikely given the high resistance of the Alloy 690 tube material to corrosion and SCC under both primary and secondary conditions. It is more feasible that small leaks will occur, usually as a result of fretting wear, which will

be detected as changes in radioactivity in the secondary circuit. The sequence of events for a severance SGTR with automatic and operator-initiated actions is discussed in Chapter 9.

The radiological consequences of an SGTR have been analysed and the assessment assumes that all of the noble gases and volatile iodine carried with primary fluid into the secondary circuit are immediately released to the environment. The nonvolatile iodine and alkali metal activity in the primary coolant is also available for release, in proportion to the steam release from the ruptured SG.

The resulting offsite and onsite radiological doses for the limiting case analysed are within the Target 4 basic safety level (BSL) for frequent faults of 20 mSv onsite and 1 mSv offsite.

The major chemistry impact on this event is the availability of iodine in the source term. The alkaline-reducing conditions in primary and secondary coolant will mitigate molecular iodine release by favouring the ionic form in solution. The analysis assumes the maximum concentration of iodine in solution is equivalent to an iodine spiking event.

21.9.4 Loss-of-Coolant Accidents

A LOCA has been assessed for a range of pipe breaks within containment. The assessment is described in Chapter 9. Two types of LOCA are defined: a large-break LOCA involving a rupture with a total cross-sectional area of more than 0.09 m^2 (1 ft^2), and a small-break LOCA, which is anything smaller than this (an analysis of LOCA event is in Chapter 10t and also considers a medium-break LOCA). In all cases, borated water is injected into the primary circuit from a variety of sources, including the CMT, accumulators, and IRWST (when the pressure difference between the IRWST and RCS is less than 0.9 bar (13 psig)). The automatic depressurisation system (ADS) depressurises the primary circuit in stages. The insertion of the control rods (in the case of a small-break LOCA) or the injection of borated water and void formation (in the case of a large-break LOCA) are sufficient to bring the reactor to safe shutdown. The required technical specifications for the boron concentrations defined within Reference 21.74 is provided below:

Technical Specification	Surveillance Requirement	Limit	Applicable Modes
3.5.1	SR 3.5.1.4	Verify the boron concentration in each accumulator is ≥ 2600 ppm and ≤ 2900 ppm.	1, 2, 3, 4
3.5.2	SR 3.5.2.5	Verify the boron concentration in each CMT is ≥ 3400 ppm, and ≤ 3700 ppm.	1, 2, 3, 4
3.5.6	SR 3.5.6.4	Verify the IRWST boron concentration is ≥ 2600 ppm and ≤ 2900 ppm.	1, 2, 3, 4
3.5.8	SR 3.5.8.3	Verify the IRWST and refueling cavity boron concentration is ≥ 2600 ppm and ≤ 2900 ppm.	6

A small line break scenario is also considered for lines outside containment. This is possible only in the RCS sample line and the discharge line from the CVS to the WLS, when in use. In the former case, operator detection is immediate because of loss of sample flow and triggering of the air and area radiation detectors. In the latter case, the flow is limited and the iodine activity is reduced by the demineralisers. Even with conservative assumptions, i.e., a fuel defect level of 0.25 percent, maximum-permitted iodine, and an iodine spike at the time of the leak, the dose at the exclusion zone boundary is less than 0.021 Sv.

LOCA events within containment release the radioactive material carried in the coolant into the containment. For modelling and assessment purposes, the reactor coolant is assumed to have activity levels consistent with operation at the Tech Spec limits of 1.04E+07 Bq/g (280 μCi/gm) dose equivalent ^{133}Xe and 3.7E+04 Bq/g (1.0 μCi/gm) dose equivalent ^{131}I (Reference 21.74).

As the reactor coolant enters the containment, the noble gases and half of the iodine activity are assumed to be released into the containment atmosphere. In addition, nuclides from the fuel are assumed to be released into the coolant. Initially, three groups are considered: noble gases, iodine, and alkali metals (caesium and rubidium). After in-vessel core melt, tellurium, noble metals, cerium, and lanthanum group elements, barium and strontium are included.

The iodine form is consistent with the NUREG-1465 model (Reference 21.64). The model shows the iodine to be predominantly in the form of nonvolatile caesium iodide with a small fraction existing as elemental iodine. Additionally, the model assumes that a portion of the elemental iodine reacts with organic materials in the containment to form organic iodine compounds. The resulting iodine species split is as follows:

- Particulate 0.95
- Elemental 0.0485
- Organic 0.0015

Alkaline conditions favour the formation of soluble iodide ions, and elemental iodine is only stable in acidic and oxidising conditions. The PXS provides sufficient TSP to the post-LOCA cooling solution to adjust the solution pH to 7.0 (25°C (77°F)) within an acceptable period following a LOCA; see Section 6.6.1.2.3. The TSP is contained in baskets and dissolves in released coolant in containment to neutralise leaked coolant.

The AP1000 plant does not include Class 1 active systems for the removal of activity from the containment atmosphere. The containment atmosphere is depleted of elemental iodine and particulates as a result of natural processes within the containment. A limited containment spray system is provided in the design for severe accidents but is not credited in the analysis.

Elemental iodine is removed by deposition onto surfaces. Particulates are removed by sedimentation, diffusiophoresis (deposition driven by steam condensation), and thermophoresis (deposition driven by heat transfer). No removal of organic iodine is assumed.

Offsite dose calculations are based on the release of activity by way of the containment purge line prior to its isolation near the beginning of the accident and the release of activity resulting from containment leakage. A maximum design basis leak rate is used in the calculations for the first 24 hours and half that rate thereafter.

The exclusion area boundary dose, calculated for the worst 2-hour period following an incident and the low population area dose and calculated for the 30 days following an incident, are shown to be less than 0.25 Sv.

A further consequence of a LOCA is the potential for damage to structural materials through exposure to the post-LOCA aqueous environment in the containment. The majority of the reactor materials wetted following a LOCA will be low-alloy or stainless steels. The neutral or mildly alkaline environment will minimise the corrosion rates of LASs and reduce the risk of SCC of stainless steels.

A study performed by Westinghouse looked at the SCC behaviour of Type 304 and 316 stainless steels in aerated water with and without boric acid and with various concentrations of chloride or fluoride. Tests were conducted at peak temperatures up to 143°C (289.4°F). Low levels of chloride, produced cracking in acidic conditions but no cracking was found in alkaline solutions with up to 1000 ppm of chloride in either annealed or sensitised stainless steels. Moderate concentrations (100 ppm) of fluoride produced SCC in stainless steels but not in borated conditions (Reference 21.62).

21.9.5 Spent Fuel Pool Faults

The chemistry of the SFP coolant is to be monitored manually every 7 days to ensure that the boron concentration in the coolant is sufficient to maintain a subcritical level. The design specification states that the minimum boron concentration in the SFP coolant is 2300 ppm. This level is maintained as a defence in depth measure as subcriticality in the SFR (Spent Fuel Racks) is passively maintained through geometry. Spent fuel pool faults are discussed in Chapter 9.

21.9.6 Severe Accident Chemistry

Severe accident chemistry is discussed in Section 10.12. Additional information on the chemistry within the containment during severe accidents with an intact containment is also discussed within Reference 21.75.

21.10 Construction and Commissioning

A number of material factors are introduced or influenced by manufacturing and construction processes or during testing and commissioning activities can influence the performance of the material in terms of its corrosion resistance. The principal factors involved are discussed below.

Metallurgical Condition

Sensitisation of stainless steels is avoided by controlling manufacturing and the use of heat treatments where necessary (Chapter 20). Cold-working of stainless steels used in pressure boundary applications is controlled by limiting the hardness of material used and adopting appropriate procedures, e.g., the solution-annealed pressuriser surge line material is formed by hot-bending followed by a resolution-annealing heat treatment.

Surface cold work is avoided during manufacture by procedures, e.g., surface grinding of pressure boundary materials is followed by graded polishing to remove the cold-worked layer (Chapter 20).

A tailored metallurgical heat treatment has been adopted for Alloy 690 components in the AP1000 plant. This treatment refines the grain size, effectively decreasing the oxide layer formed and thus increasing the SCC resistance. This structured manufacturing process route produces a microstructure with closely spaced carbide precipitates on all of the grain boundaries with a very low-density intragranular carbide precipitation. In addition, detrimental materials are controlled and surfaces are cleaned to qualifying cleaning procedures to eliminate surface contaminants.

Surface Condition

Surface finish can alter susceptibility to SCC and oxidation rates as well as affecting deposition of material from coolant. Electropolishing is to be applied to SG channel heads to minimise crud deposition during operation. Electropolishing has been shown to reduce the activity of the channel head by approximately 40 to 80 percent on test pieces in core under nominal primary water conditions (Reference 21.67), resulting in an approximately 80-percent reduction in corrosion and metal release for flat plate sections and an approximately 50-percent reduction on tubular components.

Virgin metal surfaces exposed to primary coolant will oxidise relatively rapidly at first, with the rate decreasing as the surface oxide layer develops. During the early stages of oxide development, considerable amounts of material are released into the coolant and transported through the core. An important part of the AP1000 plant commissioning process prior to fuelling is HFT, during which primary circuit materials will be exposed to normal operating conditions to develop a passive oxide layer under nonactive conditions. This preconditioning is expected to considerably reduce crud production during operation. In addition, zinc dosing will be applied during this phase at high levels to promote the formation of a zinc-enriched oxide, which provides greater stability and limits incorporation of active species, thus reducing primary circuit activity. The secondary system will also undergo a, HFT process that will mimic the conditions from modes 5 to 2. HFT also provides an opportunity to test the PSS and SSS. The AP1000 Chemistry Manual contains details about HFT procedures (Reference 21.5, Chapter 9).

Contamination

The chemical environment in the primary, secondary, and various other systems needs to be controlled to ensure that the risk of corrosion-related failure is minimised. In particular, contaminant species, notably chloride, fluoride, sulphate, and a number of metals such as lead, cadmium, and copper are eliminated as far as possible. Procedures are applied during construction and commissioning to control contamination and to clean up surfaces before operation (Reference 21. 5, Chapter 13; and Reference 21.76).

Information on preoperational testing is in the AP1000 Chemistry Manual (Reference 21.5, Chapter 8).

21.11 Conclusions

For the AP1000 standard plant design, the development of the chemistry guidance and related material selections are based upon proven industry practices to ensure that the pressure boundary is maintained, reactivity is controlled, and radioactivity is minimised with the intent of achieving ALARP.

Through system design, material selection, and appropriate strategic water chemistry programs, degradation of systems and components can be minimized. To achieve the goal of maintaining plant integrity and personnel safety, the best chemistry strategy for the AP1000 plant is prevention, control, and mitigation, thereby resulting in a safe design, which incorporates:

- Proven system designs based upon industry standards and best practices.
- Material selections based on lessons learned, customer inputs, and best practices.

- Prevention of impurity ingress.
- Timely mitigation of contaminants using improved mechanical designs and shared industry knowledge.
- Real-time chemistry monitoring and control equipment and in-line instrumentation; as well as programs, guidelines, and procedures based upon industry guidelines.
- Westinghouse's in-house research and expertise and lessons learned during service to the existing fleet of operating PWRs.

21.12 References

21.1 Not Used.

21.2 "Pressurized Water Reactor Primary Water Chemistry Guidelines," Vols. 1 and 2, Electric Power Research Institute, Palo Alto, CA: Rev. 6., 2007, EPRI Document Number 1014986.

21.3 "Closed Cooling Water Chemistry Guideline" Rev. 1 to TR-107396, "Closed Cooling Water Chemistry Guideline," Electric Power Research Institute, Palo Alto, CA: 2004, EPRI Document Number 1007821.

21.4 "Pressurized Water Reactor Secondary Water Chemistry Guidelines," Electric Power Research Institute, Palo Alto, CA: Rev. 6, 2004, EPRI Document Number 1008224.

21.5 Westinghouse Report APP-GW-GEM-200, Rev 4, "AP1000™ Chemistry Manual," March 2016.

21.6 Westinghouse Report LTR-AP1000-10-359, Rev. 1, "Westinghouse Supplement to EPRI PWR Primary Water Chemistry Guidelines, Rev. 6, for the AP1000™ Standard Plant," January 2011.

21.7 Not Used.

21.8 T. Couvant, et al., "Effect of Chlorides and Sulfates on the FAC of Austenitic Stainless Steel in PWR Environment," *13th International Conference on Environmental Degradation of Materials in Nuclear Power Systems 2007*. Canadian Nuclear Society, 2007.

21.9 Not Used.

21.10 Not Used.

21.11 Not Used.

21.12 Not Used.

21.13 Westinghouse Report APP-PSS-M3-001, Rev. 3, "AP1000® Primary Sampling System – System Specification Document," September 2015.

21.14 Westinghouse Report APP-CVS-M3-001, Rev. 7, "AP1000® Chemical and Volume Control System (CVS) System Specification Document," October 2015.

21.15 Westinghouse Report WCAP-12610-P-A, "VANTAGE+ Fuel Assembly Reference Core Report," April 1995.

21.16 Westinghouse Report WCAP-15063-P, Rev. 1, "Westinghouse Improved Performance Analysis and Design Model (PAD 4.0)," November 1999.

21.17 "Materials Reliability Program: Resistance to Primary Water Stress Corrosion Cracking of Alloy 690 in Pressurized Water Reactors (MRP-258)," Electric Power Research Institute, Palo Alto, CA: August 2009, EPRI Document Number 1019086.

21.18 "Resistance of Alloy 600 and Alloy 690 Tubing to Stress Corrosion Cracking in Environments With and Without Lead," Electric Power Research Institute, Palo Alto, CA: 2004, EPRI Document Number 1009532.

21.19 S. Szklarska-Smialowska and G. Cragnolino, "Stress Corrosion Cracking of Sensitized Type 304 Stainless Steel in Oxygenated Pure Water at Elevated Temperatures," *Corrosion* 36(12):653–65, NACE International, 1980.

21.20 Program on Technology Innovation: Proceedings – 2007 AECL/COG/EPRI Workshop on Cold Work in Iron- and Nickel-Based Alloys Exposed to High Temperature Water Environments, Electric Power Research Institute, Palo Alto, CA: 2008, EPRI Document Number 1016519.

21.21 L. Tribouilloy, et al. "Stress Corrosion Cracking on Cold-Worked Austenitic Stainless Steel in PWR Environment," In *13th International Conference on Environmental Degradation of Materials in Nuclear Systems 2007,* Canadian Nuclear Society, 2007.

21.22 C. Guerre, et al, "SCC Crack Growth Rate of Cold-Worked Austenitic Stainless Steels in PWR Primary Water Conditions," In *13th International Conference on Environmental Degradation of Materials in Nuclear Systems 2007*, Canadian Nuclear Society, 2007.

21.23 T. Couvant, et al,. Investigations on the Mechanisms of PWSCC of Strain Hardened Austenitic Stainless Steels, In *13th International Conference on Environmental Degradation of Materials in Nuclear Systems 2007,* Canadian Nuclear Society, 2007.

21.24 *Boric Acid Corrosion Guidebook: Managing Boric Acid Corrosion Issues at PWR Power Stations,* Rev. 1, Electric Power Research Institute, Palo Alto, CA: 2001, EPRI Document Number 1000975.

21.25 C. Marks, et al, "Boric Acid Corrosion Testing of PWR Reactor Pressure Vessel Closure Head Material," In *6th International Symposium on Contribution of Materials Investigations to Improve the Safety and Performance of LWRs,* French Nuclear Energy Society, 2006.

21.26 J. Ponguak, et al, "Boric Acid Corrosion of Reactor Pressure Vessel Steel Caused by an Impinging Jet of Simulated PWR Coolant," In *International Conference on Water Chemistry of Nuclear Reactor Systems*, Korea Atomic Energy Research Institute, 2006.

21.27 Y. Wada, et al, Mitigation Effect of Alkaline Water Chemistry upon Intergranular Stress Corrosion Cracking of Sensitized 304 Stainless Steel," *Journal of Nuclear Science and Technology* 38(8) (2001), 621–32.

21.28 S. Zhang, T. Shibata, and T. Haruna, Contribution of Solution pH and Buffer Capacity to Suppress Intergranular Stress Corrosion Cracking of Sensitized Type 304 Stainless Steel at 95°C," *Corrosion* 55(5) (1999), 462–8.

21.29 "Effect of Steam Generator Replacement on PWR Primary Corrosion Product Transport," Electric Power Research Institute, Palo Alto, CA: 2002, EPRI Document Number 1003601.

21.30 P. Andresen, "Ni Alloy Crack Growth: Mitigation by H_2 and Zn," MRP/PWROG Briefing to Electric Power Research Institute, July 2008.

21.31 "Materials Reliability Program: Resistance of Alloys 690, 52 and 152 to Primary Water Stress Corrosion Cracking" (MRP-237), Rev. 1., Electric Power Research Institute, Palo Alto, CA: 2008, EPRI Document Number 1018130.

21.32 "Materials Reliability Program: Mitigation of PWSCC in Nickel-Base Alloys by Optimizing Hydrogen in the Primary Water" (MRP-213), Electric Power Research Institute, Palo Alto, CA: 2007, EPRI Document Number 1015288.

21.33 Westinghouse Report WCAP-7803, "Behavior of Austenitic Stainless Steel in Post Hypothetical Loss of Coolant Environment," December 1971.

21.34 "Materials Reliability Program: Effects of B/Li/pH on PWSCC Growth Rates in Ni-Base Alloys" (MRP-217), Electric Power Research Institute, Palo Alto, CA: 2007, EPRI Document Number 1015008.

21.35 W. Yang, et al, "The Strain for Stress Corrosion Crack Initiation in Type 316 Stainless Steel in High Temperature Water," *Corrosion Science* 33(5) (1992), 735-50.

21.36 "2005 Interim Review of the Pressurized Water Reactor Primary Water Chemistry Guidelines," Rev. 5, Electric Power Research Institute, Palo Alto, CA: 2005, EPRI Document Number 1009933.

21.37 "Pressurized Water Reactor Primary Water Zinc Application Guidelines," Electric Power Research Institute, Palo Alto, CA: 2006, EPRI Document Number 1013420.

21.38 Westinghouse Report APP-SSS-M3-001, Rev. 2, "Secondary Sampling System (SSS) – System Specification Document," February 2012.

21.39 Not Used.

21.40 Steam Generator Progress Report, Rev. 13. Electric Power Research Institute, Palo Alto, CA: October 1997, TR-106365-R13.

21.41 *Steam Generator Reference Book,* Rev. 1, Volume 1, Electric Power Research Institute, Palo Alto, CA: 1994, TR-103824-V1R1.

21.42 "Pressurized Water Reactor Generic Tube Degradation Predictions: U.S. Recirculating Steam Generators with Alloy 600TT and Alloy 690TT Tubing," Electric Power Research Institute, Palo Alto, CA: 2003, EPRI Document Number 1003589.

21.43 "Improvement Factor Update: Application of Improvement Factor Data to the Analysis of a Secondary System Chemistry Upset at Ginna," Electric Power Research Institute, Palo Alto, CA and Constellation Energy Group, Inc., Baltimore, MD: 2006, EPRI Document Number 1013640.

21.44 NUREG-1841, "U.S. Operating Experience with Thermally Treated Alloy 690 Steam Generator Tubes," U.S. Nuclear Regulatory Commission, August 2007.

21.45 S. Choi, et al, "Improvement Factors for Steam Generator Tubing Alloys," Nuclear Plant Chemistry Conference 2010, Quebec City, Canada, 3-8 October 2010.

21.46 NEI Steam Generator Task Force, NRC/Industry Update of 12 August 2010.

21.47 EPRI TR-106611-R1, "Flow-Associated Corrosion in Power Plants," Electric Research Institute, August 1998.

21.48 I.S. Woolsey, et al, "The Influence of Oxygen and Hydrazine on the Erosion-Corrosion Behavior and Electrochemical Potentials of Carbon Steel Under Boiler Feedwater Conditions," In *BNES Conference on Water Chemistry of Nuclear Reactor Systems,* British Nuclear Energy Society, 1986.

21.49 R. Litman, "Condensate Oxygen Control at Seabrook Station," Presented at the Power Plant Chemistry Meeting, California, 1998.

21.50 EPRI NP-2294, "Guide to the Design of Secondary Systems and Their Components to Minimize Oxygen Induced Corrosion," Electric Research Institute, March 1982.

21.51 EPRI TR-016780-V3R8, "Advanced Light Water Reactor Utility Requirements Document," Electric Research Institute, March 1999.

21.52 Not Used.

21.53 Not Used.

21.54 Not Used.

21.55 Not Used.

21.56 Not Used.

21.57 Not Used.

21.58 Not Used.

21.59 Not Used.

21.60 Not Used.

21.61 Not Used.

21.62 Westinghouse Report APP-PXS-M3C-021, Rev. 1, "AP1000 Post LOCA pH Adjustment," April 2012.

21.63 EUR-15615, "Realistic Methods for Calculating the Release of Radioactivity Following Steam Generator Tube Rupture Faults: A Consensus Document," European Commission, December 1994.

21.64 NUREG-1465, "Accident Source Terms for Light-Water Nuclear Power Plants," U.S. Nuclear Regulatory Commission, February 1995.

21.65 Not Used.

21.66 Not Used.

21.67 Westinghouse Report APP-GW-N1-021, Rev. 2, "AP1000 Radiation Analysis Design Manual," July 2015.

21.68 INPO 06-007, Rev. 2, "Guidelines for Chemistry of Nuclear Power Stations," Institute of Nuclear Power Operations, October 1995.

21.69 Not Used.

21.70 Westinghouse Report APP-FS02-Z0-101, Rev. 2, "AP1000 Spent Fuel Storage Racks," August 2010.

21.71 Holtec Report HI-2043215, Rev. 2, "Source Book for Metamic Performance Assessment," Holtec International, September 2006

21.72 Westinghouse Report UKP-GW-GL-099, Rev. 1, "**AP1000**® Plant Primary Sampling System – Safety Evaluation," September 2016.

21.73 Westinghouse Report UKP-GW-GL-100, Rev. 1, "**AP1000**® Plant Hydrogen Injection System – Safety Evaluation," October 2015.

21.74 Westinghouse Report UKP-GW-GL-501, Rev. 0, "**AP1000**® UK Generic Technical Specifications," January 2016.

21.75 Westinghouse Report UKP-GW-GL-098, Rev. 0, "**AP1000**® Plant Accident Source Term Evaluation and Target 8 Compliance," July 2016.

21.76 Westinghouse Report APP-GW-GER-002, Rev. 7, "Summary of **AP1000®** Chemistry Characterizations," July 2015.

21.77 Westinghouse Calculation CN-AP1000-189, Rev. 1, "Advanced BOA Calculations for AP1000 [Plant] CIPS/CILC Risk Assessment," March 2010.

21.78 Westinghouse Report APP-CVS-M3C-055, Rev. 0, "Chemical and Volume Control System (CVS) Ion-Exchange Resin Tolerances," July 2010.

21.79 Not Used.

21.80 Westinghouse Report UKP-GW-GL-066, Rev. 0, "RO-AP1000-057 Response: Reactor Chemistry – Reduction in Primary-Circuit Radioactivity SFAIRP," September 2010.

21.81 Westinghouse Report APP-GW-GEC-005, Rev. 2, "AP1000 Chemistry Characterization – Fluid Type D – Component Cooling Water," January 2013.

21.82 Westinghouse Report UKP-GW-GL-081, Rev. 0, "AP1000 Spent Fuel Pool Chemistry," January 2011.

Table 21-1 AP1000 Plant Operational Modes

Modes	Title	Reactivity Condition (K_{eff})	% Thermal Rated Power	Average Reactor Coolant Temperature °C
1	Power operation	≥0.99	>5	$300.9 > T_{avg} > 292$
2	Startup	≥0.99	≤5	~292
3	Hot standby	<0.99	NA	>215.56
4	Safe shutdown	<0.99	NA	$215.56 \geq T_{avg} > 93.33$
5	Cold shutdown	<0.99	NA	≤93.33
6	Refuelling	NA	NA	≤71

Table 21-2 Component Cooling Water System Cooled Components

Reactor Section	Component
Primary circuit	RCP motor cooling with stator jacket coolers and external HXs
Primary circuit	RCP variable frequency drive (VFD) cooling
Auxiliary systems	RNS HXs (shutdown and refuelling modes only)
Auxiliary systems	SFP cooling via the SFS and/or RNS HXs
Auxiliary systems	Condenser cooling for the central chilled water system high-capacity water-cooled chiller units
Primary circuit	Letdown cooling via the CVS letdown HX
Primary circuit	PSS sample HX cooling
Auxiliary systems	WLS reactor coolant drain tank HX cooling
Primary circuit	CVS makeup pump miniflow HX cooling
Auxiliary systems	RNS pump seal cooling
Auxiliary systems	Plant air compressor cooling (compressed air system (CAS))
Auxiliary systems	CDS condensate pump motor oil cooling

Table 21-3 Secondary Sampling System (Continuous and Semi-Continuous Measurements)

Continuous Sample Points	Process Measurements
Hotwell (tube bundle condenser shell A)	Specific conductivity Cation conductivity Sodium
Hotwell (tube bundle condenser shell B)	Specific conductivity Cation conductivity Sodium
Hotwell (tube bundle condenser shell C)	Specific conductivity Cation conductivity Sodium
Hotwell (interconnecting piping between condenser shell A and condenser shell B)	Specific conductivity Cation conductivity Sodium
Hotwell (interconnecting piping between condenser shell B and condenser shell C)	Specific conductivity Cation conductivity Sodium
Condensate pump discharge	Specific conductivity Cation conductivity Sodium pH Dissolved oxygen
Deaerator inlet (condensate)	Specific conductivity Cation conductivity Sodium(1) pH Oxygen scavenger residual Dissolved oxygen
Feedwater	Specific conductivity Cation conductivity Sodium Dissolved oxygen pH Oxygen scavenger residual
Steam generator blowdown (SG 1)	Specific conductivity Cation conductivity Sodium pH Sulfate Dissolved oxygen

Table 21-3 Secondary Sampling System (Continuous and Semi-Continuous Measurements) (cont.)

Continuous Sample Points	Process Measurements
Steam generator blowdown (SG 2)	Specific conductivity Cation conductivity Sodium pH Sulfate Dissolved oxygen
Main steam system (SG 1)	Specific conductivity Cation conductivity Sodium(1) pH Dissolved oxygen
Main steam system (SG 2)	Specific conductivity Cation conductivity Sodium(1) pH Dissolved oxygen

Note:

1. Semi-continuous sampling. "Semi-continuous" means sampling instrumentation cycles through multiple individual sample streams that share a common sample header at predefined discrete intervals.

Table 21-4 Secondary Sampling System (Selective Measurements)

Condenser tube bundle B (north side)
Condenser tube bundle B (south side)
Heater drain (LP heater)
Heater drain (MSR 1st stage tube drain)
Heater drain (MSR 2nd stage tube drain)
Heater drain (MSR shell drain)
Auxiliary steam
Auxiliary boiler feedwater
Auxiliary boiler drum
Auxiliary boiler condensate
Condensate polisher outlet
Heater drain (HP heater)
Deaerator outlet (feedwater)
Startup feedwater

Table 21-5 Primary Circuit Water Chemistry Safety Limits

Conductivity	0.1 to 70 μS/cm at 25°C.
Solution pH	4.0 to 10.5
Oxygen (1)	No explicit safety limit assumed beyond the expected action level of shutdown within 24 hours if oxygen is >100 ppb at temperatures >121°C.
Chloride (2)	0.1 ppm, maximum
Fluoride (2)	0.15 ppm, maximum
Hydrogen (3)	0-80 cc H_2 (STP) / kg H_2O
Suspended Solids (4)	2 ppm, maximum
Lithium (5)	[ ] ppm (typically limited to [ ] ppm in the fuels contract [[ ] ppm at hot zero power], material selection considered [ ] ppm to account for potential future increases in the operating limits)
Boric Acid	0 to 4000 ppm boron
Silica	1.0 ppm, maximum
Aluminum	0.05 ppm, maximum
Aluminum + Calcium + Magnesium	1000 ppb, maximum (combined)
Magnesium	0.025 ppm, maximum
Zinc (6)	0.04 ppm

Notes

1. Oxygen concentration must be controlled to less than 0.1 ppm in the reactor coolant through scavenging with hydrazine prior to plant operation above 93°C. During power operation with the specified hydrogen concentration maintained in the coolant, the residual oxygen concentration shall not exceed 0.005 ppm.
2. Halogen concentrations must be maintained below the specified values regardless of system temperature.
3. Hydrogen must be maintained in the reactor coolant for plant operations with nuclear power above 1 MW. The normal operating range should be 25-50 cm^3 (STP) H_2/kg H_2O.
4. Solids concentrations expected to be determined through filter having 0.45 μm pore size.
5. The specified lithium concentrations must be established for startup testing prior to heatup beyond 66°C. During cold hydrostatic testing and hot functional testing (in the absence of boric acid), the reactor coolant limits for lithium hydroxide must be maintained to inhibit halogen stress corrosion cracking.
6. Specification is applicable during power operation when zinc is being injected. The zinc concentration is maintained at the lower of 0.04 ppm or that specified in the cycle-specific reload safety analyses.

Table 21-6 Secondary Circuit Water Chemistry Safety Limits

Steam Generator (Liquid Phase) and Steam Generator Blowdown	
Cation Conductivity	
Solution pH	
Sodium (1)	
Chloride (1)	
Fluoride (1)	
Silica (3)	
Secondary Side Steam	
pH	
Specific Conductivity	
Oxygen	
Ammonia	
Hydrazine	
Sodium	
Cation Conductivity	
Silica	
Chloride	
Sulfate	
Total Organic Carbon	
Feedwater	
pH	
Specific Conductivity	
Dissolved Oxygen	
Total Iron	
Total Copper	
Cation Conductivity	
Suspended Solids	
Sodium, Chloride, and Sulfate	
Silica	
Notes	

1. During the first 48-72 hours during shutdown, hideout return occurs which causes elevated impurity levels in the bulk solution. Hideout return occurs when concentrated impurities in sludge diffuse back into the bulk solution upon a loss of the boiling flux that causes the impurities to concentrate. Concentration may exceed impurity transient values for a short duration.

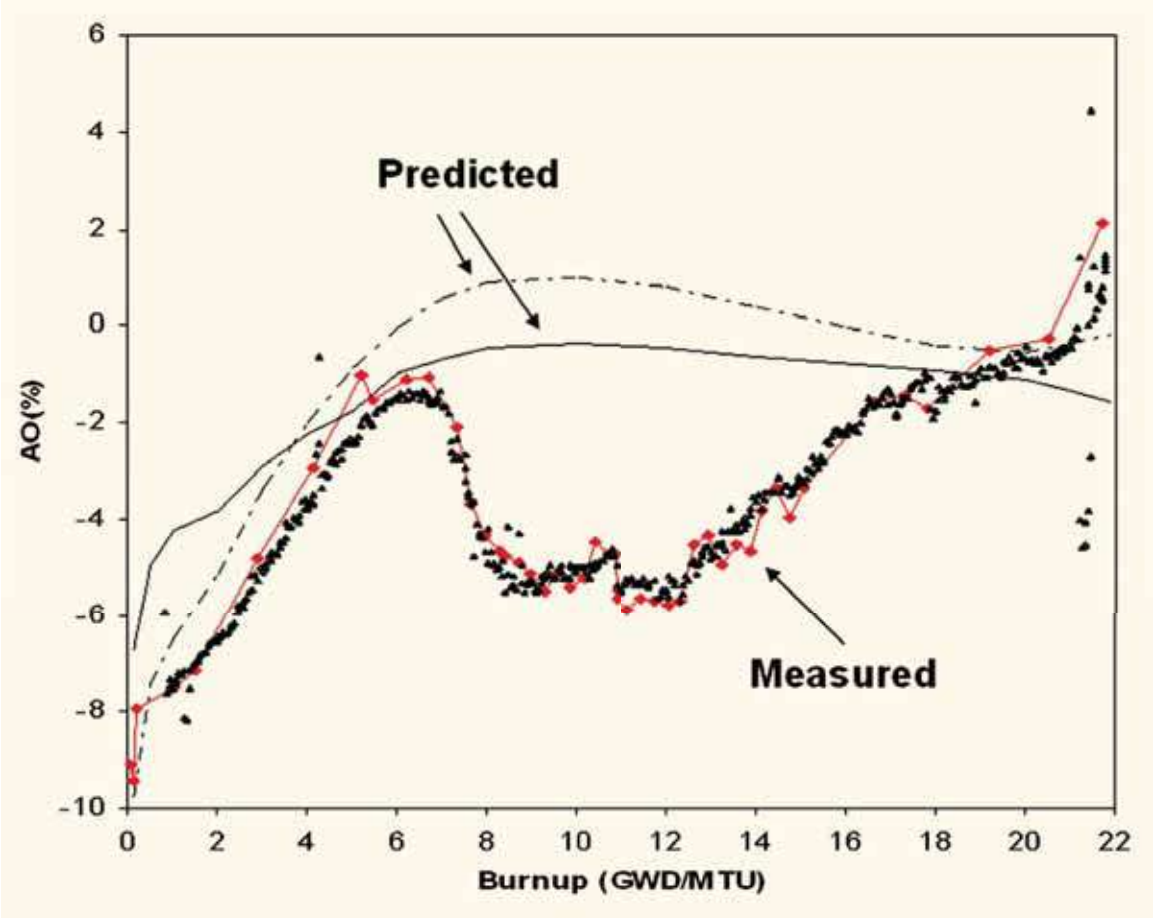


Figure 21-1 Typical Example of Crud-Induced Power Shift during a Fuel Cycle

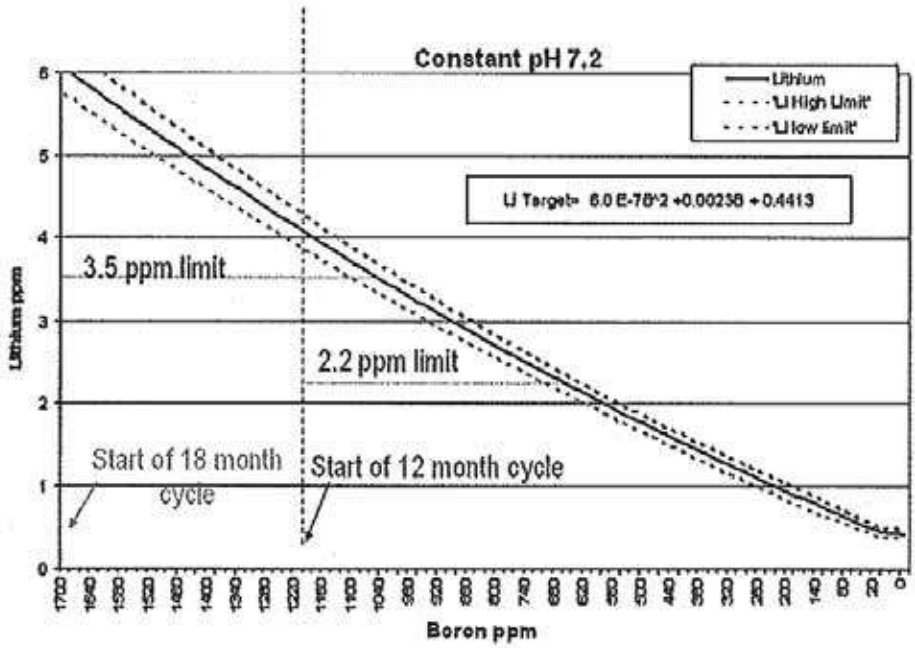


Figure 21-2 Illustration of Pressurised Water Reactor pH Control Options

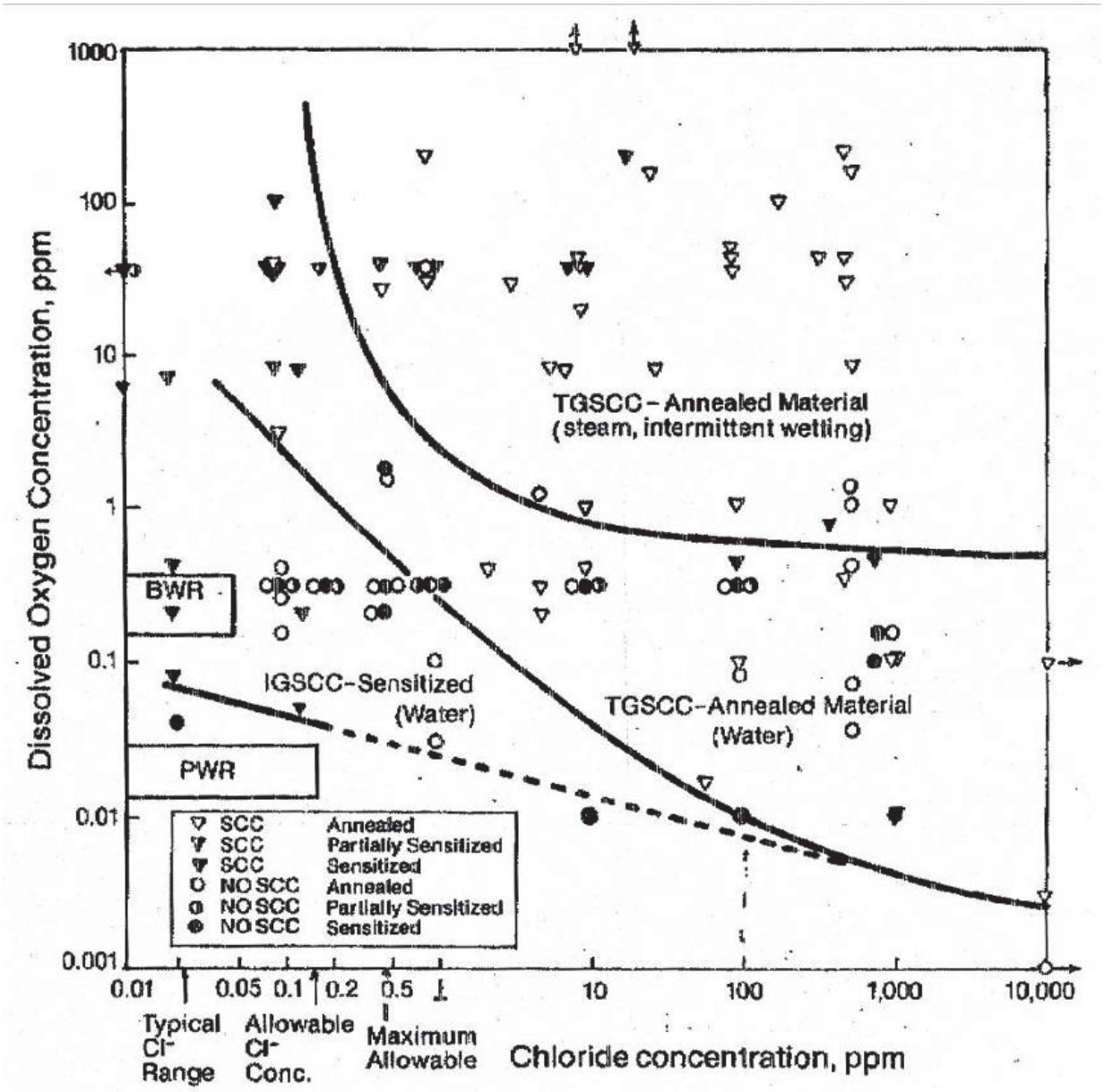


Figure 21-3 Effects of Oxygen and Chloride on the Stress Corrosion Cracking of Austenitic Steels in High-Temperature Water

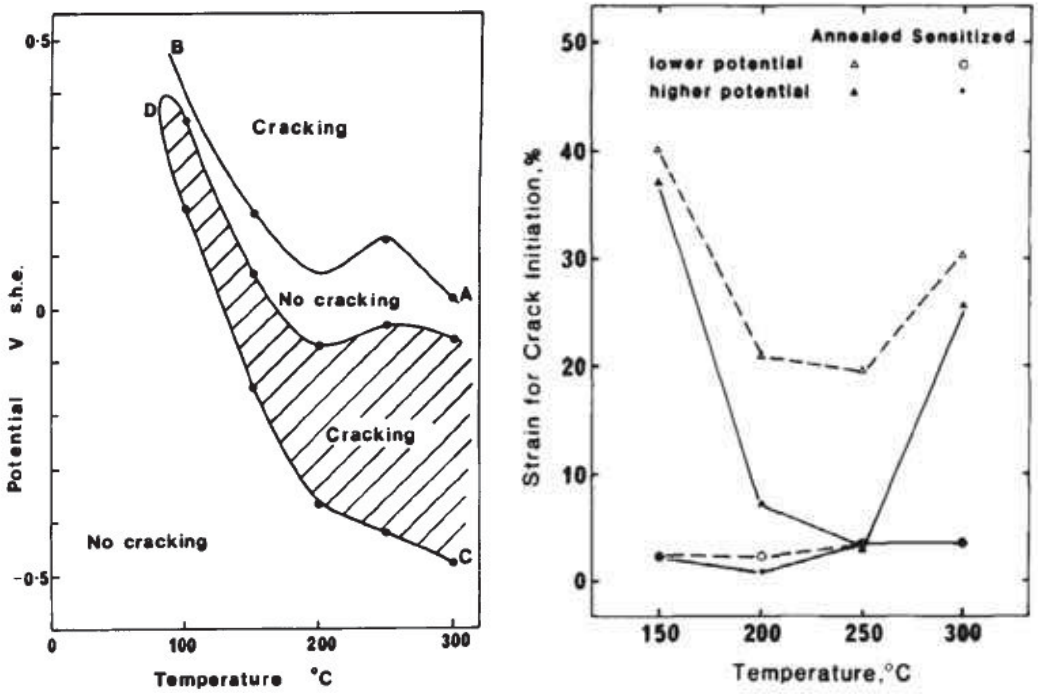
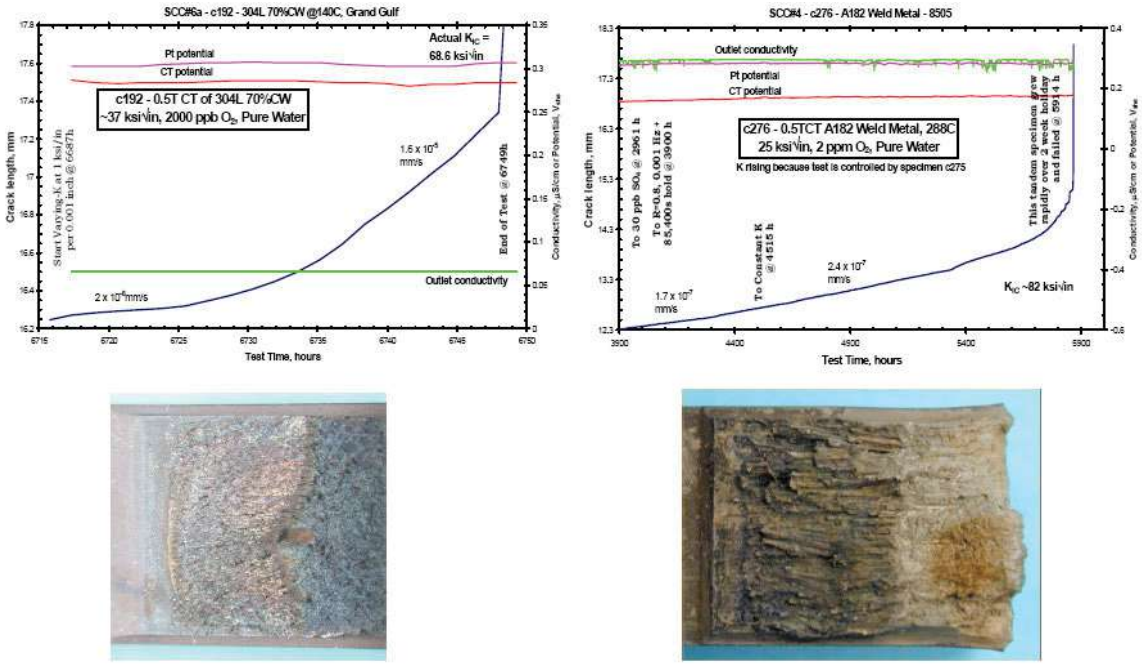
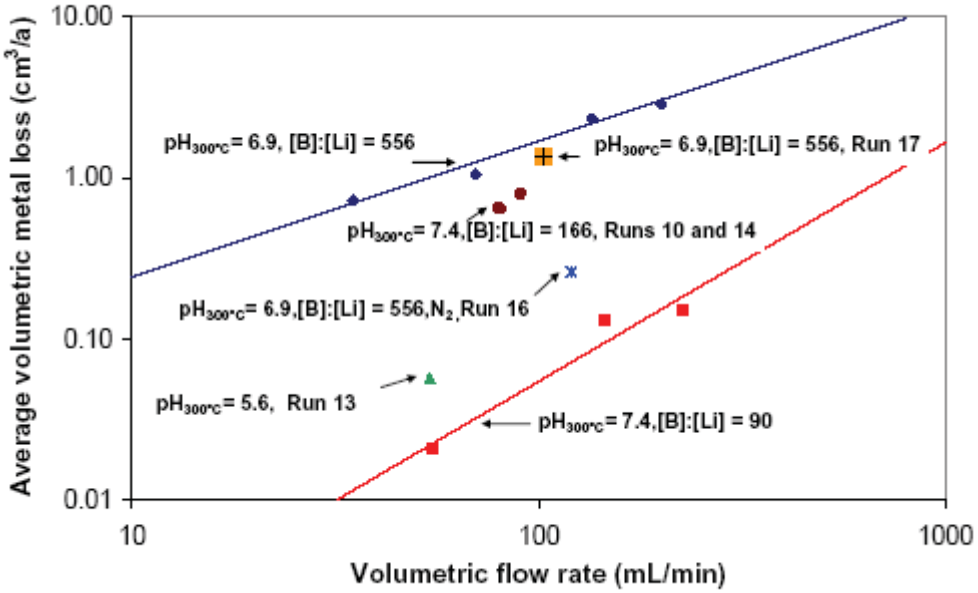


Figure 21-4 Stress Corrosion Cracking of Stainless Steels as a Function of Potential and Temperature



(Tested in 288°C water at increasing K until failure occurred. The load and crack depth at failure are very well defined, and the resulting KIC (not necessarily obtained valid conditions) is relatively low).

Figure 21-5 Comparison of Sudden Failure of Cold-Worked Stainless Steel and Alloy 182 Weld Metal



Taken from Jet Impingement Studies of flow-assisted corrosion correlated with volumetric flow rates, but are also strongly affected by the chemistry (especially the B/Li ratio) of the simulated primary coolant.

Figure 21-6 Volumetric Metal Loss Rates

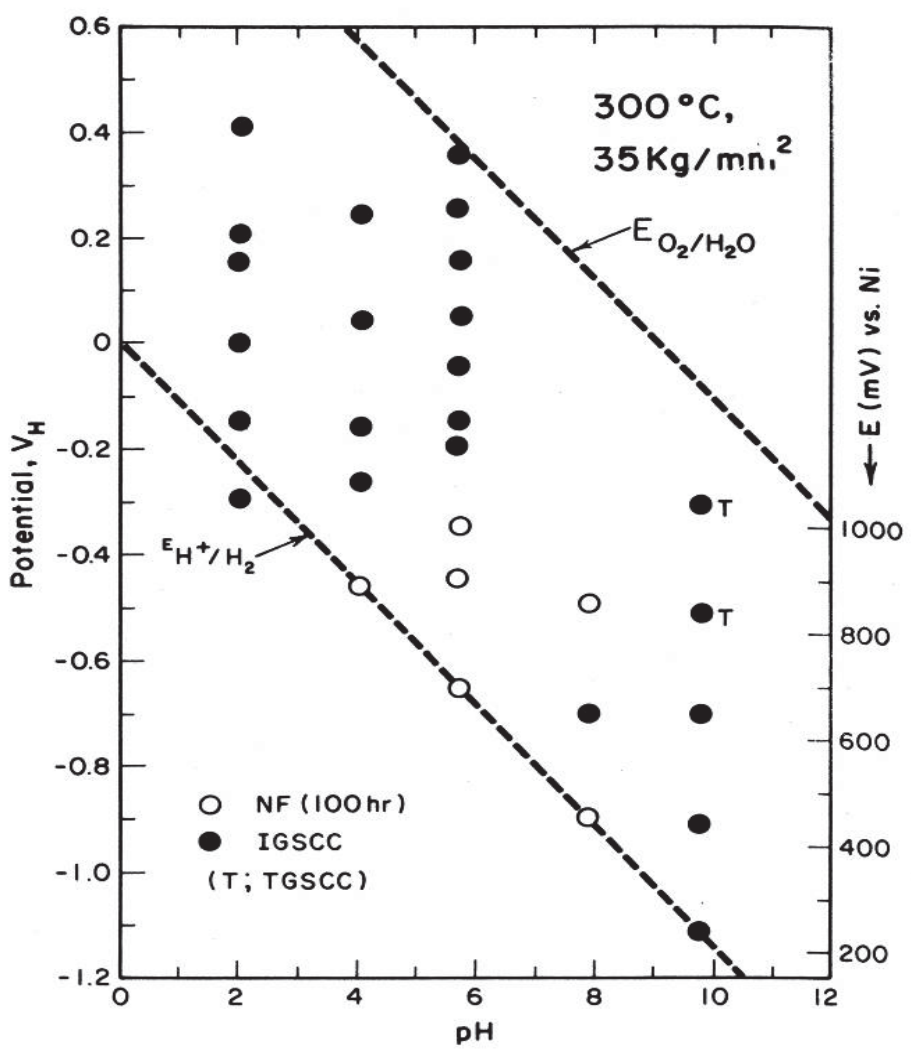


Figure 21-7 Stress Corrosion Cracking Susceptibility of Sensitised Type 304 Stainless Steel in 0.05% N Na_2SO_4 at 300°C as a Function of pH

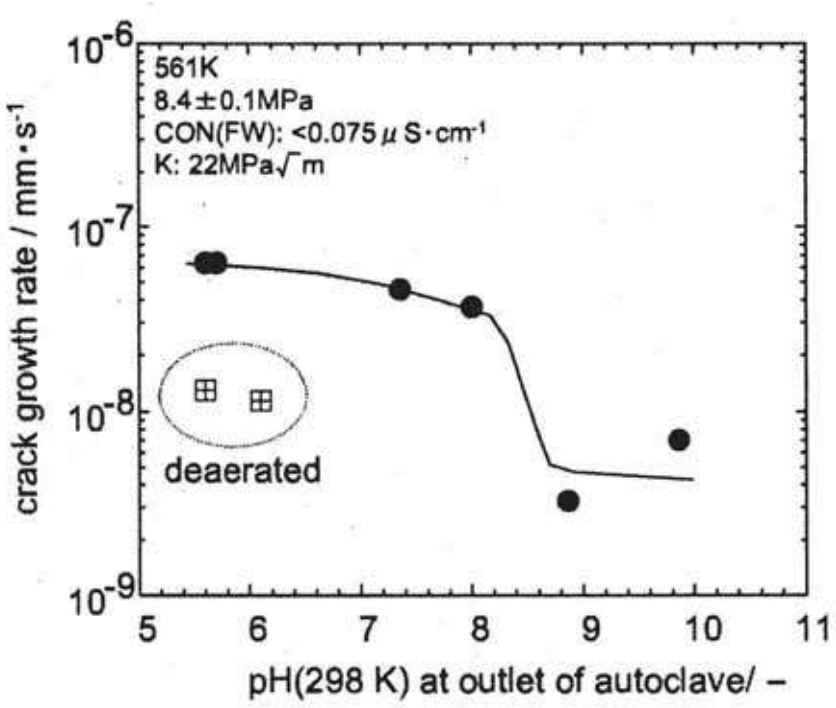


Figure 21-8 Measured Stress Corrosion Cracking Crack Growth Rates of Stainless-Steel Compact Tensile Specimens in 288°C Water at Various pH Values

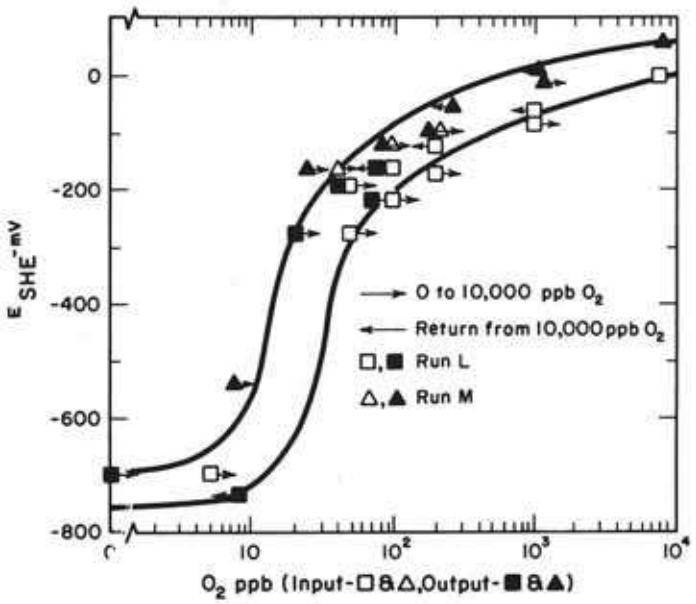


Figure 21-9 Relationship between Oxygen Concentration and Electrochemical Potential of Type 304 Stainless Steel in High-Purity Water at 274°C

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF FIGURES (cont.)

LIST OF FIGURES (cont.)

LIST OF ABBREVIATIONS, ACRONYMS, AND TRADEMARKS

AEC	Atomic Energy Commission
ALHR	average linear heat rate
ANSI	American National Standards Institute
AO	axial offset, defined as $[P_T - P_B] / [P_T + P_B]$where P_T is the integrated power in the top half of the core and P_B is the integrated power in the bottom half of the core
AOO	anticipated operational occurrences
ASME	American Society of Mechanical Engineers
ASTM	American Society for Testing and Materials
ATWT	anticipated transient without trip
B_{10}	boron-10
BA	burnable absorber
BOA	boron-induced offset anomaly risk assessment tool
BOL	beginning of life
CHF	critical heat flux
CIPS	crud-induced power shift
COLR	Core Operating Limits Report
CRDM	control rod drive mechanism
CVS	chemical and volume control system
DAS	diverse actuation system
DB	design basis
DEG	double-ended guillotine
DFBN	debris filter bottom nozzle
DNB	departure from nucleate boiling
DNBR	departure from nucleate boiling ratio
EOL	end of life
EPRI	Electric Power Research Institute
$F_{\Delta H}$	enthalpy rise hot channel factor
$F^N_{\Delta H}$	nuclear enthalpy rise hot channel factor
F_Q	heat flux hot channel factor
F^N_Q	nuclear heat flux hot channel factor
F^E_Q	engineering heat flux hot channel factor
GRCA	gray rod cluster assembly
HFLC	high-frequency, low-consequence
HMI	human-machine interface
HFP	hot fuel power
ΔI	axial flux difference, defined as $P_T - P_B$ where P_T is the integrated power in the top half of the core and P_B is the integrated power in the bottom half of the core
I/L^2	fuel rod clad moment of inertia/grid span
IAEA	International Atomic Energy Agency
IFBA	integral fuel burnable absorber
IFM	intermediate flow mixer
LBB	leak before break
LHR	linear heat rate
LOCA	loss-of-coolant accident
MCR	main control room
MES	manufacturing execution system
MOL	middle of life
MSHIM™	mechanical shim
MTC	moderator temperature coefficient
MWD/MTU	megawatt days per metric ton of uranium

LIST OF ABBREVIATIONS, ACRONYMS, AND TRADEMARKS (cont.)

NDE	nondestructive examination
OPΔT	overpower ΔT
OTΔT	overtemperature ΔT
PBF	power burst facility
PCI	pellet-clad interaction
PCM	power cooling mismatch
PCMI	pellet-cladding mechanical interaction
PCSR	Pre-Construction Safety Report
PIE	post-irradiation examination
PLHR	peak linear heat rate
PWR	pressurised water reactor
q_{vol}	volumetric power density
QMS	quality management system
QPTR	quadrant power tilt ratio
RAOC	relaxed axial offset control
RAPFE	radial averaged peak fuel enthalpy
RCCA	rod cluster control assembly
RCS	reactor coolant system
RFA	robust fuel assembly
RIA	reactivity increase accidents
RTDP	revised thermal design procedure
RTN	removable top nozzle
RTP	rated thermal power
SCC	stress corrosion cracking
SDM	shutdown margin
SLB	steam line break
STDP	standard thermal design procedure
S_m	design stress intensity
S_u	material ultimate strength
S_y	material yield strength
S(Z)	power spike factor
TD	theoretical density
TDC	thermal diffusion coefficient
Tech Spec	Technical Specification
UK	United Kingdom
WABA	wet annular burnable absorber
WIN	Westinghouse integral nozzle
ZIRLO®	zirconium alloy
ZrB_2	zirconium diboride

TRADEMARKS

22 FUEL SYSTEM, NUCLEAR AND THERMAL HYDRAULIC DESIGN

22.1 INTRODUCTION

Fuel element behaviour is of primary importance to the safety of a nuclear plant as the fuel contains the major part of the radioactive products in the plant. The fuel element performance as a heat source is crucial to safety because the release of its fission products is the likely consequence of some failure to transfer its heat to the coolant. In addition, there is a significant influence on the core reactivity and therefore upon the heat generation rate because of the feedback effect of the fuel reactivity coefficients.

The adequacy of the fuel element design and safety case is assessed in relation to relevant international standards (Reference 22.1) and best industry practice. For normal operation, this means that all reasonable steps should be taken to minimise the failure of the fuel rod cladding and thus minimise the release of radioactive fission products into the coolant. For fault conditions, the definition of satisfactory performance depends on the frequency with which the fault is expected to occur.

The limits within which the fuel can operate safely during both normal and fault conditions need to be defined and justified to demonstrate safe operation of the fuel. To achieve this, safety design bases are defined; considering the possible failure mechanisms of the materials and structures of the fuel assemblies and related components leads to the establishment of mechanical, nuclear, and thermal hydraulic design bases inherent in the safety design approach. It is also necessary to demonstrate that none of the design bases or limiting criteria are exceeded when the fuel is subjected to the full range of operational and fault conditions.

This chapter presents the safety case for the standard fuel element design in the AP1000 pressurised water reactor (PWR). This design provides very much flexibility in reload design.

First, the reactor core components are briefly described as an aid to understanding the following sections on the safety design basis (DB), safety design approach, and fuel system design. The design bases, functional requirements, and safety performance and justification for the nuclear and thermal and hydraulic design are then described.

This chapter refers extensively to Chapters 8 and 9 of this Pre-Construction Safety Report (PCSR); they define the conditions for frequent and infrequent faults both within the reactor and external to the reactor system. The results of the fault studies assessments are presented in Chapter 14. Chapter 21 is also particularly relevant as it describes the chemical controls and treatments applied in the AP1000 reactor to mitigate the impact of fuel failure in accident and fault conditions. This chapter also cross-references other relevant Westinghouse design documentation for additional details.

22.1.1 Fuel Assembly Description

The standard fuel assembly design for the AP1000 reactor is based on the Westinghouse 17x17 robust fuel assembly (RFA) design. Both the XL RFA fuel assembly and the standard AP1000 fuel assembly designs have the same active fuel length of 4.27 m. A difference between the two designs is that the AP1000 fuel assembly has been designed to interface with upper-mounted in-core instrumentation, versus bottom-mounted for the XL design.

Each standard fuel assembly consists of 264 fuel rods, 24 guide thimbles, and one instrumentation tube in a 17x17 array arranged within a supporting structure. The instrumentation thimble is located in the centre position and provides a channel for insertion of an in-core neutron detector if the fuel assembly is located in an instrumented core position. The guide thimbles provide channels for insertion of a rod cluster control assembly (RCCA), a gray rod cluster assembly (GRCA), a neutron source assembly, a burnable absorber (BA) assembly, or a thimble plug, depending on the position of the particular fuel assembly in the core. If control rods, source assemblies, and discrete BA assemblies are not required, thimble plugs are inserted to limit the fuel bypass flow. The guide thimbles are joined to the top and bottom nozzles of the fuel assembly and provide the supporting structure for the fuel grids. Figure 22-1 shows a cross-section of the fuel assembly array; Figure 22-2 shows a full-length view of the fuel assembly.

The fuel rods are loaded into the fuel assembly structure so that there is clearance between the fuel rod ends and the top and bottom nozzles. The fuel rods are supported within the fuel assembly structure by 10 structural grids (top grid (one), bottom grid (one), intermediate grids (eight)) and four non-structural grids (intermediate flow mixer (IFM) grids, plus one protective grid). Top, bottom, and intermediate grids provide axial and lateral support to the fuel rods. In addition, the four IFM grids located near the centre of the fuel assembly and between the intermediate grids provide additional coolant mixing. Debris failure mitigation is provided by a combination of the protective grid with the debris filter bottom nozzle (DFBN); the fuel cladding with oxide coating near the bottom; and the long, solid fuel rod bottom end plug.

Fuel assemblies are installed vertically in the reactor vessel and stand upright on the lower core plate, which is fitted with alignment pins to locate and orient each assembly. After the fuel assemblies are set in place, the upper support structure is installed. Alignment pins, built into the upper core plate, engage and locate the upper ends of the fuel assemblies. The upper core plate then bears down against the hold-down springs on the top nozzle of each fuel assembly to hold the fuel assemblies in place.

Improper orientation of fuel assemblies within the core is prevented by the use of an indexing hole in one corner of the top nozzle top plate. The assembly is oriented with respect to the handling tool and the core by means of a pin inserted into this indexing hole. Visual confirmation of proper orientation is also provided by an engraved identification number on the opposite corner of the top plate.

22.1.1.1 Fuel Rods

The fuel rods consist of uranium dioxide ceramic pellets contained in cold-worked and stress-relieved tubing constructed from a zirconium alloy (**ZIRLO**® High Performance Fuel Cladding Material), which is plugged and seal-welded at the ends to encapsulate the fuel. **ZIRLO** is selected for its mechanical properties and low neutron absorption cross-section (Reference 22.3). Figure 22-3 shows a schematic of the fuel rod.

The fuel pellets are right circular cylinders consisting of slightly enriched uranium dioxide powder that has been compacted by cold pressing and then sintered to the required density. The ends of each pellet are dished slightly to allow greater axial expansion at the pellet centreline and to increase the void volume for fission gas release. The ends of each pellet also have a small chamfer at the outer cylindrical surface, which improves manufacturability and mitigates potential pellet damage due to fuel rod handling.

Void volume and clearances are provided within the rods to accommodate fission gases released from the fuel, differential thermal expansion between the clad and the fuel, and fuel density changes during irradiation. To facilitate the extended burnup capability necessitated by longer operating cycles, the fuel rod is designed with two plenums (upper and lower) to accommodate the additional fission gas release. The upper plenum volume is maintained by a fuel pellet hold-down spring. The lower plenum volume is maintained by a standoff assembly.

Shifting of the fuel within the clad during handling or shipping prior to core loading is prevented by a stainless-steel helical spring that bears on top of the fuel pellet stack. The spring also prevents gaps from opening as pellets densify, and provides support to the cladding due to creepdown during steady-state operation. Assembly consists of plugging and welding the bottom of the cladding; installing the bottom plenum spacer assembly, fuel pellets, and top plenum spring; and then plugging and welding the top of the rod.

The solid bottom end plug has an internal grip feature and tapered end to facilitate fuel rod loading during fuel assembly fabrication and reconstitution. Additionally, the bottom end plug is designed to be sufficiently long to extend through the protective grid. The bottom section of the fuel rod has a protective zirconium-oxide-coated surface feature. Use of the protective grid with a longer end plug and the DFBN, in addition to the coated cladding surface, constitutes a three-level debris protection package, which enhances the fuel reliability performance against trapped debris. This precludes any breach in the fuel rod pressure boundary due to clad fretting wear induced by debris trapped at the bottom section of the fuel assembly.

The fuel rods are internally pressurised with helium during the welding process to minimise compressive clad stresses and prevent clad flattening under reactor coolant operating pressures. The fuel rods are pre-pressurised and designed so that:

- The internal gas pressure design limit referred to in Section 22.5.1 is not exceeded.
- The cladding stress-strain limits (Section 22.5.1) are not exceeded.
- Clad flattening will not occur during the fuel core life.

The AP1000 reactor fuel rod design may also include axial blankets. The axial blankets consist of fuel pellets of a reduced enrichment at each end of the fuel rod pellet stack. Axial blankets reduce neutron leakage axially and improve fuel utilization. The axial blankets use chamfered pellets that are longer than the enriched pellets to help prevent accidental mixing during manufacturing.

Furthermore, axial blankets do not significantly impact the source range detector response, since the reduction in power from the axial blanket is limited to the top and bottom 20.32 cm (8 inches) of the core, while the source range detectors are centred typically about 106.68 cm (42 inches) from the bottom of the core. Reference 22.98 shows that the axial weighting or importance of the neutron flux from the end 20.32 cm (8 inches) regions of the core to the source range detector response is relatively low compared to the centre region of the core. In addition, the neutron flux at the ends of the core is relatively low compared to the more important centre region. Therefore, the reduction in power at the ends of the core due to the introduction of axial blankets will not significantly impact the source range detector response. Additionally, the locations of the axial blankets are evident in Figure 22-20 which shows an example of a first cycle fuel rod design.

The AP1000 reactor fuel rods include integral fuel BAs (IFBAs). The IFBAs consist of zirconium diboride (ZrB_2) -coated fuel pellets, which are identical to the enriched uranium dioxide pellets except for the addition of a thin boride coating on the pellet cylindrical surface. Coated pellets occupy the central portion of the fuel column. The number and pattern of integral fuel BA rods within an assembly may vary depending on specific application (Reference 22.3).

[

]

22.1.1.2 Fuel Assembly Structure

As shown in Figure 22-2, the fuel assembly structure consists of a bottom nozzle, top nozzle, fuel rods, guide thimbles, and grids.

Bottom Nozzle

The bottom nozzle serves as the bottom structural element of the fuel assembly and directs the coolant flow distribution to the assembly. The nozzle is fabricated from Type 304 and Grade CF-3 stainless steel and consists of a perforated plate and casting that incorporates a skirt and four angle legs with bearing pads, as illustrated in Figure 22-2. The legs and skirt form a plenum to direct the inlet coolant flow to the fuel assembly. The perforated plate also prevents accidental downward ejection of the fuel rods from the fuel assembly. The bottom nozzle is fastened to the fuel assembly guide thimbles by locked thimble screws, which penetrate through the nozzle and engage with a threaded plug in each guide thimble. The flow hole pattern, together with top nozzle ligaments, limits the fuel rod movement within the cavity between the two nozzles.

Coolant flows from the plenum in the bottom nozzle upward through the penetrations in the plate to the channels between the fuel rods. The penetrations in the plate are positioned between the rows of the fuel rods.

In addition to serving as the bottom structural element of the fuel assembly, the bottom nozzle also functions as a debris filter. The bottom nozzle perforated plate contains a multiplicity of flow holes sized to minimise passage of detrimental debris particles into the active fuel region of the core while maintaining sufficient hydraulic and structural margins. Furthermore, the skirt provides improved bottom nozzle structural stability and increased design margins to reduce damage from abnormal handling.

Axial loads (from top nozzle hold-down springs) imposed on the fuel assembly and the weight of the fuel assembly are transmitted through the bottom nozzle to the lower core plate. Indexing and positioning of the fuel assembly is controlled by alignment holes in two diagonally opposite bearing pads that mate with locating pins in the lower core plate. Lateral loads on the fuel assembly are transmitted to the lower core plate through the locating pins.

The bottom nozzle also has a reconstitution design feature that facilitates easy removal of the nozzle from the fuel assembly. This design incorporates a thimble screw with a circular locking cup located around the screw head. The locking cup is crimped into a local spherical radius relief on the bottom nozzle. To remove the bottom nozzle, a counter clockwise torque is applied to the thimble screw until the locking cup (detents) is relaxed and the thimble screw is removed. This reconstitutable design permits remote unlocking, removal, and relocking of the thimble screws, as the same or a new bottom nozzle is reattached to the fuel assembly.

Top Nozzle

The reconstitutable top nozzle functions as the upper structural component of the fuel assembly and, in addition, provides a partial protective housing for the RCCA, discrete BA, or other core components. The top nozzle assembly includes four sets of hold-down springs, which are secured to the top nozzle top plate (Figure 22-4). The springs are made of Alloy 718. The other top nozzle components are made of Type 304L and Grade CF-3 stainless steel.

The adapter plate contains various-shaped holes to permit the flow of coolant upward through the top nozzle. Round holes are provided in the adapter plate to accept (guide thimble) inserts that are mechanically locked to the adapter plate using a lock tube. The unique design of the insert joint and lock tube are the key design features of the reconstitutable top nozzle.

The ligaments in the adapter plate cover the top of the fuel rods, precluding any upward ejection of the fuel rods from the fuel assembly. The enclosure is a box-like structure that establishes the distance between the adapter plate and the top plate. The top plate has a large square hole in the centre to permit access for the RCCA, BA assembly, or other components. Hold-down springs are mounted on the top plate and are retained by retaining pins located at diagonally opposite corners of the top plate.

The top plate also contains integral pads located on the two remaining top nozzle corners. The pads include alignment holes which, when fully engaged with the reactor internals upper core plate guide pins, provide proper alignment to the fuel assembly, reactor internals, and RCCA.

To remove the top nozzle assembly, a tool is first inserted through a lock tube and expanded radially to engage the bottom edge of the tube (Figure 22-5). An axial force is then exerted on the tool, which overrides local lock tube deformations and withdraws the lock tubes from the inserts. After the lock tubes have been removed, the nozzle assembly is removed by raising it off the upper slotted ends of the nozzle inserts, which deflect inwardly under the axial lift load.

With the top nozzle assembly removed, direct access is provided for fuel rod examination or replacement. Reconstitution is completed by the remounting of the nozzle assembly and the insertion of lock tubes. (Reference 22.16)

Unlike previous designs with bottom-mounted in-core instrumentation, the AP1000 design has upper-mounted instrumentation. As such, the top nozzle contains an instrumentation hole.

Guide Thimbles and Instrument Tube

The guide thimbles are structural members that provide channels for the neutron absorber rods, BA rods, neutron source rods, or other assemblies. Each guide thimble is fabricated from Zircaloy-4 or **ZIRLO** with constant outer and inner diameter over the entire length. Separate dashpot tubes, made from Zircaloy-4 or **ZIRLO** tubing, are inserted into the bottom portion of the guide thimble tubes. The larger tube diameter at the top section provides a relatively large annular area necessary to permit rapid control rod insertion during a reactor trip, as well as to accommodate the flow of coolant during normal operation. Holes provided on the guide thimble above the dashpot reduce the rod drop time and also provide sufficient cooling to the RCCAs and GRCAs when they are inserted into the core without unduly reducing the flow past the fuel rods.

The lower portion of the guide thimble with the dashpot tube results in a dashpot action near the end of the control rod travel during normal trip operation. The dashpot is closed at the bottom by means of an end plug, which is provided with a small flow port to avoid fluid stagnation in the dashpot volume during normal operation.

To accommodate the top nozzle reconstitutable feature, the top of the guide thimble is fastened to a tubular sleeve, or insert, by a three tier expansion bulge joint. An expansion tool is inserted inside the nozzle insert and guide thimble to the proper elevation. The four lobes on the expansion tool force the guide thimble and insert outward locally to a predetermined diameter, therefore joining the two components.

Upon installation of the top nozzle assembly, the bulge near the top of the nozzle insert is captured in a corresponding groove in the thimble hole of the top nozzle adapter plate. The mechanical connection between the nozzle insert-guide thimble and top nozzle is made by insertion of a lock tube into the insert (Figure 22-5). The design of the top grid sleeve-guide thimble and top nozzle insert-guide thimble bulge joint connections have been mechanically tested and found to meet applicable design criteria.

The fuel rod support grids, with the exception noted for the Alloy-718 protective grid, are secured to the guide thimbles using a similar bulge joint connection to create an integral structure. Attachment of the intermediate mixing vane and IFM grids to the guide thimbles is performed using the fastening technique depicted in Figure 22-6 and Figure 22-7.

The intermediate mixing vane and IFM grids employ a single-tier bulge connection between the grid sleeve and guide thimble as compared with the two-tier bulge connection used for the

top grid. The design of the single-tier bulge joint connection has also been mechanically tested and meets the design requirements.

The Alloy-718 bottom grid is secured to the guide thimble assembly by a double-tier bulge connection between the grid sleeve and guide thimble. The design of the double-tier bulge joint connection has also been mechanically tested and meets the design requirements.

The lower end of the guide thimble is fitted with a welded end plug. The Alloy-718 protective grid is secured to the guide thimble assembly by Alloy-718 spacers that are spot-welded to the grid. The spacer is captured between the guide thimble end plug and the bottom nozzle by means of a (thimble) locking screw (Figure 22-8).

The described methods of grid fastening are standard and have been used successfully since the introduction of guide thimbles in 1969.

The central instrumentation tube in each fuel assembly is constrained by seating in counterbores located in both top and bottom nozzles. The instrumentation tube has a constant diameter and provides an unrestricted passageway for the in-core neutron detector which enters the fuel assembly from the top nozzle. Furthermore, the instrumentation tube is secured to the top, bottom, IFM, and mid-grids with bulge joint connections similar to those previously discussed for securing the grids to the guide thimbles.

Grid Assemblies

The fuel rods are supported at intervals along their lengths by grid assemblies that maintain the lateral spacing between the rods throughout the design life of the assembly (Figure 22-2). Each fuel rod is given support at six contact points within each structural grid by the combination of support dimples and springs. The grid assembly consists of individual slotted straps assembled and interlocked into an egg-crate-type arrangement with the straps permanently joined at their points of intersection. The straps may contain springs, support dimples, and mixing vanes; or any such combination.

Two types of structural grid assemblies are used on the fuel assembly of the AP1000 design. One type, with mixing vanes projecting from the edges of the straps into the coolant stream, is used in the high-heat flux region of the fuel assemblies to promote mixing of the coolant. The other type, located at the top and bottom of the assembly, does not contain mixing vanes on the internal straps. The outside straps on the grids contain mixing vanes that, in addition to their mixing function, aid in guiding the grids and fuel assemblies past projecting surfaces during handling or loading and unloading of the core.

Because of its corrosion resistance and high-strength properties, the bottom grid material chosen for the fuel assembly design is Alloy-718. The top grid is fabricated from Alloy-718. The magnitude of the grid restraining force on the fuel rod is set high enough to minimise possible fretting without overstressing the cladding at the points of contact between the grids and fuel rods. The grid assemblies are designed to allow axial thermal expansion of the fuel rods without imposing restraint sufficient to develop buckling or distortion of the fuel rods.

The eight intermediate (mixing vane) or structural grids on the fuel assembly are made of **ZIRLO**. This material was selected to take advantage of its inherent low neutron capture cross-section. **ZIRLO**, like other zirconium alloys used in the nuclear industry, contains a high percentage of zirconium and therefore inherits the low capture cross section for thermal neutrons from zirconium. The percent of other elements [ ] in the zirconium alloy are limited to the content necessary for good mechanical properties and corrosion resistance.

The **ZIRLO** grids have thicker straps and incorporate the same grid cell support configuration as the Alloy-718 grid. The **ZIRLO** interlocking strap joints and grid/sleeve joints are fabricated by laser welding, whereas the Alloy-718 grid joints (except the protective grid) are brazed. The interlocking strap joints for the protective grid are also fabricated by laser welding.

The mixing vanes incorporated in the intermediate grids induce additional flow mixing among the various flow channels in a fuel assembly as well as between adjacent fuel assemblies. This additional flow mixing enhances thermal performance.

The IFM grids are located at selected spans between the mixing vane structural grids and incorporate a similar mixing vane array (Figure 22-2). Their prime function is mid-span flow mixing in the hotter fuel assembly spans. Each intermediate flow mixer grid cell contains four dimples that are designed to prevent mid-span channel closure in the spans containing intermediate flow mixers and fuel rod contact with the mixing vanes. This simplified cell arrangement allows short grid cells so that the intermediate flow mixer grid can accomplish its flow mixing objective with minimal pressure drop.

The IFM grids, like the mixing vane grids, are fabricated from **ZIRLO**. The IFM grids are manufactured using the same basic techniques as the structural grid assemblies and are joined to the guide thimbles and instrumentation tube via sleeves welded at the bottom of appropriate grid cells.

Grid impact testing has been performed on the **ZIRLO** structural grids and the IFM grids. The purpose of the testing was to determine the dynamic buckling, or crush strength of the grids. The grid impact testing was performed at an elevated temperature of 316°C (600°F). This temperature is a conservative value representing the core average temperature at the midgrid locations.

The IFM grids are not intended to be structural members but they do share the loads of the structural grids during faulted loading and, as such, contribute to enhance the load-carrying capability of the fuel assembly.

The dynamic crush strength of the structural grids and IFM grids envelop the calculated grid impact loading during combined seismic and pipe rupture events. A coolable geometry is therefore provided at the IFM grid elevations, as well as at the structural grid elevations.

An additional assessment was carried out to assess the structural and IFM grid response to the depressurisation of the primary circuit due to a double-ended guillotine (DEG) break of the RCS cold leg. This assessment, documented in Reference 22.97, concluded that [

] does not challenge coolable geometry of the core.

[

]

22.1.1.3 In-Core Control Components

Reactivity control is provided by neutron-absorbing rods, gray rods, BA rods, and a soluble chemical neutron absorber (boric acid). The boric acid concentration is varied to control long-term reactivity changes such as:

- Fuel depletion and fission product buildup
- Cold to hot, zero power reactivity changes
- Reactivity change produced by intermediate-term fission products such as xenon and samarium
- Burnable absorber depletion

The chemical and volume control system, which is used to adjust the level of boron in the coolant, is discussed in Section 6.1.

The rod cluster control assemblies provide reactivity control for:

- Shutdown
- Reactivity changes due to coolant temperature changes in the power range
- Reactivity changes associated with the power coefficient of reactivity
- Reactivity changes due to void formation

A negative power coefficient is maintained at hot, full-power conditions throughout the entire cycle to reduce possible deleterious effects caused by a positive coefficient during pipe rupture or loss-of-flow accidents. Since soluble boron alone is insufficient to provide a negative moderator coefficient, burnable absorber assemblies are also used. Use of burnable absorber assemblies during reloads is discussed in subsection 22.6.1.2.

The most effective reactivity control components are the RCCAs and the corresponding drive rod assemblies, which, along with the GRCAs, are the only kinetic parts in the reactor. Figure 22-9 identifies the RCCAs and drive rod assembly in addition to the arrangement of these components in the reactor relative to the interfacing fuel assembly, guide thimbles, and control rod drive mechanism (CRDM). The arrangement for the GRCAs is the same.

The guidance system for the RCCA is provided by the guide tubes (Figure 22-9). The guide tubes provide two regimes of guidance: first, in the lower section, a continuous guidance system provides support immediately above the core, which protects the rod against excessive deformation and wear caused by hydraulic loading; second, the region above the continuous section provides support and guidance at uniformly spaced intervals.

The envelope of support is determined by the pattern of the control rod cluster (Figure 22-10). The guide tubes provide alignment and support of the control rods, spider body, and drive rod while maintaining trip times at or below required limits.

Each reactivity control component is described in detail below. The neutron source assemblies provide a means of monitoring the core during periods of low neutron activity.

Rod Cluster Control Assemblies

The rod cluster control assemblies are divided into two categories: control and shutdown. The control groups compensate for reactivity changes due to variations in operating conditions of the reactor, that is, power and temperature variations. Two nuclear design criteria have been employed for selection of the control group. First, the total reactivity worth must be adequate to meet the nuclear requirements of the reactor. Second, in view of the fact that these rods may be partially inserted at power operation, the total power peaking factor should be low enough to confirm that the power capability is met. The control and shutdown groups provide adequate shutdown margin.

An RCCA comprises 24 individual neutron absorber rods fastened at the top end to a common spider assembly (Figure 22-10). The absorber material used in the control rods is silver-indium-cadmium alloy, which is essentially "black" to thermal neutrons and has sufficient additional resonance absorption to significantly increase worth. The absorber material is in the form of solid bars sealed in cold-worked stainless-steel tubes (Figure 22-11). Sufficient diametral and end clearance is provided to accommodate relative thermal expansions. The control rods have bottom plugs with bullet-like tips to reduce the hydraulic drag during reactor trip and to guide smoothly into the dashpot section of the fuel assembly guide thimbles. The material used in the absorber rod end plugs is Type 308 or 308L stainless steel. The design stresses used for the these materials are the same as those defined by the American Society of Mechanical Engineers (ASME) for Type 304 or 304L stainless steel which have essentially the same strength properties as Type 308 and 308L stainless steel, respectively.

The spider assembly is in the form of a central hub with radial vanes containing cylindrical fingers from which the absorber rods are suspended. Internal groove-like profiles to facilitate handling tool and drive rod assembly connection are machined into the upper end of the hub. Coil springs inside the spider body absorb the impact energy at the end of a trip insertion. The radial vanes may either be joined to the hub by welding and brazing, and the fingers are joined to the vanes by brazing, or the vanes and fingers may be integral with the spider body. A bolt that holds the springs and retainer is threaded into the hub within the skirt and welded to prevent loosening while in service. The components of the spider assembly are made from Types 304, 304L, and/or CF-3 (casting equivalent of 304L) stainless steel except for the retainer, which is of Type 630 material, and the springs, which are Alloy-718.

The absorber rods are fastened securely to the spider. The rods are first threaded into the spider fingers and then secured with a locking device. The end plug below the pin position is designed with a reduced section to permit flexing of the rods to correct for small operating or assembly misalignments.

The overall length of the RCCA is such that, when the assembly is withdrawn through its full travel, the tips of the absorber rods remain engaged in the fuel assembly guide thimbles so that alignment between rods and thimbles is always maintained. Since the rods are long and slender, they are relatively free to conform to any misalignments with the guide thimble. Any such misalignments are small and the RCCA rods remain positioned within the core so that flow-induced wear on the RCCA absorber rods as they sit at the top of the guide thimbles is evenly spread and within acceptable limits.

Gray Rod Cluster Assemblies

The purpose of GRCAs is to provide reactivity control capability during operation. GRCAs contain a smaller quantity of neutron absorber relative to RCCAs, and the 16 GRCAs in the AP1000 reactor are grouped into four banks with low reactivity worth. The GRCAs are used

in load follow manoeuvring and base load operation to control core temperature and power; they provide a mechanical shim capability that replaces the need for small changes in the concentration of soluble boron, that is, chemical shim, normally used for this purpose.

The mechanical design of the GRCAs plus the CRDM and the interface with the fuel assemblies and guide thimbles are identical to the RCCAs except that the 24 GRCA rodlets are fabricated of a tungsten absorber (of a reduced diameter as compared with the RCCA absorber) double encapsulated in an Alloy-718 sleeve and stainless-steel clad (Figure 22-12). The combination of the reduced diameter tungsten absorber and Alloy-718 sleeve provide the following benefits:

- [
  ]
- [
- [
  ]

Tungsten does not exhibit decreased absorber worth as a result of irradiation which provides [ ]. In addition tungsten does not introduce any detriments when compared to the silver-indium-cadmium alloy material and therefore it is deemed to be the best choice for the GRCA rodlets. Reference 22.36 provides further detail on the benefits and design of the tungsten absorber material utilised in the GRCA rodlets.

Burnable Absorber Assembly

The reactor core is cooled and moderated by light water under pressure. Soluble boron in the moderator/coolant serves as a neutron absorber. The concentration of boron is varied to control reactivity changes that occur relatively slowly, including the effects of fuel burnup. BA rods are also employed to limit the amount of soluble boron required and thereby maintain the desired negative reactivity coefficients.

Each BA assembly consists of discrete BA rods attached to a hold-down assembly (Figure 22-13). When needed for nuclear considerations, BA rods are inserted into selected thimbles within fuel assemblies.

Wet annular BAs (WABAs) consist of pellets of alumina-boron carbide material contained within zirconium alloy tubes. These tubes, which form the outer clad for the BA rod, are plugged, pressurised with helium, and seal-welded at each end to encapsulate the stack of absorber material. The absorber stack length is positioned axially within the BA rod by the use of a bottom-end spacer as necessary (Figure 22-13).

The BA rods in each fuel assembly are grouped and attached together at the top end of the rods to a hold-down assembly by a flat, perforated retaining plate, which fits within the fuel assembly top nozzle and rests on the adapter plate.

The retaining plate and the BA rods are held down and restrained against vertical motion through a spring pack attached to the plate and compressed by the upper core plate when the reactor upper internals assembly is lowered into the reactor. With this arrangement, the BA rods cannot be ejected from the core by flow forces. Each rod is attached to the baseplate by a nut that is crimped into place.

Neutron Source Assemblies

The purpose of a neutron source assembly is to provide a base neutron level to give confidence that the detectors are operational and responding to core multiplication neutrons. For the first core, a neutron source is placed in the reactor to provide a positive neutron count of at least two counts per second on the source range detectors attributable to core neutrons. The detectors, called source range detectors, are used primarily during subcritical modes of core operation.

The source assembly also permits detection of changes in the core multiplication factor during core loading, refuelling, and approach to criticality. This can be done since the multiplication factor is related to an inverse function of the detector count rate. Changes in the multiplication factor can be detected during addition of fuel assemblies while loading the core, changes in control rod positions, and changes in boron concentration.

Both primary and secondary neutron source rods are used. The primary source rod, containing a radioactive material, spontaneously emits neutrons during initial core loading, reactor startup, and initial operation of the first core. After the primary source rod decays beyond the desired neutron flux level, neutrons are then supplied by the secondary source rod. The secondary source rod contains a stable material, which is activated during reactor operation. The activation results in the subsequent release of neutrons.

Four source assemblies are typically installed in initial load of the reactor core: two primary source assemblies (Figure 22-14) and two secondary source assemblies (Figure 22-15). Each primary source assembly contains one primary source rod and a number of BA rods. Each secondary source assembly contains a symmetrical grouping of secondary source rodlets.

Neutron source assemblies are employed at opposite sides of the core. The source assemblies are inserted into the guide thimbles in fuel assemblies at selected locations. The source assemblies contain a hold-down assembly identical to that of the BA assembly (Figure 22-14 and Figure 22-15).

The primary and secondary source rods both use the same cladding material as the absorber rods. The secondary source rods contain antimony-beryllium pellets stacked to a height of approximately 2.23 m (88 inches). The primary source rods contain capsules of californium (plutonium-beryllium possible alternate) source material and alumina spacers to position the source material within the cladding. The rods in each assembly are fastened at the top end to a hold-down assembly.

The other structural members, except for the springs, are constructed of Type 304, 304L, and 308L stainless steel. The springs exposed to the reactor coolant are Alloy-718.

22.2 FAULT STUDY LIMITS

An overview of the safety case methodology is given in Figure 8-1 in Chapter 8. The approach to identifying faults for the AP1000 reactor is described in Chapter 8. A complete list of faults investigated for the fuel system design is provided in Appendix 8A. The plant characteristics and initial conditions assumed in the accident analyses for the fuel system design are shown in Chapter 9 (Tables 9.0-5 and 9.0-7). The results of the accident analyses for each fault investigated for the fuel system design, together with design-limiting values for safety-relevant parameters, are given in the appropriate sections of Chapter 9. The fundamental acceptance criteria for each fault are identified in Chapter 9, Table 9.0-3.

22.3 SAFETY DESIGN APPROACH

The safety design bases of Section 22.2 have led to the identification of a considerable number of design bases for the fuel rods, fuel assemblies, and in-core components; and for the nuclear and thermal hydraulic design of the reactor core. The design bases and acceptance limits used by Westinghouse are described in the Westinghouse Fuel Criteria Evaluation Process and its addendums (Reference 22.4), and the AP1000 Fuel Development Design Closeout Package (Reference 22.5). The fuel rods are designed to operate safely up to the design discharge burnup using the extended burnup design methods described in the Extended Burn-Up Evaluation report (References 22.6, and 22.29).

The fuel rod design for the AP1000 plant considers effects such as fuel density changes, fission gas release, clad creep, and other physical properties which vary with burnup. The integrity of the fuel rods is provided by designing to prevent excessive fuel temperatures; excessive internal rod gas pressures due to fission gas releases; and excessive cladding stresses, strains, and strain fatigue, as discussed in Section 22.5. The fuel rods are designed so that the conservative design bases of the following events envelop the lifetime operating conditions of the fuel. For each DB, the performance of the limiting fuel rod, with appropriate consideration for uncertainties, does not exceed the limits it has specified. The detailed fuel rod design also establishes such parameters as pellet size and density, clad and pellet diametral gap, gas plenum size, and helium pre-pressurisation level.

The design bases for the in-core control components are described in Section 22.5.1.3.

Compliance with the safety design bases described in Section 22.2 is demonstrated for all internally initiated faults within the reactor in the appropriate sections of Chapter 9, where an assessment of the numbers of fuel failures is made under various fault conditions. The mechanisms causing fuel failure are identified and discussed in Section 22.5.

Nonreactor faults, such as fuel failure as a result of a dropped load during refuelling and spent fuel storage, and faults arising from internal hazards also have an important impact on fuel safety. The safe operation of the fuel for nonreactor faults is demonstrated in Sections 9.11 and 9.14, and the impact on fuel safety due to internal hazards, including dropped and load mishandling, is discussed in Section 11.8.

In carrying out the transient calculations described in Chapter 9, bounding limits are defined for all safety-related parameters. These bounding limits represent a conservative assessment of the operating conditions before the fault, the inherent nuclear characteristics of the core during the ensuing transient, and the characteristics of the fuel and noncore systems for nonreactor faults and faults arising from internal hazards. As many of the safety-related parameters assume their extreme values during the first cycle, the design assessment concentrates on operation with the initial fuel loading. Where subsequent operation is expected to produce a more extreme value for any safety-related parameter, the design assessment is based on a representative equilibrium core condition.

Subsequently, each new core configuration after a refuelling operation is analysed before startup, making use of the known core state at the time. It is sufficient to establish that the safety-related parameters are still within the bounding limits and hence the fault analysis is valid.

The application of conservative bounding limits to all safety-related parameters in the assessment of the safety case gives confidence that the limiting values will never be approached during the operational lifetime of the plant. This confidence is augmented by the following:

- The use of validated codes and data to predict the reactor operating conditions
- The use of design and operational limits that are more restrictive than the bounding limits
- Administrative checks to confirm that the predicted values of the safety-related parameters are within the bounding limits
- Tests following refuelling shutdowns and during operation to validate the predicted values of the safety-related parameters
- The specification of operating procedures designed to ensure that the reactor is within operational or safe shutdown limits
- Alarm signals to indicate to the operator that a monitored safety-related parameter is approaching its operational limits
- Automatic reactor trips at settings designed to ensure that monitored safety-related parameters do not exceed their bounding limits

22.4 FUEL FAILURE CRITERIA AND SECONDARY LIMITS

In order to provide confidence that the cladding will not fail, limits are defined for the key parameters which govern clad stresses, fuel melt and other cladding failure modes. These limits are used in the safety analysis to ensure that cladding failure will not occur during frequent or infrequent faults. The parameters are listed below along with their respective limits.

The conditions at which fuel failure is assumed to occur are as follows:

- Departure from nucleate boiling ratio (DNBR) is less than or equal to the 95/95 limit.
- The volume averaged effective stress is equal to or greater than the yield stress.
- Local rod power is equal to or greater than 73.82 kW/m (22.5 kW/ft).
- Local clad stress is equal to or greater than the threshold stress due to pellet-clad interaction (PCI) during power ramps.
- Radial averaged peak fuel enthalpy rise in fast transients is greater than the limits discussed in Section 22.4.5. (Note that the at-power reactivity increase accident (RIA) failure criterion is based on DNBR; if DNB occurs the cladding is assumed to have failed.)

If any of the above criteria are exceeded for any fuel rod, then that rod is assumed to have failed. This is a conservative approach since there is only a small probability of failure at each of these conditions.

The individual criteria are discussed in more detail below.

22.4.1 Departure from Nucleate Boiling Ratio Less than or Equal to 95/95 Limit

The DNBR is the ratio of the heat flux necessary to cause departure from nucleate boiling (DNB) to the heat flux predicted to exist in the fuel rod under consideration. An empirical

DNB correlation, the WRB-2M correlation, has been developed by Westinghouse from a wide range of rod bundle test data. The correlation is used to predict the heat flux required to give DNB as a function of local fluid conditions. The WRB-2M correlation is supplemented with other DNB correlations (e.g. W-3) for conditions (e.g., low pressure) outside the WRB-2M-applicable range in safety analysis. The predicted DNBR is checked with the design limit DNBR value that accounts for uncertainties in the DNB correlation and design parameters. Above the design limit DNBR, there is at least a 95 percent probability at a 95 percent confidence level (95/95) that the limiting fuel rod in the reactor core will not experience DNB.

Additional DNBR margin is maintained when the safety analyses are performed to DNBR limits higher than the 95/95 design limit DNBR values. The difference between the design limit DNBRs and the safety analysis limit DNBRs is the DNBR margin conservatively maintained in the analysis. A portion of this margin is used to offset the rod bow DNBR penalty.

22.4.2 Clad Effective Tensile Stress Equal to or Greater than the Yield Stress

This criterion is used for normal operation and frequent faults in the fuel rod design to ensure that the cladding does not fail under high tensile stresses. It does not preclude some rod failures during normal operation and frequent faults due to minor manufacturing defects.

The possible local and average increases in rod power due to the transient are modelled in the Westinghouse fuel design code (PAD 4.0) (Reference 22.7) and bound all frequent faults. The stress calculation is conservatively made, taking into account the effects of manufacturing tolerances and local stress concentrations.

22.4.3 Local Rod Power Equal to or Greater than 73.82 kW/m

This limit assumes that uranium dioxide fuel melting will occur at above 73.82 kW/m (22.5 kW/ft) and that this will lead to fuel clad failure. Both assumptions are conservative. At a given linear heat rate, fuel temperatures are highest early in life when fuel densification is complete and clad creepdown is negligible. The calculations of fuel temperature in the Westinghouse design code contain sufficient conservatisms to be sure that, even then, fuel melting will not occur at 73.82 kW/m (22.5 kW/ft). Loading pattern variations could place fuel in higher power locations later in life, which could lead to higher actual operating fuel temperatures after the point when fuel densification is complete. However, the fuel temperatures associated with accident scenarios that could lead to reaching the linear hear rate limit of 73.82 kW/m (22.5 kW/ft) will always be lower than the fuel melt temperature.

The current limit of 73.82 kW/m (22.5 kW/ft) is consistent with current operating and fuel manufacturing practices and is consistent with the fuel centreline temperature DB (Ref. 22.74).

22.4.4 Local Clad Stress Equal to or Greater than the Threshold Stress for Pellet-Clad Interaction Failure

PCI is a potential failure mechanism for nuclear fuel. The failure occurs during power increases where the thermal expansion of the fuel pellet is greater than that of the surrounding fuel cladding. This causes stress on the cladding and is impacted further by fission products that can assist in stress corrosion cracking (SCC) of the zirconium cladding. With SCC, the clad may crack at stresses under the yield stress. A failure threshold for PCI is typically defined based on power ramp tests.

A set of methodologies exist for the evaluation of PCI fuel protection during frequent fault scenarios (Reference 22.9). These methodologies will be used to ensure that PCI limits are met during the reload fuel design process and will establish part of the basis for the overpower protection trip setpoints. Based on the evaluations and calculations performed using the Westinghouse PCI model, PCI limits will be maintained without unduly restricting normal plant operation.

22.4.5 Radial Average Peak Fuel Enthalpy in Fast Transients

This criterion covers pellet-cladding mechanical interaction (PCMI) failure of fuel clad in transients where the energy is deposited in times that are short compared with the thermal time constant of the fuel. The PCI criterion in Section 22.4.4 cannot be applied in such transients since it is only valid for times that are long compared with the time constant of the fuel. Thus, the radial average peak fuel enthalpy rise criterion is applicable for transients lasting less than 1 second, such as an RCCA ejection accident.

For transients of the same order as the time constant of the fuel, the radial average peak fuel enthalpy rise criterion is used along with DNB to ensure that conservatism is retained. In these transients, heat loss from the fuel in determining the enthalpy is taken into account. DNB is also conservative for a failure threshold since the clad ballooning that takes place under DNB may not result in failure because of the short duration of the event.

An acceptance criterion has been proposed for the peak fuel enthalpy rise, which is a function of fuel cladding corrosion in terms of the cladding oxide-to-wall-thickness ratio (Reference 22.10). The proposed interim limit is 628 J/g (150 cal/g) from 0 to 4 percent oxide thickness, reducing linearly to 314 J/g (75 cal/g) from 4 to 8 percent oxide thickness, and further reducing linearly to 251 J/g (60 cal/g) from 8 to 20 percent oxide thickness. [

] Any fuel calculated to exceed the interim limit during a simulation of the RIA is assumed to fail due to PCMI.

The limit on peak fuel enthalpy rise has been assessed for AP1000 using a bounding multidimensional rod ejection analysis (Reference 22.10). It has been confirmed that the percentage of fuel that will fail due to PCMI or other causes during the rod ejection event will not exceed the limit for fuel failure assumed in the offsite dose analysis. The bounding multidimensional rod ejection analysis was performed assuming multiple fuel loading patterns, which were developed to intentionally yield high ejected rod worths and peaking factors in high burnup fuel. The analysis includes significant conservatisms to account for potential future changes, and specific values may change in the future as the interim limits are finalised and inevitable enhancements to fuel assembly design and core analysis methodologies occur.

Application of the above criteria defined in Section 22.4 conservatively determines how many fuel rods will fail in a given accident. If the limits are not transgressed, the fuel is not damaged such that its performance in a subsequent accident is impaired. For example, if a fuel rod approaches the DNBR limit but the DNBR remains above the limit, it is not damaged such that it becomes more vulnerable to DNB or any other failure mechanism in later faults.

The one conceivable mechanism in which fuel behaviour in a fault might be influenced by a prior transient in which the failure limits were not transgressed is for the transient to give minor PCI damage without clad failure. This might take the form of partially penetrating cracks or local wall thinning.

As to the first possibility, SCC propagation is very sensitive to the stress in the clad so that a small reduction in stress, below the level at which complete penetration occurs, is sufficient to prevent any crack propagation. The stress threshold for PCI failure defined above is sufficiently conservative to be sure that there will be no appreciable crack propagation below the threshold and hence no effect in subsequent transients.

As to the second possibility, it is believed that local wall thinning (i.e., wall thinning in clad over radial fuel cracks) can accumulate during power cycling to eventually give rise to fuel clad failure. There is no evidence of local wall thinning in PWR clad and calculations indicate that many thousands of severe power cycles are required to produce clad failure in this way, since the local wall thinning at each power increase is extremely small. It is therefore concluded that fault transients that are below the failure limits will have no significant effect on subsequent fault behaviour.

In addition, there are a number of secondary limits for fuel rod failure, which are specified in Table 22-1 together with statements as to the fuel degradation mechanisms avoided by not transgressing the limits. The limits differ between the types of fault because of differences in the fuel environments arising in the faults in terms of the variation and duration of pressures and temperatures occurring during the transients.

The loss-of-coolant accident (LOCA) secondary limits have been derived from the available experimental evidence. The secondary limit for RIA, for example the rod ejection fault, is also justified by the experimental evidence. The limit is in terms of a maximum allowable peak fuel enthalpy rise and peak clad temperature during the fault.

The last category of faults for which a secondary limit has been derived is power cooling mismatch (PCM) faults. A PCM fault occurs when a change in coolant flow rate, pressure, or local rod power produces increasing clad temperatures due to the DNB. The degradation limit given in Table 22-1 is derived from the available experimental data and is imposed to limit the degree to which the clad becomes embrittled.

A limited range of postulated large-break LOCAs can give rise to temperature transients in which the fuel rod cladding may be calculated to reside for many tens of seconds at its most ductile condition. For such events, with the reactor depressurised, the internal gas pressure of the fuel causes the cladding to expand or balloon and possibly rupture. This behaviour, which is termed clad ballooning, leads to a reduction in the size of the coolant passages around those rods so affected. If several adjacent rods were to balloon in a similar manner, the ability to cool that region of the fuel could be brought into question. It is a requirement of the safety case to show that even in the unlikely event of such an accident, the fuel assemblies remain coolable during and after the event.

22.5 FUEL SYSTEM DESIGN

This section has two main sections: 22.5.1 (Design Bases), which details the design criteria of the fuel assembly and fuel rod, and 22.5.2 (Design Evaluation), which shows that the fuel assembly and fuel rod designs do not violate the design criteria.

The fuel rod design bases only apply to the fuel rods during normal operation and frequent faults. The number of fuel rod failures expected as a result of an infrequent fault is given in the appropriate sections of Chapter 9 or supporting topical reports. The fuel assembly design criteria also cover structural integrity under infrequent faults.

The design bases given in this section have been established to meet the safety design bases given in Section 22.2.

22.5.1 Design Bases

The fuel rods are designed for a maximum fuel rod average burnup of 62,000 megawatt days per metric ton of uranium (MWD/MTU) (References 22.6, and 22.29). Note that this is an extension of the original licensed limit of 60,000 MWD/MTU (Reference 22.4).

Integrity of the fuel assembly structure is provided by setting limits on stresses and deformations due to various loads and by preventing the assembly structure from interfering with the functioning of other components. The following three types of loads are considered:

- Nonoperational loads, such as those due to shipping and handling
- Normal and abnormal loads, which are defined for normal operation and frequent faults
- Abnormal loads, which are defined for infrequent faults

The design bases for the in-core control components are described in Section 22.5.1.3.

Fuel performance analyses are performed using the PAD code, as described in Section 22.5.2.

22.5.1.1 Fuel Assembly

As discussed above, the structural integrity of the fuel assemblies is provided by setting design limits on stresses and deformations due to various nonoperational, operational, and accident loads. These limits are applied to the design and evaluation of the fuel assembly components, including top and bottom nozzles, grids, guide thimbles, and thimble joints. The design bases and acceptance limits used by Westinghouse are described in References 22.4 and 22.5.

A summary of the individual criteria and design bases for evaluating the structural integrity are discussed below.

a) Nonoperational

The nonoperational load is a loading of 4G axial (longitudinal) and 6G lateral (transverse) with dimensional stability.

b) Normal Operation and Frequent Faults

For the normal operation condition and frequent faults the fuel assembly component structural design criteria are established for the two primary material categories, austenitic steels and zirconium alloys (including **ZIRLO**). The stress categories and strength theory developed by ASME are used as a general guide. The maximum shear theory (Tresca criterion) for combined stresses is used to determine the stress intensities for the austenitic steel components. The stress intensity is defined as the largest numerical difference between the various principal stresses in a 3-D field. The design stress intensity value, S_m, for austenitic steels and zirconium alloys is given by the lowest of the following:

- One-third of the specified minimum tensile strength or two-thirds of the specified minimum yield strength at room temperature.

- One-third of the tensile strength or 90 percent of the yield strength at temperature but not to exceed two-thirds of the specified minimum yield strength at room temperature.

The stress limits for the austenitic steel components are given below where S_m represents the design stress intensity:

- General primary membrane stress intensity – 1.0 S_m
- Local primary membrane stress intensity – 1.5 S_m
- Primary membrane plus bending stress intensity – 1.5 S_m
- Local primary plus secondary stress intensity – 3.0 S_m

The zirconium alloy structural components, which consist of guide thimbles and fuel tubes, are in turn subdivided into two categories because of material difference and functional requirements. The maximum shear theory is used to evaluate the guide thimble design. For conservative purposes, the zirconium alloy unirradiated properties are used to define the stress limits.

c) Infrequent Accidents and Limiting Faults

Typical worst-case abnormal loads during infrequent faults are represented by seismic and pipe rupture loadings. The design criteria for this category of loadings are as follows:

- Deflections or excessive deformation of components cannot interfere with the ability to insert the control rods or emergency cooling of the fuel rods.

- The fuel assembly structural components stresses under faulted conditions are evaluated primarily using the methods developed by ASME. Since the current analytical methods use linear elastic analysis, the allowable stresses are defined as the smaller value of 2.4 S_m or 0.7S_u (where S_u represents the material ultimate strength) for primary membrane and 3.6 S_m or 1.05S_u for primary membrane plus primary bending. For the austenitic steel fuel assembly components, the stress intensity is defined in accordance with the rules described in the previous section for normal operating conditions. For the zirconium alloy components, the stress intensity limits are set at two-thirds of the material yield strength (S_y) at reactor operating temperature, resulting in the zirconium alloy stress limits being the smaller value of 1.6 S_y or 0.70 material ultimate strength ($S_{u)}$ for primary membrane and 2.4 S_y or 1.05 S_u for primary membrane plus bending. For conservative purposes, the zirconium alloy unirradiated properties are used to define the stress limits.

The design bases for the principal fuel assembly components—top nozzle, bottom nozzle, and grids—are discussed in detail below.

Top Nozzle

The top nozzle assembly design for the AP1000 reactor fuel is a one-piece Westinghouse integral nozzle (WIN) with the removal top nozzle (RTN) type (split insert with lock tube) of joint connection for attachment to the skeleton assembly. The design bases and acceptance limits used by Westinghouse are described in References 22.4 and 22.5.

A summary of the individual criteria and design bases for the top nozzle are discussed below.

a) Requirement for Normal Operation and Frequent Fault Loads

Loadings on the top nozzle that are expected during the life of the fuel assembly shall not result in permanent deformations, loss of structural integrity, or excessive wear of mating components. These loads shall not result in any effects that prevent the continued use of

the fuel assembly for its full design life. The stress intensity for the worst combination of normal operation and frequent fault loads shall not exceed the stress intensity limits determined by the methods used in the mechanical design.

This criterion ensures that the top nozzle does not inelastically deform.

b) Requirement for Infrequent Fault Loads

Loadings on the top nozzle under accidents and other unanticipated events shall not result in deformation that would prevent effective emergency cooling of the fuel or that would prevent safe reactor shutdown. In particular, full insertion of the RCCA shall not be prevented. The stress intensity for the worst combination of infrequent fault loads shall not exceed the stress intensity limits. These limits permit some local yielding of the structure but prevent any major deformation.

c) Requirement for Shipping and Handling Loads

Loadings on the top nozzle during shipping and handling shall not result in permanent deformation, loss of structural integrity, or any other damage that would prevent the top nozzle from meeting all functional requirements for its design life. For a static force equivalent to 4G acting axially or 6G laterally, the stress intensity shall not exceed the limits for frequent fault loadings as determined by the methods used in the mechanical design.

The loadings of 4G axially and 6G laterally are based on fuel shipping and handling experience and have proven to be conservative (Reference 22.11). The stress limits and deformation limits ensure that no significant permanent deformations will result from shipping and handling; the top nozzle will not be damaged and will meet design drawing requirements.

d) Requirement for Cyclic Loads

Cyclic loadings on the top nozzle that are expected during the life of the fuel assembly shall not result in fatigue failure of the top nozzle. The cumulative usage factor shall be less than 1.0 for 1000 cycles of combined maximum range frequent fault loads and 1000 cycles of maximum shipping and handling loads. Normal operation and frequent fault loads are the combined effect of an RCCA scram and hold-down spring force. The maximum shipping and handling loads are calculated by the methods used in the mechanical design. The design fatigue curves for the materials involved are obtained at the maximum operating temperature.

The use of 1000 cycles is based on past practice and has been proven by experience to result in a satisfactory design. The 1000 cycles for design substantially exceeds the actual number of cycles.

e) Requirement for Materials

The materials used in the top nozzle shall provide satisfactory strength and other mechanical properties, corrosion resistance, dimensional stability, and fabrication characteristics for the range of environmental conditions that the top nozzle will experience in service. This includes consideration of temperature, coolant chemistry, fluency, and fabrication processes.

f) Requirement for Coolant Flow

The top nozzle shall maintain adequate distribution of reactor coolant flow from the exit of the flow channels between the fuel rods. It shall accomplish this without an unacceptable pressure loss and it shall ensure that adequate flow is maintained with the unanticipated condition where the upper ends of the fuel rods are in contact with the bottom of the top nozzle because of fuel rod displacement or growth. The uniformity of the flow leaving the coolant channels between the fuel rods and the total pressure loss shall be within the appropriate design allowances for the particular core design.

g) Requirement for Spring Containment

In the event of a single failure of a hold-down spring leaf or a spring fastener, the design of the top nozzle and spring pack shall be such that interference with the motion of core components, especially an RCCA, is unlikely. The top nozzle shall prevent rotation of a broken spring leaf such that it interferes with the movement of a core component, especially an RCCA. The top nozzle shall include design features that maintain all components of the hold-down spring pack in a captured state in the event of breakage of a single spring leaf or spring fastener.

This criterion ensures that control of fuel assembly reactivity, especially rapid RCCA insertion, is not prevented by interference with any component of the hold-down spring pack system such as might occur in the event of a fastener failing. This criterion also ensures that a broken spring leaf does not become a loose part in the core and damage other core or reactor coolant system (RCS) components or obstruct reactor coolant flow to the core. It also provides assurance that core components can be installed and removed without difficulty.

Bottom Nozzle

The DFBN in the AP1000 plant is a slight variation on the current Westinghouse DFBN, which was designed with 4G shipping and handling loads being limiting. The design bases and acceptance limits used by Westinghouse are described in References 22.4 and 22.5.

A summary of the individual criteria and design bases for the bottom nozzle are discussed below.

a) Requirements for Normal Operation and Frequent Fault Loads

The loads on the bottom nozzle that are expected during the life of the fuel assembly shall not result in permanent deformations. These loads shall not result in any effects that prevent continued use of the fuel assembly for its design life. The stress intensity value for the worst combination of normal operation and frequent fault loads shall not exceed the limits below:

- General primary membrane stress intensity – 1.0 S_m
- Local primary membrane stress intensity – 1.5 S_m
- Primary membrane plus bending stress intensity – 1.5 S_m
- Local primary plus secondary stress intensity – 3.0 S_m

This criterion ensures that the fuel assembly bottom nozzle does not deform and that dimensional stability is maintained.

b) Requirements for Infrequent Fault Loads

Loadings on the bottom nozzle under accidents and other unanticipated events shall not result in deformations of the components that would prevent emergency cooling of the fuel or safe reactor shutdown. The stress intensity for the worst combination of infrequent fault loads shall not exceed the limits below.

- Primary membrane stress intensity – 2.4 S_m or 0.70S_u
- Primary membrane plus bending stress intensity – 3.6 S_m or 1.05S_u

These limits permit some local yielding of the structure but prevent any major deformation.

c) Requirements for Shipping and Handling Loads

Loadings expected during shipping and handling shall not result in deformation of or damage to the bottom nozzle that would prevent it from meeting all operating requirements for its design life. For a static force equivalent to 4G acting axially and 6G acting laterally, the stress intensity shall not exceed the limits for normal operation and frequent faults.

In lieu of meeting the stress intensity limits, the permanent deformation for a static load of 4G may be determined by testing. For that testing, the permanent deformation shall not exceed 0.05 mm on top plate flatness and dimensional stability must be shown for interface considerations.

The loading of 4G is based on experience with fuel shipping and handling and has proved to be conservative. The use of stress intensity limits for normal operation and frequent fault loads will ensure that deformations are very small. The deflection limits have been proven by experience and testing to have no effect on the functions of the bottom nozzle.

d) Requirement for Cyclic Loads

Cyclic loadings on the bottom nozzle that are expected during the life of the fuel assembly shall not result in fatigue failure of the bottom nozzle. The cumulative usage factor shall be less than 1.0 for 1000 cycles of combined maximum range normal operation and frequent fault loads and 1000 cycles of maximum shipping and handling loads. Normal operation and frequent fault loads are the combined effect of an RCCA scram, hold-down spring force, and fuel assembly weight.

The use of 1000 cycles is based on past practice and has been proven by experience to result in a satisfactory design. The 1000 cycles for design substantially exceeds the actual number of cycles.

e) Requirements for Materials

The materials used in the bottom nozzle shall provide satisfactory strength and other mechanical properties, corrosion resistance, dimensional stability, and fabrication characteristics for the range of environmental conditions that the bottom nozzle will experience in service. This includes consideration of the temperature, coolant chemistry, fluency, and fabrication processes.

f) Requirement for Coolant Flow

The bottom nozzle shall provide adequate distribution of reactor coolant flow to the entrance of the flow channels between the fuel rods. It shall accomplish this without an unacceptable loss of pressure. When it is included as a feature of the design, the bottom nozzle shall provide a filtering action that minimises particles of debris that would cause fuel clad failure from entering the fuel flow channel. The uniformity of the pressures above the bottom nozzle (across the outlet of the nozzle structure) and the total pressure loss shall be within the appropriate design allowances for the particular core design.

The thermal and hydraulic design of the core is based on limiting the maldistribution and pressure loss to certain allowable values. In general, the two attributes are related such that the distribution is improved as the pressure losses increase; consequently, the design has to be properly balanced to meet this criterion.

g) Debris Effectiveness

The bottom nozzle in combination with the protective grid shall prevent metallic particles that could result in fuel clad failure from passing through the nozzle flow passages.

Experience with operating plants has shown that a high fraction of fuel failures can be traced to debris in the reactor coolant that becomes lodged in the grids and results in eventual perforation of the cladding.

Grids

The design bases and acceptance limits used by Westinghouse are described below (Reference 22.4 and 22.5):

a) Requirement for Positioning

The grid assemblies shall maintain the relative lateral position of fuel rods, guide thimbles, and the instrumentation tube; and provide structural support as part of the fuel assembly skeleton structure. This includes providing features that control the straightness and bowing of the assembly, including the fuel rods, guide thimbles, and instrumentation tube. The physical arrangement of the grid assembly shall satisfy nuclear, thermal and hydraulic, and reactor internals design requirements.

This criterion assures compliance with fuel assembly nuclear and thermal and hydraulic design requirements. It also ensures that RCCAs and core component assemblies can properly engage the guide thimbles, the instrumentation probes can be inserted into the instrumentation tube, and the fuel assembly is compatible with the reactor internals.

b) Requirement for Fuel Rod Support

The grids shall support individual fuel rods in a manner that permits the fuel to achieve its design lifetime. This includes features to avoid flow-induced vibration and clad wear (fretting) that could result in failure of the fuel cladding. Flow-induced fuel rod vibration can lead to fuel rod failures that can limit assembly lifetime and thus must be controlled and limited. Experience has shown that by meeting these support requirements, excessive fretting of the fuel rod clad is prevented.

The fuel assembly design shall prevent the amplitude of self-excited vibration at specific frequencies from exceeding amplitudes that are sufficient to cause fuel rod fretting [

]. In addition, the fuel assembly natural frequency shall not be in resonance with the frequency of the reactor coolant pumps. All grid assembly supports shall be designed to limit fuel rod clad fretting [ ], considering all pertinent factors such as worst-case tolerances, spring relaxation due to irradiation, and clad creepdown.

c) Thermal and Hydraulic Characteristics

The grid assemblies shall provide thermal and hydraulic characteristics that are consistent with the DB requirements. This includes features that determine the pressure loss in the grids and the character of the flow in the channels between the fuel rods. The grids shall maintain the lateral spacing of the fuel rods with respect to each other and with respect to the guide thimbles and the instrumentation tube within acceptable limits. The grid shall not permit or cause rod bowing that exceeds the allowable limits for channel closure for the fuel assembly lifetime. In the case of IFM or protective grids, the rod bowing in any span shall not be increased compared with fuel that does not incorporate those types of grids. The pressure loss coefficient of the grid assemblies shall be acceptable.

The allowable channel spacing deviations are determined by their effect upon a statistical evaluation of as-built channel spacing measurements. Spacing deviations beyond the values assumed in the fuel assembly thermal and hydraulic analyses can reduce the thermal margins. Channel spacing measurements are taken during manufacturing and are also used as a final quality control check to detect changes in fabrication.

Rod bow depends, in part, on the constraints (both lateral and axial) provided by the grids. The selection of incorrect grid parameters can result in increased rod bow under some circumstances.

d) Requirement for Structural Integrity

The grid assemblies shall maintain their structural integrity under design loadings so that the required functions such as the positioning of the fuel, guide thimbles, and the support of the fuel rods can be achieved, in particular as follows:

- For loadings expected during the life of the fuel assembly (normal operation and frequent faults), there shall be no permanent deformations or other effects that would prevent the use of the fuel assembly for its full design life.

- For loadings under accidents and other unanticipated events (infrequent faults), there shall be no deformation or other effects that would prevent effective emergency cooling of the fuel or safe reactor shutdown.

- For loadings during shipping and handling, there shall be no permanent deformations or other effects that would prevent the use of the fuel assembly for its full design life.

No normal operation event or frequent faults result in significant loads on the grid assembly. Accordingly, the mechanical strength requirements of the grid assembly are controlled by dynamic loadings resulting from infrequent faults, and no specific criteria are required for normal operation or frequent fault loads.

For infrequent faults, the grid assembly shall withstand the combined effects of the maximum design basis earthquake and the most adverse LOCA. To meet this criterion,

the following detailed criteria shall be met to confirm grid performance under infrequent fault loads:

- The grid deformation due to the most limiting horizontal impact load for infrequent faults shall not result in unacceptable fuel rod flow channel closure, that is, closure that could result in clad temperatures above those of a coolable geometry or unacceptable thimble tube deformation, which could impede control rod motion.

- The requirement may be satisfied by demonstrating that the calculated infrequent fault impact loads shall not exceed the lower 95 percent confidence limit calculated from the true mean grid crush strength at operating temperature, where the crush strength is defined as the dynamic impact load at which buckling just begins as determined by tests.

- The requirement may also be satisfied by showing that the calculated infrequent fault impact loads do not affect the coolable geometry of the grid and insertion of the control rods is not impacted for infrequent faults, excluding large-break LOCA events.

The mechanical strength requirements of grids are dictated by dynamic loadings resulting from infrequent faults. For an infrequent fault, the reactor must be able to be brought to a safe state with only a small fraction of fuel rods damaged, although sufficient damage might occur to preclude resumption of operation without considerable outage time. For an infrequent fault the reactor must also be able to be brought to a safe state and the core kept subcritical with acceptable heat transfer geometry.

It is not practical to apply stress limits to determine the stresses because of the complexity of the analysis. Since irradiation enhances the mechanical strength of **ZIRLO** (Reference 22.12) and the grid will be operating in essentially the elastic range with the above acceptance limit, it is conservative to use test results from unirradiated grids to establish the buckling strength of the grid assembly. The grids should be tested at operating temperature, however, to account for the adverse effect of temperature on grid strength.

It should be noted that an additional assessment was carried out to assess the structural and IFM grid response to the depressurisation of the primary circuit due to a DEG break of the RCS cold leg. This assessment, documented in Reference 22.97, concluded that the fuel assemblies will not preclude the reactor from being able to be brought to safe state or limit flow through the inboard fuel assemblies.

e) Requirement for Handling of Fuel Assemblies

The configuration of the grid assemblies shall be such that handling of the fuel assemblies, including insertion and removal from the core and the handling in and out of transfer, shipping, or storage facilities, does not result in damage to the fuel assembly itself, to neighbouring fuel assemblies, or to other reactor components and plant equipment.

The grid assembly peripheral dimensions shall be consistent with the overall fuel assembly envelope to ensure that the fuel assembly can be installed in the required shipping containers, fuel storage racks, fuel transfer mechanisms, fuel elevators, and spent fuel shipping casks. Also, the nominal cold grid-to-grid clearance in core shall be consistent with LOCA blowdown impact load analyses assumptions. [

] The grid assembly shall have suitable lead-in tabs and vanes on the outer straps to prevent fuel assembly hangup during insertion or removal operations considering possible fuel assembly distortion due to operation.

Compliance with this criterion ensures that fuel assembly interface compatibility requirements are met, and that the grid-to-grid spacing is sufficient for fuel handling operations and is not so large that it unduly increases LOCA blowdown impact loads.

f) Requirement for Materials

The materials used in the grid assemblies shall provide satisfactory strength and other mechanical properties, corrosion resistance, nuclear properties, dimensional stability, and fabrication characteristics for the range of environmental conditions that the grid assemblies will experience in service. This includes consideration of temperature, coolant chemistry, fluence, and fabrication processes.

Irradiation changes the physical properties of the grid material throughout life. The grid design must account for these changes to ensure that the grid physical requirements are met throughout the fuel lifetime. Grid corrosion must be limited to ensure that the grid maintains sufficient strength and grid growth does not impede fuel assembly handling operations to meet the design requirements throughout its lifetime.

Assembly Bow

The AP1000 reactor fuel assemblies shall be built with a high degree of resistance to assembly bowing, thus minimising or eliminating the potential for any impact on safety margins. This is accomplished through changes in the guide tube wall and dashpot mechanical design to increase lateral stiffness, selection of skeleton materials that minimise fuel assembly growth, and optimisation of the top nozzle hold-down spring forces. The relative resistance of the design to assembly bow is evaluated through comparison with existing Westinghouse fuel designs with known assembly bow characteristics.

22.5.1.2 Fuel Rod

Fuel Material

The fuel material is enriched uranium in the form of cylindrical pellets of uranium dioxide. The design bases and acceptance limits used by Westinghouse are described in References 22.4 and 22.5.

A summary of the individual criteria and design bases for the fuel material are discussed below.

a) Fuel Centreline Temperature

The centre temperature of the hottest pellet is below the melting temperature of the uranium dioxide. The melting temperature of unirradiated uranium dioxide, 2804.44°C (5080°F), decreases by 32.22°C (58°F) per 10,000 MWD/MTU (Reference 22.13).

The nominal design density of the fuel is approximately 95.5 percent of the theoretical density. This limit is discussed further in Section 3.7.2.1.1 of Reference 22.5.

b) Fuel Dimensional Changes

Once the fuel pellet and cladding are in contact, the fission product swelling of the fuel must not cause clad failure. [

]

[

] The criteria for internal fuel rod pressure and gap reopening are discussed in section 3.7.2.1.2 of Reference 22.5.

c) Fuel Chemical Properties

Due to the potential for adverse chemical reactions between the fuel pellet and the cladding the moisture content in the fuel pellets is controlled to minimise the potential for hydride induced failures of the cladding. The moisture content is limited as part of the total hydrogen requirement defined in the pellet production specification, Reference 22.101.

d) Zirconium Diboride Material Properties

There are manufacturing specifications on variability of the rod-by-rod ZrB_2 content within a region and the region average ZrB_2 loading. These specifications address total core reactivity and the impact on local radial power distribution changes. Further details on ZrB_2 loading specifications are provided in Reference 22.92.

Cladding

The cladding is made of **ZIRLO**, which combines neutron economy (low-absorption cross-section); high corrosion resistance to coolant, fuel, and fission products; and high strength and ductility at operating temperatures. **ZIRLO** is an advanced zirconium-based alloy that has the same or similar properties and advantages as Zircaloy-4 and was developed to support extended fuel burnup. A discussion of the chemical and mechanical properties of the **ZIRLO** cladding material and a comparison with Zircaloy-4 is provided in Reference 22.3.

The design bases and acceptance limits used by Westinghouse are described in References 22.4 and 22.5. A summary of the individual criteria and design bases for the fuel cladding is presented below.

a) Clad Stress

The volume average effective stress, considering interference due to uniform cylindrical pellet-clad contact caused by pellet thermal expansion, pellet swelling, uniform clad creep, and pressure differences, must be less than the 0.2 percent offset yield stress with due consideration of temperature and irradiation effects for normal operation and frequent faults. While the clad has some capability for accommodating plastic strain, the yield stress has been accepted as a conservative design limit. The stress calculations are conservative and take into account the effects of temperature and irradiation on the yield stress.

Excessive clad stress can arise because of local power increases of rapid rate such that the clad creep cannot accommodate the pellet thermal expansion. Limiting effective stress levels to the yield strength of the material is a well-accepted and conservative design practice since some ductility is available following yielding. This limit is discussed further in section 3.7.2.1.4 of Reference 22.5.

b) Clad Strain (Transient)

The acceptance limit for fuel clad strain during frequent faults is that the total tensile strain due to uniform cylindrical pellet thermal expansion should be less than 1 percent from the pre-transient value.

The intent of this criterion is to minimise the potential for clad failure due to excessive clad straining. The criterion addresses slow strain rate mechanisms where the clad effective stress never reaches the yield strength of the material because of stress relaxation. Fuel swelling can result in small clad strains (<1 percent) for expected discharge burnups, but the associated clad stresses are very low because of clad creep (thermal and irradiation-induced creep). Furthermore, the 1 percent strain criterion is extremely conservative for fuel-swelling-driven clad strain because the strain rate associated with solid fission products swelling is very slow. In-pile experiments have shown that the cladding exhibits "super-plasticity" at slow strain rates during neutron irradiation. In design, this criterion is currently interpreted in terms of a uniform circumferential strain. This limit is discussed further in section 3.7.2.1.5 of Reference 22.5.

c) Clad Strain (Steady-State)

For steady-state operation, the total plastic tensile creep strain due to uniform clad creep and cylindrical fuel pellet expansion associated with fuel swelling and thermal expansion is less than 1 percent from the unirradiated condition.

The intent of this criterion is to minimise the potential for clad failure due to excessive clad straining. The criterion addresses slow strain rate mechanisms where the clad effective stress never reaches the yield strength of the material because of stress relaxation. The present 1 percent limit on circumferential strain is based on the results of tensile and high strain rate biaxial tests on irradiated tubing as discussed in item (b) above. In design, this criterion is currently interpreted in terms of a uniform circumferential strain. This limit is discussed further in section 3.7.2.1.6 of Reference 22.5.

d) Clad Corrosion

An oxide thickness limit established to ensure the cladding integrity during normal operation and anticipated operational occurrences (AOOs).

A hydrogen pickup criterion is required to limit loss of ductility due to hydrogen embrittlement, which occurs as a portion of the free hydrogen is absorbed into the base metal as zirconium hydride precipitates or platelets. This limit precludes a condition of low-temperature embrittlement (Reference 22.89). Further details on clad corrosion are provided in section 3.7.2.1.7 of Reference 22.5.

e) Clad Flattening

The fuel rod design shall preclude clad flattening during the projected lifetime of the fuel. This criterion was established to prevent the long-term creep collapse of the fuel cladding into axial gaps that can form within the fuel column. This criterion is discussed further in section 3.7.2.1.8 of Reference 22.5.

f) Clad Fatigue

The fatigue usage factor shall be less than 1.0: that is, for a given strain range, the number of strain fatigue cycles is less than required for failure, considering a minimum safety factor of 2 on the stress amplitude or a minimum safety factor of 20 on the number of cycles, whichever is more conservative.

The concern of this criterion is the accumulated effect of short-term, cyclic cladding stress and strain that result primarily from daily load follow operation. The accumulated effects of cyclic strains associated with normal plant shutdowns and returns to full power are also considered. This criterion is discussed further in section 3.7.2.1.9 of Reference 22.5.

g) Clad Wall Thickness and Ovality

The clad wall thickness variations and initial ovality affect fuel rod bow, flattening, and clad stresses and therefore must be controlled to preclude incipient clad collapse during normal operation. The maximum-allowed clad wall thickness variation around the circumference at any location and the maximum allowed ovality shall be acceptable from a fuel performance standpoint. Limits on clad wall thickness and ovality are discussed further in section 3.7.2.3.1 of Reference 22.5.

h) Clad Scratch Limits

Scratches on the outside diameter of the clad shall be limited to depths that do not significantly affect clad integrity during the life of the fuel rod. [

]

Excessively deep or wide scratches could result in clad failures before fuel rod design life is reached. The scratch limits of the criterion have been found to be acceptable based on rod performance, fracture mechanics, and finite element analyses: that is, scratches of the size allowed do not degrade fuel rod performance. This limit is discussed further in section 3.7.2.3.2 of Reference 22.5.

i) Rod Bowing

The design of the fuel assembly shall not increase the rod bow penalty above acceptable limits. Further details on this criterion are provided in sections 3.4.1.2 and 3.4.2.3.2 of Reference 22.5. The effects of rod bow on DNB are discussed further in section 3.9.2.6 of Reference 22.5.

Fuel Rod

A summary of the individual criteria and design bases for the fuel rod are discussed below. These criteria are discussed in more detail in Reference 22.5.

a) Fuel Rod Internal Gas Pressure (Departure from Nucleate Boiling Propagation)

The fuel rod internal pressure will be limited to a value below that which could cause extensive propagation of DNB due to clad ballooning during transients. This limit is discussed further in section 3.7.2.1.3 of Reference 22.5.

b) Fuel Rod Internal Gas Pressure (Gap Reopening)

The fuel rod internal pressure will be limited to a value below that which could cause the fuel pellet-clad gap to increase because of outward cladding creep during steady-state operation. The limits and supporting analysis are provided in Reference 22.5. Restricting the fuel-clad gap from increasing will prevent accelerated fission gas release at high burnup and preclude high burnup fuel from becoming limiting from a LOCA viewpoint. This limit is discussed further in section 3.7.2.1.2 of Reference 22.5.

c) Fuel Axial Growth

The overall length of the fuel rod (over the end plugs) and the space between the nozzles (plate-to-plate) shall be such that the rod does not contact both nozzles. This includes the effects of fuel growth, guide tube growth and creep, and thermal expansion of the components.

This criterion should consider the effects of fuel growth, guide tube and instrumentation tube growth and creep, and thermal expansion of those members. To prevent overstressing guide thimble tubes and/or guide thimble tube-to-nozzle joints, excessive interference should not occur. This limit is discussed further in section 3.7.2.1.10 of Reference 22.5.

d) End Plug Weld Integrity

The fuel rod end plug shall maintain its integrity during normal operation and frequent faults and shall not contribute to any additional fuel failures above those already considered for infrequent faults.

The intent of this criterion is to ensure that fuel rod failures will not occur due to the tensile pressure differential loads that can exist across the weld. The current inspection limits for the end plug weld allows for the existence of small defects within the weld and under maximum tensile pressure differential, failure of the weld should not occur. This criterion is discussed further in section 3.7.2.1.12 of Reference 22.5.

e) Fuel Rod Straightness

The clad and fuel rod shall be straight within the limits defined in Reference 22.92.

Controlling fuel rod straightness ensures that fuel rod channel spacing is adequate throughout service life. This limit is discussed further in section 3.7.2.2.1 of Reference 22.5.

f) Hold-Down Spring Radial Support of Clad

The fuel rod in the plenum region shall not collapse during normal operating conditions for the fuel rod design lifetime.

This criterion precludes fuel rod collapse and associated failure in the plenum region of the fuel rod where the cladding is not supported by the presence of the fuel pellet stack. This criterion is discussed further in section 3.7.2.3.3 of Reference 22.5.

g) Axial Location of Fuel Pellet Stack

Prior to irradiation, the spring shall provide a minimum hold-down force on the fuel pellet stack of four times the nominal weight of the fuel stack.

Experience has shown that designing the hold-down force to meet this criterion will prevent any significant fuel pellet motion and chipping during shipping and handling. In addition, to ensure that the shipping loads do not exceed the hold-down force, accelerometers are mounted in the shipping package during transport. After the fuel is installed in the core and operation begins, a high spring force is no longer required because in-plant handling loads are expected to be low and because mechanical interaction between the pellet and cladding minimises the potential for pellet stack motion. This criterion is discussed further in section 3.7.2.5 of Reference 22.5.

h) Fuel Rod Outer Diameter at Weld

The maximum outer diameter of the fuel rod at the weld shall not cause the grid cell size to exceed the maximum allowable size for the particular grid design.

If the fuel rod maximum outer diameter at the weld significantly exceeds the clad outer diameter, it could result in unacceptable plastic setting of grid springs as the weld passes through a grid cell during loading of fuel rods into the skeleton. This condition could cause spring forces to be below the values established to avoid unacceptable fretting damage to the clad in service. This limit is discussed further in section 3.7.2.6.1 of Reference 22.5.

i) Standoff Tube Design

Fuel rod gases shall have access to communicate with the tube internal volume throughout life to provide greater fuel rod internal pressure margin. In addition, the standoff tube design shall prevent fuel pellets or large pellet fragments from entering the lower plenum space to maintain fuel stack integrity. This criterion is discussed further in section 3.7.2.7 of Reference 22.5.

j) Potentially Damaging Temperature Effects during Transients

Thermal expansion of the fuel rods should be considered in the fuel design so that the loads imposed on the fuel rods during a thermal transient will not result in unacceptable fuel performance or damage to the fuel. Further details on the criteria which limit the potential for stress due to thermal expansion are provided in sections 3.7.2.1.1, 3.7.2.1.4, 3.7.2.1.5, and 3.7.2.1.6 of Reference 22.5.

k) Fuel Element Burnout and Potential Energy Release

The AP1000 reactor core should be protected from DNB over the full range of possible operating conditions. Further details on the criteria and bases which provide controls to ensure the core is protected against DNB are provided in section 3.9.2 of Reference 22.5.

l) Fuel/Cladding Mechanical Interaction

One factor in fuel element duty is potential mechanical interaction of the fuel and clad. This fuel/clad interaction produces cyclic stresses and strains in the clad, which in turn reduce clad life. The reduction of fuel/clad interaction is therefore a design goal. This criterion is discussed further in section 3.7.2.1.9 of Reference 22.5.

22.5.1.3 In-Core Control Components

The in-core control components are subdivided into permanent and temporary devices. The permanent components are the RCCAs, GRCAs, thimble plugs, and secondary neutron source assemblies. The temporary components are the primary neutron source assemblies (normally used only in the initial core) and the BA assemblies. Note that for some reloads, the use of BA assemblies may be necessary for power distribution control and/or to achieve an acceptable moderator temperature coefficient throughout core life. Materials for both permanent and temporary devices are selected for the following features:

- Compatibility in the PWR environment
- Adequate mechanical properties at room and operating temperatures
- Resistance to adverse property changes in a radioactive environment
- Compatibility with interfacing components

The design bases and acceptance limits used by Westinghouse are described in References 22.4 and 22.5.

A summary of the individual criteria and design bases for evaluating the structural integrity are discussed below.

a) Control Rods

For normal operation and frequent faults, the stress categories and strength theory developed by ASME are used as a general guide in the design of the RCCA and GRCA structural parts in addition to absorber cladding.

The design bases are as follows:

- External pressure equal to the RCS operating pressure with appropriate allowance for overpressure transients
- Wear allowance equivalent to 1000 reactor trips
- Bending of the rod due to a misalignment in the guide thimble
- Forces imposed on the rods during rod drop
- Loads imposed by the accelerations of the CRDM
- Radiation exposure during maximum core life
- The absorber material temperature shall not exceed its melting temperature (790°C (1454°F) for silver-indium-cadmium (Reference 22.13), and 3380°C (6116°F) for tungsten [Reference 22.36]). Confirmation that the RCCA silver-indium-cadmium absorber material will not exceed the melting temperature is provided in the analysis

contained in References 22.102 and 22.103. The supporting analysis for the GRCA tungsten absorber is contained in References 22.104, 22.105, and 22.5.

- Temperature effects at operating conditions

b) Burnable Absorber Rods

For normal operation and frequent faults, the stress categories and strength theory developed by ASME are used as a general guide in the design of the BA cladding. For abnormal loads during infrequent faults, code stresses are not considered limiting. Failures of the BA rods during these conditions must not interfere with reactor shutdown or emergency cooling of the fuel rods. The BA material is non-structural. The structural elements of the BA rod are designed to maintain the absorber geometry even if the absorber material is fractured.

To reduce the dissolved boron requirement for control of excess reactivity, WABA rods have been incorporated in the core design. The WABA material is boron carbide contained in an alumina matrix. Thermal-physical and gas release properties of alumina-boron carbide are described in Westinghouse technical reports (References 22.13 and 22.15). Discrete BA rods are designed so that the absorber temperature does not exceed 649°C (1200°F) during normal operation or an overpower transient. The units maximum temperature helium gas release in a discrete BA rod will not exceed 30 percent of theoretical (Reference 22.15).

c) Neutron Source Rods

The neutron source rods are designed to withstand the following:

- The external pressure equal to RCS operating pressure with appropriate allowance for overpressure transients

- An internal pressure equal to the pressure generated by released gases over the source rod life

22.5.2 Design Evaluation

The fuel assemblies, fuel rods, and in-core control components are designed to satisfy the performance and safety criteria and the mechanical design bases described in Section 22.5.1 and Reference 22.4.

The PAD code is used to confirm the performance of the fuel. The design bases and acceptance limits used by Westinghouse are described in References 22.4 and 22.5. Fuel rod and assembly models used for the performance evaluations are documented and maintained under the Westinghouse Software Engineering Methodology and Quality Assurance process. This includes processes used to benchmark new data against the models used within the PAD code. Material properties used in the design evaluations are given in Reference 22.3.

With the development of PAD 5 a new topical report was created which consolidates the methodology, analysis, and results into one comprehensive report. While the AP1000 plant currently uses the PAD 4 model, it is anticipated that the transition will be made to PAD 5 for UK AP1000 plants. At that time the PAD 5 topical report, WCAP-17642-P, (Ref. 22.94) will be the reference for all relevant analysis and results using the PAD code.

22.5.2.1 Fuel Assembly

The fuel assembly component stress levels are limited by the design. For example, stresses in the fuel rod due to thermal expansion and **ZIRLO** irradiation growth are limited by the relative motion of the rod as it slips over the grid spring and dimple surfaces. Clearances between the fuel rod ends and nozzles are provided so that **ZIRLO** irradiation growth does not result in rod end interference. Stresses in the fuel assembly caused by tripping of the RCCA have little influence on fatigue usage margin because of the small number of events during the life of an assembly. Assembly components and prototype fuel assemblies made from production parts have been subjected to structural tests to verify that the DB requirements are met.

The fuel assembly design loads for shipping have been established at 4G axial and 6G lateral. Accelerometers are permanently placed in the shipping cask to monitor and detect fuel assembly accelerations that would exceed the criteria. Experience indicates that loads exceeding the allowable limits rarely occur. Exceeding the limits requires reinspection of the fuel assembly for damage. Tests on various fuel assembly components, such as the grid assembly, sleeves, inserts, and structure joints, have been performed to confirm that the shipping design limits do not impair fuel assembly function.

To demonstrate that the fuel assemblies will maintain a geometry capable of being cooled under the worst-case accident infrequent fault, a plant-specific or bounding seismic analysis is performed. The fuel assembly response resulting from safe shutdown earthquake condition is analysed using time-history numerical techniques. The vessel motion for this type of event primarily causes lateral loads on the reactor core. Consequently, the methodology and analytical procedures described in References 22.16, 22.17, and 22.18 are used to assess the fuel assembly deflections and impact forces.

The motions of the reactor internals upper and lower core plates and the core barrel at the upper core plate elevation, which are simultaneously applied to simulate the reactor core input motion, are obtained from the time-history analysis of the reactor vessel and internals. The fuel assembly response, namely the displacements and impact forces, is obtained with the reactor core model. Similar dynamic analyses of the core were performed using reactor internals motions indicative of the postulated pipe rupture. Scenarios regarding breaches in the pressure boundary have been investigated to determine the most limiting structural loads for the fuel assembly. The application of leak before break (LBB) limits the size of the pipe rupture loads for the fuel assembly. The pipe rupture used in the fuel assembly analysis is the largest pipe connected to the RCS that does not satisfy the LBB criteria. Mechanistic pipe break is discussed in Appendices 20D and 20E.

The maximum grid impact force obtained from seismic analyses is less than the allowable grid strength. Westinghouse has demonstrated that a simultaneous safe shutdown earthquake and pipe rupture event is highly unlikely. The fatigue cycles, crack initiation, and crack growth due to normal operating and seismic events will not realistically lead to a pipe rupture (Reference 22.19).

Based on the deterministic fracture mechanics evaluation of small flaws in piping components, Westinghouse has demonstrated that the dynamic effects of a large pipe rupture in the primary coolant piping system for the AP1000 design does not have to be considered.

A DB for the piping design in the AP1000 plant is that the reactor coolant loop and surge lines will satisfy the LBB criteria for mechanistic pipe break. In addition, the piping connected to the RCS that is 152.4-mm (6 inches) nominal diameter or larger is evaluated for LBB. The result of a pipe leakage event consistent with the mechanistic pipe break evaluation

would be to impose insignificant asymmetric loadings on the reactor core system. Thus, fuel assembly grid loads due to large pipe ruptures are unrealistic and, as such, are not included in the analysis.

The pressure boundary integrity for numerous branch lines is analysed to determine the most limiting break of a line not qualified for LBB for the dynamic loading of the reactor core. Grid loads resulting from a combined seismic and pipe rupture event do not cause unacceptable grid deformation as to preclude a core coolable geometry.

The stresses induced in the various fuel assembly nongrid components are assessed based on the most limiting seismic condition. The fuel assembly axial forces resulting from the hold-down spring load together with its own weight distribution are the primary sources of the stresses in the guide thimbles and fuel assembly nozzles. The fuel rod accident-induced stresses, which are generally very small, are caused by bending due to the fuel assembly deflections during a seismic event. The seismic-induced stresses are compared with the allowable stress limits for the fuel assembly major components. The component stresses, which include normal operating stresses, are below the established allowable limits. Consequently, the structural designs of the fuel assembly components are acceptable for the DB accident conditions for the AP1000 plant.

Localised yielding and slight deformation in some fuel assembly components are allowed to occur during an infrequent fault. The maximum permanent deflection, or deformation, does not result in any violation of the functional requirements of the fuel assembly. In the early phase of the transient following the coolant circuit break, the high axial loads (which could be generated by the difference in thermal expansion between fuel clad and thimbles) are relieved by slippage of the fuel rods through the grids. The relatively low drag force restraint on the fuel rods will induce only minor thermal bowing, which is insufficient to close the fuel rod to thimble tube gap.

It should be noted that an additional assessment was carried out to assess the structural and IFM grid response to the depressurisation of the primary circuit due to a DEG break of the RCS cold leg. This assessment, documented in Reference 22.97, concluded that the fuel assemblies will not preclude the reactor from being able to be brought to safe state or limit flow through the inboard fuel assemblies.

Westinghouse has developed and evolved the RFA design, adding features such as thicker guide tube walls, a stronger guide tube dashpot, optimised top nozzle hold-down springs, and the low-growth **ZIRLO** alloy in order to improve assembly stiffness characteristics and resistance to assembly bow and incomplete rod insertion. With the continued deployment of RFA, the occurrence of incomplete control rod insertion upon reactor trip has been eliminated and the occurrence of grid damage during fuel handling significantly reduced.

In the event that AP1000 plant fuel assembly bow measurements are inconsistent with RFA performance expectations, Westinghouse has developed detailed mechanical and nuclear methods for the modelling the effects of assembly bow on the core power distribution (Reference 22.20). Any potential peaking factor penalties would be expected to be small and available margins could be reallocated to accommodate these small penalties without affecting the conclusions of the AP1000 plant safety case.

Top Nozzle

A summary of the evaluation of the individual criteria and design bases for the top nozzle are discussed below.

a) Requirement for Normal Operation and Frequent Faults

Shipping and handling loads are more limiting than normal operation and frequent faults for the top nozzle, as an axial load equal to four times the weight of the fuel assembly plus an RCCA will bound all loads imposed on the top nozzle by those events. A verification test was performed in which the production nozzles were axially loaded (at room temperature) in both tension and compression to loads significantly greater than would be calculated for normal operation and frequent faults.

The resulting deformation of the adapter plate was then characterised and evaluated. The test results concluded that when the top nozzle was tested in tension (the largest load applied during testing) to represent handling conditions, [ ]. When the top nozzle was tested in compression to represent shipping conditions, [ ].

Along with these two tests, a test with a vertical load imposed by RCCA impact on the adaptor plate was performed. The adaptor plate was characterised after the test and there was no permanent displacement. After each test, the ability to remove and reinstall the top nozzle was not impaired and there was no difficulty installing the lock tubes in the inserts.

b) Requirement for Infrequent Faults

Shipping and handling loads are more limiting than Infrequent faults for the top nozzle, as an axial load equal to four times the weight of the fuel assembly plus an RCCA will bound all loads imposed on the top nozzle by those events. A verification test was performed in which production nozzles were axially loaded (at room temperature) in both tension and compression to loads significantly greater than would be calculated for infrequent faults, with results the same as those described in item a) above.

c) Requirement for Shipping and Handling

A verification test was performed in which production nozzles were axially loaded (at room temperature) in both tension and compression to loads greater than four times the weight of the fuel assembly plus an RCCA. The resulting deformation of the adapter plate was then characterised and evaluated. The test results concluded that when the top nozzle was tested in tension to represent handling conditions, [ ]. When the top nozzle was tested in compression to represent shipping conditions, [ ]. After each test, the ability to remove and reinstall the top nozzle was not impaired and there was no difficulty installing the lock tubes in the inserts. Thus, the loadings on the top nozzle during shipping and handling do not result in permanent deformation, loss of structural integrity, or any other damage that would prevent it from meeting all functional requirements during its design life.

d) Requirement for Cyclic Loads

Analyses performed on top nozzles representative of the AP1000 design have consistently yielded fatigue usage factors two orders of magnitude or more less than the ASME Code limit of 1.0.

e) Requirement for Materials

Materials used in the WIN design for the AP1000 plant have been used successfully in previous Westinghouse top nozzles. Calculations have been performed based on measurements reported in the literature to ensure that casting cracks smaller than those that can be detected by the nondestructive examination (NDE) programme will not propagate due to inherent notch sensitivity, SCC, or radiation- and corrosion-assisted fatigue (Reference 22.22).

f) Requirement for Coolant Flow

The top nozzle adaptor plate has a new flow pattern versus the 17×17 XL top nozzle, which has the typical flow pattern used in previous Westinghouse top nozzle designs. The flow pattern in the XL top nozzle consists of flow slots arranged in one direction, thus providing half-symmetry of the flow pattern. The new flow pattern has a quadrant symmetric pattern, thus providing quarter-symmetry of the flow pattern. As such, the top nozzle will provide a more uniform flow distribution in the fuel rod coolant channels from quadrant to quadrant than the XL top nozzle.

g) Requirement for Spring Containment

Confirmatory testing has demonstrated that if top, middle two, or bottom leaf springs are severed at the root bend, they remain captured in the top nozzle and have no range of motion (Reference 22.23). It should be noted that the lower bend for the bottom spring is constrained by the WIN pad gussets. For the extreme case where all four leaves were severed, the test showed a range of motion comparable to that observed in the previous WIN designs. This range of motion will not obstruct the movement of a core component.

Bottom Nozzle

A summary of the evaluation of the individual criteria and design bases for the bottom nozzle are discussed below.

a) Requirements for Normal Operation and Frequent Fault Loads

Design loads for normal operation and frequent faults include fuel assembly weight, hold-down spring force, and scram loads. These loads are bounded by the 4G shipping and handling loads. The evaluation of the shipping and handling loads described below shows that these loads are acceptable.

b) Requirements for Infrequent Fault Loads

The maximum axial loading on the bottom nozzle for infrequent faults is the sum of the vertical seismic (inertia) load, the LOCA load, and the fuel assembly and RCCA weight, plus the (hot) hold-down spring force. The resulting stresses are well below their corresponding allowable limits (Reference 22.5).

c) Requirements for Shipping and Handling Loads

The AP1000 plant fuel assembly [
]; therefore, [
]. The resulting primary membrane stress intensity and primary membrane plus bending stress intensity are well below the corresponding design limits for this criterion (Reference 22.5).

d) Requirement for Cyclic Loads

Previous analyses have consistently shown that the cumulative fatigue usage factor for bottom nozzles [ ] versus a limit of 1.0. This indicates that bottom nozzles can easily withstand the combined transients described without fatigue failure. Since the AP1000 design of the bottom nozzle is essentially unchanged from previous bottom nozzle designs and the cyclical loadings are also similar, the previous analysis results are used to show that it meets the requirements for cyclic loads.

e) Requirements for Materials

The AP1000 design incorporates the standard casting and adaptor plate material used in earlier fuel assembly designs and so the bottom nozzle is unchanged with respect to material requirements. The operating conditions and operational experience and testing performed on other Westinghouse fuel assembly designs shows that the materials will maintain their physical properties and other functional requirements over the full core lifetime.

f) Requirement for Coolant Flow

The bottom nozzle design is a combination of the low-profile type used in fuel assemblies for 3.65-m (12 foot) high cores and the tall leg type used in fuel assemblies for current (XL) 4.27-m (14 foot) high cores. One feature that is common to all three bottom nozzle designs is the flow hole design (bore diameter and hole pattern). This similarity minimises the pressure distribution difference between the nozzle designs, with the AP1000 plant pressure distribution bounded by the other two nozzle types.

In thermal design space, the maldistribution and pressure loss for the AP1000 design are within the experience base of current Westinghouse designs. Therefore, the existing thermal design methodology for Westinghouse designs can be applied to the AP1000 plant.

g) Debris Effectiveness

Debris filtering tests indicate that a typical DFBN, similar to the bottom nozzle in the AP1000 design, stops more than 70 percent of the debris, by weight, compared to a non-DBFN. In combination with the protective grid, nearly all metallic debris that could induce fuel rod failures is trapped by the nozzle.

Grids

A summary of the evaluation of the individual criteria and design bases for the grids are discussed below.

a) Requirement for Positioning

The 17×17 mid and IFM grid assemblies have drawing specifications describing features affecting this criterion that are consistent with a 17×17 RFA design. The top and bottom grid assemblies used on the AP1000 plant fuel assembly both have the same cell pitch, thimble cell array, and instrument cell position (centre location) as existing Westinghouse 17×17 grid designs.

b) Requirement for Fuel Rod Support

An unbalanced mixing vane pattern is the primary mechanism for self-excited fuel assembly vibration. The RFA and IFM grids include the standard RFA symmetric, balanced vane pattern, eliminating this known mechanism for fuel assembly vibration. Testing of the symmetric, balanced mixing vane pattern confirms that these assemblies are not subject to self-excited resonant vibration (Reference 22.5).

Most of the excitation energy from the pumps that could contribute to fuel vibration occurs at the vane passing frequencies. [

] At hot end-of-life (EOL) conditions, the fuel frequencies will be lower. Thus, the fuel assembly frequencies are well below the lowest pump frequencies and there is no direct correspondence between any of these fuel assembly modal and pump impellor vane passing frequencies.

There has been considerable post-irradiation examination (PIE) of the 17x17 RFA-type fuel assembly designs that demonstrates very good fretting performance [ ]. For the AP1000 design, test data shows significantly improved fuel rod cladding fretting performance relative to current RFA-type designs with sufficient margin to meet [ ] fretting wear criterion.

c) Thermal and Hydraulic Characteristics

The grid designs incorporate into the grid drawings the same tolerances and specifications as the drawings for current Westinghouse 17x17 standard grids to control the channel spacing. Thus, the as-built deviations of the fuel rods from nominal spacing will be consistent with that of current Westinghouse grid designs.

With four IFMs and an increased dimple-to-dimple span within the mid grid, fuel assembly span lengths are reduced in comparison with 17x17 XL RFA assemblies. The AP1000 plant top grid design incorporates the reduced rod bow spring design, which has a reduced grid spring force on the fuel rod. This reduces the potential for bowing, accommodating rod growth by allowing it to slip through the top grid. This end grid design has a satisfactory reactor operating history.

The pressure loss coefficients of the grids were determined by testing and an evaluation performed to demonstrate acceptability (Reference 22.5).

d) Requirement for Structural Integrity

Grid dynamic crush testing was performed to determine the dynamic impact characteristics of the RFA and IFM grid designs (References 22.24 and 22.25). The test results (crush strength and stiffness) compared with the calculated impact loads from the dynamic analysis show that the maximum calculated impact loads are less than the lower 95 percent confidence limit crush strengths for the mid and IFM grids.

Based on seismic and LOCA analyses, the lateral impact loads on the top and bottom end grids are negligible. This is consistent with results from previous analyses for current operating plants.

The fatigue of the mid grid has also been shown to be acceptable. The calculated fatigue usage factor is well below the allowable limit of 1.0.

Previous analyses have shown that the fatigue usage of end grids is very low. The end grid designs for the AP1000 plant are the same as those used on previous Westinghouse 17x17 fuel assemblies.

e) Requirement for Handling of Fuel Assemblies

The grid assembly peripheral dimensions are consistent with the overall fuel assembly envelope and identical to the peripheral dimensions of previous Westinghouse 17x17 fuel assembly grids. Operating experience with these grids has shown that the fuel assembly can be satisfactorily installed in shipping containers, fuel storage racks, fuel transfer mechanisms, fuel elevators, and spent fuel shipping casks.

The mid and IFM grid designs feature anti-snag outer strap designs, having guide vanes and guide tabs at each inner strap location. The mid grid guide tab and guide vane offsets have also been increased compared with those of the standard RFA design, reducing the potential of damaging grid-to-grid engagement. The IFM grid utilises the same guide vane and guide tab geometry as the current 17x17 RFA design. The inner-to-outer strap weld joints have been made more robust by moving them outward from the grid lateral centreline, in effect isolating the weld-created heat-affected zones from the thin inner strap ligaments. In summary, these changes both reduce the probability of grid-to-grid snagging occurring during fuel handling operations and minimise the probability of loose parts being created should snagging occur.

f) Requirement for Materials

Alloy-718 will be used to fabricate the top, bottom, and protective grids. **ZIRLO** will be used to fabricate all other grids. There is extensive satisfactory experience with the grid materials and their chemical properties (References 22.3 and 22.13).

Appropriate mechanical properties are specified in design documents (drawings and material specifications) to ensure that the grid assembly design loads can be satisfactorily accommodated and that satisfactory experience with previous grid designs remains applicable.

Material property changes due to irradiation are accounted for in the design of a grid. Successful operating experience with these grid materials (**ZIRLO** and Alloy-718) has shown that irradiation-induced creep and growth will not lead to fuel rod fretting or fuel handling problems.

A corrosion evaluation of the **ZIRLO** grids, based on typical power histories, [

]. The SCC resistance of welded Alloy-718 in the Westinghouse PWR coolant environment was verified during development of prior Westinghouse fuel assembly designs.

Effects of Assembly Bow on Safety Margin

The primary design features for the fuel assembly that provide resistance to fuel assembly bow are the following:

- Increased thickness of the guide tube wall

- Changing the dashpot region of the guide tube to a tube-in-tube design, effectively further increasing the guide tube wall thickness in this critical region

- Implementing **ZIRLO** as the grid and guide tube material to reduce neutron fluence induced growth

- Optimised top nozzle hold-down spring forces

Lateral stiffness experiments have been performed for the fuel assembly design and compared with the existing RFA designs. The results show that the fuel assembly lateral stiffness is the same as or better than the current RFA designs (Reference 22.20). The use of **ZIRLO** versus Zr-4 as the guide tube material will result in significantly less fuel assembly axial growth due to neutron fluence accumulation. This reduces the top nozzle hold-down spring compressive force and therefore reduces the risk of assembly bow for **ZIRLO**-based fuel relative to Zr-4.

Therefore, the fuel in the AP1000 design is not expected to suffer from excessive distortion.

Westinghouse has developed a methodology for predicting assembly bow (Reference 22.20). Given the initial bow conditions of the assemblies loaded into the core at the beginning of the cycle along with the depletion history and operating conditions of the cycle, a detailed mechanical model provides a good estimate of the fuel assembly bow expected at the end of the cycle. The model has been used to develop a cycle-independent set of in-core gap distributions for the purposes of developing a conservative set of cycle-independent peaking factor penalties. The predicted conservative peaking factor penalties are quite small and less than those observed for RFA fuel. In the event that the AP1000 plant fuel assembly bow measurements are inconsistent with RFA performance expectations, available margins could be reallocated to accommodate the small potential penalties without affecting the conclusions of the AP1000 plant safety case.

Another potential impact of assembly bow on the safety case is incomplete control rod insertion upon reactor trip, which would result in a reduction in available shutdown margin. The design features described above increase the lateral stiffness of the assembly, thus reducing the potential for guide tube distortion. As these features have been implemented within the current operating fleet of Westinghouse plants, the risk of incomplete rod insertion has been significantly reduced.

A surveillance programme will be conducted to confirm the dimensional stability of the fuel assembly. This programme will include pre- and post-irradiation measurements of fuel assembly length (to determine growth) and fuel assembly bow and twist. These measurements will be conducted on assemblies expected to have the highest burnups. In addition, RCCA drag force and RCCA drop time will be measured. Any unusual results that might indicate fuel assembly distortion beyond the expected limits will be evaluated as necessary.

22.5.2.2 Fuel Rod

Fuel Material

Sintered, high-density uranium dioxide fuel reacts only slightly with the clad at core operating temperatures and pressures. In the event of clad defects, the high resistance of uranium dioxide to attack by water protects against fuel deterioration, although limited fuel erosion can occur. The consequences of defects in the clad are greatly reduced by the ability

of uranium dioxide to retain fission products, including those that are gaseous or highly volatile.

The evaluation of the individual criteria and design bases for the fuel materials is summarised below.

a) Fuel Centreline Temperature

The Westinghouse standard methodology for the fuel temperature calculations was used to determine the allowed linear heat rate for the prevention of fuel centreline melt.

b) Fuel Dimensional Changes

Observations from several early Westinghouse PWRs have shown that fuel pellets can densify under irradiation to a density higher than the manufactured values (Reference 22.27). Fuel densification and subsequent settling of the fuel pellets can result in local and distributed gaps in the fuel rods. The densification process is related to the elimination of very small as-fabricated porosity in the fuel during irradiation. Early fuels were intentionally manufactured to low initial density and were under-sintered, which resulted in a large fraction of very small pores.

Densification behaviour in current fuel is controlled by improved manufacturing process controls and by specifying a nominal 95.5 percent initial fuel density, which results in reduced levels of small, densifying porosity. The evaluation of fuel densification effects and the treatment of fuel swelling and fission gas release are described in References 22.7 and 22.28.

c) Fuel Chemical Properties

Due to the potential for adverse chemical reactions between the fuel pellet and the cladding the moisture content in the fuel pellets is controlled to minimise the potential for hydride induced failures of the cladding. The moisture content is limited as part of the total hydrogen requirement defined in the pellet production specification, Reference 22.101.

d) Zirconium Diboride Material Properties

The rod average bias in the axial ZrB2 loading is monitored by manufacturing to identify and correct issues that would create significant variations in the axial loading caused by the manufacturing process.

The monitoring is performed using an active gamma scan of every fuel rod. [

]

[

]

Cladding

The evaluation of the individual criteria and design bases for the fuel cladding is summarised below.

a) Clad Stress

Cladding stress analyses are performed with a bounding methodology approach. Important fuel rod dimensions and models that can adversely affect the cladding stress analysis are all set to their limiting values in the same PAD code clad stress run.

Cladding stress analyses are performed to determine the allowable frequent fault local power as a function of initial local power and local burnup so that the cladding yield stress is not exceeded. Cladding stress analyses are performed for a large spectrum of possible steady-state rod power histories with the PAD code. This spectrum of power histories covers the entire range of possible rod powers from low to high and a range of rod burnups.

The most limiting final local power for a given initial local power and local burnup is provided to the core designer. The core designer then ensures that the final allowed local power as a function of initial local power and local burnup will not be exceeded based upon the normal operating range and on the plant protection system. If necessary, constraints on the normal operation range are imposed or more limiting plant trip setpoints are implemented so that the plant will trip prior to exceeding the allowed final local power allowed by the stress analysis.

Another fuel rod design criterion that sets limits on the allowed local power during frequent faults is the one to prevent the cladding total tensile strain due to uniform cylindrical pellet thermal expansion from exceeding 1 percent from the pre-transient value. The cladding stress criterion is more limiting than the 1 percent transient cladding strain criterion. That is, the allowed local power for meeting the stress criterion is less than that allowed for meeting the strain criterion. This cladding stress analysis is purely an analytical calculation to ensure that the yield stress is not exceeded during normal operation and frequent faults..

b) Clad Strain (Transient)

Based upon previous analysis experience and generic analyses, transient clad stress is always more limiting than transient clad strain for a frequent fault. That is, the cladding yield strength would be reached prior to the transient clad strain reaching 1 percent.

c) Clad Strain (Steady State)

The steady-state clad strain mechanism is controlled by the relatively slow processes of fuel swelling and densification and clad creep. Following pellet-clad contact, the clad strain is driven primarily by fuel solid swelling, which is a function of fuel burnup. Outward clad creep associated with operation with rod internal pressure greater than system pressure has only a second-order effect on clad steady-state strain. Since steady-state strain is controlled in large part by fuel behaviour, factors that affect fuel pellet geometry will also affect cladding strain.

d) Clad Corrosion

For the clad corrosion analyses, the best-estimate clad oxide thickness and hydrogen pickup remain less than the criteria limits (Reference 22.89).

e) Clad Flattening

Current fuel rod designs employ fuel with a nominal density of 95.5 percent theoretical density (TD) with improved in-pile stability and high helium backfill pressures that provide adequate assurance that no clad flattening will occur. Westinghouse has undertaken an evaluation of clad flattening based upon available post-irradiation and in-core flux trace data (Reference 22.28). These data confirm that significant axial gaps do not occur for current Westinghouse fuel and concluded that clad flattening will not occur.

According to the lower plenum design criteria, fuel cladding in the lower plenum region shall not be flattened due to creep (thermal- and irradiation-induced) ovalisation during normal operations for the fuel rod design life. This criterion was verified by performing autoclave tests and by operating experience. For the instantaneous and thermal creep collapse, two autoclave tests were performed. The test results (Reference 22.5) indicate that no collapse occurred and that none of the test samples show significant cladding creepdown or flattening.

For the irradiation creep collapse, even though the in-reactor irradiation creep part of the evaluation for the standoff tube was not included in the autoclave tests, the operating experience of the lower plenum standoff design has shown that no issues have ever been reported on the in-reactor irradiation creep effect. The lower plenum design has been used in multiple plant applications for more than three decades. A summary of operating experience is given in Reference 22.5.

f) Clad Fatigue

The fatigue analysis considered three-cycle fuel in 18-month cycles with load follow occurring over 100 percent of each cycle length. [

] Axial power shapes associated with all-rods-out operation were also assumed in the analysis. This spectrum of peaking factor assumptions, along with the load follow core power swing assumption [
] (assumed for fuel rod design purposes only) power provided a wide range of possible initial local powers for the analysis. Both the IFBA fuel rod and the non-IFBA fuel rod were analysed. The IFBA fuel rod was more limiting because of the ZrB_2 coating on the pellet, causing pellet-clad contact sooner than the non-IFBA fuel rod and resulting in more pellet-cladding contact and more strain cycles during load follow.

The standard fatigue methodology is to perform a best-estimate fatigue analysis for all the possible power histories and then to perform an uncertainty analysis for the limiting rod power histories to obtain the upper bound fatigue usage. The methodology includes the important parameters for determining cladding strains as part of the uncertainties consistent with References 22.4, 22.6, 22.30, and 22.5 [

].

The reference analysis in Reference 22.5 analysed a spectrum of power histories for three cycles worth of fuel. Typically, the three cycle is the limiting cycle with the longest pellet-clad contact pressure and resulting strain on the cladding to produce the highest fatigue considering load follow and no grid frequency control.

[

]

[

]

[

]

g) Clad Wall Thickness and Ovality

The fuel cladding wall thickness requirement and maximum-allowed ovality are specified and controlled through product drawings. These specified limits are the same as for previous Westinghouse designs and are acceptable based on successful operating history.

h) Clad Scratch Limits

Fuel cladding scratch limitation is specified and controlled through product drawings and specifications and inspected using visual standards. This specified limit is the same as for previous Westinghouse designs and is acceptable based on successful operating history.

i) Rod Bowing

Potential for rod bow is minimised by control of the fuel element design parameters identified below. Analyses have shown the following conditions to be influential in this context:

[

Rod bow observations have been evaluated for [ ] 14×14-, 15×15-, and 17×17-type cores [ ] (Reference 22.66). This large statistical base has been used to validate the model used for the evaluation of fuel rod bowing in the AP1000 design.

Fuel Rod

In the calculation of the steady-state performance of a nuclear fuel rod, the following interacting factors are considered:

- Clad creep and elastic deflection.
- Pellet density changes, thermal expansion, gas release, and thermal properties as a function of temperature and fuel burnup.
- Internal pressure as a function of fission gas release, rod geometry, and temperature distribution.

These effects are evaluated with PAD using fuel rod design models that include appropriate models for time-dependent fuel densification (Reference 22.7). With these interacting factors considered, the model determines the fuel rod performance characteristics for a given rod geometry, power history, and axial power shape. In particular, internal gas pressure, fuel and clad temperatures, and clad deflections are calculated. The fuel rod is divided into several axial sections and radially into a number of annular zones for the model. The parameters are reconfirmed every cycle using the PAD code to ensure that they remain below their respective limits.

The initial rod internal pressure is selected to delay fuel/clad mechanical interaction and to avoid the potential for clad flattening. It is limited, however, by the design criteria for the rod internal pressure.

The gap conductance between the pellet surface and the clad inner diameter is calculated as a function of the composition, temperature, and pressure of the gas mixture; and the gap size or contact pressure between the clad and pellet. After computing the fuel temperature for each pellet zone, the fractional fission gas release is assessed using an empirical model derived from experimental data (Reference 22.7). The total amount of gas released is based on the average fractional release within each axial and radial zone and the gas generation rate, which, in turn, is a function of burnup. Finally, the gas released is summed up over the zones and the pressure is calculated.

The model shows close agreement in fit for a variety of published and proprietary data on fission gas release, fuel temperatures, and clad deflections. These data include variations in power, time, fuel density, and geometry.

The evaluation of the individual criteria and design bases for the fuel rod performance are summarised below.

a) Fuel Rod Internal Gas Pressure (Departure from Nucleate Boiling Propagation)

Two methodologies exist for verifying this criterion: probabilistic (Reference 22.90) and mechanistic (Reference 22.91). The use of the mechanistic DNB methodology can provide additional flexibility in fuel management and peaking factor space by allowing the use of more IFBA rods and/or the use of nonstandard IFBA patterns. The acceptable strain value is one that ensures that the flow channel closure due to the cladding strain during the transient will not result in additional rods to experience DNB. It also ensures that cladding burst will not take place because of the strain that occurs while the rod is in DNB during the transient.

b) Fuel Rod Internal Gas Pressure (Gap Reopening)

The Westinghouse fuel performance model was used in the analysis of this criterion. The rod internal analysis considers a best estimate plus total uncertainty methodology to obtain the upper bound rod internal pressure. The IFBA rod is limiting because of the helium released from the ZrB_2 coating. For the standard rod internal pressure analysis, the limiting IFBA rod internal pressure was less than the gap-re-opening limit. Analysis of simulated MSHIM operation is necessary to determine the potential effects of local power peaking perturbations on rod internal pressure.

c) Fuel Axial Growth

The Westinghouse standard methodology for fuel rod growth has been used for the verification analysis. This analysis shows that contact will be precluded, conservatively assuming upper bound fuel rod growth, lower bound fuel assembly growth, minimum initial rod to nozzle gap, upper bound fuel rod fast fluence (E>1.0 MeV), and nominal differential thermal expansion between the fuel rod cladding and the fuel assembly structure. The analysis indicates that the design criterion is satisfied considering a lead rod burnup of 62 GWD/MTU.

d) End Plug Weld Integrity

For infrequent faults, the limit is that which produces the maximum tensile differential pressure loads. The limiting event is steam line break (SLB), which produces significant depressurisation of the primary system. This reduced system pressure, along with a return to power during the event (that concentrates the power under the worst-stuck RCCA) can result in high rod internal pressure and high differential pressure loads across the weld.

Generic end plug weld integrity analyses performed for standard fuel rod designs show that [

] the end plug weld integrity criterion would be met. The analysis for the SLB event in the AP1000 design shows a hot rod average power well below this limit for the initial core. The hot rod average power is calculated for each cycle and while the calculated value may vary for a given cycle, it must remain below the limit defined for SLB above.

e) Fuel Rod Straightness

The requirement for fuel cladding and fuel rod assembly straightness in the AP1000 design is specified and controlled through product drawings. This specified limit is the same as for previous Westinghouse designs and is acceptable based on successful operating history.

f) Hold-Down Spring Radial Support of Clad

Verification of this criterion is shown by demonstrating that the springs in the AP1000 design are bounded by previous spring designs. Previous standard pitch springs and variable pitch springs have undergone extensive autoclave testing and have demonstrated acceptable in-pile performance and so provide a sound DB for the design of the plenum springs in the AP1000 design. It has been verified that the wire diameter, the compressed spring midpitch, and the coil diameter of the springs are bounded by previous spring designs. On the basis of this evaluation (Reference 22.5), it is concluded that the fuel rod plenum spring design for the AP1000 plant is capable of providing sufficient radial support to the cladding in the plenum region to preclude collapse.

g) Axial Location of Fuel Pellet Stack

The minimum plenum spring hold-down force on the fuel pellet stack is greater than [ ] times the weight of the [ ] (Reference 22.5). Since the minimum spring force is greater than [ ] times the weight, this design criterion is satisfied.

h) Fuel Rod Outer Diameter at Weld

The fuel rod end plug design and fuel rod outer diameter at the weld are identical to those in previous Westinghouse fuel assembly designs. Successful operating experience with these previous designs and the testing performed on the AP1000 design shows that it will not cause unacceptable fretting damage to the clad in service.

i) Standoff Tube Design

The dimension and shape of the pellet stack base and standoff tube allow fission gases to communicate with the standoff tube internal volume through the centre hole on the pellet

stack base as shown in Figure 22-16. In addition, the hole diameter is designed to be smaller than the wall thickness of the annular pellet. The pellet stack base will therefore prevent fuel pellets or large pellet fragments from entering the lower plenum region.

j) Potentially Damaging Temperature Effects during Transients

The fuel rod experiences many operational transients (intentional manoeuvres) during its residence in the core. A number of thermal effects must be considered when analysing the fuel rod performance.

The clad can be in contact with the fuel pellet at some time in the fuel lifetime. Clad/pellet interaction occurs if the fuel pellet temperature is increased after the clad is in contact with the pellet. Clad/pellet interaction is discussed below.

Clad flattening is precluded during the fuel residence in the core by the use of stable fuel.

Potential differential thermal expansion between the fuel rods and the guide thimbles during a transient is considered in the design. Excessive bowing of the fuel rods is precluded because the grid assemblies allow axial movement of them relative to the grids. Specifically, thermal expansion of the fuel rods is considered in the grid design so that axial loads imposed on them during a thermal transient will not result in excessively bowed fuel rods.

k) Fuel Element Burnout and Potential Energy Release

The core is protected from DNB over the full range of possible operating conditions. In the extremely unlikely event that DNB occurs, the clad temperature will rise because of the steam blanketing at the rod surface and the consequent degradation in heat transfer. During this time, there is a potential for chemical reaction between the cladding and the coolant; however, because of the relatively sufficient film boiling heat transfer following DNB, the energy release resulting from this reaction is insignificant compared with the power produced by the fuel.

l) Fuel/Cladding Mechanical Interaction

The gap between the fuel and clad is initially sufficient to prevent hard contact between the two, but during power operation, a gradual compressive creep of the clad onto the fuel pellet occurs because of the external pressure exerted on the rod by the coolant. Clad compressive creep eventually results in fuel/clad contact. Once this contact occurs, changes in power level result in changes in clad stresses and strains. By using pre-pressurised fuel rods to partially offset the effect of the coolant external pressure, the rate of clad creep toward the surface of the fuel is reduced. Fuel rod pre-pressurisation delays the time at which fuel/clad contact occurs and hence significantly reduces the extent of cyclic stresses and strains experienced by the clad both before and after contact. These factors result in an increase in the fatigue life margin of the clad and lead to greater clad reliability.

22.5.2.3 In-Core Control Components

a) Internal Pressure and Cladding Stresses during Normal, Transient, and Accident Conditions

The designs of the BA, source, and gray rods provide a sufficient cold void volume to accommodate the internal pressure increase during operation. This is not a concern for

the RCCA absorber rod because no significant amount of gas is released by the silver-indium-cadmium absorber material.

For the discrete BA rod, there is sufficient cold void volume to limit the internal pressure to a value that satisfies the design criteria. For the source rods, a void volume is provided within the rod to limit the maximum internal pressure increase at EOL.

During normal transient and accident conditions, the void volume limits the internal pressures to values that satisfy the criteria in Section 22.5.1.3. These limits are established not only to prevent the peak stresses from reaching unacceptable values but also to limit the amplitude of the oscillatory stress component in consideration of the fatigue characteristics of the materials.

Rod, guide thimble, and dashpot flow analyses indicate that the flow is sufficient to prevent coolant boiling within the guide thimble.

b) Thermal Stability of the Absorber Material, Including Phase Changes and Thermal Expansion

The radial and axial temperature profiles within the source and absorber rods are determined by considering gap conductance, thermal expansion, neutron or gamma heating of the contained material, as well as gamma heating of the clad.

The maximum temperatures of the silver-indium-cadmium RCCA or tungsten GRCA absorber materials are calculated and found to be significantly less than the material melting point and to occur axially at only the highest flux region.

The maximum temperature of the alumina-boron carbide WABA pellet is expected to be less than 649°C (1200°F), which occurs following the initial power ascent. As the operating cycle proceeds, the BA pellet temperature decreases because of a reduction in heat generation from boron depletion and better gap conduction as the helium produced diffuses into the gap.

Sufficient diametral and end clearances have been provided in the neutron absorber, BA, and source rods to accommodate the relative thermal expansions between the enclosed material and the surrounding clad and end plug.

c) Irradiation Stability of the Absorber Material, Taking into Consideration Gas Release and Swelling

Irradiation produces no deleterious effects in the silver-indium-cadmium absorber material (Reference 22.13). As mentioned above, gas release is not a concern for the control rod material because no gas is produced by the absorber material. Sufficient diametral and end clearances are provided to accommodate any potential expansion and/or swelling of the absorber material for both RCCA and GRCA absorber rods. The irradiation stability of the tungsten absorber material is discussed in Reference 22.36.

Irradiation produces no deleterious effects in the tungsten absorber material of the gray rodlets. Some minor cracking of the tungsten material may occur, but this cracking does not affect the absorber column geometric stability due to the small clearance between the absorber and sleeve (Reference 22.36).

The alumina-boron carbide BA pellets are designed such that gross swelling or crumbling of the pellets is not predicted during reactor operation. Some minor cracking of the pellets may occur, but it should not affect the overall absorber and stack integrity.

d) Potential for Chemical Interaction, Including Possible Water-Logging Rupture

The structural materials selected have good resistance to irradiation damage and are compatible with the reactor environment. Corrosion of the materials exposed to the coolant is quite low, and proper control of chloride and oxygen in the coolant minimises the potential for stress corrosion. By controlling the coolant chemistry in accordance with the guidance provided in Reference 22.95, the potential for corrosion of components exposed to coolant is minimised and thus the potential for the interference with RCCA movement due to possible corrosion phenomena is very low.

Water-logging rupture is not a failure mechanism associated with the control rods in the AP1000 design. Furthermore, a breach of the cladding for any postulated reason does not result in serious consequences. The silver-indium-cadmium absorber material is relatively inert and will remain so even when subjected to high coolant velocity regions. Rapid loss of reactivity control material will not occur. Test results concluded that additions of indium and cadmium to silver, in the amounts to form the silver-indium-cadmium absorber material composition, result in small corrosion rates (Reference 22.13). In the unlikely event of a GRCA rod cladding breach, loss of absorber material will not occur because the inner sleeve encapsulates the tungsten absorber (Reference 22.36).

For the discrete BA, in the unlikely event that the zirconium alloy clad is breached, the boron carbide in the affected rods could be leached out by the coolant water. If this occurs, normal examination of primary chemistry would indicate presence of boron or in-core instruments would detect peaking factor changes, and corrective action would be taken if warranted. A postulated clad breach after substantial irradiation would have no significant effect on peaking factors since the boron will have been depleted. Breaching of the zirconium alloy clad by internal hydriding is not expected because of moisture controls employed during fabrication. The moisture content is limited as part of the total hydrogen requirement defined in the pellet production specification, Reference 22.101. Reference 22.110 provides the process and inspection requirements to achieve the design requirement during manufacturing. Rods of this design have performed very well with no failures observed.

22.5.3 Testing and Inspection Plan

Westinghouse fuel and core component manufacturing has an extensive amount of information available characterising the success in implementing quality assurance programmes over many years. As a result, the Westinghouse fuel and core components have an extremely high success rate in performing their function, thus demonstrating the robustness of meeting the design criteria described in this chapter. The Westinghouse quality assurance, development, testing, and inspection programmes are described briefly below.

22.5.3.1 Quality Assurance Programme

The Quality Assurance Programme Plan of the Westinghouse Commercial Nuclear Fuel Division provides for control over activities affecting product quality, commencing with design and development and continuing through procurement, materials handling, fabrication, testing and inspection, storage, and transportation. The programme also provides for the indoctrination and training of personnel and for the auditing of activities affecting product quality through a formal auditing programme.

Westinghouse drawings and product, process, and material specifications identify the inspections to be performed.

22.5.3.2 Quality Control

Quality control philosophy is generally based on the following inspections being performed to a 95 percent confidence level that at least 95 percent of the product meets specification, unless otherwise noted.

a) Fuel System Components and Parts

The characteristics inspected depend on the component parts. The quality control programme includes dimensional and visual examinations, check audits of test reports, material certification, and NDE such as X-ray and ultrasonic.

b) Fuel Pellets

Inspection is performed for dimensional characteristics such as diameter, density, length, and squareness of ends. Additional visual inspections are performed for cracks, chips, and surface conditions. Reference 22.111 provides the process and inspection requirements to achieve the design requirements during manufacturing.

Density is determined in terms of weight per unit length and is plotted on zone charts used in controlling the process. Chemical analyses are taken on a specified sample basis throughout pellet production.

c) Rod Inspection

Inspections of fuel rods, rod cluster control rods, discrete BA rods, and source rods consist of the following NDE techniques and methods, as applicable, as follows:

- Each rod is leak tested using a calibrated mass spectrometer, with helium being the detectable gas.
- Rod welds are inspected by ultrasonic test or X-ray in accordance with a qualified technique and Westinghouse specifications meeting the requirements of American Society for Testing Materials (ASTM)-E-142-86 (Reference 22.31).
- Rods are dimensionally inspected prior to final release. The requirements include such items as length, camber, and visual appearance.
- Fuel rods are inspected by gamma scanning to confirm proper plenum dimensions.
- Fuel rods are inspected by gamma scanning to confirm that no significant gaps exist between pellets.

- Fuel rods are actively and/or passively gamma-scanned to verify enrichment control prior to acceptance for assembly loading.

- Traceability of rods and associated rod components is established by quality control.

d) Fuel Assemblies

Each fuel rod, control rod, BA rod, and source rod assembly is inspected for compliance with drawing and/or specification requirements. Other in-core control component inspection and specification requirements are given in Section 22.5.3.3.

e) Other Inspections

The following inspections are performed as part of the routine inspection operation:

- Tool and gauge inspection and control, including standardisation to primary and/or secondary working standards. Tool inspection is performed at prescribed intervals on serialised tools. Complete records are kept of calibration and conditions of tools.

- Audits are performed of inspection activities and records to confirm that prescribed methods are followed and that records are correct and properly maintained.

- Surveillance inspection, where appropriate, and audits of outside contractors are performed to confirm conformance with specified requirements.

f) Process Control

Generally, all items used in fabrication of fuel assemblies and core components are tracked using a manufacturing execution system (MES) interfacing with a database. The local human-machine interfaces (HMIs) vary widely but all are "qualified" in accordance with the quality management system (QMS). The qualification process ensures that the HMI uses and transmits data as intended. Steps in the manufacturing procedures include activities with the HMIs. The HMIs mine the data for the particular items being used to make up the subsequent item or assembly and will only allow the use of items that meet expectations of the programme, or the operator will be unable to complete the operation.

To prevent the possibility of mixing enrichments during fuel manufacture and assembly, strict enrichment segregation and other process controls are exercised.

The uranium dioxide powder is kept in sealed containers. The contents are fully identified both by descriptive tagging and unique bar code numbers. A quality control identification tag completely describing the contents is affixed to the containers before transfer to powder storage. Isotopic content is confirmed by analysis.

Powder can be withdrawn from storage by only one authorised group, which directs the powder to the correct pellet production line. The pellet production lines are physically separated from each other, and pellets of only a single nominal enrichment and density are produced in a given production line at any given time.

Finished pellets are placed on trays identified with the same colour code as the powder containers and transferred to segregated storage racks within the confines of the pelleting area. Samples from each pellet lot are tested for isotopic content and impurity levels prior to acceptance by quality control. Physical barriers are used to prevent mixing of pellets of

different nominal densities and enrichments in the pellet storage area. Unused powder and substandard pellets are returned to storage in the original colour-coded containers.

Loading of pellets into the clad is performed in isolated production lines; only one density and enrichment (with possible exception of top and bottom (axial blanket) zones) are loaded on a line at a time.

A serialised traceability code is placed on each fuel tube, which identifies the contract and enrichment. The end plugs are inserted and then welded (in an inert gas atmosphere) to seal the tube. The fuel tube remains coded and traceability identified until just prior to installation in the fuel assembly.

Similar traceability is provided for WABA, source, and control rods, as required.

22.5.3.3 In-Core Control Component Testing and Inspection

Tests and inspections are performed on each reactivity control component to verify the mechanical characteristics. In the case of the RCCA, prototype testing has been conducted. Manufacturing tests and inspections and functional testing at the plant site are performed.

During the component manufacturing phase, the following requirements apply to the reactivity control components to provide proper functioning during reactor operation:

- Materials are procured to specifications to attain the desired standard of quality.
- Rods are checked for integrity by the applicable nondestructive methods.
- To confirm proper fit with the fuel assembly, the rod cluster control, discrete BA, and source assemblies are installed in the fuel assembly and checked for binding in the dry condition.

The RCCAs and GRCAs are also functionally tested following core loading but prior to criticality to demonstrate reliable operation of the assemblies. Each assembly is operated (and tripped) one time at full-flow/hot conditions. In addition, any assembly that has a drop time greater than a two-sigma limit from the average rod drop time is subjected to additional rod drops to confirm drop time. Thus, each assembly is sufficiently tested to confirm proper functioning and operation. [

]

To demonstrate continuous free movement of the RCCAs and GRCAs and to provide acceptable core power distributions during operations, partial movement checks are performed as required by the Tech Specs. [

] In addition, periodic drop tests of the assemblies are performed at each refuelling shutdown to demonstrate continued ability to meet trip time requirements.

If an RCCA cannot be moved by its mechanism and is determined to be untrippable, adjustments in the boron concentration of the coolant provide that adequate SDM will be achieved following a trip. Thus, inability to move one assembly can be tolerated until the

reactor can be safely taken to Mode 3. Short-term operation with more than one inoperable RCCA may be tolerated as well, depending on the amount of excess SDM initially available, but would impose additional demands on the plant operator.

Upon discovery of one or more inoperable RCCAs, the plant Tech Specs require the operator to confirm adequate SDM and adjust the boron concentration if necessary to achieve it, and then be in Mode 3 within 6 hours of discovery. No allowance is made for continued operation past 6 hours with one or more inoperable RCCAs even if adequate SDM can be maintained with adjustments to the boron concentration. The discovery of an inoperable GRCA is not associated with a requirement to shut down because rapid GRCA insertion is not currently credited for safety purposes. The operator can compensate for the operational effects of an inoperable GRCA by adjusting boron more often or by switching to an alternate GRCA bank.

22.5.3.4 In-Service Surveillance

Westinghouse has gained significant fuel assembly operating experience over many years by conducting a programme to examine detailed aspects of the 17x17 fuel assembly (Reference 22.32). This operating experience is periodically updated to provide recent results of operating experience with Westinghouse fuel and in-core control components. A surveillance programme similar to those conducted in the past will be performed on irradiated fuel assemblies and core components of the AP1000 plant.

22.5.3.5 Onsite Receipt Inspection

Written procedures are used for the post shipment inspection of the new fuel assemblies in addition to reactivity control and source components. Fuel handling procedures specify the sequence in which handling and inspection take place.

Loaded fuel containers, when received onsite, are externally inspected to confirm that labels and markings are intact and security seals are unbroken. After the containers are opened, the shock indicators attached to the suspended internals are inspected to determine whether movement during transit exceeded design limitations.

Following removal of the fuel assembly from the container in accordance with detailed procedures, the fuel assembly plastic wrapper is examined for evidence of damage. The polyethylene wrapper is then removed and a visual inspection of the entire fuel assembly is performed.

Control rod, gray rod, secondary source rod, and discrete BA rod assemblies are usually shipped in fuel assemblies. They are inspected prior to removal of the fuel assembly from the container. The control rod assembly is withdrawn a few inches from the fuel assembly to confirm free and unrestricted movement; the exposed section is visually inspected for mechanical integrity, replaced in the fuel assembly, and stored with the fuel assembly. Control rod, secondary source, or discrete BA assemblies may be stored separately or within fuel assemblies in the new fuel storage area.

Primary source rods will be shipped to site in separate containers because of the radioactive properties of the source material. Inspection of the rods will be carried out prior to fixing into the core component assemblies.

22.6 NUCLEAR DESIGN

22.6.1 Design Bases

This section describes the design bases and functional requirements used in the nuclear design of the fuel and reactivity control system. The design bases are the fundamental criteria that must be met using analytical techniques.

The initial fuel loading of the reactor and the nuclear performance during the first operating cycle are important periods of the nuclear design. This is because some of the safety-related nuclear parameters may assume their most extreme values during this period. Where subsequent operation is expected to produce more extreme values of any safety-related parameter, a representative reload core condition is derived to evaluate it.

Conservative upper and lower limits are specified for all safety-related parameters and a prime purpose of the nuclear design basis is to ensure that no safety parameter moves outside its permitted bandwidth. The safety case for the lifetime of the plant is based on these conservative limiting values and there is a high degree of confidence that these limits will not be exceeded during the operating lifetime of the plant.

The core design power distribution limits related to fuel integrity are met for frequent faults through conservative design and are maintained by the action of the control system.

The requirements for frequent faults are met by providing an adequate protection system that monitors reactor parameters.

The control and protection systems for core monitoring and control and for fuel handling and storage systems are described in Chapter 19.

The consequences of faults are described in appropriate sections of Chapter 9.

22.6.1.1 Fuel Burnup

A limitation on initial installed excess reactivity or average discharge burnup is not required other than as is quantified in terms of other design bases, such as overall negative power reactivity feedback discussed below. A maximum fuel rod average burnup of 62,000 MWD/MTU has been adopted for the core (Reference 22.29). Note that this is an extension of the original licensed limit of 60,000 MWD/MTU (Reference 22.4).

Burnup is a measure of fuel depletion that represents the integrated energy output of the fuel in MWD/MTU and is a useful means for quantifying fuel exposure criteria.

The core design lifetime, or design discharge burnup, is achieved by installing sufficient initial excess reactivity in each fuel region and subsequently following a fuel replacement programme that meets the safety-related criteria in each cycle of operation.

Initial excess reactivity installed in the fuel, although not a DB, must be sufficient to maintain core criticality at full-power operating conditions throughout cycle life with equilibrium xenon, samarium, and other fission products present. BAs, control rods, and/or chemical shim are used to compensate for the excess reactivity. The end of design cycle life is defined as occurring when the chemical shim concentration is essentially zero with control rods present to the degree necessary for operational requirements.

22.6.1.2 Reactivity Coefficients

For the initial fuel cycle, the fuel temperature coefficient must be negative and the moderator temperature coefficient of reactivity must also be negative for power operating conditions, thereby providing negative reactivity feedback characteristics.

When compensation for a rapid increase in reactivity is considered, there are two major effects: the resonance absorption (Doppler) effects associated with changing fuel temperature and the neutron spectrum and reactor composition change effects resulting from changing moderator density. These basic physics characteristics are often identified by reactivity coefficients. The use of slightly enriched uranium results in a Doppler coefficient of reactivity that is negative. This coefficient provides the most rapid reactivity compensation.

The initial core is also designed to have an overall negative moderator temperature coefficient of reactivity during power operation so that average coolant temperature changes or void content provides another, slower compensatory effect. For some core designs, if the compensation for excess reactivity is provided only by chemical shim, the moderator temperature coefficient could become positive. Nominal power operation is permitted only in a range of overall negative moderator temperature coefficient. The negative moderator temperature coefficient can be achieved through the use of discrete BAs and/or integral fuel BAs and/or control rods by limiting the reactivity controlled by soluble boron.

BA content (quantity and distribution) is not stated as a DB; however, for some initial core designs or subsequent reloads, the use of BAs may be necessary for power distribution control and/or to achieve an acceptable moderator temperature coefficient throughout core life. In any core design, a sufficient number of BAs are provided to achieve a negative moderator temperature coefficient at the conditions expected for initial criticality. Thus, there can be no significant transient due to moderator feedback during the initial startup of a cycle. During subsequent operation, the core reactivity may initially increase for the first few months of a cycle and will then begin to decrease after the majority of the BA absorber material has been depleted. Continued operation at or near full power will maintain the negative moderator temperature coefficient condition without any additional operating restrictions during the peak reactivity point in the cycle. If low power operations or a startup are required at the peak reactivity point in the cycle, however, it may be necessary to establish additional limits on control rod withdrawal or maximum soluble boron concentration to maintain the negative moderator temperature coefficient at low power levels. The establishment of such limits would not impact actual operation because the normal boron concentration and position of control rods during MSHIM operation would not challenge the limits required to ensure compliance with the moderator temperature coefficient (MTC) limit.

22.6.1.3 Control of Power Distribution

The nuclear DB is the following, with at least a 95 percent confidence level:

- The fuel will not operate with a power distribution that would result in exceeding the DNB DB (i.e., the DNBR shall be greater than the design limit DNBR) under normal operation and frequent faults, including the maximum overpower condition.

- Under abnormal conditions, including the maximum overpower condition, the peak linear heat rate (PLHR) will not cause fuel melting.

- Fuel management will be such as to produce values of fuel rod power and burnup consistent with the assumptions in the fuel rod mechanical integrity analysis in Section 22.5.

- The fuel will not be operated at PLHR values greater than those found to be acceptable within the body of the safety analysis under normal operating conditions, including an allowance of 1 percent for calorimetric error.

Calculation of extreme power shapes that affect fuel design limits are performed with proven methods. The conditions under which limiting power shapes are assumed to occur are chosen conservatively with regard to any permissible operating state. A nuclear uncertainty is applied to the calculated power distribution. Such margins are provided both for the analysis for normal operating states and for anticipated transients.

22.6.1.4 Maximum Controlled Reactivity Insertion Rate

The maximum reactivity insertion rate due to withdrawal of RCCAs or GRCAs or by boron dilution is limited by plant design, hardware, and basic physics. During normal power operation, the maximum controlled reactivity insertion rate is limited. The maximum reactivity change rate for accidental withdrawal of two control banks is set such that PLHR and the DNBR limitations are not challenged.

The maximum reactivity worth of control rods and the maximum rates of reactivity insertion employing control rods are limited to preclude rupture of the coolant pressure boundary or disruption of the core internals to a degree that would impair core cooling capacity because of a rod withdrawal or an ejection accident.

Following any infrequent fault, such as rod ejection or SLB, the reactor can be brought to the shutdown condition and the core maintains acceptable heat transfer geometry.

Reactivity addition associated with an accidental withdrawal of a control bank (or banks) is limited by the maximum rod speed (or travel rate) and by the worth of the banks. For the AP1000 reactor, the maximum control and gray rod speed is 1.14 m/minute (45 inches/minute).

The reactivity change rates are conservatively calculated, assuming unfavourable axial power and xenon distributions. The typical peak xenon burnout rate is significantly lower than the maximum reactivity addition rate for normal operation and for accidental withdrawal of two banks.

22.6.1.5 Shutdown Margins

The minimum shutdown margin as specified in the Tech Specs is required in all operating modes. In analyses involving reactor trip, the single highest-worth RCCA is postulated to remain untripped in its full-out position (stuck-rod criterion).

Two independent reactivity control systems are provided: control rods and soluble boron in the coolant. The control rods provide reactivity changes that compensate for the reactivity effects of the fuel and water density changes accompanying power level changes over the range from full load to no load. The control rods provide the minimum shutdown margin for normal operation; they are capable of making the core subcritical rapidly enough to prevent exceeding acceptable fuel damage limits (very small number of rod failures), assuming that the highest worth control rod is stuck-out upon trip.

The boron system can compensate for xenon burnout reactivity changes and maintain the reactor in the cold shutdown condition. Thus, backup and emergency shutdown provisions are provided by mechanical and chemical shim control systems that satisfy the design criteria. Reactivity changes due to fuel depletion are accommodated with the boron system.

When fuel assemblies are in the pressure vessel and the vessel head is not in place, k_{eff} will be maintained at or below 0.95 with control rods and soluble boron. Furthermore, the fuel will be maintained sufficiently subcritical that removal of the RCCAs will not result in criticality.

ANSI N18.2a (Reference 22.33) specifies a k_{eff} not to exceed 0.95 in spent fuel storage racks and transfer equipment flooded with pure water; and a k_{eff} not to exceed 0.98 in normally dry new fuel storage racks, assuming optimum moderation. This is an established criterion within the nuclear industry. No criterion is given for the refuelling operation; however, a 5 percent margin, which is consistent with spent fuel storage and transfer and the new fuel storage, is adequate for the controlled and continuously monitored operations involved.

The boron concentration required to meet the refuelling shutdown criteria is specified in the Core Operating Limits Report (COLR). Verification that these shutdown criteria are met, including uncertainties, is achieved using standard design methods. The subcriticality of the core is continuously monitored as described in the Tech Specs.

When considering maintaining shutdown margin in the long term following a trip, periodic calculations are made of the required RCS boron concentrations necessary to ensure the correct shutdown margin. These calculations will be based on conservative assumptions such as no-xenon conditions and limiting temperature for each applicable operating mode.

Calculations are also made by the online core monitoring system of the required RCS boron concentration to maintain shutdown margin immediately after a reactor trip. These calculations assume the current core xenon condition, that the highest-worth RCCA will remain stuck out of the core, and that the plant will reach the zero-power no-load temperature following the trip. When compared with the current operating boron concentration, these calculations are an indication of how much excess shutdown margin above the required Tech Spec limit will be available immediately after the reactor trip. Additional information on the online core monitoring system including the safety claims, arguments, and evidence for the system are provided in Reference 22.96.

Following trip, operations procedures will be initiated that will direct the operator to confirm or take action to ensure adequate SDM for the current condition and the anticipated final operating mode and the post-trip condition. When this step in the procedure is reached, the RCS boron concentration data will be readily available.

Assuming that the plant trips into a condition with the Tech Spec minimum-required SDM, the initial buildup of xenon following the trip will provide the operator with at least 8 hours to identify the expected final mode, borate the RCS to the required long-term boron concentration (if necessary), and confirm the concentration by sample. This is more than adequate time in present plants and the AP1000 plant is not substantially different in this matter.

22.6.1.6 Stability

The core will be inherently stable to power oscillations at the fundamental mode. Spatial power oscillations within the core with a constant core power output, should they occur, can be reliably and readily detected and suppressed.

Oscillations of the total power output of the core, from whatever cause, are readily detected by the loop temperature sensors and by the nuclear instrumentation. The core is protected by these systems; a reactor trip occurs if power increases unacceptably, thereby preserving the design margins to fuel design limits. The combined stability of the turbine, steam generator, and reactor power control systems are such that total core power oscillations are not normally possible. The redundancy of the protection circuits results in a low probability of exceeding design power levels.

The core is designed so that diametral and azimuthal oscillations due to spatial xenon effects are self-damping: no operator action or control action is required to suppress them. The stability to diametral oscillations is so great that this excitation is highly improbable. Convergent azimuthal oscillations can be excited by prohibited motion of individual control rods.

Indications of power distribution anomalies are continuously available from an online core monitoring system. The online monitoring and safety systems process information provided by the fixed in-core detectors, in-core thermocouples, and loop temperature measurements. Radial power distributions are therefore continuously monitored, thus power oscillations are readily observable and alarmed. The ex-core long ion chambers also provide surveillance and alarms of anomalous power distributions. In proposed core designs, these horizontal plane oscillations are self-damping by virtue of reactivity feedback effects inherent to the basic core physics.

Axial xenon spatial power oscillations may occur during core life, especially late in the cycle. The online core monitoring system provides continuous surveillance of the axial power distributions. Additional information on the online core monitoring system including the safety claims, arguments, and evidence for the system are provided in Reference 22.96. The control rod system provides both manual and automatic control systems for controlling the axial power distributions.

Confidence that fuel design limits are not exceeded is provided by reactor protection system overpower ΔT ($OP\Delta T$) and overtemperature ΔT ($OT\Delta T$) trip functions, which use the loop temperature sensors, pressuriser pressure indication, and measured axial offset as an input.

22.6.1.7 Anticipated Transients without Trip

The diverse reactor trip actuation system is independent of the reactor trip breakers used by the protection monitoring system. The diverse reactor trip reduces the probability and consequences of postulated anticipated transient without trip (ATWT). These effects are considered to be low probability design basis events which are considered using more realistic inputs and analysis methods and have more relaxed acceptance criteria than higher probability design basis events. Analysis has shown that the likelihood of such a hypothetical event is negligibly small. Furthermore, analysis of the consequences of a hypothetical failure to trip following anticipated transients has shown that no significant core damage would result, system peak pressures should be limited to acceptable values, and no failure of the RCS would result (Reference 22.34). A detailed discussion of ATWT is given in Chapter 9.

22.6.2 Design Description

22.6.2.1 Nuclear Design Description

The reactor core consists of a specified number of fuel rods held in bundles by spacer grids and top and bottom fittings. The fuel rods are fabricated from cylindrical tubes made of

zirconium based alloy(s) containing uranium dioxide fuel pellets. The bundles, known as fuel assemblies, are arranged in a pattern which approximates a right circular cylinder.

Each fuel assembly contains a 17 x 17 rod array composed nominally of 264 fuel rods, 24 rod cluster control thimbles, and an in-core instrumentation thimble. Figure 22-1 shows a cross-sectional view of a 17 x 17 fuel assembly and the related rod cluster control guide thimble locations. Detailed descriptions of the AP1000 fuel assembly design features are given in Section 22.5.

Both the initial and reload core loading patterns can employ various fuel management techniques including “low-leakage” designs, and are anticipated to operate approximately 18 months between refuelling. For reload core loading patterns, the initial and final positions of assemblies and the number of fresh assemblies and their placement are dependent on the energy requirement for the reload cycle and burnup and power histories of the previous cycles.

For the initial core loading, the fuel rods within certain assemblies contain varying uranium enrichments in both the radial and axial planes. Fuel containing up to five average enrichments will be used in the initial core load to establish a favourable radial power distribution simulating the reactivity distribution of a low leakage reload core. Figure 22-17 shows the fuel loading pattern used in the initial cycle. The higher enriched regions will be configured in the core interior consistent with the feed fuel placement in a reload core, and the lower enriched regions will approximate the reactivity of the burned fuel assemblies of a reload core. The enrichments for the initial cycle are shown in Table 22-2.

Reload core loading patterns can employ various fuel management techniques including “low-leakage” designs where the feed fuel is interspersed checkerboard-style in the core interior and depleted fuel is placed on the periphery. Low-leakage designs in general result in lower fuel cycle costs and reduced fluence accumulation on the reactor vessel internals. Regardless of the fuel management technique employed, the reactor vessel fluence is maintained below analysed limits. This is accomplished through metallurgical sampling, radiation analysis, and, if necessary, the implementation of loading pattern constraints on the peripheral core power distribution. Reload core designs, as well as the initial cycle design, are anticipated to operate approximately 18 months between refuelling, accumulating a cycle average burnup of approximately 21,000 MWD/MTU. The exact reloading pattern, the initial and final positions of assemblies, and the number of fresh assemblies and their placement depend on the energy requirement for the reload cycle and burnup and power histories of the previous cycles.

The core average enrichment is determined by the amount of fissionable material required to provide the desired energy requirements. The physics of the burnout process is such that operation of the reactor depletes the amount of fuel available because of the absorption of neutrons by the U-235 atoms and their subsequent fission. In addition, the fission process results in the formation of fission products, some of which readily absorb neutrons. These effects, the depletion and the buildup of fission products, are partially offset by the buildup of plutonium, which occurs due to the parasitic absorption of neutrons in U-238.

At the beginning of any cycle, therefore, a reactivity reserve equal to the depletion of the fissionable fuel and the buildup of fission product poisons, less the buildup of fissile fuel over the specified cycle life, is built into the reactor. This excess reactivity is controlled by removable neutron-absorbing material in the form of boron dissolved in the primary coolant, control rod insertion, BA rods, and/or IFBAs. The stack length of the BA rods and/or integral absorber bearing fuel may vary for different core designs, with the optimum length

determined on a design-specific basis. Figure 22-18 shows a plot of the initial core soluble boron concentration versus core depletion.

The concentration of the soluble neutron absorber is varied to compensate for reactivity changes due to fuel burnup; fission product poisoning, including xenon and samarium; BA depletion; and the cold-to-operating moderator temperature change. Throughout the operating range, the CVS is designed to provide changes in RCS boron concentration to compensate for the reactivity effects of fuel depletion, peak xenon burnout and decay, and cold shutdown boration requirements.

BA rods are strategically located to provide a favourable radial power distribution and provide for negative reactivity feedback. Figures 22-19 and 22-20 show the burnable absorber distributions within a fuel assembly for the several patterns used in a 17 x 17 array. The initial core burnable absorber loading pattern is shown in Figure 22-21.

Tables 22-3 and 22-4 contain summaries of reactor core design parameters including reactivity coefficients, delayed neutron fraction, and neutron lifetimes. Sufficient information is included to permit an independent calculation of the nuclear performance characteristics of the core.

22.6.2.2 Power Distribution

Relative power distributions within the reactor are quantified in terms of hot channel factors (Reference 22.35). These hot channel factors are normalised ratios of maximal absolute power generation rates and are a measure of the peak pellet power within the reactor core relative to the average pellet (F_Q) and the energy produced in a coolant channel relative to the core average channel ($F_{\Delta H}$). Absolute power generation rates are expressed in terms of quantities related to the nuclear or thermal design; more specifically, volumetric power density (q_{vol}) is the thermal power produced per unit volume of the core.

The **linear heat rate (LHR)** is the thermal power produced per unit length of active fuel (kW/m). Since the fuel assembly geometry is standardised, LHR is the unit of absolute power density most commonly used. For practical purposes, LHR differs from q_{vol} by a constant factor that includes geometry effects and the heat flux deposition fraction. The PLHR is defined as the maximum linear heat rate occurring throughout the reactor. It directly affects fuel temperatures and decay power levels and thus is a significant safety analysis parameter.

The **average linear heat rate (ALHR)** is the total thermal power produced in the fuel rods expressed as heat flux divided by the total active fuel length of the rods in the core.

The **local heat flux** is the heat flux at the surface of the cladding. For nominal rod parameters, this differs from LHR by a constant factor.

The **rod power** is the total power generated in one rod (kW).

The **average rod power** is the total thermal power produced in the fuel rods divided by the number of fuel rods.

The hot channel factors used in the discussion of power distributions in this section are defined below.

The **heat flux hot channel factor (F_Q)** is defined as the maximum local heat flux on the surface of a fuel rod divided by the average fuel rod heat flux, allowing for manufacturing tolerances on fuel pellets and rods.

The **nuclear heat flux hot channel factor (F_Q^N)**, is defined as the maximum local fuel rod linear heat rate divided by the average fuel rod linear heat rate, assuming nominal fuel pellet and rod parameters.

The **engineering heat flux hot channel factor (F_Q^E)**, is the allowance on heat flux required for manufacturing tolerances. The engineering factor allows for local variations in enrichment, pellet density and diameter, BA content, surface area of the fuel rod, and eccentricity of the gap between pellet and clad. Combined statistically, the net effect is a factor of 1.03 to be applied to the fuel rod surface heat flux.

The **nuclear enthalpy rise hot channel factor ($F_{\Delta H}^N$)**, is defined as the ratio of the maximum integrated rod power within the core to the average rod power.

Manufacturing tolerances, hot channel power distribution, and surrounding channel power distributions are treated explicitly in the calculation of the DNBR described in Section 22.7.

It is convenient for the purposes of discussion to define subfactors of F_Q; however, design limits are set in terms of the total peaking factor.

$$F_Q = \text{total peaking factor or heat flux hot channel factor} = \frac{PLHR}{ALHR}$$

Without densification effects:

$$F_Q = F_Q^N \times F_Q^E = F_{XY}^N \times F_Z^N \times F_U^N \times F_Q^E$$

where,

F_U^N = Factor for calculation uncertainty, assumed to be 1.05

F_{XY}^N = Ratio of peak power density to average power density in the horizontal plane of peak local power

F_Z^N = Ratio of the power per unit core height in the horizontal plane of peak local power to the average value of power per unit core height. If the plane of peak local power coincides with the plane of maximum power per unit core height, then F_Z^N is the core average axial peaking factor.

22.6.2.3 Radial Power Distribution

The power shape in horizontal sections of the core at full power is a function of the fuel assembly and BA rod loading patterns, the control rod pattern, and the fuel burnup distribution. Thus, at any time in the cycle, a horizontal section of the core can be characterised as being unrodded or being with control rods. These two situations combined with burnup effects determine the radial power shapes that can exist in the core at full power. Typical first cycle values of $F_{\Delta H}^N$, the nuclear enthalpy rise hot channel factors from BOL to EOL, are given in Table 22-3.

The effects on radial power shapes of power level, xenon, samarium, and moderator density are also considered, but these are quite small. The effect of non-uniform flow distribution is negligible. While radial power distributions in various planes of the core are often illustrated, since the moderator density is directly proportional to enthalpy, the core radial enthalpy rise distribution, as determined by the integral of power up each channel, is of greater interest. Figures 22-22 through 22-27 show typical normalised power density distributions for one-quarter of the core for representative operating conditions. These conditions are as follows:

- Hot full power (HFP) near beginning of life, unrodded, no xenon
- Hot full power near beginning of life, unrodded, equilibrium xenon
- Hot full power near beginning of life, gray bank MA+MB in, equilibrium xenon
- Hot full power near middle of life (MOL), unrodded equilibrium xenon
- Hot full power near end of life, unrodded, equilibrium xenon
- Hot full power near end of life, gray bank MA+MB in, equilibrium xenon

Since the position of the hot channel varies from time to time, a single-reference radial design power distribution is selected for DNB calculations. This reference power distribution is chosen conservatively to concentrate power in one area of the core, minimising the benefits of flow redistribution. Assembly powers are normalised to core average power. The radial power distribution within a fuel rod and its variation with burnup as utilised in thermal calculations and fuel rod design are discussed in Section 22.7.

22.6.2.4 Assembly Power Distribution

For the purpose of illustration, typical rodwise power distributions for the BOL and EOL conditions are given in Figure 22-28 and Figure 22-29, respectively. Since the detailed power distribution surrounding the hot channel varies from time to time, a conservatively flat radial assembly power distribution is assumed in the DNB analysis, described in Section 22.7, with the rod of maximum integrated power artificially raised to the design value of $F^N_{\Delta H}$. Care is taken in the nuclear design of the fuel cycles and operating conditions to confirm that a flatter assembly power distribution does not occur with limiting values of $F^N_{\Delta H}$.

22.6.2.5 Axial Power Distribution

The distribution of power in the axial or vertical direction is largely under the control of the operator through either manual operation of the control rods or the automatic motion of control rods in conjunction with manual operation of the CVS. The automated mode of operation is referred to as MSHIM and discussed in Section 22.6.2.12. The rod control system automatically modulates the insertion of the AO control bank controlling the axial power distribution simultaneous with the MSHIM gray and control rod banks to maintain programmed coolant temperature. Operation of the CVS is initiated manually by the operator to compensate for fuel burnup and maintain the desired MSHIM bank insertion. Nuclear effects that cause variations in the axial power shape include moderator density, Doppler effect on resonance absorption, spatial distribution of xenon, burnup, and axial distribution of fuel enrichment and BA. Automatically controlled variations in total power output and rod motion are also important in determining the axial power shape at any time.

The online core monitoring system provides the operator with detailed power distribution information in both the radial and axial sense, continuously using signals from the fixed in-core detectors. Additional information on the online core monitoring system including the safety claims, arguments, and evidence for the system are provided in Reference 22.96 Signals are also available to the operator from the ex-core ion chambers, which are long ion

chambers outside the reactor vessel running parallel to the axis of the core. Separate signals are taken from each ion chamber, then processed and calibrated against the in-core measurements such that an indication of the power in the top of the core less the power in the bottom of the core is derived. The calibrated difference in power between the core top and bottom halves, called the flux difference (ΔI), is derived for each of the four channels of ex-core detectors and is displayed on the control panel. The principal use of the flux difference is to provide the shape penalty function to the OTΔT DNB protection and the OPΔT protection.

22.6.2.6 Local Power Peaking

Fuel densification occurred early in the evolution of PWR fuel manufacture under irradiation in several operating reactors, causing the fuel pellets to shrink both axially and radially. The pellet shrinkage combined with random hang up of fuel pellets resulted in gaps in the fuel column when the pellets below the hung-up pellet settled in the fuel rod. The gaps varied in length and location in the fuel rod. Because of decreased neutron absorption in the vicinity of the gap, power peaking occurs in the adjacent fuel rods, resulting in an increased power peaking factor. A quantitative measure of this local peaking is given by the power spike factor S(Z), where Z is the axial location in the core (References 22.27 and 22.37).

Modern PWR fuel manufacturing practices have essentially eliminated significant fuel densification impact on reactor design and operation. It has since been concluded and accepted that a densification power spike factor of 1.0 is appropriate for Westinghouse fuel (Reference 22.28).

22.6.2.7 Limiting Power Distribution

High-Frequency, Low Consequence (HFLC) faults are those expected frequently or regularly in the course of power operation, maintenance, or manoeuvring of the plant (refer to Chapter 8 for a list of these faults). As such, HFLC faults are accommodated with margin between any plant parameter and the value of that parameter, which would require either automatic or manual protective action. HFLC faults are considered from the point of view of affecting the consequences of fault conditions. Analysis of each fault condition described is based on a conservative set of corresponding initial conditions.

The list of steady-state and shutdown conditions, permissible deviations, and operational transients is given in Chapter 9. Implicit in the definition of normal operation is proper and timely action by the reactor operator; that is, the operator follows recommended operating procedures for maintaining appropriate power distributions and takes any necessary remedial actions when alerted to do so by the plant instrumentation.

The analysis to support the online monitoring system evaluates the consequences of limiting power distributions based upon the conditions prevalent in the reactor at the current time. Operating space evaluations performed by the online monitoring system include the most limiting power distributions that can be generated by inappropriate operator or control system actions given the current core power level, xenon distribution, MSHIM or AO bank insertion, and core burnup. Thus, as stated, the worst or limiting power distribution that can occur during normal operation is considered as the starting point for analysis of faults.

Improper procedural actions or errors by the operator are assumed in the design as frequent faults. The limiting power shapes that result from frequent fault occurrences are those power distributions that deviate from the normal operating condition within the allowable operating space as defined in the core operating limits; e.g., because of lack of proper action by the

operator during a xenon transient following a change in power level brought about by control rod motion. Power distributions that fall in this category are used for determining the reactor protection system setpoints to maintain margin to overpower or DNB limits.

The means for maintaining power distributions within the required absolute power generation limits are described in the Technical Specifications (Tech Specs). The online core monitoring system provides the operator with the current allowable operating space, detailed current power distribution information, thermal margin assessment, and operational recommendations to manage and maintain required thermal margins. As such, the online monitoring system provides the primary means of managing and maintaining required operating thermal margins during normal operation. Additional information on the online core monitoring system including the safety claims, arguments, and evidence for the system are provided in Reference 22.96. The axial flux difference and quadrant power tilt ratio (QPTR) limits defined in the Technical specifications provide additional confirmation of acceptable margin during normal operation.

In the unlikely event that the online monitoring system is out of service, power distribution controls based on bounding, precalculated analysis are also provided to the operator such that the online monitoring system is not a required element for short-term reactor operation. Limits are placed on the axial flux difference so that the heat flux hot channel factor F_Q is maintained within acceptable limits. A discussion of pre-calculated power distribution control in Westinghouse PWRs is included in Reference 22.39. Detailed background information on the design constraints on local power density in a Westinghouse PWR, on the defined operating procedures, and on the measures taken to preclude exceeding design limits is presented in Reference 22.40. The following paragraphs summarise this report and describe the calculations used to establish the upper bound on peaking factors.

The calculations used to establish the upper bound on peaking factors, F_Q and $F_{\Delta H}^N$, include the nuclear effects that influence the radial and axial power distributions throughout core life for various modes of operation, including load follow, reduced power operation, and axial xenon transients. As described above, the online core monitoring system provides a means for monitoring of the peaking factors directly during operation to confirm that they remain below the acceptable levels defined in the Tech Specs.

Power distributions are calculated for the full-power condition. Fuel and moderator temperature feedback effects are included within these calculations in each spatial dimension. The steady-state nuclear design calculations are done for normal flow with the same mass flow in each channel and flow redistribution effects neglected. The effect of flow redistribution is calculated explicitly where it is important in the DNB analysis of accidents. The effect of xenon on radial power distribution is small (compare Figures 22-22 and 22-23) but is included as part of the normal design process.

The core axial profile can experience significant changes that occur rapidly as a result of rod motion and load changes and more slowly due to xenon distribution. Several thousand cases are examined for the study of points of closest approach to thermal margin limits. Since the properties of the nuclear design dictate what axial shapes can occur, boundaries on the limits of interest can be set in terms of the parameters readily observed on the plant. Specifically, the nuclear design parameters significant to the axial power distribution analysis are as follows:

- Core power level
- Core height
- Coolant temperature and flow

- Coolant temperature programme as a function of reactor power
- Fuel cycle lifetimes
- Rod bank worth
- Rod bank overlaps

Normal operation of the plant assumes compliance with the following conditions:

- Control rods in a single bank move together with no individual rod insertion differing from the bank demand position by more than the number of steps identified in the Tech Specs.
- Control banks are sequenced with overlapping banks.
- The control bank insertion limits are not violated.
- Axial power distribution control procedures, which are given in terms of flux difference control and control bank position, are observed.

The axial power distribution procedures referred to above are part of the required operating procedures followed in normal operation with the online monitoring system out of service. In service, the online core monitoring system provides continuous indication of power distribution, SDM, and margin-to-design limits.

The relaxed axial offset control (RAOC) procedures were developed to provide wide control band widths and, consequently, more operating flexibility (Reference 22.41). These wide operating limits, particularly at lower power levels, increase plant availability by allowing quicker plant startup and increased manoeuvring flexibility without trip.

This procedure has been modified to accommodate MSHIM operation in the AP1000 plant. It is applied to analysis of axial power distributions under MSHIM control for the purpose of defining the allowed normal operating space such that thermal margin limits are maintained and frequent fault occurrences are adequately protected by the reactor protection system when the online monitoring system is out of service.

The purpose of this analysis is to find the widest permissible ΔI versus power operating space by analysing a wide range of achievable xenon distributions, MSHIM/ axial offset (AO) bank insertion, and power level.

The bounding analyses performed offline in anticipation of the online monitoring system being out of service are similar to those based on the RAOC analysis, which uses a xenon reconstruction model (Reference 22.41). This is a practical method used to define the power operating space allowed with MSHIM operation. Each resulting power shape is analysed to determine if LOCA constraints are met or exceeded.

The online monitoring system evaluates the effects of radial xenon distribution changes due to operational parameter changes continuously and therefore eliminates the need for overly conservative bounding evaluations when the system is available. The calculated values have been increased by a factor of 1.05 for method uncertainty and a factor of 1.03 for the engineering factor F_Q^E.

The envelope drawn in Figure 22-30 represents an upper bound envelope on local power density versus elevation in the core. This envelope is a conservative representation of the bounding values of local power density.

The online monitoring system measures the core condition continuously and evaluates the thermal margin condition directly in terms of PLHR and margin to DNB limitations directly.

Allowing for fuel densification effects, the average linear power at 3400 MW is 18.76 kW/m (5.72 kW/ft). The conservative upper bound value of normalised local power density, including uncertainty allowances, is 2.60 corresponding to a PLHR of 49.26 kW/m (15.0 kW/ft) for each core elevation at 101 percent power.

To determine reactor protection system setpoints with respect to power distributions, three categories of events are considered: rod control equipment malfunctions and operator errors of commission or omission. In evaluating these three categories, the core is assumed to be operating within the four constraints described above.

The first category comprises uncontrolled rod withdrawal (with rods moving in the normal bank sequence) for both AO and MSHIM banks. Also included are motions of the AO and MSHIM banks below their insertion limits, which could be caused, for example, by uncontrolled dilution or primary coolant cooldown. Power distributions are calculated throughout these occurrences, assuming short-term corrective action; that is, no transient xenon effects are considered to result from the malfunction. The event is assumed to occur from typical normal operating situations, which include normal xenon transients. It is further assumed in determining the power distributions that total core power level would be limited by reactor trip to below the overpower protection setpoint of nominally 118 percent rated thermal power (RTP). Since the study is to determine protection limits with respect to power and AO, no credit is taken for OTΔT or OPΔT trip setpoint reduction due to flux difference. The peak power density that can occur in such events, assuming reactor trip at or below 118 percent, is less than that required for fuel centreline melt, including uncertainties and densification effects.

The second category assumes that the operator mispositions the AO and/or MSHIM rod banks in violation of the insertion limits and creates short-term conditions not included in normal operating conditions.

The third category assumes that the operator fails to take action to correct a power distribution limit violation (such as boration and dilution transient) assuming automatic operation of the rod control system, which will maintain constant reactor power.

For each of the above categories, the trip setpoints are designed so as not to exceed fuel centreline melt criteria as well as fuel mechanical design criteria.

The appropriate hot channel factors F_Q and $F^N_{\Delta H}$ for peak local power density and for DNB analysis at full power are based on analyses of possible operating power shapes and are addressed in the Tech Specs. The methodology for the power shape analysis is described in Reference 22.41. The maximum allowable F_Q can be increased with decreasing power. Increasing $F^N_{\Delta H}$ with decreasing power is permitted by the DNB protection setpoints and allows radial power shape changes with rod insertion to the insertion limits. The allowance for the increased $F^N_{\Delta H}$ permitted is addressed in the Tech Specs.

This becomes a design basis criterion used for establishing acceptable control rod patterns and control bank sequencing. Likewise, fuel loading patterns for each cycle are selected with consideration of this design criterion. The worst values of $F^N_{\Delta H}$ for possible rod configurations occurring in normal operation are used in verifying that this criterion is met.

The worst values generally occur when the rods are assumed to be at their insertion limits. Operation with rod positions above the allowed insertion limits provides increased margin to

the $F^N_{\Delta H}$ criterion. It has been determined that the Tech Specs' limits are met, provided the above conditions are observed (Reference 22.42). These limits are taken as input to the thermal-hydraulic DB as described in Section 22.7.

In normal operation, when a situation could result in local power densities in excess of those assumed as the precondition for a subsequent hypothetical accident but would not itself cause fuel failure, administrative controls and alarms are provided for returning the core to a safe condition.

The independence of the various individual uncertainties constituting the uncertainty factor on F_Q enables the uncertainty (F^U_Q) to be calculated by statistically combining the individual uncertainties on the limiting rod. The standard deviation of the resultant distribution of F^U_Q is determined by taking the square root of the sum of the variances of each of the contributing distributions (Reference 22.35). The values for F^E_Q and F^N_U are 1.03 and 1.05, respectively. The value for the rod bow factor, F^B_Q, is 1.056, which accounts for the maximum F_Q penalty as a function of burnup due to rod bow effects.

22.6.2.8 Experimental Verification of Power Distribution Analysis

This subject is discussed in References 22.35 and 22.43. A summary of these reports and the extension to include the fixed in-core instrumentation system is given below. Power-distribution-related measurements are incorporated into the evaluation of calculated power distribution information using the in-core instrumentation processing algorithms contained within the online monitoring system.

The processing algorithms contained within the online monitoring system are functionally identical to those historically used for the evaluation of power distribution measurements in Westinghouse PWRs. Advances in technology allow a complete functional integration of reaction rate measurement algorithms and the expected reaction rate predictive capability within the same software package. The predictive software integrated within the online monitoring system supplies accurate, detailed information about current reactor conditions (Reference 22.43).

The measured versus calculation comparison is performed continuously by the online monitoring system throughout the core life. The online monitoring system operability requirements are specified in the Tech Specs.

In a measurement of the reactor power distribution and the associated thermal margin limiting parameters, with the in-core instrumentation system, the following uncertainties must be considered:

1. Reproducibility of the measured signal

2. Errors in the calculated relationship between detector current and local power generation within the fuel bundle

3. Errors in the detector current associated with the depletion of the emitter material, manufacturing tolerances, and measured detector depletion

4. Errors due to the inference of power generation some distance from the measurement thimble.

The appropriate allowance for Category A has been accounted for through the imposition of strict manufacturing tolerances for the individual detectors. This approach is accepted industry practice and has been used in PWRs with fixed in-core instrumentation worldwide.

Errors in Category B are quantified by calculation and evaluation of critical experiment data on arrays of rods with simulated guide thimbles, control rods, and BAs. These critical experiments provide the quantification of errors of categories A and D.

Errors in Category C have been quantified through direct experimental measurement of the depletion characteristics of the detectors being used, including the precision of the in-core instrumentation system's measurement of the current detector depletion. The description of the experimental measurement of detector depletion can be found in Reference 22.38.

Critical experiments have been performed at the Westinghouse Reactor Evaluation Centre and measurements have been taken on two Westinghouse plants with movable fission chamber in-core instrumentation systems (Reference 22.35). The measurement aspects of the movable fission chamber share the previous uncertainty categories less Category C, which is independent of the other sources of uncertainty. It is concluded that the uncertainty associated with PLHR ($F_Q \cdot P$) is less than 5 percent at the 95 percent confidence level with only 5 percent of the measurements greater than the inferred value.

In comparing measured power distributions (or detector currents) with calculations for the same operating conditions, it is not possible to isolate the detector reproducibility. Thus, a comparison between measured and predicted power distributions includes some measurement error. Such comparisons are given in Reference 22.35. Since the first publication of Reference 22.35, hundreds of measurements have been taken on reactors all over the world. These results confirm the adequacy of the 5 percent uncertainty allowance on the calculated PLHR ($ALHR \cdot F_Q \cdot P$).

A similar analysis for the uncertainty in hot rod integrated power ($F_{\Delta H} \cdot P$) measurements results in an allowance of 4 percent at the equivalent of a 95 percent confidence level.

A measurement in the fourth cycle of a 157-assembly, 3.66-m (12 foot) core is compared with a simplified 1-D core average axial calculation in Figure 22-22. This calculation does not give explicit representation of the fuel grids.

The accumulated data on power distributions in actual operation are basically of three types:

- Much of the data is obtained in steady-state operation at constant power in the normal operating configuration

- Data with unusual values of AO are obtained as part of the ex-core detector calibration exercise performed monthly

- Special tests performed in load follow and other transient xenon conditions that have yielded useful information on power distributions

These data are presented in detail in Reference 22.42.

22.6.2.9 Testing

A series of physics tests are planned to be performed on the first core. These tests and the criteria for satisfactory results are described in Chapter 7. Since not all limiting situations can be created at BOL, the main purpose of the tests is to provide a check on the calculation methods used in the predictions for the conditions of the test. Tests performed at the beginning of each reload cycle are limited to verification of the selected safety-related parameters of the reload design.

22.6.2.10 Monitoring Instrumentation

The adequacy of instrument numbers, spatial deployment, required correlations between readings and peaking factors, calibration, and errors are described in Reference 22.43. The core monitoring system, utilising signals from the fixed in-core detectors, allows for an online measurement of the 3-D power distribution and core reactivity condition and an accurate assessment of available margins to reactor thermal and shutdown reactivity limits (PLHR, DNBR, and SDM).

The online core monitoring system also incorporates features that allow for the analysis and prediction of core behaviour. The margin to actual reactor operational thermal and shutdown reactivity limits is monitored using the same 3-D nodal and thermal hydraulic methods of the Westinghouse codes licensed for core design and safety analysis.

The online 3D monitoring licensed for control room Tech Spec power distribution surveillance provides many benefits over traditional core monitoring, including the following:

- Direct continuous monitoring of DNB, PLHR, and nuclear hot channel or nuclear enthalpy rise hot channel factors

- Direct monitoring of margin results in a Tech Spec so that there is a continuous display of the minimum margin available in any of the monitored parameters (PLHR, nuclear hot channel power, and DNBR).

- In addition, online confirmation of SDM and some associated relaxation of rod insertion limits is also provided.

Additional information on the online core monitoring system including the safety claims, arguments, and evidence for the system are provided in Reference 22.96.

Provided that the limitations on rod insertion and flux difference are observed, the in-core and ex-core detector systems provide adequate monitoring of power distributions when the online monitoring system is out of service. Further details about specific limits on the observed rod positions and flux difference, along with a discussion of their bases, are given in the Tech Specs. Limits for alarms and reactor trip are also given in the Tech Specs.

22.6.2.11 Reactivity Coefficients

The kinetic characteristics of the reactor core determine its response to changing plant conditions or to operator adjustments made during normal operation, as well as its response during abnormal or accidental transients. These kinetic characteristics are quantified in reactivity coefficients.

The reactivity coefficients reflect the changes in the neutron multiplication due to varying plant conditions, such as thermal power, moderator and fuel temperatures, coolant pressure, or void conditions. Since reactivity coefficients change during the life of the core, ranges of coefficients are employed in transient analysis to determine the response of the plant throughout life. The results of such simulations and the reactivity coefficients used are presented in Chapter 9. The reactivity coefficients used in transient simulations are summarized in the Safety Analysis Checklist (SAC) (Reference 22.99). The reactivity coefficient limits are divided between those used for the standard safety case and those used for the diverse ATWT case. The latter set of limits are calculated based on better estimate assumptions consistent with analysis of the ATWT case.

The reactivity coefficients are calculated with approved nuclear methods. The analytical methods and calculation models are provided in Section 22.6.3. The effect of the radial and axial power distribution on core average reactivity coefficients is not significant under normal operating conditions. For example, a skewed axial xenon distribution that results in changing AO by 5 percent typically changes the moderator and Doppler temperature coefficients by less than 0.018 pcm/°C (0.01 pcm/°F). An artificially skewed radial xenon distribution that results in changing the radial $F^N_{\Delta H}$ by 3 percent typically changes the moderator and Doppler temperature coefficients by less than 0.054 pcm/°C (0.03 pcm/°F) and 0.0018 pcm/°C (0.001 pcm/°F), respectively. The spatial effects are accentuated in some transient conditions, for example, in postulated rupture of the main steam line and rupture of an RCCA mechanism housing.

The analytical methods and calculation models used in calculating the reactivity coefficients are given in Section 22.6.3. These models have been confirmed through extensive qualification efforts performed for core and lattice designs.

Quantitative information is given below for calculated reactivity coefficients including fuel-Doppler coefficient, moderator coefficients (density, temperature, pressure, and void), and power coefficient.

a) Fuel Temperature (Doppler) Coefficient

The fuel temperature (Doppler) coefficient is defined as the change in reactivity per degree change in effective fuel temperature and is primarily a measure of the Doppler broadening of U-238 and Pu-240 resonance absorption peaks. Doppler broadening of other isotopes is also considered but their contribution to the Doppler effect is small. An increase in fuel temperature increases the effective resonance absorption cross-sections of the fuel and produces a corresponding reduction in reactivity.

The fuel temperature coefficient is calculated using approved nuclear methods. The moderator temperature is held constant and the power level is varied. Spatial variation of fuel temperature is taken into account by calculating the effective fuel temperature as a function of power density.

A typical Doppler temperature coefficient is shown in Figure 22-32 as a function of the effective fuel temperature (at BOL and EOL conditions). The effective fuel temperature is lower than the volume-averaged fuel temperature since the neutron flux distribution is non-uniform through the pellet and gives preferential weight to the surface temperature.

A typical Doppler-only contribution to the power coefficient, defined later, is shown in Figure 22-33 as a function of relative core power. The integral of the differential curve in Figure 22-33 is the Doppler contribution to the power defect and is shown in

Figure 22-34 as a function of relative power. The Doppler temperature coefficient becomes more negative as a function of life as the Pu-240 content increases, thus increasing the Pu-240 resonance absorption. The upper and lower limits of Doppler coefficient used in accident analyses are given in Chapter 9.

b) Moderator Coefficients

The moderator coefficient is a measure of the change in reactivity due to a change in specific coolant parameters, such as density/temperature, pressure, or void.

The moderator temperature (density) coefficient is defined as the change in reactivity per degree change in the moderator temperature. Generally, the effects of the changes in moderator density and the temperature are considered together.

The soluble boron used in the reactor as a means of reactivity control also has a secondary effect on the moderator density coefficient, since the soluble boron density and the water density are decreased when the coolant temperature rises. A decrease in the soluble boron density introduces a positive component in the moderator coefficient. If the concentration of soluble boron is large enough, the net value of the coefficient may be positive.

The initial core hot boron concentration is sufficiently low that the moderator temperature coefficient is negative at operating temperatures with the BA loading specified. Discrete or IFBA rods can be used in reload cores to confirm that the moderator temperature coefficient is negative over the range of power operation. The effect of control rods is to make the moderator coefficient more negative, since the thermal neutron mean free path, and hence the volume affected by the control rods, increases with an increase in temperature.

With burnup, the moderator coefficient becomes more negative, primarily as a result of boric acid dilution but also to a significant extent from the effects of the buildup of plutonium and fission products. In the first few months of a cycle, however, the moderator coefficient can become less negative as the BA is depleted and core reactivity and soluble boron concentration increases. The moderator temperature coefficient is maintained at a negative value during power operation.

The moderator coefficient is calculated for a range of plant conditions by performing two group two- or 3-D calculations, in which the moderator temperature is varied by about ±2.8°C (5°F) around each of the mean temperatures, resulting in density changes consistent with the temperature change.

The moderator temperature coefficient is shown as a function of core temperature and boron concentration for the core in Figure 22-35 to Figure 22-37. The temperature range covered is from cold (about 21.1°C(68°F)) to about 287.8°C (550°F). The contribution due to Doppler coefficient (because of change in moderator temperature) has been subtracted from these results.

Figure 22-38 shows the unrodded, hot, full-power MTC plotted as a function of burnup for the initial cycle. The temperature coefficient corresponds to the unrodded critical boron concentration present at hot full-power operating conditions.

The moderator coefficients presented here are calculated to describe the core behaviour in normal and accident situations when the moderator temperature changes can be considered to affect the entire core.

The moderator pressure coefficient relates the change in moderator density resulting from a reactor coolant pressure change to the corresponding effect on neutron production. This coefficient is much less significant than the MTC because pressure changes have a much smaller effect on the moderator density over the normal range of operation in a PWR. This is due to the relative incompressibility of liquid water under high pressure. A change of 0.345 MPa (50 psi) in pressure has approximately the same effect on reactivity as a 0.28ºC (0.5°F) change in moderator temperature. This coefficient can be determined from the MTC by relating change in pressure to the corresponding change in density. The typical moderator pressure coefficient may be negative over a portion of the moderator temperature range at BOL (-0.58 pcm/MPa) (-0.004 pcm/psi) but is always positive at operating conditions and becomes more positive during life (+43.5 pcm/MPa (+0.3 pcm/psi) at EOL).

The moderator void coefficient relates the change in neutron multiplication to the presence of voids in the moderator. In a PWR, this coefficient is not very significant because of the low void content in the coolant. The core void content is less than one-half of one percent and is due to local or statistical boiling. The typical void coefficient varies from 50 pcm/percent void at BOL and at low temperatures to -250 pcm/percent void at EOL and at operating temperatures. The void coefficient is always negative during power operation and becomes more negative with fuel burnup.

c) Power Coefficient

The combined effect of moderator temperature and fuel temperature change as the core power level changes is called the total power coefficient and is expressed in terms of reactivity change per percent power change. Since a 3-D calculation is performed in determining total power coefficients and total power defects, the axial redistribution reactivity component is implicitly included. A typical power coefficient at BOL and EOL conditions is given in Figure 22-39. The total power coefficient becomes more negative with burnup, reflecting the combined effect of moderator and fuel temperature coefficients with burnup. The power defect (integral reactivity effect) at BOL and EOL is given in Figure 22-40.

d) Reactivity Coefficients Used in Transient Analysis

Table 22-3 gives the limiting values as well as typical best-estimate values for the reactivity coefficients for the initial cycle. The limiting values are used as design limits in the standard safety case transient analysis. The exact values of the coefficient used in the analysis depend on whether the transient of interest is examined at the BOL or EOL, whether the most negative or the most positive (least negative) coefficients are appropriate, and whether spatial non-uniformity must be considered in the analysis. Conservative values of coefficients, considering various aspects of analysis, are used in the transient analysis. This is described in Chapter 9.

The reactivity coefficients used in transient simulations are summarized in the Safety Analysis Checklist (SAC) (Reference 22.99). The reactivity coefficient limits are divided between those used for the standard safety case and those used for the diverse ATWT case. The latter set of limits are calculated based on better estimate assumptions consistent with analysis of the ATWT case.

The reactivity coefficients shown in Figure 22-32 to Figure 22-40 are typical best-estimate values calculated for the initial cycle. Limiting values are chosen to encompass the best-estimate reactivity coefficients, including the uncertainties over appropriate operating conditions. The most positive, as well as the most negative, values are selected to form the DB range used in the transient analysis.

In many instances, the most conservative combination of reactivity coefficients is used in the transient analysis even though the extreme coefficients assumed may not simultaneously occur at the conditions assumed in the analysis. The need for a re-evaluation of any accident in a subsequent cycle is contingent upon whether the coefficients for that cycle fall within the identified range used in the analysis presented in Chapter 9 with due allowance for the calculation uncertainties.

Section 22.6.3 describes the comparison of calculated and experimental reactivity coefficients in detail. Experimental evaluation of the reactivity coefficients will be performed during the physics startup tests described in Chapter 7.

22.6.2.12 Shutdown Requirements and Reactivity Control

22.6.2.12.1 Shutdown Requirements

To establish the required shutdown margin stated in the COLR under conditions where a cooldown to ambient temperature is required, concentrated soluble boron is added to the coolant. Boron concentrations for several core conditions are listed in Table 22-3 for the initial cycle. For core conditions including refuelling, the boron concentration is well below the solubility limit. The rod cluster control assemblies are employed to bring the reactor to the shutdown condition. The minimum required shutdown margin is given in the COLR.

The ability to meet the shutdown margin requirements for hot conditions is demonstrated for the initial cycle and for an equilibrium reload cycle by performing a bounding calculation, the results of which are shown in Table 22-4. Table 22-4 compares the difference between the rod cluster control assembly reactivity available with an allowance for the worst stuck rod with that required for control and protection purposes. The shutdown margin includes an allowance of seven percent for analytic uncertainties which assumes the use of silver-indium-cadmium rod cluster control assemblies. Use of a seven percent uncertainty allowance on rod cluster control assembly worth is discussed and shown to be acceptable in Reference 22.45. The largest reactivity control requirement appears at the EOL when the moderator temperature coefficient reaches its peak negative value as reflected in the larger power defect.

Any available negative reactivity insertion from withdrawn tungsten GRCAs is conservatively excluded when determining the available shutdown margin at hot operating conditions, even though all GRCAs are released into the core on a reactor trip (Reference 22.36). Only silver-indium-cadmium control rods are assumed to insert when the reactor is tripped for purposes of demonstrating that adequate shutdown margin is available at hot operating conditions. As such, the use of a seven percent uncertainty allowance for the credited trip rod worth remains appropriate in Table 22-4. After the reactor is brought to a shutdown condition, the presence of GRCAs which are confirmed to be inserted and which have met the applicable physics testing acceptance criteria may be credited in confirming that the required shutdown margin is maintained during any cooldown period and as the result of long term xenon decay (Reference 22.36).

During plant operation, the available shutdown margin for hot operating conditions is continuously confirmed by the online monitoring system, by comparing the operating soluble boron concentration at current core conditions to the shutdown boron concentration that would be required immediately following a reactor trip from those conditions. Additional information on the online core monitoring system including the safety claims, arguments, and evidence for the system are provided in Reference 22.96. The required shutdown boron concentration used in this type of calculation is conservatively determined at the target shutdown reactivity condition, assuming that all control rods insert except for the 16 tungsten GRCAs and the highest worth silver-indium-cadmium RCCA.

The control rods are required to provide sufficient reactivity to account for the power defect from full power to zero power and to provide the required shutdown margin. The reactivity addition resulting from power reduction consists of contributions from Doppler effect, moderator temperature, flux redistribution, and reduction in void content as discussed below.

Doppler Effect

The Doppler effect arises from the broadening of U-238 and Pu-240 resonance cross-sections with an increase in effective pellet temperature. This effect is most noticeable over the range of zero power to full power due to the large pellet temperature increase with power generation. The Doppler effect is implicitly included in the total power defects shown in Table 22-4.

Variable Average Moderator Temperature

When the core is shut down to the hot zero-power condition, the average moderator temperature changes from the equilibrium full-load value determined by the steam generator and turbine characteristics (such as steam pressure, heat transfer, tube fouling) to the equilibrium no-load value, which is based on the steam generator shell side design pressure. The design change in temperature is conservatively increased to account for the control system dead band and measurement errors.

When the moderator coefficient is negative, there is a reactivity addition with power reduction. The moderator coefficient becomes more negative as the fuel depletes because the boron concentration is reduced. This effect is the major contributor to the increased requirement at EOL. The change in average moderator temperature is implicitly included in the total power defects shown in Table 22-4.

Redistribution

During full-power operation, the coolant density decreases with core height. This, together with partial insertion of control rods, results in less fuel depletion near the top of the core. Under steady-state conditions, the relative power distribution will be slightly asymmetric toward the bottom of the core. On the other hand, at hot zero-power conditions, the coolant density is uniform up the core, and there is no flattening due to Doppler effect. The result will be a flux distribution which at zero power can be skewed toward the top of the core. Since a three-dimensional calculation is performed in determining total power defect, flux redistribution is implicitly included in this calculation. The three-dimensional total power defects specified in Table 22-4 were calculated including the use of a conservatively skewed adverse axial xenon distribution which increases the redistribution effect.

Void Content

A small void content in the core is due to nucleate boiling at full power. The void collapse coincident with power reduction makes a small positive reactivity contribution which has been added to the calculated total power defects shown in Table 22-4.

Rod Insertion Allowance

The MSHIM and AO banks are operated within a prescribed band of travel to compensate for changes in temperature and axial offset which are caused by fuel depletion and power manoeuvres. In calculating the available shutdown margin at hot operating conditions, the pre-trip control rod insertion can affect both the available trip rod worth and the total power defect control requirements. In addition, since the tungsten GRCAs are assumed not to insert on a reactor trip (Reference 22.36), the initial gray rod positions assumed prior to the trip can also have a small effect on the worth of the silver-indium-cadmium control rods that insert after the trip. In the bounding calculations shown in Table 22-4, the effect of the most limiting allowed control rod insertion is implicitly included in the calculated trip rod worth and total power defect values reported in the table. The most limiting allowed control rod insertion was determined by performing a series of three-dimensional shutdown margin calculations over the range of allowed control rod motion, and selecting the conditions which resulted in the minimum calculated shutdown margin.

Installed Excess Reactivity for Depletion

Excess reactivity is installed at the beginning of each cycle to provide sufficient reactivity to compensate for fuel depletion and fission product buildup throughout the cycle. This reactivity is controlled by the addition of soluble boron to the coolant, control rod insertion, and by burnable absorbers when necessary. The soluble boron concentration for several core configurations and the unit boron worth are given in Table 22-3 for the initial cycle. Since the excess reactivity for burnup is balanced during operation by negative reactivity from the above sources, it is not included in control rod requirements.

Xenon and Samarium Poisoning

Changes in xenon and samarium concentrations in the core occur at a sufficiently slow rate, even following rapid power level changes, so that the resulting reactivity change can be controlled by changing the gray and/or control rod insertion.

pH Effects

Changes in reactivity due to a change in coolant pH, if any, are sufficiently small in magnitude and occur slowly enough to be controlled by the boron system (Reference 22.44).

22.6.2.12.2 Reactivity Control

Core reactivity is controlled by means of a chemical poison dissolved in the coolant, rod cluster control assemblies, gray rod cluster assemblies and burnable absorbers as described below.

Chemical Shim

Boron in solution as boric acid is used to control relatively slow reactivity changes associated with:

- The moderator temperature defect in going from cold shutdown at ambient temperature to the hot operating temperature at zero power
- Transient xenon and samarium reactivity effects, following power changes
- The reactivity effects of fissile inventory depletion and buildup of long-life fission products
- The depletion of the burnable absorbers

The boron concentrations for various core conditions are presented in Table 22-3 for the initial cycle.

Rod Cluster Control Assemblies

The number of rod cluster control assemblies is given in Table 22-2. The rod cluster control assemblies are used for shutdown and control purposes to offset fast reactivity changes associated with:

- The required shutdown margin in the hot zero power, stuck rod condition
- The reactivity compensation as a result of an increase in power above hot zero power (power defect, including Doppler and moderator reactivity changes)
- Unprogrammed fluctuations in boron concentration, coolant temperature, or xenon concentration (with rods not exceeding the allowable rod insertion limits)
- Reactivity changes resulting from load changes

The allowed control bank reactivity insertion is limited at full power to maintain shutdown capability. As the power level is reduced, control rod reactivity requirements are also reduced, and more rod insertion is allowed. The control bank position is monitored, and the operator is notified by an alarm if the limit is approached. The determination of the insertion limit uses conservative xenon distributions and axial power shapes. In addition, the rod cluster control assembly withdrawal pattern determined from the analyses is used in determining power distribution factors and in determining the maximum worth of an inserted rod cluster control assembly ejection accident. For further discussion, refer to the technical specifications on rod insertion limits.

Power distribution, rod ejection, and rod misalignment analyses are based on the arrangement of the shutdown and control groups of the rod cluster control assemblies shown in Figure 22-41. Shutdown rod cluster control assemblies are withdrawn before withdrawal of the control and AO banks is initiated. The approach to critical is initiated by using the chemical and volume control system to establish an appropriate boron concentration based upon the estimated critical condition then withdrawing the AO bank above the zero power insertion limit and finally withdrawing the control banks sequentially. The limits of rod insertion and further discussion on the basis for rod insertion limits are provided in the COLR.

Gray Rod Cluster Assemblies

The rod cluster control assembly control banks include four gray rod banks consisting of gray rod cluster assemblies (GRCAs). Gray rod cluster assemblies consist of 24 rodlets fastened at the top end to a common hub or spider. Geometrically, it is the same as an RCCA except that the GRCA design uses tungsten encapsulated in an Alloy 718 sleeve as an absorber. The term gray rod refers to the reduced reactivity worth relative to that of an RCCA consisting of 24 silver-indium-cadmium rodlets. The GRCAs are used in base load operation and load follow maneuvering and provide a mechanical shim reactivity mechanism which reduces the need for changes to the concentration of soluble boron (that is, chemical shim).

Burnable Absorbers

Discrete burnable absorber rods and integral fuel burnable absorber rods will be used to provide partial control of the excess reactivity available during the first operating cycle. In doing so, the burnable absorber loading controls peaking factors and prevents the moderator temperature coefficient from being positive at normal operating conditions. The burnable absorbers perform this function by reducing the requirement for soluble boron in the moderator at the beginning of the fuel cycle. For purposes of illustration, the initial cycle burnable absorber pattern is shown in Figure 22-21. Figures 22-19 and 22-20 show the burnable absorber distribution within a fuel assembly for several burnable absorber patterns used in the 17 x 17 array. The boron in the rods is depleted with burnup but at a slow rate so that the peaking factor limits are not exceeded and the resulting critical concentration of soluble boron is such that the moderator temperature coefficient remains within the limits stated above for power operating conditions.

Peak Xenon Startup

Compensation for the peak xenon buildup may be accomplished using the boron control system. Startup from the peak xenon condition is accomplished with a combination of rod motion and boron dilution. The boron dilution can be made at any time, including during the shutdown period, provided the shutdown margin is maintained.

Load Follow Control and Xenon Control

During load follow manoeuvres, power changes are primarily accomplished using control rod motion alone, as required. Control rod motion is limited by the control rod insertion limits as provided in the COLR. The power distribution is maintained within acceptable limits through limitations on control rod insertion. Reactivity changes due to the changing xenon concentration are also controlled by rod motion. The soluble boron concentration may also be changed during large load change manoeuvres or during extended reduced power operation to maintain the control rods in a more optimum range for power distribution control.

Rapid power increases (five percent/min) from part power during load follow operation are accomplished with rod motion.

The rod control system is designed to automatically provide the power and temperature control described above 30 percent rated power for most of the cycle length without the need to change boron concentration as a result of the load manoeuvre. The automated mode of operation is referred to as MSHIM because of the usage of mechanical means to control reactivity and power distribution simultaneously. MSHIM operation allows load manoeuvring without boron change because of the degree of allowed insertion of the control banks in conjunction with the independent power distribution control of the AO control bank. The worth and overlap of the MA, MB, MC, MD, M1, and M2 control banks are designed

such that their movement will not result in drastic fluctuations in AO. The AO control bank insertion limit versus power level is designed such that AO bank insertion will always result in a monotonically decreasing axial offset; the AO bank cannot be inserted to the point of concentrating the neutron flux to the bottom of the core such that further AO bank insertion results in the flux suddenly shifting towards the top of the core. MSHIM operation uses the MA, MB, MC, MD, M1, and M2 control banks to maintain the programmed coolant average temperature throughout the operating power range. The AO control bank is independently modulated by the rod control system to maintain a nearly constant axial offset throughout the operating power range.

While the primary means for controlling the coolant average temperature is the M banks, the movement of the AO bank also results in some adjustment of coolant temperature. In the event that both the M and AO banks are demanded to move in the same direction the M banks will be paused to allow the AO bank to adjust AO and coolant temperature. Should the M and AO banks be demanded to move in opposite directions, the movement of the M banks are moved to their demand position at an accelerated rate to restore the coolant average temperature quickly and then the AO bank is moved. This provides efficient management of both coolant average temperature and AO. The target axial offset used during MSHIM operation is established at a more negative value than the axial offset associated with the all rods out condition. The negative bias is necessary to maintain both positive and negative axial offset control effectiveness by the AO-bank. Operation with gray control rod banks (MA, MB, MC, and MD) inserted has less of an effect on the core axial power distribution than insertion of the black control rods banks (M1 and M2) and results in a smaller negative bias in the target axial offset. Load change operations that are large enough to require a black control rod bank to enter the core may require a more negative target axial offset to accomplish. However, the boron system can optionally be used to maintain operation in the more optimum range of gray rod motion during such manoeuvres. The degree of control rod insertion under MSHIM operation allows rapid return to power without the need to change boron concentration.

Extended base load operation is performed by controlling axial offset to the target value using the AO control bank, and by controlling the coolant average temperature to the programmed value with the M-banks. Boron concentration changes are made periodically as the fuel depletes to reposition the M-banks and allow for a periodic exchange of the gray rod bank insertion sequence. MSHIM load follow and base load operations (including the gray rod bank insertion sequence exchanges) are considered normal operations.

Burnup

Control of the excess reactivity for burnup is accomplished using soluble boron, control rod insertion, and/or burnable absorbers. The boron concentration is limited during operating conditions to maintain the moderator temperature coefficient within its specified limits. A sufficient burnable absorber loading is installed at the beginning of a cycle to give the desired cycle lifetime, without exceeding the boron concentration limit. The end of a fuel cycle is reached when the soluble boron concentration approaches the practical minimum boron concentration in the range of 0 to 10 ppm.

Rapid Power Reduction System

The reactor power control system is designed with the capability of responding to full load rejection without initiating a reactor trip using the normal rod control system, reactor control system, and the rapid power reduction system. Load rejections requiring greater than a fifty percent reduction of rated thermal power initiate the rapid power reduction system. The rapid power reduction system utilizes preselected control rod groups and/or banks which are

intentionally tripped to rapidly reduce reactor power into a range where the rod control and reactor control systems are sufficient to maintain stable plant operation. The consequence of accidental or inappropriate actuation of the rapid power reduction system is included in the cycle specific safety analysis and licensing process.

22.6.2.13 Control Rod Patterns and Reactivity Worth

The RCCAs are designated by function as the control groups and the shutdown groups. The terms group and bank are used synonymously to describe a particular grouping of control assemblies. The control banks are labelled MA, MB, MC, MD, M1, M2, and AO (Figure 22-41) with the MA, MB, MC, and MD banks comprising GRCAs; the shutdown banks are labelled SD1, SD2, SD3, and SD4. Each bank of more than four RCCAs, although operated and controlled as a unit, is composed of two or more subgroups. The axial position of the RCCAs may be controlled manually or automatically. All control rods are dropped into the core following actuation of reactor trip signals.

Two criteria have been employed for selection of the control groups. First, the total reactivity worth must be adequate to meet the requirements specified in Table 22-4. Second, in view of the fact that these rods may be partially inserted at power operation, the total power peaking factor should be low enough to meet the power capability requirements.

Analyses indicate that the first requirement can be met either by a single group or by two or more banks whose total worth equals at least the required amount. The axial power shape is more peaked following movement of a single group of rods worth 3 to 4 percent $\Delta\rho$; therefore, control bank RCCAs have been separated into several bank groupings. Typical control bank worths for the initial cycle are shown in Table 22-3.

The position of control banks for criticality under any reactor condition is determined by the concentration of boron in the coolant. On an approach to criticality, boron is adjusted so that criticality will be achieved with control rods above the insertion limit set by shutdown and other considerations. Early in the cycle, there may also be a withdrawal limit at low power or a limitation on the maximum-allowed RCS boron concentration to maintain the MTC within the specified limits for that power level. The current nuclear design philosophy is to provide a sufficient number of BAs to achieve a negative MTC at the conditions of the initial criticality for a cycle. The MTC becomes more negative as the power level is increased and xenon builds in, so operation during the initial startup and power escalation occurs with an increasingly negative MTC. During the first few months of the cycle, the BA absorber depletes significantly and the reactivity of the core may slowly increase before it starts to decrease due to fuel burnup. This is observable in the soluble boron concentration curve as shown for example in Figure 22-18. As long as the core is operating at or near RTP, the moderator temperature coefficient remains negative. If, however, reduced power operation should occur or if a startup is required during these first few months of increased core reactivity, it may be necessary to establish limits on the maximum boron concentration or control rod withdrawal limits for the low power conditions. This would only be the case if the core reactivity increase due to BA depletion is large enough to cause a non-negative MTC at the low power condition. This would also be the case if the MTC were mistakenly predicted at the beginning of the cycle so that a positive MTC was measured during startup physics testing. The establishment of such limits would not impact actual operation because the normal boron concentration and position of control rods during MSHIM operation would not challenge the limits required to ensure compliance with the MTC limit. A restriction on the maximum boron concentration or a rod withdrawal limit would maintain compliance with the MTC technical specification and is comparable to the establishment of rod insertion limits

and minimum boron concentration requirements to maintain compliance with other core-related Tech Specs.

Allowable deviations due to misaligned control rods are discussed in the Tech Specs.

A representative differential rod worth calculation for two banks of control rods withdrawn simultaneously (rod withdrawal accident) is given in Figure 22-42.

Calculation of control rod reactivity worth versus time following reactor trip involves both control rod velocity and differential reactivity worth. For nuclear design purposes, the reactivity worth versus rod position is calculated by a series of steady-state calculations at various control positions, assuming the rods out of the core as the initial position to minimise the initial reactivity insertion rate. Also, to be conservative, the rod of highest worth is assumed to be stuck out of the core, and the flux distribution (and thus reactivity importance) is assumed to be skewed to the bottom of the core.

The shutdown groups provide additional negative reactivity to establish adequate SDM. SDM is the amount by which the core would be subcritical at hot shutdown if the RCCAs were tripped, but assuming that the highest-worth assembly remained fully withdrawn and no changes in xenon or boron took place. The loss of control rod worth due to the depletion of the absorber material is negligible.

The results in Table 22-4 show that the available reactivity in withdrawn RCCAs provides the design bases' minimum SDM, allowing for the highest-worth cluster to be at its fully withdrawn position. An allowance for the uncertainty in the calculated worth of N-1 rods is made before determining the SDM.

22.6.2.14 Core Loading Procedure

During the initial core loading, only fresh fuel is used to construct the core as detailed in a fuel loading sequence procedure. As the core is being loaded, three nuclear monitoring channels of temporary core loading instrumentation are used in addition to the two plant-installed source range instrumentation system detectors. The temporary core loading instrumentation detectors are positioned in the reactor vessel at predetermined locations and are monitored by instrumentation located in the reactor building on the operating deck.

Data from all the nuclear monitoring channels are used to calculate the inverse count rate ratio, which in turn is used to assess the safety of the core loading operations. During the core loading operations, the response of at least one responding detector shall be displayed continuously on a strip chart recorder at all times when fuel is being added to the reactor vessel.

22.6.2.15 Core Reload Safety

Since the late 1960s and early 1970s, Westinghouse has used a safety analysis checklist for first cores and a reload safety analysis checklist for reload cores to document and track the core parameters utilised in the transient analysis.

The safety analysis checklist has one column of parameters that may include the maximum and minimum values, depending on the sensitivity of the transient to the parameter. Reference 22.100 provides information about how the values of these parameters are determined.

The reload safety analysis checklist is the same as the safety analysis checklist, except that transient statepoint information from the safety analysis of record are also included. The first column is the value of the parameter that has been used in the safety analysis of record; the second column is the value of the parameter as determined for the reload core. The safety analysis then determines if the reload parameter is bounded by the parameter for the safety analysis of record.

The reload safety analysis checklist is recalculated for each cycle. With the exception of rod ejection, for the hundreds of reload cores evaluated, it has rarely been necessary to perform the transients again, unless a new fuel design is incorporated.

22.6.2.16 Criticality of Fuel Assemblies during Refuelling

The basis for maintaining the reactor subcritical during refuelling is presented in Section 22.6.1.5; a discussion of how control requirements are met is in Sections 22.6.2.12 and 22.6.2.13.

Criticality of fuel assemblies outside the reactor is precluded by adequate design of fuel transfer, shipping, and storage facilities and by administrative control procedures. The two principal methods of preventing criticality are limiting the fuel assembly array size and limiting assembly interaction by fixing the minimum separation between assemblies and/or inserting neutron poisons between assemblies.

The design criteria and requirements are as follows:

- The maximum K-effective value, including all biases and uncertainties, must be less than 0.95 with for normal operation and less than 0.98 for credible abnormal operation. If no credit for soluble boron is taken, the K-effective of the spent fuel storage racks loaded with fuel of the maximum fuel assembly reactivity must not exceed 0.95, at a 95/95 confidence level during normal operation.

- The maximum enrichment of fresh fuel assemblies must be less than or equal to 5 weight-percent U-235. The maximum nominal U-235 enrichment of the fresh fuel assemblies is limited to 5 weight-percent.

The following conditions are assumed in meeting these design bases:

- The fuel assembly contains the highest enrichment authorised without any control rods or nonintegral BA rods and is at its most reactive point in life.

- For flooded conditions, the moderator is pure water at the temperature within the design limits that yields the largest reactivity.

- The array is either infinite in lateral extent or is surrounded by a conservatively chosen reflector, whichever is appropriate for the design.

- Mechanical uncertainties are treated by combining both the worst-case bounding value and sensitivity study approaches.

- Credit is taken for the neutron absorption in structural materials and in solid materials added specifically for neutron absorption (Reference 22.46).

22.6.2.17 Stability

The stability of PWR cores against xenon-induced spatial oscillations and the control of such transients has been discussed extensively (References 22.21, 22.39, 22.47, and 22.48). A summary of these reports is given below, and the design bases are given in Section 22.6.1.6.

In a large reactor core, xenon-induced oscillations can take place with no corresponding change in the total power of the core. The oscillation may be caused by a power shift in the core that occurs rapidly by comparison with the xenon-iodine time constants. Such a power shift occurs in the axial direction when a plant load change is made by control rod motion and results in a change in the moderator density and fuel temperature distributions. Such a power shift could occur in the diametral plane of the core as a result of abnormal control action.

Due to the negative power coefficient of reactivity, PWR cores are inherently stable to oscillations in total power. Protection against total power instabilities is provided by the control and protection system.

The core in the AP1000 reactor has an active fuel length that is 0.6096 m (2 foot) longer (nominal) than that for previous Westinghouse PWRs licensed in the US with 157 fuel assemblies. For this reason, it is expected that this core will be as stable as the 3.658-m (12 foot) designs with respect to radial and diametral xenon oscillations since the radial core dimensions have not changed.

This core will be slightly less stable than the 3.658-m (12 foot), 157-assembly cores with respect to axial xenon oscillations because the active core height has been increased by 0.6096 m (2 foot). The effect of this increase will be to decrease the burnup at which the axial stability index becomes zero.

The MTCs and the Doppler temperature coefficients of reactivity will be similar to those of previous designs. Control banks included in the core design are sufficient to dampen any xenon oscillations that may occur.

22.6.2.18 Vessel Irradiation

A review of the methods and analyses used in the determination of neutron and gamma ray flux attenuation between the core and the pressure vessel is provided below. A more complete discussion on the pressure vessel irradiation and surveillance program is given in Chapter 20.

The materials that serve to attenuate neutrons originating in the core and gamma rays from both the core and structural components consist of the core shroud, core barrel, and associated water annuli. These are within the region between the core and the pressure vessel.

In general, few group neutron diffusion theory codes are used to determine fission power density distributions within the active core, and the accuracy of these analyses is verified by in-core measurements on operating reactors. Region and rodwise power-sharing information from the core calculations is then used as source information in two-dimensional transport calculations which compute the flux distributions throughout the reactor.

The neutron flux distribution and spectrum in the various structural components vary significantly from the core to the pressure vessel. Representative values of the neutron flux distribution and spectrum are presented in Table 22-7.

As discussed in Chapter 20, the irradiation surveillance program utilises actual test samples to verify the accuracy of the calculated fluxes at the vessel.

22.6.3 Analytical Codes and Methods

Calculations required in nuclear design consist of the following three distinct types, which are performed in sequence:

- Determination of effective fuel temperatures
- Generation of microscopic few-group parameters
- Space-dependent, few-group diffusion calculations

These calculations are carried out by computer codes that can be executed individually. Most of the codes required have been linked to form an automated design sequence that minimises design time, avoids errors in transcription of data, and standardises the design methods.

22.6.3.1 Fuel Temperature (Doppler) Calculations

Temperatures vary radially within the fuel rod, depending on the heat generation rate in the pellet; the conductivity of the materials in the pellet, gap, and clad; and the temperature of the coolant.

The fuel temperatures for use in most nuclear design Doppler calculations are obtained from a simplified version of the Westinghouse fuel rod design model, which considers the effect of radial variation of pellet conductivity; expansion coefficient and heat generation rate; elastic deflection of the clad; and a gap conductance that depends on the initial fill gas, the hot open-gap dimension, and the fraction of the pellet over which the gap is closed. The fraction of the gap assumed closed represents an empirical adjustment used to produce close agreement with observed reactivity data at beginning of life. Further gap closure occurs with burnup and accounts for the decrease in Doppler defect with burnup which has been observed in operating plants. For detailed calculations of the Doppler coefficient, such as for use in xenon stability calculations, a more sophisticated temperature model is used that accounts for the effects of fuel swelling, fission gas release, and plastic clad deformation.

Radial power distributions in the pellet as a function of burnup are obtained from LASER calculations (Reference 22.49).

The effective U-238 temperature for resonance absorption is obtained from the radial temperature distribution by applying a radially dependent weighing function. The weighing function was determined from REPAD Monte Carlo calculations of resonance escape probabilities in several steady-state and transient temperature distributions (Reference 22.50). In each case, a flat pellet temperature that produced the same resonance escape probability as the actual distribution was determined. The weighing function was empirically determined from these results.

The effective Pu-240 temperature for resonance absorption is determined by a convolution of the radial distribution of Pu-240 densities from LASER burnup calculations and the radial weighing function. The resulting temperature is burnup-dependent but the difference between U-238 and Pu-240 temperatures, in terms of reactivity effects, is small.

The effective pellet temperature for pellet dimensional change is that value that produces the same outer pellet radius in a virgin pellet as the one obtained from the temperature model. The effective clad temperature for dimensional change is its average value.

The temperature calculation model has been validated by plant Doppler defect data and Doppler coefficient data, as shown in Figure 22-43. Stability index measurements also provide a sensitive measure of the Doppler coefficient near full power (Section 22.6.2.17).

22.6.3.2 Macroscopic Group Constants

PHOENIX-P (Reference 22.51) and PARAGON (Reference 22.58) have been used for generating the macroscopic cross-sections needed for the spatial few group codes (Reference 22.51). Both codes can be used for reload designs for the AP1000 plant.

PHOENIX-P is a 2-D, multigroup, transport-based lattice code capable of providing necessary data for PWR analysis. Since it is a dimensional lattice code, PHOENIX-P does not rely on predetermined spatial/spectral interaction assumptions for the heterogeneous fuel lattice and can therefore provide an accurate multigroup spatial flux solution.

The solution for the detailed spatial flux and energy distribution is divided into two major steps in PHOENIX-P. First, a 2-D fine energy group nodal solution is obtained, coupling individual subcell regions (e.g., pellet, clad, and moderator) as well as surrounding pins, using a method based on Carlvik's collision probability approach and heterogeneous response fluxes that preserve the heterogeneous nature of the pin cells and their surroundings. The nodal solution provides an accurate and detailed local flux distribution, which is then used to homogenise the pin cells spatially to few groups.

Next, a standard S4 discrete ordinates calculation solves for the angular distribution based on the group-collapsed and homogenised cross-sections from the first step. These S4 fluxes normalise the detailed spatial and energy nodal fluxes, which are then used to compute reaction rates and power distributions and to deplete the fuel and BA rods. A standard B1 calculation evaluates the fundamental mode critical spectrum, providing an improved fast diffusion coefficient for the core spatial codes.

PHOENIX-P employs a 70-energy group library derived mainly from the ENDF/B-VI files. This library was designed to capture the integral properties of the multigroup data properly during group collapse and to model important resonance parameters properly. It contains neutronics data necessary for modelling fuel, fission products, cladding and structural materials, coolant, and control and BA rod materials present in PWRs.

Group constants for BA cells, control rod cells, guide thimbles and instrumentation thimbles, or other nonfuel cells, can be obtained directly from PHOENIX-P without any adjustments such as those required in the cell or 1D lattice codes.

PHOENIX-P has been validated through an extensive qualification effort that includes calculation-measurement comparison of the Strawbridge-Barry critical experiments (Reference 22.52), the KRITZ high-temperature criticals (Reference 22.53), the Babcock and Wilcox criticals (References 22.54, 22.76, and 22.77) sponsored by the Atomic Energy Commission (AEC), and measured actinide isotopic data from fuel pins irradiated in the Saxton and Yankee Rowe cores (References 22.55 and 22.78 through 22.81). In addition, calculation-measurement comparisons have been made to operating reactor data measured during startup tests and normal power operation.

Confirmatory critical experiments on burnable absorber rods are described in WCAP-7806 (Reference 22.82).

Group constants for tungsten GRCAs are generated using the PARAGON lattice code. Like PHOENIX-P, PARAGON is a two-dimensional, multi-group, transport-based lattice code

capable of providing necessary data for PWR (Reference 22.58). Reference 22.36 contains a description of the nuclear methods for modelling tungsten and PARAGON benchmark results to Monte-Carlo simulations for assemblies containing tungsten GRCAs.

The PARAGON lattice code is also capable of generating all of the group constants generated by PHOENIX-P, and has been benchmarked and qualified to the same degree as PHOENIX-P. The primary difference between PARAGON and PHOENIX-P is that PARAGON uses Collision Probability theory with the interface current method to solve the integral transport equation. PARAGON also allows increased flexibility in modelling the exact assembly and pin cell geometry. The group constants generated by PARAGON are coupled to the spatial few-group code using the NEXUS nuclear data methodology (Reference 22.83).

22.6.3.3 Spatial Few Group Diffusion Calculations

The 3D ANC code permits the introduction of advanced fuel designs with axial heterogeneities, such as axial blankets and part-length BA rods, and allows such features to be modelled explicitly (References 22.56 and 22.84). The 3-D nature of this code provides both radial and axial power distribution.

Spatial few-group calculations are performed to determine the critical boron concentrations and power distributions. The moderator coefficient is evaluated by varying the inlet temperature in the same kind of calculations used for power distribution and reactivity predictions.

Validation of the reactivity calculations is associated with validation of the group constants themselves, as discussed in Section 22.6.3.2. Validation of the Doppler calculations is associated with the fuel temperature validation discussed in Section 22.6.3.1. Validation of the moderator coefficient calculations is obtained by comparison with plant measurements at hot zero-power conditions.

Axial calculations may be used in place of the full 3D model to determine differential control rod worth curves (reactivity versus rod insertion) and to demonstrate load follow capability. Group constants are obtained from the 3-D nodal model by flux-volume weighing on an axial slicewise basis. Radial bucklings are determined by varying parameters in the buckling model while forcing the 1-D model to reproduce the axial characteristics (AO, midplane power) of the 3-D model.

Validation of the spatial codes for calculating power distributions involves the use of in-core and ex-core detectors and is discussed in Section 22.6.2.8.

Calculation-measurement comparisons have been made with operating reactor data measured during startup tests and normal power operation. These comparisons include a variety of core geometries and fuel loading patterns and incorporate a reasonably extreme range of fuel enrichment, BA rod loading, and cycle burnup. Qualification data indicates small mean and standard deviations relative to measurement that are equal to or less than those found in previous reviews of similar or parallel methodologies (References 22.51, 22.58, and 22.83). For the reload designs, the spatial codes described above are used.

22.7 THERMAL AND HYDRAULIC DESIGN

The thermal and hydraulic design of the reactor core provides adequate heat transfer compatible with the heat generation distribution in the core. This provides adequate heat

removal by the RCS, the normal residual heat removal system, or the passive core cooling system.

22.7.1 Design Bases

To satisfy the heat transfer performance requirements for all modes of operation the following design bases have been established for the thermal and hydraulic design of the reactor core.

22.7.1.1 Departure from Nucleate Boiling Design Basis

There is at least a 95 percent probability at a 95 percent confidence level that DNB does not occur on the limiting fuel rods during normal operation and operational transients and any transient conditions arising from faults of moderate frequency (frequent faults).

With the Revised Thermal Design Procedure (RTDP) (Reference 22.64) uncertainties in plant operating parameters, nuclear and thermal parameters, fuel fabrication parameters, computer codes, and DNB correlation predictions are considered statistically to obtain DNB uncertainty factors. Based on the DNB uncertainty factors, RTDP design limit DNBR values are determined such that there is at least a 95 percent probability at a 95 percent confidence level that DNB will not occur on the most limiting fuel rod during normal operation and operational transients and during transient conditions arising from faults of moderate frequency (frequent faults).

Assumed uncertainties in the plant operating parameters (pressuriser pressure, primary coolant temperature, reactor power, and RCS flow) are evaluated. Only the random portion of the plant operating parameter uncertainties is included in the statistical combination. Instrumentation bias is treated as a direct DNBR penalty. Since the parameter uncertainties are considered in determining the RTDP design limit DNBR values, the plant safety analyses are performed using input parameters at their nominal values.

For those transients that use the VIPRE-01 computer program (subsection 22.7.1) and the WRB-2M correlation, the RTDP design limits are 1.25 for the typical cell and 1.25 for the thimble cell. These values may be revised (slightly) when plant specific uncertainties are available.

To maintain DNBR margin to offset DNB penalties such as those due to fuel rod bow, the safety analyses are performed to DNBR limits higher than the design limit DNBR values. The difference between the design limit DNBRs and the safety analysis limit DNBRs results in DNBR margin. A portion of this margin is used to offset the rod bow and or other DNBR penalties not directly modelled in the DNBR calculation.

The Standard Thermal Design Procedure (STDP) is used for [
] analyses where RTDP is not applicable. Rod withdrawal from subcritical must be analysed using STDP since this transient is initiated at zero power and the plant-specific uncertainties are not available at this power. Steamline break at hot-zero power is always analysed using STDP since the statepoints are out of the range of applicability of RTDP. In the STDP method, the parameters used in the analysis are treated in a conservative way from a DNBR standpoint. The parameter uncertainties are applied directly to the plant safety analyses input values to give the lowest minimum DNBR. The DNBR limit for STDP is the appropriate DNB correlation limits increased to give sufficient margins to cover any DNBR penalties associated with the analysis.

By preventing DNB, adequate heat transfer is provided from the fuel clad to the reactor coolant, thereby preventing clad damage from inadequate cooling. Maximum fuel rod surface temperature is not a DB, since it is within a few degrees of coolant temperature during operation in the nucleate boiling region. Limits provided by the nuclear control and protection systems are such that this DB is met for transients associated with frequent faults, including overpower transients. There is an additional large DNBR margin at rated power operation and during normal operating transients.

22.7.1.2 Fuel Temperature Design Basis

During modes of operation associated with normal operation and frequent faults, there is at least a 95 percent probability at a 95 percent confidence level that the peak linear heat rate fuel rods will not exceed the uranium dioxide melting temperature. The melting temperature of uranium dioxide is 2804.44°C (5080°F) (Reference 22.85) unirradiated, decreasing by 32.22°C (58°F) per 10,000 MWD/MTU. By precluding uranium dioxide melting, the fuel geometry is preserved and possible adverse effects of molten uranium dioxide on the cladding are eliminated. Design evaluations for normal operation and frequent faults have shown that fuel melting will not occur for achievable local burnups up to 75,000 MWD/MTU (Reference 22.89).

Fuel rod thermal evaluations are performed at rated power and maximum overpower and during transients at various burnups. These analyses confirm that this DB and the fuel integrity design bases given in Section 22.5 are met. They also provide input for the evaluation of infrequent faults given in Chapter 9.

The centreline temperature limit has been applied to reload cores with an extended burnup limit of 62,000 MWD/MTU. For higher burnups, the peak linear heat rate experienced during normal operation and frequent faults is limited to that maximum value sufficient to provide that the fuel centreline temperatures remain below the melting temperature for the fuel rods. Thus, the fuel rod DB that fuel rod damage due to fuel melting does not occur continues to be met.

22.7.1.3 Core Flow Design Basis

The maximum bypass flow fraction of 5.9 percent is calculated [

].

The 5.9 percent bypass flow fraction assumes the use of thimble plugging devices in the rod cluster control guide thimble tubes that do not contain any other core components.

Subtracting the 5.9 percent bypass flow fraction from the total thermal flow rate provides a minimum value of 94.1 percent that is assumed to pass through the fuel rod region of the core and is effective for fuel rod cooling. Coolant flow through the thimble and instrumentation tubes and the leakage between the core barrel and core shroud, head cooling flow, and leakage to the vessel outlet nozzles are not considered effective for heat removal. The shroud core cavity flow is considered as active flow effective for fuel rod cooling.

22.7.1.4 Hydrodynamic Stability Design Basis

Modes of operation associated with normal operating transients and frequent faults do not lead to hydrodynamic instability.

22.7.2 Design Description

22.7.2.1 Summary Comparison

Table 22-5 provides a comparison of the design parameters for the AP1000 and AP600 plants and a licensed Westinghouse-designed plant using standard XL RFA fuel.

22.7.2.2 Critical Heat Flux Ratio or Departure from Nucleate Boiling Ratio and Mixing Technology

The minimum DNBRs for the rated power and anticipated transient conditions are given in Table 22-5. The minimum DNBR in the limiting flow channel is typically downstream of the peak heat flux location (hot spot) due to the increased downstream enthalpy rise.

DNBRs are calculated by using the correlation and definitions described below. The VIPRE-01 computer code described is used to determine the flow distribution in the core and the local conditions in the hot channel for use in the DNB correlation.

The primary DNB correlation used for the analysis of the fuel is the WRB-2M correlation (Reference 22.57). The WRB-2M correlation was developed specifically for the RFAs, which are planned to be used in the AP1000 reactor core. This correlation applies to most AP1000 plant conditions. The applicable range of parameters for the WRB-2M correlation is as follows (SI units):

Pressure (P)	10.308 to 16.720 MPa abs
Local mass velocity (G_{loc})	4.74 to 15.1 x 10^6 kg/(m² hr)
Local quality (X_{loc})	-0.1 to 0.29
Heated length, inlet to CHF location (L_h)	≤ 426.72 cm
Grid spacing (g_{sp})	25.4 to 52.32 cm
Equivalent hydraulic diameter (D_e)	9.4 to 11.7 mm
Equivalent heated hydraulic diameter (D_h)	11.7 to 13.7 mm

The applicable range of parameters for the WRB-2M correlation is as follows (Imperial units):

Pressure (P)	1495 to 2425 psia
Local mass velocity (G_{loc})	0.97 to 3.1 x 10^6 lb/(ft² hr)
Local quality (X_{loc})	-0.1 to 0.29
Heated length, inlet to CHF location (L_h)	≤ 14 feet
Grid spacing (g_{sp})	10 to 20.6 inches
Equivalent hydraulic diameter (D_e)	0.37 to 0.46 inches
Equivalent heated hydraulic diameter (D_h)	0.46 to 0.54 inches

The WRB-2 (Reference 22.16), ABB-NV (Reference 22.86) or WLOP (Reference 22.87) correlation is used whenever the WRB-2M correlation is not applicable The WRB-2 correlation 95/95 limit is 1.17.

The applicable range of parameters for the WRB-2 correlation is as follows (SI units):

Pressure (P)	9.928 to 17.168 MPa abs
Local mass velocity (G_{loc})	4.4 to 18.1 x 10^6 kg/(m^2 hr)
Local quality (X_{loc})	-0.1 to 0.3
Heated length, inlet to CHF location (L_h)	≤ 426.7 cm
Grid spacing (g_{sp})	25.4 to 66.04 cm
Equivalent hydraulic diameter (D_e)	9.4 to 13.0 mm
Equivalent heated hydraulic diameter (D_h)	11.7 to 15.0 mm

The applicable range of parameters for the WRB-2 correlation is as follows (Imperial units):

Pressure (P)	1440 to 2490 psia
Local mass velocity (G_{loc})	0.9 to 3.7 x 10^6 lb/(ft² hr)
Local quality (X_{loc})	-0.1 to 0.3
Heated length, inlet to CHF location (L_h)	≤ 14 feet
Grid spacing (g_{sp})	10 to 26 inches
Equivalent hydraulic diameter (D_e)	0.37 to 0.51 inches
Equivalent heated hydraulic diameter (D_h)	0.46 to 0.59 inches

In the heated region below the first mixing vane grid, the ABB-NV correlation, References 22.86 and 22.87, which is based on CHF data from fuel assemblies without mixing vane grids, is used to calculate DNBR values. For system pressures and flow rates where the above correlations are not applicable, the WLOP correlation, Reference 22.87, is used to calculate DNBR values.

The DNB heat flux ratio, DNBR, as applied to typical cells (flow cells with all walls heated) and thimble cells (flow cells with heated and unheated walls), is defined as follows:

$$DNBR = \frac{q''_{DNB,predicted}}{q''_{actual}}$$

where,

$$q''_{DNB,predicted} = \frac{q''_{WRB-2M}}{F} \quad \text{or} \quad q''_{DNB,predicted} = \frac{q''_{WRB-2}}{F}$$

q''_{WRB-2M} = Uniform DNB heat flux as predicted by the WRB-2M DNB correlation

q''_{WRB-2} = Uniform DNB heat flux as predicted by the WRB-2 DNB correlation

F = Flux shape factor to account for non-uniform axial heat flux distributions (Reference 22.88) with the term "C" modified as in Reference 22.59

q''_{actual} = Actual local heat flux

Thermal Diffusion Coefficient

The rate of heat exchange by mixing between flow channels is proportional to the difference in the local mean fluid enthalpy of the respective channels, the local fluid density, and the flow velocity. The proportionality is expressed by the dimensionless thermal diffusion coefficient (TDC), which is defined as:

$$TDC = \frac{w'}{\rho V a}$$

where,

w' = Flow exchange rate per unit length (kg/m-s)
ρ = Fluid density (kg/m^3)
V = Fluid velocity (m/s)
a = Lateral flow area between channels per unit length (m^2/m)

A series of tests, using the "R" mixing vane grid design on 33.02 cm, 66.04 cm, and 81.28 cm (13 inch, 26 inch, and 32 inch)grid spacing, were conducted in pressurised water loops at Reynolds numbers similar to those of the AP1000 reactor core under the following single- and two-phase (subcooled boiling) flow conditions (Reference 22.26) as follows (in SI units):

Pressure	10.342 to 16.547 MPa abs
Inlet temperature	166.67 to 338.89°C
Mass velocity	4.9 to 17.1 x 10^6 kg/(m^2 hr)
Reynolds number	1.34 to 7.45 x 10^5
Bulk outlet quality	-52.1 to -13.5 percent

and in Imperial units:

Pressure	1500 to 2400 psia
Inlet temperature	332 to 642°F
Mass velocity	1.0 to 3.5 x 10^6 lbm/(hr-ft^2)
Reynolds number	1.34 to 7.45 x 10^5
Bulk outlet quality	-52.1 to -13.5 percent

The TDC is determined by comparing subchannel code predictions with the measured subchannel exit temperatures. The TDC is found to be independent of the Reynolds number, mass velocity, pressure, and quality over the ranges tested. The two-phase data (local, subcooled boiling) falls within the scatter of the single-phase data. In the subcooled boiling

region, the values of the TDC are indistinguishable from the single-phase values. In the quality region, in the case with rod spacing similar to that in the AP1000 reactor core geometry, the value of the TDC increased with quality to a point and then decreased, but never below the single-phase value.

The data from these tests on the "R" mixing vane grid show that a design TDC value of 0.038 (for 66.04 cm (26 inch) grid spacing) can be used in determining the effect of coolant mixing in the THINC analysis. An equivalent value of the mixing coefficient is used in the VIPRE-01 evaluations (Reference 22.61). A mixing test programme similar to the one just described was conducted for the current 17x17 geometry and mixing vane grids on a 66.04 cm (26 inch) spacing (Reference 22.62). The mean value of the TDC obtained from these tests is 0.059.

Including the IFM grids in the upper spans of the AP1000 plant fuel assembly results in grid spacing of approximately 25.4 cm (10 inch), giving higher values of the TDC. A conservative value of the TDC, 0.038, is used to determine the effect of coolant mixing in the core thermal performance analysis.

The total hot channel factors for heat flux and enthalpy rise are defined as the maximum-to-core-average ratios of these quantities. The heat flux hot channel factor considers the local maximum linear heat generation rate at a point (the hot spot), and the enthalpy rise hot channel factor involves the maximum integrated value along a channel (the hot channel).

Each total hot channel factor is composed of a nuclear hot channel factor describing the neutron power distribution and an engineering hot channel factor, which allows for variations in flow conditions and fabrication tolerances. The engineering hot channel factors are made up of subfactors that account for the influence of the variations of fuel pellet diameter, density, enrichment, eccentricity, inlet flow distribution, flow redistribution and flow mixing.

Heat Flux Engineering Hot Channel Factor, F_Q^E

The heat flux engineering hot channel factor is used to evaluate the maximum linear heat generation rate in the core. This subfactor is determined by statistically combining the fabrication variations for fuel pellet diameter, density, and enrichment. No DNB penalty need be taken for the short, relatively low-intensity heat flux spikes caused by variations in the above parameters, as well as fuel pellet eccentricity and fuel rod diameter variation (Reference 22.63).

Enthalpy Rise Engineering Hot Channel Factor, $F_{\Delta H}^E$

The effect of variations in flow conditions and fabrication tolerances on the hot channel enthalpy rise is directly considered in the VIPRE-01 core thermal subchannel analysis under any reactor opening condition. The following items are considered as contributors to the enthalpy rise engineering hot channel factor:

Pellet Diameter, Density, and Enrichment

Variations in pellet diameter, density, and enrichment are considered statistically in establishing the limit DNBRs for the Revised Thermal Design Procedure (Reference 22.64). Uncertainties in these variables are determined from sampling manufacturing data.

Inlet Flow Mal-distribution

A DB of 5 percent reduction in coolant flow to the hot assembly is used in the VIPRE-01 analyses. [

]

Flow Redistribution

The flow redistribution accounts for the reduction in flow in the hot channel resulting from the high-flow resistance in it due to the local or bulk boiling. The effect of the non-uniform power distribution is inherently considered in the VIPRE-01 analyses for every operating condition evaluated.

Flow Mixing

The subchannel mixing model incorporated in the VIPRE-01 code and used in reactor design is based on experimental data. The mixing vanes incorporated in the spacer grid design induce additional flow mixing between the various flow channels in a fuel assembly as well as between adjacent assemblies. This mixing reduces the enthalpy rise in the hot channel resulting from local power peaking or unfavourable mechanical tolerances.

Effects of Rod Bow on DNBR

The phenomenon of fuel rod bowing is accounted for in the DNBR safety analysis of frequent faults for each plant application. Applicable generic credits for margin resulting from retained conservatism in DNBR limit and/or margin in the core design parameter ([ ]), can be used to offset the effect of rod bow.

For the safety analysis of the AP1000 design, sufficient DNBR margin was maintained to accommodate the full- and low-flow rod bow DNBR penalties. The penalties are applicable to the analyses using the WRB-2M or WRB-2 DNB correlations.

The maximum rod bow penalties (less than about 2 percent DNBR) accounted for in the design safety analysis are based on an assembly average burnup of 24,000 MWD/MTU. At burnups greater than 24,000 MWD/MTU, credit is taken for the effect of $F^N_{\Delta H}$ burndown because of the decrease in fissionable isotopes and the buildup of fission product inventory, and no additional rod bow penalty is required.

In the upper spans of the fuel assembly, additional restraint is provided with the IFM grids such that the grid-to-grid spacing in those spans with IFM grids is approximately 25.4 cm (10 inch) compared with approximately 50.8 cm in the other spans. The use of a scaling factor (Reference 22.66) results in predicted channel closure in the limiting 25.4 cm (10 inch) spans of less than 50 percent closure; therefore, no rod bow DNBR penalty is required in the 25.4 cm (10 inch) spans in the safety analyses.

22.7.2.3 Linear Heat Generation Rate

The core average and maximum linear heat generation rates are given in Table 22-5.

22.7.2.4 Void Fraction Distribution

The calculated core average and the hot subchannel maximum and average void fractions are presented in Table 22-5 for operation at full power. The void models used in the VIPRE-01 code are described in Section 22.7.2.7.

22.7.2.5 Core Coolant Flow Distribution

The VIPRE-01 code is used to calculate the flow and enthalpy distribution in the core for use in safety analysis.

22.7.2.6 Core Pressure Drops and Hydraulic Loads

The core pressure drop includes those in the fuel assembly, lower core plate, and upper core plate. The full-power operation pressure drop values shown in Table 22-5 are the unrecoverable pressure drops across the vessel, including the inlet and outlet nozzles, and across the core. Since the best-estimate flow is that flow most likely to exist in an operating plant, the calculated core pressure drops in Table 22-5 are based on this best-estimate flow rather than the thermal design flow. The uncertainties associated with the core pressure drop values are presented in Section 22.7.2.7.

The fuel assembly hold-down springs are designed to keep the fuel assemblies in contact with the lower core plate under normal operation and frequent faults, except for the turbine overspeed transient associated with a loss of external load. The hold-down springs are designed to tolerate the possibility of an overdeflection associated with fuel assembly lift-off for this case and to provide contact between the fuel assembly and the lower core plate following this transient. More adverse flow conditions occur during a LOCA.

Hydraulic loads at normal operating conditions are calculated considering the best-estimate flow, accounting for the minimum core bypass flow based on manufacturing tolerances. Core hydraulic loads at cold plant startup conditions are based on the cold best-estimate flow but are adjusted to account for the coolant density difference. Conservative core hydraulic loads for a pump overspeed transient, which could possibly create a flow rate 18 percent greater than the best-estimate flow, are evaluated to be approximately twice the fuel assembly weight.

22.7.2.7 Correlation and Physical Data

Forced convection heat transfer coefficients are obtained from the Dittus-Boelter correlation with the properties evaluated at bulk fluid conditions. This correlation has been shown to be conservative for rod bundle geometries with pitch-to-diameter ratios in the range used by PWRs. The onset of nucleate boiling occurs when the clad wall temperature reaches the amount of superheat predicted by Thom's correlation. The justification of the Westinghouse VIPRE-01 modelling for PWR applications and related correlation choices is documented in Reference 22.61.

The analytical model used in the VIPRE-01 code (Reference 22.67) and the experimental data used to calculate the pressure drops shown in Table 22-5 are described below. Unrecoverable pressure losses occur as a result of viscous drag (friction) and/or geometry changes (form) in the fluid flow path. The flow field is assumed to be incompressible, turbulent, single-phase water. Those assumptions apply to the core and vessel pressure drop calculations for the purpose of establishing the primary loop flow rate. Two-phase considerations are neglected in the vessel pressure drop evaluation because the core average

void is negligible, as shown in Table 22-5. Two-phase flow considerations in the core thermal subchannel analysis are considered in the calculation of the core and vessel pressure losses.

Fluid density is assumed to be constant at the appropriate value for each component in the core and vessel. Because of the complex core and vessel flow geometry, precise analytical values for the form and friction loss coefficients are not available; therefore, experimental values for these coefficients are obtained from geometrically similar models.

Values are quoted in Table 22-5 for unrecoverable pressure loss across the reactor vessel, including the inlet and outlet nozzles, and across the core. The results of full-scale tests of core components, and fuel assemblies are used in developing the core pressure loss characteristic.

Tests of the primary coolant loop flow rates are made prior to initial criticality to verify that the flow rates used in the design, which are determined in part from the pressure losses calculated by the method described here, are conservative.

VIPRE-01 considers two-phase flow in two steps: first, a quality model is used to compute the flowing vapour mass fraction (true quality), including the effects of subcooled boiling; then given the true void quality, a bulk void model is applied to compute the vapour volume fraction (void fraction).

VIPRE-01 uses a profile fit model for determining subcooled quality. It calculates the local vapour volumetric fraction in forced convection boiling by: 1) predicting the point of bubble departure from the heated surface and 2) postulating a relationship between the true local vapour fraction and the corresponding thermal equilibrium value.

The void fraction in the bulk boiling region is predicted by using homogeneous flow theory and assuming no slip (Reference 22.61). The void fraction in this region is therefore a function only of the thermodynamic quality.

22.7.2.8 Thermal Effects of Operational Transients

DNB core safety limits are generated as a function of coolant temperature, pressure, core power, and axial power imbalance. Steady-state operation within these safety limits provides that the DNB design basis is met. The OTΔT trip provides protection against anticipated operational transients that are slow with respect to fluid transport delays in the primary system. In addition, for fast transients (such as uncontrolled rod bank withdrawal at power incident), specific protection functions are provided. The use of these protection functions is described in Chapter 9.

22.7.2.9 Uncertainties in Estimates

a) Uncertainties in Fuel and Clad Temperatures

The fuel temperature is a function of crud, oxide, clad, pellet-clad gap, and pellet conductances. Uncertainties in the fuel temperature calculation are essentially of two types: fabrication uncertainties, such as variations in pellet and clad dimensions and pellet density; and model uncertainties, such as variations in pellet conductivity and gap conductance.

These uncertainties have been quantified by comparison of the thermal model with the in-pile thermocouple measurements, by out-of-pile measurements of the fuel and clad properties, and by measurements of the fuel and clad dimensions during fabrication. The

resulting uncertainties are then used in the evaluations involving the fuel temperature. The effect of densification on fuel temperature uncertainties is also included in the calculation of the total uncertainty.

In addition to the temperature uncertainty described above, the measurement uncertainty in determining the local power and the effect of density and enrichment variations on the local power are considered in establishing the heat flux hot channel factor.

Reactor trip setpoints, as specified in the Tech Specs, include allowance for instrument and measurement uncertainties such as calorimetric error, instrument drift and channel reproducibility, temperature measurement uncertainties, noise, and heat capacity variations.

Uncertainty in determining the cladding temperature results from uncertainties in the crud and oxide thicknesses. Because of the adequate heat transfer between the surface of the rod and the coolant, the film temperature drop does not appreciably contribute to the uncertainty.

b) Uncertainties in Pressure Drops

Core and vessel pressure drops based on the best-estimate flow are quoted in Table 22-5. The uncertainties quoted are based on the uncertainties in both the test results and the analytical extension of these values to the reactor application.

A major use of the core and vessel pressure drops is to determine the primary system coolant flow rates. In addition, tests on primary system prior to initial criticality are conducted to verify that a conservative primary system coolant flow rate has been used in the design and analysis of the plant.

c) Uncertainties due to Inlet Flow Maldistribution

The effects of uncertainties in the inlet flow maldistribution criteria used in the core thermal analyses are described in Section 22.7.2.2.

d) Uncertainty in Departure from Nucleate Boiling Correlation

The uncertainty in the DNB correlation is written as a statement on the probability of not being in DNB based on the statistics of the DNB data.

e) Uncertainties in Departure from Nucleate Boiling Ratio Calculations

The uncertainties in the DNBRs calculated by the VIPRE-01 analyses due to uncertainties in the nuclear peaking factors are accounted for by applying conservatively high values of the nuclear peaking factors. Measurement error allowances are included in the statistical evaluation of the DNBR limit. In addition, conservative values for the engineering hot channel factors are used. The results of a sensitivity study with THINC-IV, a VIPRE-01 equivalent code, show that the minimum DNBR in the hot channel is relatively insensitive to variations in the corewide radial power distribution (for the same value of $F^N_{\Delta H}$) (Reference 22.65).

Studies have been performed to determine the sensitivity of the minimum DNBR to the void fraction correlation and the inlet flow distributions (Reference 22.67). The results of these studies show that the minimum DNBR is relatively insensitive to variation in these

parameters. Furthermore, the VIPRE-01 flow field model for predicting conditions in the hot channels is consistent with that used in the derivation of the DNB correlation limits, including void and quality modelling, turbulent mixing, cross-flow, and two-phase flow.

f) Uncertainties in Flow Rates

A thermal design flow is defined for use in core thermal performance evaluations accounting for both prediction and measurement uncertainties. In addition, another 5.9 percent of the thermal design flow is assumed to be ineffective for core heat removal capability because it bypasses the core through the various available vessel flow paths.

g) Uncertainties in Hydraulic Loads

Hydraulic loads on the fuel assembly are evaluated for a pump overspeed transient that creates flow rates 18 percent greater than the best-estimate flow. The best-estimate flow is the most likely flow rate value for the actual plant operating condition.

h) Uncertainties in Mixing Coefficient

A conservative value of the mixing coefficient, that is, the TDC, is used in the VIPRE-01 analyses.

22.7.2.10 Flux Tilt Considerations

Significant quadrant power tilts are not anticipated during normal operation since this phenomenon is caused by some asymmetric perturbation. A dropped or misaligned RCCA could cause changes in hot channel factors. These events are analysed separately in Chapter 9.

Other possible causes for quadrant power tilts include X-Y xenon transients, inlet temperature mismatches, enrichment variations within tolerances, and so forth.

In addition to unanticipated quadrant power tilts as described above, other readily explainable asymmetries may be observed during calibration of the ex-core detector quadrant power tilt alarm. During operation, in-core maps are taken at least one per month and additional maps are obtained periodically for calibration purposes. Each of these maps is reviewed for deviations from the expected power distributions.

Asymmetry in the core, from quadrant to quadrant, is frequently a consequence of the design when assembly and/or component shuffling and rotation requirements do not allow exact symmetry preservation. In each case, the acceptability of an observed asymmetry, planned or otherwise, depends solely on meeting the required accident analyses assumptions. In practice, once acceptability has been established by review of the in-core maps, the quadrant power tilt alarms and related instrumentation are adjusted to indicate zero quadrant power tilt ratio as the final step in the calibration process. This action confirms that the instrumentation is correctly calibrated to alarm in the event that an unexplained or unanticipated change occurs in the quadrant-to-quadrant relationships between calibration intervals.

Proper functioning of the quadrant power tilt alarm is significant. No allowances are made in the design for increased hot channel factors due to unexpected developing flux tilts, since likely causes are presented by design or procedures or are specifically analysed.

Finally, in the event that unexplained flux tilts do occur, the Tech Specs provide appropriate corrective actions to provide continued safe operation of the reactor.

22.7.2.11 Fuel and Cladding Temperatures

Consistent with the thermal hydraulic design bases described in Section 22.7.1, the following discussion pertains mainly to fuel pellet temperature evaluation.

The thermal hydraulic design provides that the maximum fuel temperature is below the melting point of uranium dioxide. To preclude centre melting and to serve as a basis for overpower protection system setpoints, a calculated centreline fuel temperature of 2593.33°C (4700°F) is selected as the overpower limit. This provides sufficient margin for uncertainties in the thermal evaluations.

The temperature distribution within the fuel pellet is predominantly a function of the local power density and the uranium dioxide thermal conductivity, but the computation of radial fuel temperature distributions combines crud, oxide, clad gap, and pellet conductances. The factors that influence these conductances, such as gap size (or contact pressure), internal gas pressure, gas composition, pellet density, and radial power distribution within the pellet, have been combined into a semiempirical thermal model that includes a model for time-dependent fuel densification. See Reference 22.7 for the section on "Revised PAD Thermal Model Calibration and Verification" for the statistics from the thermal calibration and verification of this model. This thermal model enables the determination of these factors and their net effects on temperature profiles. The temperature predictions have been compared with in-pile fuel temperature measurements and melt radius data with good results.

Fuel rod thermal evaluations (fuel centreline and average and surface temperatures) are performed at several times in the fuel rod lifetime (with consideration of time-dependent densification) to determine the maximum fuel temperatures.

The principal factors used in determining the fuel temperature are as follow:

a) Uranium Dioxide Thermal Conductivity

The thermal conductivity of uranium dioxide was evaluated from published data (Reference 22.68). At the higher temperatures, thermal conductivity is best obtained by using the integral conductivity to melt. From an examination of the data, it has been concluded that the best estimate is the following:

$$\int_0^{2800} \mathrm{KDT} = 93\ \mathrm{W/cm}$$

The design curve for the thermal conductivity is shown in Figure 22-44. The section of the curve at temperatures between 0° and 1300°C is in agreement with the recommendation of the International Atomic Energy Agency (IAEA). The section of the curve above 1300°C is derived for an integral value of 93 W/cm.

Thermal conductivity for uranium dioxide at 95 percent theoretical density can be represented by the following equation:

$$\mathrm{K} = \frac{1}{11.8 + 0.0238\mathrm{T}} + 8.775 \times 10^{-13}\,\mathrm{T}^3$$

where,

K = W/cm-°C
T = °C

b) Radial Power Distribution in Uranium Dioxide Fuel Rods

An accurate description of the radial power distribution as a function of burnup is needed for determining the power level for incipient fuel melting and other important performance parameters, such as pellet thermal expansion, fuel swelling, and fission gas release rates. Radial power distribution in uranium dioxide fuel rods is determined with the neutron transport theory code, LASER.

The LASER code has been validated by comparing the code predictions on radial burnup and isotopic distributions with measured radial microdrill data (Reference 22.69). A radial power depression factor, f, is determined using radial power distributions predicted by LASER. The factor, f, enters into the determination of the pellet centreline temperature, T_c, relative to the pellet surface temperature, T_g, through the expression:

$$\int_{T_i}^{T_c} K(T)dT = \frac{q''f}{4\pi}$$

where,

K(T) = Thermal conductivity for uranium dioxide with a uniform density distribution
q″ = Linear power generation rate

c) Gap Conductance

The temperature drop across the pellet-clad gap is a function of the gap size and the thermal conductivity of the gas in the gap. The gap conductance model is selected so that when combined with the uranium dioxide thermal conductivity model, the calculated fuel centreline temperatures reflect the in-pile temperature measurements. A more detailed description of the gap conductance model is presented in Reference 22.7.

d) Fuel Clad Temperatures

The outer surface of the fuel rod at the hot spot operates at a temperature a few degrees above fluid temperature for steady-state operation at rated power throughout core life because of the onset of nucleate boiling. At BOL, this temperature is the same as the clad metal outer surface.

During operation over the life of the core, the buildup of oxides and crud on the fuel rod surface causes the clad surface temperature to increase. To preclude fuel centre melting and to serve as a basis for overpower protection system setpoints, a calculated centreline fuel temperature of 2593.33°C (4700°F) is selected as the limit. This provides sufficient margin for uncertainties in the thermal evaluations. The temperature distribution within the fuel pellet is predominantly a function of the local power density and the uranium dioxide thermal conductivity, however, the computation of radial fuel temperature distributions combines crud, oxide, clad gap, and pellet conductances. The factors that influence these conductances, such as gap size (or contact pressure), internal gas pressure, gas composition, pellet density, and radial power distribution within the pellet,

have been combined into a semiempirical thermal model that includes a model for time-dependent fuel densification. This thermal model enables the determination of these factors and their net effects on temperature profiles.

Since the thermal hydraulic DB limits DNB, adequate heat transfer is provided between the fuel clad and the reactor coolant so that the core thermal output is not limited by considerations of clad temperature.

e) Treatment of Peaking Factors

The design value of the total heat flux hot channel factor F_Q is 2.6 for normal operation.

The centreline fuel temperature must be below the uranium dioxide melt temperature over the lifetime of the rod, including allowances for uncertainties. The fuel temperature DB results in a maximum allowable calculated centreline temperature of 2593.33°C (4700°F). The peak linear power for prevention of centreline melt is 73.82 kW/m (22.5 kW/ft). The centreline temperature at the peak linear power resulting from overpower transients and operator errors (assuming a maximum overpower of 118 percent) is below that required to produce melting. This is ensured for each operating cycle as part of the nuclear design reload safety analysis and the confirmation of the adequacy of the OPΔT and OTΔT trip setpoints (Reference 22.74).

22.7.3 Evaluation of the Validity of Thermal Hydraulic Design Techniques

22.7.3.1 Critical Heat Flux

The CHF correlations used in the core thermal analysis are explained in Section 22.7.2.

22.7.3.2 Core Hydraulics

The following flow paths for core bypass are considered:

1. Flow through the spray nozzles into the upper head for head cooling purposes
2. Flow entering the rod cluster control and gray rod cluster guide thimbles
3. Leakage flow from the vessel inlet nozzle directly to the vessel outlet nozzle through the gap between the vessel and the barrel
4. Flow between the core barrel and the core shroud for the purpose of cooling and not considered available for core cooling

The above contributions are evaluated to confirm that the design value of the core bypass flow is met. Of the total allowance, one part is associated with the core (item 2 above) and the rest is associated with the internals (items 1, 3 and 4 above). Calculations have been performed using drawing tolerances in the worst direction and accounting for uncertainties in pressure losses. Based on these calculations, the core bypass is no greater than the 5.9 percent design value.

A reduction in core inlet flow distribution of 5 percent to the hot assembly inlet is used in the VIPRE-01 analyses of DNBR in the AP1000 reactor core. Studies made with THINC-IV, a VIPRE-01 equivalent code, show that flow distributions significantly more non-uniform than 5 percent have a very small effect on DNBR (Reference 22.65).

The friction factor for VIPRE-01 in the axial direction, parallel to the fuel rod axis, is evaluated using a correlation for a smooth tube (Reference 22.67). The effect of two-phase flow on the friction loss is expressed in terms of the single-phase friction pressure drop and a two-phase friction multiplier. The multiplier is calculated using the homogenous equilibrium flow model (Reference 22.61).

The flow in the lateral directions, normal to the fuel rod axis, views the reactor core as a large tube bank. This correlation is of the form:

$$FL = A\,Re_L^{-0.2}$$

where,

A = Function of the rod pitch and diameter a
Re_L = Lateral Reynolds number based on the rod diameter

22.7.3.3 Influence of Power Distribution

The core power distribution, which is largely established at BOL by fuel enrichment, loading pattern, and core power level, is also a function of variables such as control rod worth and position, and fuel depletion through lifetime. Radial power distributions in various planes of the core are often illustrated for general interest; however, the core radial enthalpy rise distribution, as determined by the integral of power up each channel, is of greater importance for DNBR analyses. These radial power distributions, characterised by $F_{\Delta H}^N$, as well as axial heat flux profiles, are discussed below.

Given the local power density q′ (kW/m) at a point *x, y,* and *z* in a core with *N* fuel rods and height H, then:

$$F_{\Delta H}^N = \frac{\text{hot rod power}}{\text{average rod power}} = \frac{\underset{0}{\overset{H}{\text{Max}\int}} q'(x_0 y_0 z_0)dz}{\frac{1}{N}\sum_{\text{all rods}} \int_0^H q'(x_0 y_0 z_0)dz}$$

The way in which $F_{\Delta H}^N$ is used in the DNBR calculation is important. The location of minimum DNBR depends on the axial profile, and the value of DNBR depends on the enthalpy rise to that point. Basically, the maximum value of the rod integral power is used to identify the most likely rod for minimum DNBR. An axial power profile is obtained that, when normalised to the design value of $F_{\Delta H}^N$, recreates the axial heat flux along the limiting rod. The surrounding rods are assumed to have the same axial profile with rod average powers that are typical distributions found in hot assemblies. In this manner, worst-case axial profiles can be combined with worst-case radial distributions for reference DNBR calculations.

It should be noted again that $F_{\Delta H}^{N}$ is an integral and is used as such in DNBR calculations. Local heat fluxes are obtained by using hot channel and adjacent channel explicit power shapes that take into account variations in horizontal power shapes throughout the core. For operation at a fraction of full power, the design $F_{\Delta H}^{N}$ used is given by:

$$F_{\Delta H}^{N} = F_{\Delta H}^{RTP}\left[1 + 0.3\left(1 - P\right)\right]$$

where,

$F_{\Delta H}^{RTP}$ = Limit at RTP
P = Fraction of RTP

The permitted relaxation of $F_{\Delta H}^{N}$ is included in the DNB protection setpoints and allows radial power shape changes with rod insertion to the insertion limits. This allows greater flexibility in the nuclear design.

The axial heat flux distribution can vary as a result of rod motion or power change, or of a spatial xenon transient that may occur in the axial direction. The ex-core nuclear detectors are used to measure the axial power imbalance. The information from the ex-core detectors is used to protect the core from excessive axial power imbalance. The reactor trip system provides automatic reduction of the trip setpoints on excessive axial power imbalance. To determine the magnitude of the setpoint reduction, the reference shape is supplemented by other axial shapes skewed to the bottom and top of the core.

The course of those accidents in which DNB is a concern is analysed in Chapter 9, assuming that the protection setpoints have been set on the basis of these shapes. In many cases, the axial power distribution in the hot channel changes throughout the course of the accident because of rod motion, coolant temperature, and power level changes.

The initial conditions for the accidents that require DNB protection are assumed to be those permissible within the specified AO control limits. In the case of the loss-of-flow accident, the hot channel heat flux profile is very similar to the power density profile in normal operation preceding the accident. It is therefore possible to illustrate the calculated minimum DNBR for conditions representative of the loss-of-flow accident as a function of the flux difference initially in the core. The power shapes are evaluated with a full-power radial peaking factor ($F_{\Delta H}^{N}$). The radial contribution to the hot rod power shape is conservative both for the initial condition and for the condition at the time of minimum DNBR during the loss-of-flow transient. The minimum DNBR is calculated for the design power shape for non-overpower/overtemperature DNB events. This design shape results in calculated DNBR that bounds the normal operation shapes.

22.7.3.4 Core Thermal Response

A general summary of the steady-state thermal hydraulic design parameters, including thermal output and flow rates, is provided in Table 22-5.

As stated in Section 22.7.1, the design bases of the application are to prevent DNB and to prevent fuel melting for frequent faults. The AP1000 plant protective systems are designed to meet these bases. The response of the core to frequent faults is given in Chapter 9.

22.7.3.5 Codes and Analytical Techniques

The objective of reactor core thermal design is to determine the maximum heat removal capability in all flow subchannels and to show that the core safety limits, as presented in the Tech Specs, are not exceeded while combining engineering and nuclear effects. The thermal design takes into account local variations in dimensions, power generation, flow redistribution, and mixing.

The Westinghouse version of VIPRE-01 contains a 3-D subchannel code that has been developed to account for hydraulic and nuclear effects on the enthalpy rise in the core and hot channels (Reference 22.67). VIPRE-01 modelling of a PWR core is based on a one-pass modelling approach. In this one-pass modelling, hot channels and their adjacent channels are modelled in detail, while the rest of the core is modelled simultaneously on a relatively coarse mesh.

The behaviour of the hot assembly is determined by superimposing the power distribution upon the inlet flow distribution while allowing for flow mixing and flow distribution between flow channels. Local variations in fuel rod power, fuel rod and pellet fabrication, and turbulent mixing are also considered in determining conditions in the hot channels. Conservation equations of mass, axial and lateral momentum, and energy are solved for the fluid enthalpy, axial flow rate, lateral flow, and pressure drop.

The VIPRE-01 core model is used with the applicable DNB correlations to determine DNBR distributions along the hot channels of the reactor core under all expected operating conditions. The effect of crud on the flow and enthalpy distribution in the core is not directly accounted for in the VIPRE-01 evaluations. However, conservative treatment by the Westinghouse VIPRE-01 modelling method has been demonstrated to bound this effect in DNBR calculations (References 22.61 and 22.86).

Westinghouse is very familiar with the Electric Power Research Institute (EPRI) guidelines for fuel cladding crud and corrosion, however, since it originally started the development of the methodology and associated computer codes and is one of the key contributors to the guidelines. Westinghouse and EPRI then worked jointly with the utilities and consultants to finalise the supporting methodology and resulting codes associated with these guidelines.

Using these guidelines and computer codes, Westinghouse has performed an initial assessment for the AP1000 design of crud formation effects on core power distribution, also known as crud-induced power shift (CIPS) (Reference 22.70). Burnup-dependent core power distributions are predicted by the Westinghouse 3-D neutronics code ANC. These power distributions are then input to the Westinghouse version of the EPRI VIPRE thermal and hydraulic code (VIPRE-01) to calculate the local thermal hydraulic conditions in three dimensions.

The local thermal hydraulic conditions from VIPRE and relevant coolant chemistry data such as boron concentration and pH levels are then input to the EPRI BOA code[1] to calculate the local subcooled boiling rates, deposition of crud on the fuel clad surface, and the deposition of boron from the coolant into the crud layer throughout the cycle. This assessment has determined that the AP1000 plant will have a low risk of operational issues due to crud formation on the fuel cladding surface. Conservative treatment by the Westinghouse

1. The Boron-induced Offset Anomaly Risk Assessment Tool (BOA) is a widely used industry code.

VIPRE-01 modelling method has been demonstrated to bound this effect in DNBR calculations (Reference 22.67).

To reduce the amount of crud being deposited on the fuel clad surface and hence the risk of operational issues, Westinghouse is implementing zinc injection for the AP1000 plant. Zinc injection has been shown to reduce the corrosion rate of primary system surfaces in operating PWRs. This will reduce the source of material available to deposit on the core as crud.

EPRI guidelines will also be followed to minimise corrosion of system surfaces, release of corrosion products to the coolant, corrosion product transport, and corrosion product deposition on the fuel. Reduced crud formation is expected in AP1000 plant because of the use of zinc addition. Plants that have implemented zinc addition following steam generator replacement have reported much less crud deposition on the fuel, which is attributed to the effect of zinc addition reducing corrosion rates from fresh metal surfaces.

For the AP1000 plant, zinc addition will commence with the initial hot functional testing and continue thereafter. The EPRI guidelines recommend zinc addition for plants replacing steam generators to reduce the risk of crud formation. This recommendation is also applicable to new plants. Core designs can also influence crud deposition by changing the amount and distribution of subcooled boiling on fuel cladding surfaces. Westinghouse applies the VIPRE BOA crud risk evaluation methods to minimise the risk of crud deposition for first core and reload designs. The use of these tools helps in developing designs that are more tolerant of crud deposits. Specifically, the tools can be used to avoid core designs that result in thick local crud deposits.

Estimates of uncertainties are discussed in Section 22.7.2.9.

Extensive additional experimental verification of VIPRE-01 has been undertaken (Reference 22.67). The VIPRE-01 analysis is based on a knowledge and understanding of the heat transfer and hydrodynamic behaviour of the coolant flow and the mechanical characteristics of the fuel elements. The use of the VIPRE-01 analysis provides a realistic evaluation of the core performance and is used in the thermal hydraulic analyses as described above.

VIPRE-01 is capable of transient DNB analysis. The conservation equations in the VIPRE-01 code contain the necessary accumulation terms for transient calculations. The input description can include one or more of the following time-dependent arrays:

- Inlet flow variation
- Core heat flux variation
- Core pressure variation
- Inlet temperature or enthalpy variation

At the beginning of the transient, the calculation procedure is carried out as in the steady-state analysis. The time is incremented by an amount determined either by the user or by the time-step control options in the code itself. At each new time step, the calculations are performed with the addition of the accumulation terms that are evaluated using the information from the previous time step. This procedure is continued until a preset maximum time is reached.

At time intervals selected by the user, a complete description of the coolant parameter distributions as well as DNBR is printed out. In this manner, the variation of any parameter with time can be readily determined.

22.7.3.6 Flow Instability

Boiling flow may be susceptible to thermohydrodynamic instabilities (Reference 22.71). These instabilities are undesirable in reactors since they may cause a change in thermal hydraulic conditions that may lead to a reduction in the DNB heat flux relative to that observed during a steady flow condition or to undesired forced vibrations of core components. A thermal hydraulic design criterion was therefore developed: it states that modes of operation under normal operation and frequent faults shall not lead to thermohydrodynamic instabilities.

Two specific types of flow instabilities are considered for AP1000 plant operation: the Ledinegg (or flow excursion) type of static instability and the density wave type of dynamic instability.

The Ledinegg instability involves a sudden change in flow rate from one steady state to another. This instability occurs when the scope of the RCS pressure drop-flow rate curve,

$$\left(\frac{\partial \Delta P}{\partial G} \bigg| \text{int ernal} \right)$$

becomes algebraically smaller than the loop supply (pump head) pressure drop-flow rate curve,

$$\left(\frac{\partial \Delta P}{\partial G} \bigg| \text{external} \right)$$

The criterion for stability is thus:

$$\left(\frac{\partial \Delta P}{\partial G} \bigg| \text{int ernal} \geq \frac{\partial \Delta P}{\partial G} \bigg| \text{external} \right)$$

The reactor coolant pump head curve has a negative slope ($\partial \Delta P/\partial G$ external less than zero), whereas the RCS pressure drop-flow curve has a positive slope ($\partial \Delta P/\partial G$ internal greater than zero) over the normal and frequent fault operational ranges. Thus, the Ledinegg instability does not occur.

The mechanism of density wave oscillations in a heated channel is such that an inlet flow fluctuation produces an enthalpy perturbation. This perturbs the length and the pressure drop of the single-phase region and causes quality or void perturbations in the two-phase regions that travel up the channel with the flow. The quality and length perturbations in the two-phase region create two-phase pressure drop perturbations; however, since the total pressure drop across the core is maintained by the characteristics of the fluid system external to the core, the two-phase pressure drop perturbation feeds back to the single-phase region. These resulting perturbations can be either attenuated or self-sustained.

A simple method has been developed for parallel closed-channel systems to evaluate whether a given condition is stable with respect to the density wave type of dynamic instability. This

method had been used to assess the stability of typical Westinghouse reactor designs in normal operation and frequent faults. The results indicate that a large margin-to-density-wave instability exists. Increases on the order of 150 percent of rated reactor power would be required for the predicted inception of this type of instability.

The application of this method to Westinghouse reactor designs is conservative because of the parallel open-channel feature of Westinghouse PWR cores. For such cores, there is little resistance to lateral flow leaving the flow channels of high-power density. There is also energy transfer from channels of high-power density to lower-power density channels. This coupling with cooler channels leads to the conclusion that an open-channel configuration is more stable than the above closed-channel analysis under the same boundary conditions.

Flow stability tests have been conducted where the closed channel systems were shown to be less stable than when the same channels were cross-connected at several locations. The cross-connections were such that the resistance to channel crossflow and enthalpy perturbations would be greater than those in a PWR core that has a relatively low resistance to crossflow.

Flow instabilities that have been observed have occurred almost exclusively in closed-channel systems operating at low pressures relative to the Westinghouse PWR operating pressures. Evidence that flow instabilities do not adversely affect thermal margin is provided by data from rod bundle DNB tests. Many Westinghouse rod bundles have been tested over wide ranges of operating conditions for the mixing vane DNB correlations with no evidence of premature DNB or inconsistent data that might indicate flow instabilities in the rod bundle.

In summary, it is concluded that thermohydrodynamic instabilities will not occur under normal operation and frequent faults for Westinghouse PWR designs. A large power margin, greater than 150 percent of rated power, exists to predicted inception of such instabilities. Analysis has shown that minor plant-to-plant differences in Westinghouse reactor designs such as fuel assembly arrays, power-to-flow ratios, and fuel assembly length do not result in gross deterioration of the above power margins.

22.7.3.7 Fuel Rod Behaviour Effects from Coolant Flow Blockage

Coolant flow blockages can occur within the coolant channels of a fuel assembly or external to the reactor core. The effects of fuel assembly blockage within the assembly on fuel rod behaviour are more pronounced than external blockages of the same magnitude. In both cases, the flow blockages cause local reductions in coolant flow. The amount of local flow reduction, where the reduction occurs in the reactor, and how far along the flow stream the reduction persists are considerations that will influence the fuel rod behaviour.

The effects of coolant flow blockages in terms of maintaining rated core performance are determined both by analytical and experimental methods. The experimental data are usually used to augment analytical tools such as computer programmes similar to the VIPRE-01 programme. Inspection of the DNB correlation shows that the predicted DNBR depends upon the local values of quality and mass velocity.

The VIPRE-01 code is capable of predicting the effects of local flow blockages on DNBR within the fuel assembly on a subchannel basis, regardless of where the flow blockage occurs (Reference 22.67). For a fuel assembly similar to the Westinghouse design, VIPRE-01 accurately predicts the flow distribution within the fuel assembly when the inlet nozzle is completely blocked. Full recovery of the flow was found to occur about 76.20 cm (30 in)

downstream of the blockage. With the reactor operating at the nominal full-power conditions specified in Table 22-4, the effects of an increase in enthalpy and decrease in mass velocity in the lower portion of the fuel assembly would not result in the fuel rods reaching the DNBR limit.

The open literature supports the conclusion that flow blockage in open-lattice cores, similar to the Westinghouse cores, causes flow perturbations that are local to the blockage. For example, A. Ohstubo and S. Uruwashi show that the mean bundle velocity is approached asymptomatically about 10.2 cm (4 in) downstream from the flow blockage in a single-flow cell (Reference 22.72).

Similar results were also found for two and three cells completely blocked, tested on an open-lattice fuel assembly in which 41 percent of the subchannels were completely blocked in the centre of the test bundle between spacer grids. These results show that the stagnant zone behind the flow blockage essentially disappears after 1.65 L/De or about 12.70 cm (5 in) for their test bundle. It was also found that leakage flow through the blockage tended to shorten the stagnant zone or, in essence, the complete recovery length.

Thus, local flow blockages within a fuel assembly have little effect on subchannel enthalpy rise and rod bundle test results showed no adverse effect on DNB (Reference 22.73).

Coolant flow blockages induce local crossflows as well as promote turbulence. Fuel rod behaviour is changed under the influence of a sufficiently high crossflow component. Fuel rod vibration could occur, caused by this crossflow component, through vortex shedding or turbulent mechanisms. If the crossflow velocity exceeds the limit established for fluid elastic stability, large amplitude whirling results.

The limits for a controlled vibration mechanism are established from studies of vortex shedding and turbulent pressure fluctuations. The crossflow velocity required to exceed fluid elastic stability limits depends on the axial location of the blockage and the characterisation of the crossflow (jet flow or not). These limits are greater than those for vibratory fuel rod wear. Crossflow velocity above the established limits can lead to mechanical wear of the fuel rods at the grid support locations. Fuel rod wear due to flow-induced vibration is considered in the fuel rod fretting evaluation as discussed in Section 22.5.

22.7.4 Testing and Verification

22.7.4.1 Tests prior to Initial Criticality

A reactor coolant flow test is performed following fuel loading but prior to initial criticality. Coolant loop pressure data is obtained in this test. This data allows determination of the coolant flow rates at reactor operating conditions. This test verifies that proper coolant flow rates have been used in the core thermal and hydraulic analysis.

22.7.4.2 Initial Power and Plant Operation

Core power distribution measurements are made at several core power levels. These tests are used to confirm that conservative peaking factors are used in the core thermal and hydraulic analysis.

Additional demonstration of the overall conservatism of the THINC analysis was obtained by comparing THINC predictions with in-core thermocouple measurements (Reference 22.65). VIPRE-01 has been confirmed to be as conservative as the THINC code (Reference 22.67).

22.7.4.3 Components and Fuel Inspections

Inspections performed on the manufactured fuel are described in Section 22.5.3. Fabrication measurements critical to thermal and hydraulic analysis are obtained to verify that the engineering hot channel factors in the design analyses are met.

22.7.5 Instrumentation Requirements

22.7.5.1 In-core Instrumentation

The primary function of the in-core instrumentation system is to provide a 3-D flux map of the reactor core. This map is used to calibrate neutron detectors used by the protection and safety monitoring system as well as to optimise core performance.

A secondary function of the in-core instrumentation system is to provide the protection and safety monitoring system with the signals necessary for monitoring core exit temperatures. This secondary function is the result of the mechanical design that groups the detectors used for generating the flux map in the same thimble as the core exit thermocouples.

The in-core instrumentation system consists of in-core instrument thimble assemblies that house fixed in-core detectors, core exit thermocouple assemblies contained within an inner and outer sheath assembly, and associated signal processing and data processing equipment. There are 42 in-core instrument thimble assemblies, each composed of multiple fixed in-core detectors and one thermocouple.

The thimbles are inserted into the active core through the upper head and internals of the reactor vessel. The signals output from the fixed in-core detectors are digitised inside containment and multiplexed out of the containment. The signal processing software integral to the in-core instrumentation system allows the fixed in-core detector signals to be used to calculate an accurate 3-D core power distribution suitable for developing calibration information for the ex-core nuclear instrumentation input to the OTΔT and OPΔT reactor trip setpoints. This calibration information is developed using the online core monitoring system and confirmed via the Data Display and Processing System prior to entry into the Plant Monitoring and Safety System. The system is also capable of accurately determining whether the reactor power distribution is currently within the operating limits defined in the Tech Specs while the reactor is operating above approximately 20 percent of RTP.

The in-core instrument system data processor receives the transmitted digitised fixed in-core detector signals from the signal processor and combines the measured data with analytically derived constants and certain other plant instrumentation sensor signals to generate a full 3-D indication of nuclear power distribution in the reactor core. It also edits the 3-D indication of power distribution to extract pertinent power distribution parameter outputs for use by the plant operators and engineers. The data processor also generates hardcopy representations of the detailed 3-D nuclear power indications.

The hardware and software that calculate the 3-D power distribution are capable of executing the calculation algorithms and constructing graphical and tabular displays of core conditions at intervals of 1 minute or less. The software provides information to enable the reactor operator to ascertain how the measured peaking factor performance agrees with the peaking factor performance predicted by the design model used to determine the acceptability of the fuel loading pattern. The analysis software provides information required to activate a visual alarm display to alert the reactor operator about the current existence of, or the potential for, reactor operating limit violations.

The calculation algorithms are capable of determining the three-dimensional reactor core power distribution using a minimum set of the total 42 in-core instrumentation thimble assemblies. Each in-core instrumentation thimble assembly consists of multiple fixed in-core detector elements that start at the top of the active fuel and have sequentially increasing lengths such that the longest element reaches the bottom of the active fuel in the fuel assembly. The calculation algorithms use the measured signal from detectors of different lengths within the assembly. The difference in signal from two operable detectors in the same assembly is defined as a detector segment. The minimum number of in-core detectors required for operability of the system is at least 75 percent operating detector segments during the initial power distribution measurement required in each operating cycle, and at least 40 percent operating detector segments following the cycle initial power distribution measurement. A minimum of 15 operating detector segments in each quadrant (with at least six detector segments per quadrant below the core midplane and six per quadrant above the core midplane) is required both prior to and following the cycle initial power distribution measurement. The hardware that performs the online power distribution monitoring is configured so that a single hardware failure will not necessitate a reactor maximum power reduction or restrict normal reactor operations.

During plant operation, the in-core instrument thimble assembly is positioned within the fuel assembly and exits through the top of the reactor vessel seal connection. The fixed in-core detector and core exit thermocouple signal exit the detector through a multi-pin connector to the in-core instrument thimble tube cables. The fixed in-core detector and core exit thermocouple cables are then routed to different data conditioning and processing stations. The data is processed and the results are available for display in the main control room (MCR).

22.7.5.2 Departure from Nucleate Boiling and High Power Instrumentation

The OTΔT trip protects the core against low DNBR. The OPΔT trip protects against excessive power (fuel rod rating protection). Factors included in establishing the OTΔT and OPΔT trip setpoints include the reactor coolant temperature in each loop and the axial distribution of core power as seen by ex-core neutron detectors.

22.7.5.3 Instrumentation to Limit Maximum Power Output

The signals from the three ranges (source, intermediate, and power) of neutron flux detectors are used to limit the maximum power output of the reactor within their respective ranges.

There are eight radial locations containing a total of 12 neutron flux detectors installed around the reactor between the vessel and the primary shield. Four proportional counters for the source range are located at the highest fluence portions of the core containing the primary startup sources at an elevation approximately one-fourth of the core height.

Four pulse fission chambers for the intermediate range, located in the same instrument wells as the source range detectors, are positioned at an elevation corresponding to one-half of the core height.

Four uncompensated ionisation chamber assemblies for the power range are installed vertically at the four corners of the core. These assemblies are located equidistant from the reactor vessel along the length and, to minimise neutron flux pattern distortions, within approximately 1 foot of the reactor vessel. Each power range detector provides two signals corresponding to the neutron flux in the upper and lower sections of a core quadrant.

The three ranges of detectors are used as inputs to monitor neutron flux from a completely shutdown condition to 120 percent of full power, with the capability of recording overpower excursions up to 200 percent of full power.

The output of the power range channels is used for the following:

- Protecting the core against the consequences of rod ejection accidents
- Protecting the core against the consequences of adverse power distributions resulting from dropped rods
- Rod speed control function
- Alerting the operator to an excessive power imbalance between the quadrants

The intermediate range detectors also provide signals for the post-accident monitoring system. Details about the neutron detectors, nuclear instrumentation design, and control and trip logic are contained in Sections 19.1.2.7, 19.2.2, 19.2.3, 19.2.5, and 19.12. The limits on neutron flux operation and trip setpoints are given in the Tech Specs.

22.8 FUNCTIONAL DESIGN OF REACTIVITY CONTROL SYSTEMS

22.8.1 Information for Control Rod Drive System

The CRDM and operation of the control rod drive system are described in Reference 22.2. No hydraulic system is associated with the functioning of the control rod drive system. The instrumentation and controls for the reactor trip system and the reactor control system are described here in Sections 19.1.4, 19.2.2, 19.2.3.1, 19.2.5, and 19.3.6.

The parts of the CRDMs and control rod drive line exposed to reactor coolant are made of metals that resist the corrosive action of the coolant. Three types of metals are used exclusively: stainless steels; nickel-chromium-iron alloys; and, to a limited extent, cobalt-based alloys. These materials have provided many years of successful operation in similar CRDMs. In the case of stainless steels, only austenitic and martensitic stainless steels are used.

The material selection is based in part on the duty cycle specified for the CRDMs and control rods. The materials are specified so that the components do not suffer adverse effects, such as excessive wear or galling, as a result of a minimum 300 trips from full power and 60 coupling and decoupling cycles of the drive rod coupling assembly.

The material for the CRDMs and the control rod assemblies is selected for acceptable performance, that is, the design goal is to achieve a service life of 9×10^6 full-step cycles. Inspection or changes in operation indicate the need for replacement or refurbishment.

The worst-case result of undetected wear of a CRDM or drive rod is a rod assembly drop or a failure to drop an assembly during a trip. Both events are accounted for in safety analyses. The pressure boundary components are not subject to significant wear due to stepping cycles.

The drive rod assembly is also immersed in the reactor coolant and uses a Type 410 stainless-steel drive rod. The drive rod coupling is machined from Type 403 stainless steel. Other parts are Type 304 stainless steel with the exception of the springs, which are nickel-chromium-iron alloy, and the locking button, which is fabricated of cobalt-alloy bar stock or a qualified substitute.

The absorber rodlets in the RCCAs and the GRCAs are closed stainless-steel tubes (cladding) containing absorber material. The stainless-steel cladding isolates from the reactor coolant, the absorber material, and other substances inside the tubes. The containment function of the control rod cladding and the effects of neutron flux in the control rod materials are addressed in Section 22.5.

The CRDMs are contained within an integrated head package located on top of the reactor vessel head. This assembly provides the support required for seismic restraint in conjunction with the attachment of the CRDMs to the reactor vessel head. An outer shroud and the seismic restraint structure isolate the CRDMs from the effects of ruptures of high-energy lines outside the shroud and from missiles.

The shroud also is used to direct air from the cooling fans past the CRDMs. The cooling system maintains the temperatures of the coils in the CRDMs below the design operating temperature. The integrated head package provides the proper support and required separation for electrical lines providing power to the CRDMs and signals from the rod position sensors.

The line for the reactor head vent system is located among the CRDMs and is supported by the integrated head package. This line is pressurised to RCS pressure and considered to be a high-energy line; it is constructed to the appropriate requirements of the ASME Code.

22.8.2 Evaluation of the Control Rod Drive System

Rod control systems of the type used in the AP1000 design have been analysed in detailed reliability studies. These studies include fault tree analysis and failure mode and effects analyses. These studies, and the analyses presented in Chapter 9, demonstrate that the control rod drive system performs its intended safety-related function: a reactor trip. The control rod drive system puts the reactor in a subcritical condition when a safety-related system setting is reached with an assumed credible failure of a single active component.

The essential elements of the control rod drive system (those required to provide reactor trip) are isolated from nonessential portions of the rod control system by the reactor trip switchgear. The essential portion of the control rod drive system is shielded from the direct effects of postulated moderate- and high-energy line breaks by the integrated head package. The dynamic effects of pipe ruptures do not have to be considered for those pipes that satisfy the requirements for mechanistic pipe break.

The reactor vessel head vent lines and instrumentation conduits are 25.4-mm (1 inch) nominal diameter or smaller. Breaks in lines of this size do not have to be postulated for dynamic effects, pressurisation, and spray wetting. The pressure boundary housing of the CRDMs is constructed to ASME requirements and a break in this pressure boundary is not credible.

The only instrumentation required of the CRDM and supporting systems to operate safely is the rod position indicator. A break in the cables connected to the rod position indicators would neither preclude a reactor trip nor result in an unplanned withdrawal of a rod assembly. A break in the power cable to the CRDM coils results in a drop of the rod assembly.

Information on the pressure and temperature of the CRDMs and surrounding areas is not required for safe operation. The design pressure and temperature of the CRDM housing is the same as the RCS, which is protected by safety valves. Overheating of the CRDM coils caused by a failure of the cooling system would in the worst case result in a drop of one or more rod

assemblies. The reactor and reactor protection system are designed to accommodate and protect against rod drop events.

22.8.3 Testing and Verification of the Control Rod Drive System

The control rod drive system is extensively tested prior to its operation. These tests may be subdivided into the following five categories:

- Prototype tests of components
- Prototype control rod drive system tests
- Production tests of components following manufacture and prior to installation
- Onsite preoperational and initial startup tests
- Periodic in-service tests

These tests are conducted to verify the operability of the control rod drive system when called upon to function.

22.8.4 Evaluation of Combined Reactivity Control Performance

The evaluations of the SLB, the feedwater line break, and the small-break LOCA, which presume the combined actuation of the reactor trip system, the control rod drive system, and the passive safety injection, are presented in Chapter 9, Sections 9.1.5, 9.1.6, 9.2.8, and 9.6. Reactor trip signals and signals to actuate passive safety features for these events are generated from functionally diverse sensors. These signals actuate diverse means of reactivity control, i.e., control rod insertion and injection of soluble neutron absorber.

Nondiverse but redundant types of equipment are used only in processing the incoming sensor signals into appropriate logic, which initiates the protective action. In particular, protection from equipment failures is provided by redundant equipment and periodic testing. Reliability studies, including failure mode and effects analysis for this type of equipment, verify that a single failure does not have an adverse effect upon the engineered safety features actuation system.

In addition to providing automatic actuations, the diverse actuation system (DAS) also provides for manual actuation of the reactor trip.

The probability of a common mode failure impairing the ability of the reactor trip system to perform its safety-related function is extremely low (see Chapters 10, 26 and 27). For all frequent faults an analysis is performed which considers failure of the reactor trip system, as presented in Chapter 9. The large-break LOCA is analysed assuming a failure of rod insertion, due to hydrodynamic effects. The evaluation of the large-break LOCA in Section 9.9 demonstrates that voiding in combination with borated injection water shuts down the reactor with no rods required. Decay heat is removed via passive injection and venting through the break and ADS valves.

22.9 REACTOR OPERATION

22.9.1 Operating Constraints

The fuel system requires constraints on the operating regime of the reactor to continue to meet the safety criteria defined in Section 22.2. Operational constraints are initially defined in the safety analysis of the first core design and then are either validated or modified for reload cores in the reload safety analysis. The key operational parameters that are constrained and the associated required corrective actions are defined in the plant Tech Specs. The specific numerical limits associated with the constrained parameters for each core design are provided in the COLR. Periodic surveillance measurements are also implemented in the plant Tech Specs to confirm that the plant is operating within the allowed constraints and that the fuel system is performing within DB limits.

Some of the fuel DB limits are monitored directly through the on-line core monitoring system. These limits include F_Q and $F_{\Delta H}^N$, DNBR, and SDM. The core monitoring system provides alarms upon approaching or exceeding these parameters and the Tech Specs define requirements for corrective actions should the limits ever be exceeded. Additional information on the online core monitoring system including the safety claims, arguments, and evidence for the system are provided in Reference 22.96.

In the unlikely event the core monitoring system becomes nonfunctional during a cycle, the axial flux difference and QPTR Tech Specs which are confirmed using the Data Display and Processing System remain applicable and contingency Tech Specs become applicable to ensure that fuel design limits and operating constraints continue to be met. Specifically, the rod insertion limits become more restrictive to ensure that the power distribution and SDM limits will be met in all normal operating scenarios. The axial flux difference and QPTR limits will remain applicable to ensure that the F_Q limit is met. The contingency Tech Spec limits are more restrictive because they are developed under the assumption that the plant is operating with limiting transient xenon conditions and because the surveillance requirements on the DB limits are performed only periodically as opposed to continuously by the core monitoring system.

Plant trip setpoints on OPΔT and OTΔT also define operating constraints that protect the fuel DB limits under frequent fault conditions. The trip setpoints are independent of core monitoring system operation. Continued applicability of the trip setpoints is confirmed prior to each operating cycle.

The design analysis performed for the fuel system prior to each operating cycle in conjunction with the operating constraints defined by the plant Tech Specs ensures that the fuel safety criteria defined in Section 22.2 will continue to be met.

22.10 CONCLUSIONS

This chapter provides a safety justification of the fuel elements in the AP1000 reactor. For normal operation, this means that all reasonable steps should be taken to minimise the failure of the fuel rod cladding and thus minimise the release of radioactive fission products into the coolant. For fault conditions, the definition of satisfactory performance depends on the frequency with which the fault is expected to occur.

The limits within which the fuel can operate safely during both normal and fault conditions have been defined and justified to demonstrate safe operation of the fuel. To achieve this, safety design bases and design limiting criteria have been defined, leading to the

establishment of mechanical, nuclear, and thermal hydraulic design bases inherent in the safety design approach. It is demonstrated that none of the design bases or limiting criteria is exceeded when the fuel is subjected to the full range of operational and fault conditions.

22.11 REFERENCES

22.1 IAEA NS-G-1.12, "Design of the Reactor Core for Nuclear Power Plants," International Atomic Energy Agency, April 2005.

22.2 Westinghouse Document APP-RXS-M3-001, Rev. 6, "Reactor System (RXS) System Specification Document (SSD)," May 2014.

22.3 Westinghouse Document WCAP-14342-A, "VANTAGE+ Fuel Assembly Reference Core Report," April 1995. Addendum 1, February 2003.

22.4 Westinghouse Documents WCAP-12488-A and WCAP-14204-A, "Westinghouse Fuel Criteria Evaluation Process," October 1994.

22.5 Westinghouse Document NRFE-10-59, Rev. 2, "AP1000 Fuel Development Design Closeout," July 2011.

22.6 Westinghouse Documents WCAP-10125-P-A and WCAP-10126-NP-A, "Extended Burnup Evaluation of Westinghouse Fuel," December 1985.

22.7 Westinghouse Document WCAP-15064-NP-A, "Westinghouse Improved Performance Analysis and Design Model (PAD 4.0)," July 2000.

22.8 Not Used.

22.9 Westinghouse Letter DCP_JNE_000376, Rev. 0, "Demonstration of Protection Against PCI Fuel Failure," September 2010.

22.10 Westinghouse Letter DCP_JNE_000375, Rev. 0, "RIA Fault Safety Margins," September 2010.

22.11 Westinghouse Report NRFE-10-45, "AP1000 Top Nozzle Mechanical Confirmatory Test Report," November 2009.

22.12 Water Reactor Fuel Performance Meeting, Post Irradiation Examinations on 67-75GWd/t Rods for Confirmation of the Integrity and Appropriate Performance of the Claddings for Future, Kyoto, Japan, October 2005, Paper No. 1057.

22.13 Westinghouse Documents WCAP-9179 and WCAP-9224, "Properties of Fuel and Core Component Materials," July 1978.

22.14 Not Used.

22.15 Westinghouse Document WCAP-10377-A, "Westinghouse Wet Annular Burnable Absorber Evaluation Report," October 1983.

22.16 Westinghouse Document WCAP-10445-NP-A, "Reference Core Report VANTAGE 5 Fuel Assembly," September 1985.

22.17 Westinghouse Document WCAP-8288, "Safety Analysis of the 17×17 Fuel Assembly for Combined Seismic and Loss of Coolant Accident," December 1973.

22.18 Westinghouse Document WCAP-9402-A, "Verification, Testing and Analysis of the 17×17 Optimised Fuel Assembly," August 1981.

22.19 Westinghouse Document WCAP-9283, "Integrity of the Primary Piping Systems of Westinghouse Nuclear Power Plants During Postulated Seismic Events," March 1978.

22.20 Westinghouse Letter DCP_JNE_000327, Rev. 0, "The Effects of Assembly Bow on Safety Margins," August 2010.

22.21 Westinghouse Document WCAP-3680-22 (EURAEC-2116), "Xenon-Induced Spatial Instabilities in Three Dimensions," September 1969.

22.22 Westinghouse Report MFRD-01-142, "Corrosion Crack Susceptibility of Stainless Steel Top Nozzle Castings in PWR Primary Coolant," September 2001.

22.23 Westinghouse Report NRFE-10-9, "AP1000 Top Nozzle Holddown Spring Loose Parts Final Confirmatory Test Report," January 2010.

22.24 Westinghouse Report NRFE-10-149, "AP1000 Longitudinal eIFM Grid Dynamic Crush Strength Final Verification Test Report," August 2010.

22.25 Westinghouse Report NRFE-10-136, "AP1000 Longitudinal eRFA Mid Grid Dynamic Crush Strength Final Verification Test Report," August 2010.

22.26 Westinghouse Document WCAP-7941-P-A, "Effect of Axial Spacing on Interchannel Thermal Mixing with the R Mixing Vane Grid," January 1975.

22.27 Westinghouse Document WCAP-8219-A, "Fuel Densification Experimental Results and Model for Reactor Application," March 1975.

22.28 Westinghouse Document WCAP-13589-A, "Assessment of Clad Flattening and Densification Power Spike Factor Elimination in Westinghouse Nuclear Fuel," March 1993.

22.29 USNRC Letter, Peralta, J. D. to Maurer, B. F., "Approval for Increase in Licensing Burnup to 62,000 MWD/MTU (TAC No. MD1486)," May 25, 2006

22.30 Westinghouse Document WCAP-9500-A, "Reference Core Report 17x17 Optimised Fuel Assembly," May 1982.

22.31 ASTM E142-86, "Standard Method for Controlling Quality of Radiographic Testing," ASTM International, 1986.

22.32 Westinghouse Document WCAP-8183, Rev. 23, "Operational Experiences with Westinghouse Cores," December 1994.

22.33 ANSI N18.2a-75, "Nuclear Safety Criteria for the Design of Stationary Pressurized Water Reactor Plants." 1975.

22.34 Westinghouse Document WCAP-8330, "Westinghouse Anticipated Transients Without Reactor Trip Analysis," August 1974.

22.35 Westinghouse Document WCAP-7308-L-P-A, "Evaluation of Nuclear Hot Channel Factor Uncertainties," June 1988.

22.36 Westinghouse Documents WCAP-16943-P-A and WCAP-16943-NP-A, "Enhanced GRCA Rodlet Design," September 2012.

22.37 Westinghouse Document WCAP-8359, "Effects of Fuel Densification Power Spikes on Clad Thermal Transients," July 1974.

22.38 EPRI NP-3814, "Rhodium In-Core Detector Sensitivity Depletion, Cycles 2-6," Electric Power Research Institute, December 1984.

22.39 Westinghouse Document WCAP-7811, "Power Distribution Control of Westinghouse Pressurised Water Reactors," December 1971.

22.40 Westinghouse Documents WCAP-8385 and WCAP-8403, "Power Distribution Control and Load Following Procedures," September 1974.

22.41 Westinghouse Document WCAP-10217-A-R1A, "Relaxation of Constant Axial Offset Control, F_Q Surveillance Technical Specification," February 1994.

22.42 Westinghouse Document WCAP-7912-A, "Power Peaking Factors," January 1975.

22.43 Westinghouse Document WCAP-12473-A, "BEACON – Core Monitoring and Operations System," August 1994: Addendum 1, May 1996; Addendum 2, March 2001; Addendum 4, September 2012.

22.44 Westinghouse Document WCAP-3696-8, "Pressurised Water Reactor pH – Reactivity Effect Final Report," October 1968.

22.45 Westinghouse Documents WCAP-9217 and WCAP-9218, "Results of the Control Rod Worth Program," October 1977.

22.46 Studsvik/SOA-95/1, CASMO-4, "A Fuel Assembly Burn-up Program User's Manual," December 1981.

22.47 Westinghouse Document WCAP-3680-20, "Xenon-Induced Spatial Instabilities in Large Pressurised Water Reactors," March 1968.

22.48 Westinghouse Document WCAP-3680-21, "Control Procedures for Xenon-Induced X-Y Instabilities in Large Pressurised Water Reactors," February 1969.

22.49 Westinghouse Document WCAP-6073, "LASER – A Depletion Program for Lattice Calculations Based on MUFT and THERMOS," April 1966.

22.50 Westinghouse Document WCAP-2048, "The Doppler Effect for a Non-Uniform Temperature Distribution in Reactor Fuel Elements," July 1962.

22.51 Westinghouse Document WCAP-11597-A, "Qualification of the PHOENIX/ANC Nuclear Design System for Pressurised Water Reactor Cores," June 1988.

22.52 Nuclear Science and Engineering, Criticality Calculation for Uniform Water-Moderated Lattices, September 1965.

22.53 NUCLEX 72 Technical Meeting, High Temperature Critical Experiments with H_2O Moderated Fuel Assemblies in KRITZ, October 1972.

22.54 BAW-3647-20, "Physics Verification Program Part III Summary Report," Babcock & Wilcox, March 1971.

22.55 Westinghouse Document WCAP-3017-6094, "Yankee Core Evaluation Program Final Report," January 1971.

22.56 Westinghouse Document WCAP-10966-A, "ANC: A Westinghouse Advanced Nodal Computer Code," September 1986.

22.57 Westinghouse Document WCAP-15026-NP-A, "Modified WRB-2 Correlation, WRB-2M, for Predicting Critical Heat Flux in 17x17 Rod Bundles with Modified LPD Mixing Vane Grids," April 1999.

22.58 Westinghouse Document WCAP-16045-P-A, "Qualification of the Two-Dimensional Transport Code PARAGON," August 2004.

22.59 AEC Critical Review Series, TID-25887, "Boiling Crisis and Critical Heat Flux," September 1972.

22.60 Westinghouse Document WCAP-7959-A, "Effect of Axial Spacing on Interchannel Thermal Mixing with the R Mixing Vane Grid," January 1975.

22.61 Westinghouse Document WCAP-15306-NP-A, "VIPRE-01 Modeling and Qualification for Pressurised Water Reactor Non-LOCA Thermal-Hydraulic Safety Analysis," October 1999.

22.62 Westinghouse Documents WCAP-8296-P-A and WCAP-8297-A, "The Effect of 17×17 Fuel Assembly Geometry on DNB," February 1975.

22.63 Westinghouse Document WCAP-8174-P-A, "Effect of Local Heat Flux Spikes on DNB in Non-Uniformly Heated Rod Bundles," February 1975.

22.64 Westinghouse Document WCAP-11397-A, "Revised Thermal Design Procedure," April 1989.

22.65 Westinghouse Documents WCAP-8054-P-A and WCAP-8195-A, "Applications of the THINC-IV Program to PWR Design," February 1989.

22.66 Westinghouse Documents WCAP-8691-R1 and WCAP-8692-R1, "Fuel Rod Bow Evaluation," July 1979.

22.67 EPRI NP-2511-CCM-A, "VIPRE-01: A Thermal Hydraulic Code for Reactor Core," Electric Power Research Institute, August 1989.

22.68 Gyllander, J. A., AE-411, "In-Pile Determination of the Thermal Conductivity of UO_2 in the Range 500 to 2500°C," January 1971.

22.69 Westinghouse Document WCAP-6069, "Burnup Physics of Heterogeneous Reactor Lattices," June 1965.

22.70 Westinghouse Letter DCP_JNE_000373, Rev. 0, "Effect of Crud on Fuel Safety Margins and Associated Regulatory Observation Actions," September 2010.

22.71 Nuclear Engineering Design, "Review of Two Phase Flow Instability," September 1973.

22.72 Nuclear Science Technology, "Stagnant Fluid Due to Local Flow Blockage," October 1972.

22.73 Westinghouse Document WCAP-8175, "Effect of Flow Blockage on DNB," January 1994.

22.74 Westinghouse Documents WCAP-8745-P-A and WCAP-8746-A, "Design Bases for the Thermal Overpower ΔT and Thermal Overtemperature ΔT Trip Functions," September 1986.

22.75 Not Used.

22.76 BAW-3647-30, "Physics Verification Program Part III, Task 11: Quarterly Technical Report January-March 1974," Babcock & Wilcox, July 1974.

22.77 BAW-3647-31, "Physics Verification Program Part III, Task 11: Quarterly Technical Report July-September 1974," Babcock & Wilcox, February 1975.

22.78 Westinghouse Document WCAP-3385-56 Part II, "Saxton Core II Fuel Performance Evaluation Part II: Evaluation of Mass Spectrometric and Radiochemical Analyses of Irradiated Saxton Plutonium Fuel," July 1970.

22.79 Westinghouse Document WCAP-3385-56 Part I, "Saxton Core II - Fuel Performance Evaluation Part I: Materials," September 1971.

22.80 Westinghouse Document WCAP-3385-36, "Saxton Plutonium Project – Quarterly Progress Report for the Period Ending June 20, 1973," July 1973.

22.81 Westinghouse Document WCAP-3385-37, "Saxton Plutonium Project – Quarterly Progress Report for the Period Ending September 30, 1973," December 1973.

22.82 Westinghouse Document WCAP-7806, "Nuclear Design of Westinghouse Pressurized Water Reactors with Burnable Poison Rods," December 1971.

22.83 Westinghouse Document WCAP-16045-P-A Addendum 1-A, "Qualification of the NEXUS Nuclear Data Methodology," August 2007.

22.84 Westinghouse Document WCAP-10965-P-A Addendum 2-A, "Qualification of the New Pin Power Recovery Methodology," September 2010.

22.85 Westinghouse Document WCAP-6065, "Melting Point of Irradiated UO_2," February 1965.

22.86 Westinghouse Document WCAP-14565-P-A Addendum 1-A, "Addendum 1 to WCAP-14565-P-A Qualification of ABB Critical Heat Flux Correlations with VIPRE-01 Code," August 2004.

22.87 Westinghouse Document WCAP-14565-P-A Addendum 2-A, "Addendum 2 to WCAP-14565-P-A Extended Application of ABB-NV Correlation and Modified ABB-NV Correlation WLOP for PWR Low Pressure Applications," April 2008.

22.88 Journal of Nuclear Energy 21, "Prediction of Departure from Nucleate Boiling for an Axially Nonuniform Heat Flux Distribution," pp 241-248, 1967.

22.89 Westinghouse Document WCAP-12610-P-A, Addendum 2-A, WCAP-1432-A & CENPD-404-NP-A, Addendum 2-A, "Westinghouse Clad Corrosion Model for ZIRLO and Optimized ZIRLO," October 2013.

22.90 Westinghouse Document WCAP-8963-P-A, November 1976 and WCAP-8964-A, "Safety Analysis for the Revised Fuel Rod Internal Pressure Design Basis," August 1977.

22.91 Westinghouse Document WCAP-8963-P-A, Addendum 1-A, Rev. 1-A, "Safety Analysis for the Revised Fuel Rod Internal Pressure Design Basis (Departure from Nucleate Boiling Mechanistic Propagation Methodology)," June 2006.

22.92 Westinghouse Document PDPELI00, Rev. 57, "BURNABLE ABSORBER COATED URANIUM DIOXIDE PELLETS," 2016.

22.93 Westinghouse Document APP-RXS-M3C-025, Rev. 6, "AP1000 Plant Design - Thermal-Hydraulic Analysis Using the THRIVE Code," November 2015.

22.94 Westinghouse Document WCAP-17642-P, Rev. 0, "Westinghouse Performance Analysis and Design Model (PAD5)," October 2013.

22.95 Westinghouse Document APP-GW-GEM-200, Rev. 4, "AP1000 Chemistry Manual," March 2016.

22.96 Westinghouse Document UKP-GW-GL-162, Rev. 1, "UK AP1000 BEACON Core Monitoring System Basis of Safety Case," October 2016.

22.97 Westinghouse Document UKP-GW-GLR-035, Rev. 0, "UK AP1000® Fuel Tolerability Assessment of Depressurisation of the Primary Circuit," August 2016.

22.98 Westinghouse Document APP-RXS-M3C-105, Rev. 1, "Source Range Detector Weighting Factors for AP1000 Sub-Critical Rod Worth Measurement Application," August 2016.

22.99 Westinghouse Document UKP-SSAR-F5-001, Rev. 0, "AP1000 Safety Analysis Checklist (SAC) & Future Limits," July 2016.

22.100 Westinghouse Document WCAP-9272-P-A, Rev. 0, "Westinghouse Reload Safety Evaluation Methodology," July 1985.

22.101 Westinghouse Document PDPELEAP00, Rev. 1, "Standardized Uranium Dioxide Pellets Specification," March 2016.

22.102 Westinghouse Document CN-NFPE-08-26, Rev. 0, "Absorber Temperature Evaluation of Preliminary NG RCCA designs," June 2008.

22.103 Westinghouse Document CN-AP1000-SA-060, Rev. 3, "Revision 3** Absorber Rod Cooling Analysis," May 2011.

22.104 Westinghouse Document CN-NRFE-09-47, Rev. 2, "AP1000 Gray Rod Absorber Temperature Evaluation for Tungsten Absorber," February 2011.

22.105 Westinghouse Document CN-NRFE-10-29, Rev. 1, "AP1000 Gray Rod Absorber Temperature Evaluation for Tungsten Absorber under Faulted Conditions," January 2011.

22.106 Westinghouse Document APP-FA01-V2-101, Rev. 3, "AP1000 Fuel Assembly Interface Parameters 17x17x168 Active Fuel (.374 DIA Fuel Rod)," September 2011.

22.107 Westinghouse Document APP-FA01-V2-001, Rev. 2, "AP1000 Fuel Rod Layout 168" Active Fuel," April 2009.

22.108 Westinghouse Document MATBZLAP00, Rev. 1, "Seamless ZIRLO® Tubing," July 2013.

22.109 Westinghouse Document APP-FA01-V2-107, Rev. 1, "AP1000 Fuel Assembly Cross Section Layout," July 2010.

22.110 Westinghouse Document PS-PELE04, Rev. 2, "MANUFACTURE of URANIUM DIOXIDE PELLETS," December 2013.

Table 22-1. Fuel Rod Secondary Limits

Type of Fault	Limits	Degradation Mechanisms to which Limits Relate
LOCA	Peak clad temperature ≤1204°C (2200°F) local clad oxidation ≤17%	Remaining below limits ensures that embrittlement of the fuel clad will not occur so that loss of coolable geometry or escape of pellets into the coolant circuit would occur.
RIA	Radial average peak fuel enthalpy rise at hot spot during transients ≤628 J/g (150 cal/g) Peak clad temperature ≤1482°C (2700°F)	Remaining within these limits ensures that disruption of the clad by interaction with the pellet will not occur so that coolable geometry would be lost or fuel pellets could escape into the coolant circuit. Remaining within this limit ensures that embrittling of the fuel clad will not occur so that loss of coolable geometry or escape of pellets into the coolant circuit would occur.
PCM accidents	Peak clad temperature ≤1204°C (2200°F) for boiling times <350 s. For longer boiling times, the allowable peak clad temperature is reduced linearly with log (time) being 875°C (1607°F) at 10,000 s.	Remaining within this limit ensures that embrittling of the fuel clad will not occur so that loss of coolable geometry or escape of pellets into the coolant circuit would occur.

Table 22-2. Reactor Core Description (First Cycle)

Active Core	
Equivalent diameter	304.0 cm (119.7 in)
Active fuel height first core (cold)	426.7 cm (168 in)
Height-to-diameter ratio	1.40
Total cross-section area	7.26 m^2 (78.14ft^2)
H_2O/U molecular ratio (cell, cold)	2.40
Reflector Thickness and Composition	
Top – water plus steel	~25.4 cm (10 in)
Bottom – water plus steel	~25.4 cm (10 in)
Side – water plus steel	~38.1 cm (15 in)
Fuel Assemblies	
Number	157
Rod array	17x17
Rods per assembly	264
Rod pitch	1.26 cm (0.496 in)
Overall transverse dimensions	21.402 x 21.402 cm (8.426 x 8.426 in)
Fuel weight, as uranium dioxide	95,975 kg (211,588 lb)
ZIRLO clad weight	19,552 kg (43,105 lb)
Number of grids per assembly	
Top and bottom	2 Alloy 718
Intermediate	8 **ZIRLO**
IFM	4 **ZIRLO**
Protective	1 Alloy 718
Number of guide thimbles per assembly	24
Composition of guide thimbles	**ZIRLO**
Diameter of guide thimbles – upper part	1.123 cm ID x 1.224 cm OD (0.442 in ID x 0.482 in OD)
Diameter of guide thimbles – lower part	1.008 cm ID x 1.224 cm OD (0.397 in ID x 0.482 in OD)
Diameter of instrument guide thimbles	1.123 cm ID x 1.224 cm OD (0.442 in ID x 0.482 in OD)

Table 22-2. Reactor Core Description (First Cycle) (cont.)

Fuel Rods	
Number	41,448
Outside diameter	0.950 cm (0.374 in)
Diameter gap	0.0165 cm (0.0065 in)
Clad thickness	0.0572 cm (0.225 in)
Clad material	**ZIRLO**
Fuel Pellets	
Material	Uranium dioxide sintered
Density (% of theoretical) (nominal)	95.5
Fuel enrichments, first core (average w/o midzone/blanket)	
Region 1	0.74 / ---
Region 2	1.58 / ---
Region 3	3.20 / 1.58
Region 4	3.776 / 3.20
Region 5	4.376 / 3.20
Diameter	0.81915 cm (0.3225 in)
Length	0.983 cm (0.387 in)
Mass of uranium dioxide per unit length of fuel rod	0.545 kg/m (0.366 lb/ft)
RCCAs	
Neutron absorber	Ag-In-Cd
Diameter	0.866 cm (0.341 in)
Density	10.16 g/cm^3 (0.367 lb/in^3)
Cladding material	Type 304 or 304L, cold-worked SS
Cladding OD	0.968 cm (0.381 in)
Cladding thickness	0.047 cm (0.0185 in)
Number of clusters – full length	53
Number of absorber rods per cluster	24

Table 22-2. Reactor Core Description (First Cycle) (cont.)

GRCAs	
Neutron absorber	Tungsten / Alloy 718
Diameter	Tungsten 0.500 cm (0.197 in) / Alloy 718 0.787 cm (0.310 in)
Density	Tungsten 19.24 g/cm^3 (0.695 lb/in^3) / Alloy 718 8.19 g/cm^3 (0.296 lb/in^3)
Cladding material	Type 304 or 304L, cold-worked SS
Clad thickness	0.065 cm (0.0255 in)
Number of clusters – full length	16
Number of absorber rods per cluster	24
Discrete BA Rods (First Core)	
Number	592
Material	Alumina Boron-Carbide
Outer diameter	0.968 cm (0.381 in)
Inner tube, outer diameter	0.678 cm (0.267 in)
Clad material	Zircaloy
Inner tube material	Zircaloy
B-10 content	6.03 mg/cm (0.0004 lb/ft)
Absorber length	See Figure 22.20
IFBAs (First Core)	
Number	5632
Type	IFBA
Material	Boride coating
B-10 content	0.773 mg/cm (0.000052 lb/ft)
Absorber length	386.1 cm (152 in)
Excess Reactivity	
Maximum fuel assembly K∞ (cold, clean, unborated water)	1.392
Maximum core reactivity k_{eff} (cold, zero power, beginning of cycle, zero soluble boron)	1.201

Table 22-3. Nuclear Design Parameters (First Cycle)

Core average linear power, including densification effects	18.76 kW/m (5.72 kW/ft)	
Total heat flux hot channel factor, F_Q	≤2.60	
Nuclear enthalpy rise hot channel factor, $F^N_{\Delta H}$	≤1.72	
Reactivity coefficients	Design Limits	Typical Best Estimate
Doppler-only power coefficients (see Figure 9.0-3) (pcm/% power)(1)		
Upper curve	-19.4 to -12.6	-14.6 to -9.0
Lower curve	-10.2 to -6.7	-12.4 to -8.9
Doppler temperature coefficient (pcm/°C)(1)	-6.3 to -1.8	-3.8 to -2.5
(Doppler temperature coefficient (pcm/°F)(1)	-3.5 to -1.0	-2.1 to -1.4)
Moderator temperature coefficient (pcm/°C)(1)	0 to -72	0 to -63
(Moderator temperature coefficient (pcm/°F)(1)	0 to -40	0 to -35)
Boron coefficient (pcm/ppm)(1)	-13.5 to -5.0	-11.3 to -7.2
Rodded moderator density coefficient (pcm/g/cm^3)(1)	≤ 0.47x10^5	≤ 0.45x10^5
Delayed neutron fraction and lifetime, β_{eff}	0.0075(0.0044)(2)	
Prompt Neutron Lifetime, ℓ^*, μs	19.8	
Control rods		
Rod requirements	See Table 22-4	
Maximum ejected rod worth	See Chapter 9	
Typical Bank worth HZP no overlap (pcm)(1)	BOL, Xe Free	EOL, Eq. Xe
MA Bank	238	257
MB Bank	248	327
MC Bank	232	194
MD Bank	239	271
M1 Bank	686	757
M2 Bank	1363	1031
AO Bank	1627	1544

Table 22-3. Nuclear Design Parameters (First Cycle) (cont.)

Typical Hot Channel Factors $F^N_{\Delta H}$ [6]	BOL	EOL
Unrodded	1.44	1.38
MA bank	1.48	1.44
MA + MB banks	1.51	1.43
MA + MB + MC banks	1.51	1.42
MA + MB + MC + MD banks	1.54	1.47
MA + MB + MC + MD + M1 banks	1.63	1.53
AO bank	1.68	1.61
Typical Boron concentrations (ppm)		
Zero power, k_{eff} = 0.99, cold[3] RCCAs out		1427
Zero power, k_{eff} = 0.99, hot[4] RCCAs out		1429
Design basis refuelling boron concentration		2700
Zero power, $k_{eff} \leq 0.95$, cold[3] RCCAs in		1061
Zero power, k_{eff} = 1.00, hot[4] RCCAs out		1321
Full power, no xenon, k_{eff} = 1.0, hot RCCAs out		1160
Full power, equilibrium xenon, k = 1.0, hot RCCAs out		844
Reduction with fuel burnup		
First cycle (ppm)/(GWD/MTU)[5]		See Figure 22-17
Reload cycle (ppm)/(GWD/MTU)		~40

Notes:

1. 1 pcm = 10^{-5} $\Delta\rho$ where $\Delta\rho$ is calculated from two statepoint values of k_{eff} by ln (k_1/k_2).
2. Bounding lower value used for safety analysis.
3. Cold means 20°C (68°F), 0.1 MPa (14.7 psia).
4. Hot means 291.7°C (557°F), 15.5 MPa (2250 psia).
5. 1 GWD = 1000 MWD.
6. Rodded hot channel factors reflect full insertion of each bank at hot full power conditions. Rod Insertion limits for the first cycle prohibit full insertion of the M1 and AO-banks during full power operation. The Rodded hot channel factors for these conditions are therefore not indicative of permitted operating conditions at full rated thermal power.

Table 22-4. Reactivity Requirements for RCCAs

Requirement	First Cycle BOL Worths (%Δρ)	First Cycle EOL Worth (%Δρ)	Equilibrium Cycle EOL Representative Worths (%Δρ)
(1) Total power defect (%Δρ)[1]	1.66	3.14	3.50
Trip rod worth [2]	7.24	6.02	6.41
(2) Less 7% [3]	6.73	5.60	5.96
Shutdown Margin			
Calculated margin (2) – (1)	5.07	2.46	2.46
Required shutdown margin [4]	1.60	1.60	1.60

Notes:

1. Includes Doppler, Moderator Temperature, Redistribution, and Void collapse reactivity effects associated with reducing power from full power to zero. Also includes the effect of inserted control rods at the most limiting allowed insertion point on the total power defect.
2. Negative reactivity inserted by RCCAs on the reactor trip. Assumes RCCAs start at the most limiting allowed insertion point and fully insert on the reactor trip except for the highest worth stuck RCCA. Also conservatively excludes negative reactivity from withdrawn GRCAs which are designed to insert on the reactor trip.
3. 7 percent adjustment to accommodate uncertainties (this assumes the use of Ag-In-Cd RCCAs).
4. The design basis minimum shutdown margin is 1.60 percent.

Table 22-5. Thermal and Hydraulic Comparison (SI units)

Design Parameters	AP1000	AP600	Typical XL Plant
Reactor core heat output (MWt)	3,400	1,933	3800
Reactor core heat output (E+6 BTU/hr)	11,601	6596	12,969
Heat generated in fuel (%)	97.4	97.4	97.4
System pressure, nominal (MPa abs)	15.513	15.513	15.513
System pressure, minimum (MPa abs)	15.100	15.168	15.196
Minimum DNBR at Nominal Conditions			
Typical flow channel	2.59	3.48	2.20
Thimble (cold wall) flow channel)	2.60	3.48	2.12
Minimum DNBR for design transients			
Typical flow channel	>1.25	>1.23	>1.26
Thimble (cold wall) flow channel)	>1.25	>1.22	>1.24
DNB correlation	WRB-2M	WRB-2	WRB-1
Coolant Conditions			
Vessel minimum measured flow rate (t/hr)	52412.6	33747.3	67,539.9
Vessel thermal design flow rate (t/hr)	51482.7	33066.9	65,770.9
Effective flow rate for heat transfer (t/hr)	48443.7	30073.2	60,191.7
Effective flow area for heat transfer (m^2)	3.88	3.58	4.75
Average velocity along fuel rods (m/s)	4.816	3.231	5.060
Average mass velocity (kg/(m^2 hr))	12.45 E+6	8.40 E+6	12.69 E+6
Coolant Temperature			
Nominal inlet (°C)	279.44	278.22	294.00
Average rise in vessel (°C)	42.89	38.67	35.33
Average rise in core (°C)	45.22	42.11	38.17
Average in core (°C)	303.39	300.33	314.33
Average in vessel (°C)	300.89	297.56	311.67
Heat Transfer			
Active heat transfer surface area (m^2)	5267.60	4169.86	6475.34
Average heat flux (W/m^2)	6.287 E+5	4.511 E+5	5.716 E+5

Table 22-5 Thermal and Hydraulic Comparison (SI units) (cont.)

Design Parameters	AP1000	AP600	Typical XL Plant
Maximum heat flux for normal operation (W/m^2)	1.635 E+6	1.174 E+6	1.572 E+6
Average linear power (kW/m)	18.77	13.48	17.06
Peak linear power for normal operation (kW/m)	48.88	35.10	45.93
Peak linear power resulting from overpower transients/operator errors, assuming a maximum overpower of 118% (kW/m)	73.65	73.82	73.65
Peak linear power for prevention of centreline melt (kW/m)	73.82	73.82	73.65
Power density (kW/litre of core)	109.7	78.82	98.8
Specific power (kW/kg uranium)	40.2	28.89	36.6
Fuel central temperature			
Peak at peak linear power for prevention of centreline melt (°C)	2593.33	2593.33	2593.33
Pressure Drop			
Across core (MPa)	0.267±0.027	0.121±0.012	0.268±0.027
Across vessel, including nozzle (MPa)	0.447±0.045	0.312±0.031	0.412±0.041

Table 22-5. Thermal and Hydraulic Comparison (Imperial units)

Design Parameters	AP1000	AP600	Typical XL Plant
Reactor core heat output (MWt)	3,400	1,933	3800
Reactor core heat output (E+6 BTU/hr)	11,601	6596	12,969
Heat generated in fuel (%)	97.4	97.4	97.4
System pressure, nominal (psia)	2250	2250	2250
System pressure, minimum (psia)	2190	2200	2204
Minimum DNBR at Nominal Conditions			
Typical flow channel	2.59	3.48	2.20
Thimble (cold wall) flow channel)	2.60	3.48	2.12
Minimum DNBR for design transients			
Typical flow channel	>1.25	>1.23	>1.26
Thimble (cold wall) flow channel)	>1.25	>1.22	>1.24
DNB correlation	WRB-2M	WRB-2	WRB-1
Coolant Conditions			
Vessel minimum measured flow rate (10^6 lbm/hr) (gpm)	 115.55 310,670	 74.4 193,200	 148.9 403,000
Vessel thermal design flow rate (10^6 lbm/hr) (gpm)	 113.5 296,000	 72.9 189,600	 145.0 392,000
Effective flow rate for heat transfer (10^6 lbm/hr) (gpm)	 106.8 278,500	 66.3 172,500	 132.7 358,700
Effective flow area for heat transfer (ft^2)	41.8	38.5	51.1
Average velocity along fuel rods (ft/s)	15.8	10.6	16.6
Average mass velocity (10^6 lbm/hr-ft^2)	2.55	1.72	2.60
Coolant Temperature			
Nominal inlet (°F)	535.0	532.8	561.2
Average rise in vessel (°F)	77.2	69.6	63.6
Average rise in core (°F)	81.4	75.8	68.7
Average in core (°F)	578.1	572.6	597.8
Average in vessel (°F)	573.6	567.6	593.0

Table 22-5. Thermal and Hydraulic Comparison (Imperial units)

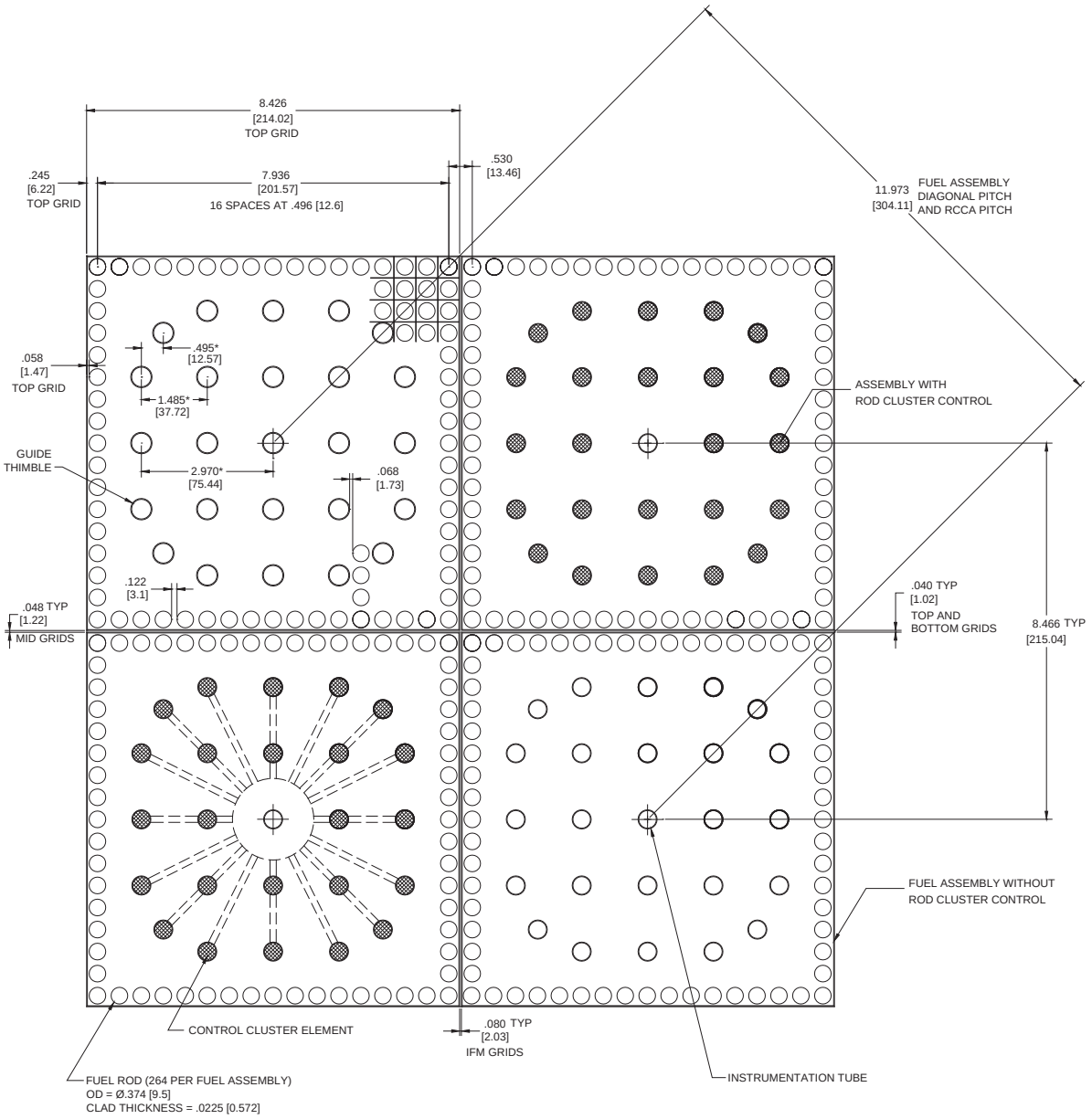
Design Parameters	AP1000	AP600	Typical XL Plant
Heat Transfer			
Active heat transfer surface area (ft^2)	56,700	44,884	69,700
Average heat flux (BTU/hr-ft^2)	193,300	143,000	181,200
Maximum heat flux for normal operation (BTU/hr-ft^2)	518,200	372,226	498,200
Average linear power (kW/ft)	5.72	4.11	5.20
Peak linear power for normal operation (kW/ft)	14.9	10.7	14.0
Peak linear power resulting from overpower transients/operator errors, assuming a maximum overpower of 118% (kW/ft)	22.45	22.5	22.45
Peak linear power for prevention of centreline melt (kW/ft)	22.5	22.5	22.45
Power density (kW/litre of core)	109.7	78.82	98.8
Specific power (kW/kg uranium)	40.2	28.89	36.6
Fuel central temperature Peak at peak linear power for prevention of centreline melt (°C)	4700	4700	4700
Pressure Drop			
Across core (psi)	38.7±3.9	17.5±1.7	38.8±3.9
Across vessel, including nozzle (psi)	64.8±6.5	45.3±4.5	59.7±6.0

Table 22-6. Void Fractions at Nominal Reactor Conditions with Design Hot Channel Factors

	Average	Maximum
Core (%)	0.0	–
Hot subchannel (%)	0.3	2.1

Table 22-7. Typical Neutron Flux Levels (n/cm^2/s) At Full Power

	E ≥ 1.0 MeV	1.00 MeV > E ≥5.53 KeV	5.53 KeV > E ≥0.625 eV	E < 0.625 eV
Core centre	$1.12x10^{14}$	$1.76x10^{14}$	$1.28x10^{14}$	$5.47x10^{13}$
Core outer radius at midheight	$3.86x10^{13}$	$6.08x10^{13}$	$4.42x10^{13}$	$1.83x10^{13}$
Core top, on axis	$3.02x10^{13}$	$4.75x10^{13}$	$3.46x10^{13}$	$2.17x10^{13}$
Core bottom, on axis	$2.92x10^{13}$	$4.59x10^{13}$	$3.34x10^{13}$	$2.40x10^{13}$
Pressure vessel ID azimuthal peak	$4.71x10^{10}$	$8.4x10^{10}$	$5.56x10^{10}$	$5.32x10^{10}$



PRIMARY DIMENSIONS ARE IN INCHES (NOMINAL)
SECONDARY DIMENSIONS ARE IN MILLIMETERS

* GUIDE THIMBLE LOCATIONS
AT TOP NOZZLE ADAPTER PLATE

Figure 22-1. Fuel Assembly Cross-Section

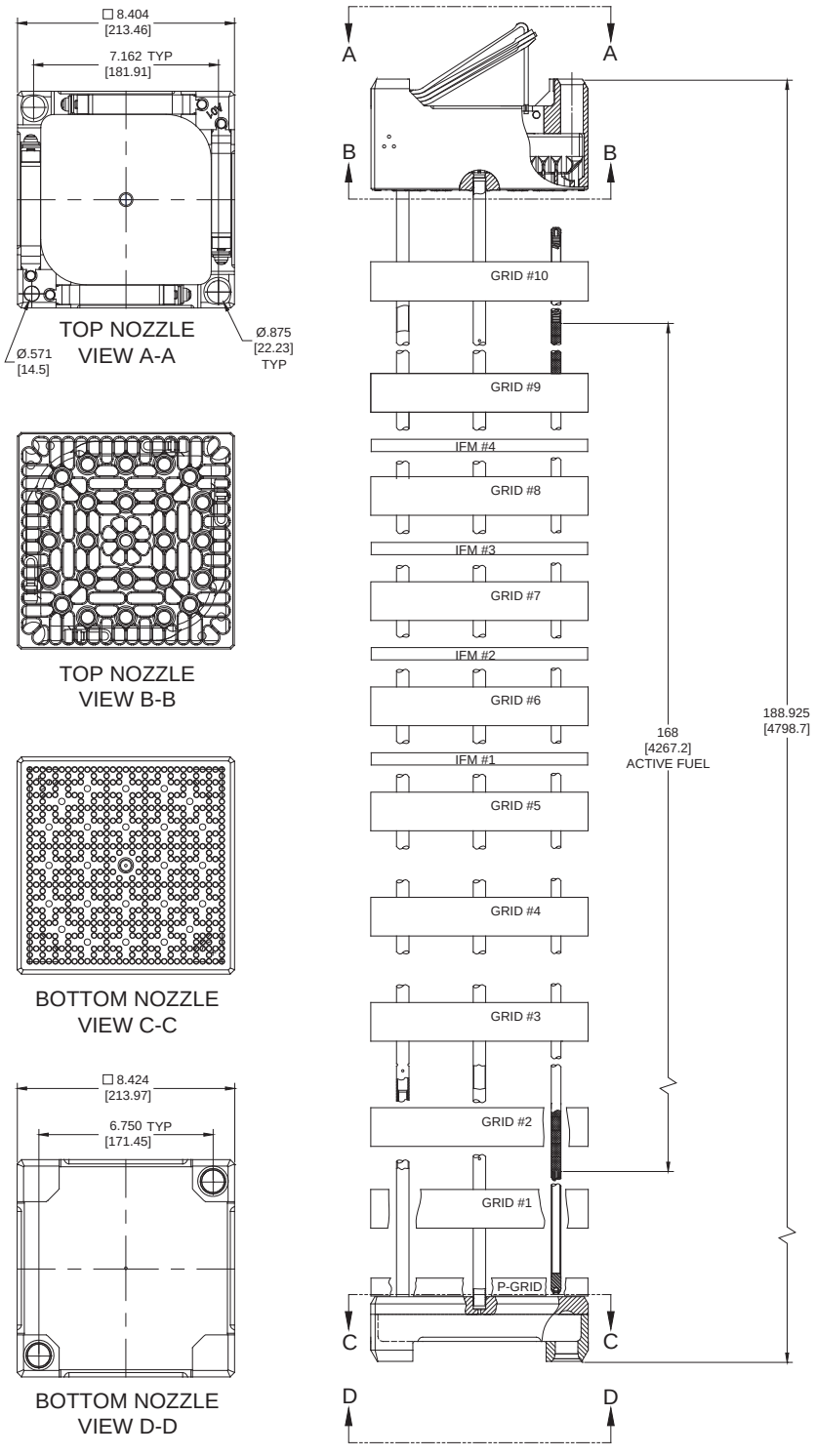


Figure 22-2. Fuel Assembly Outline

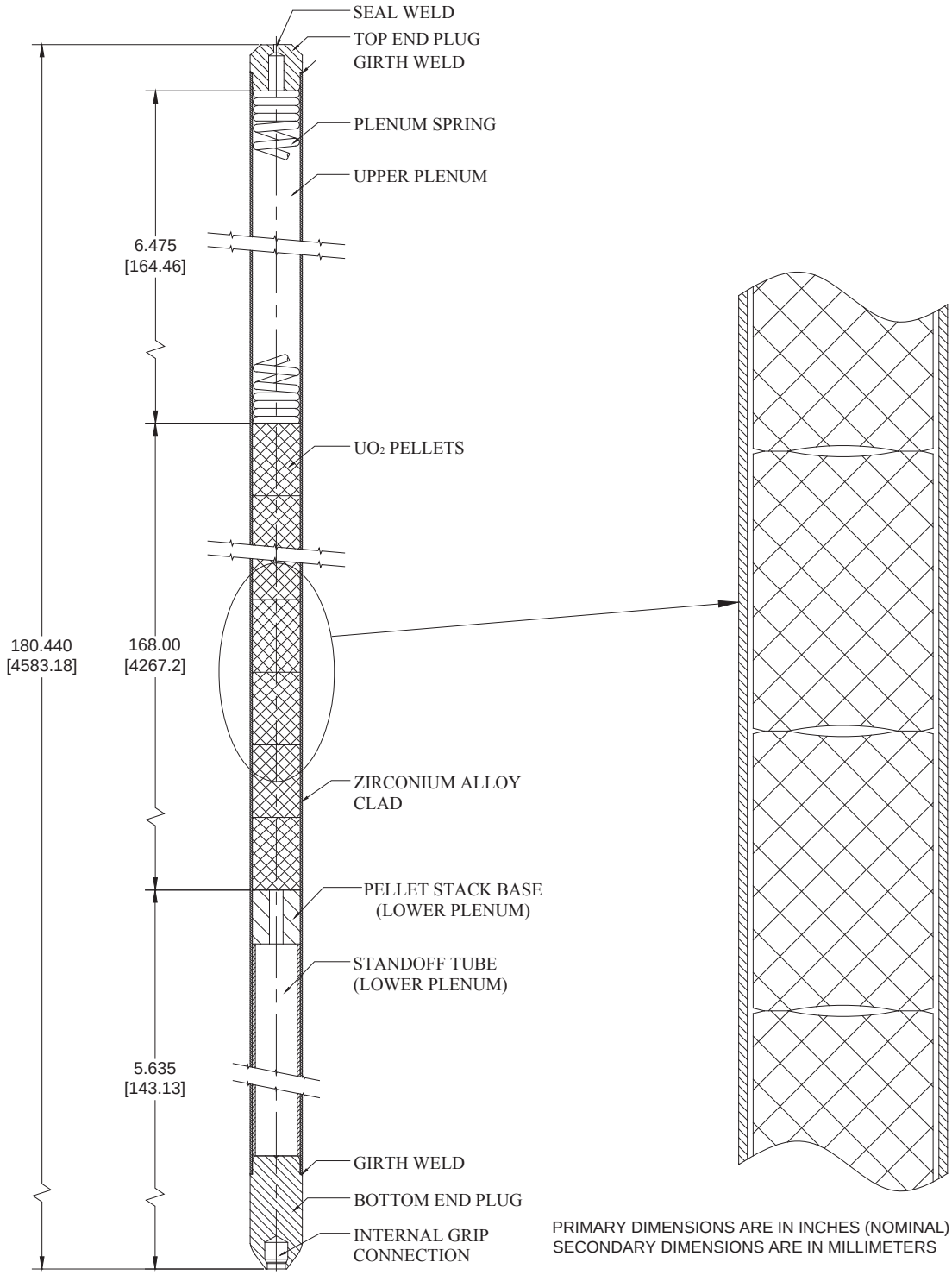


Figure 22-3. Fuel Rod Schematic

Figure 22-4. AP1000 Plant Top Nozzle Assembly

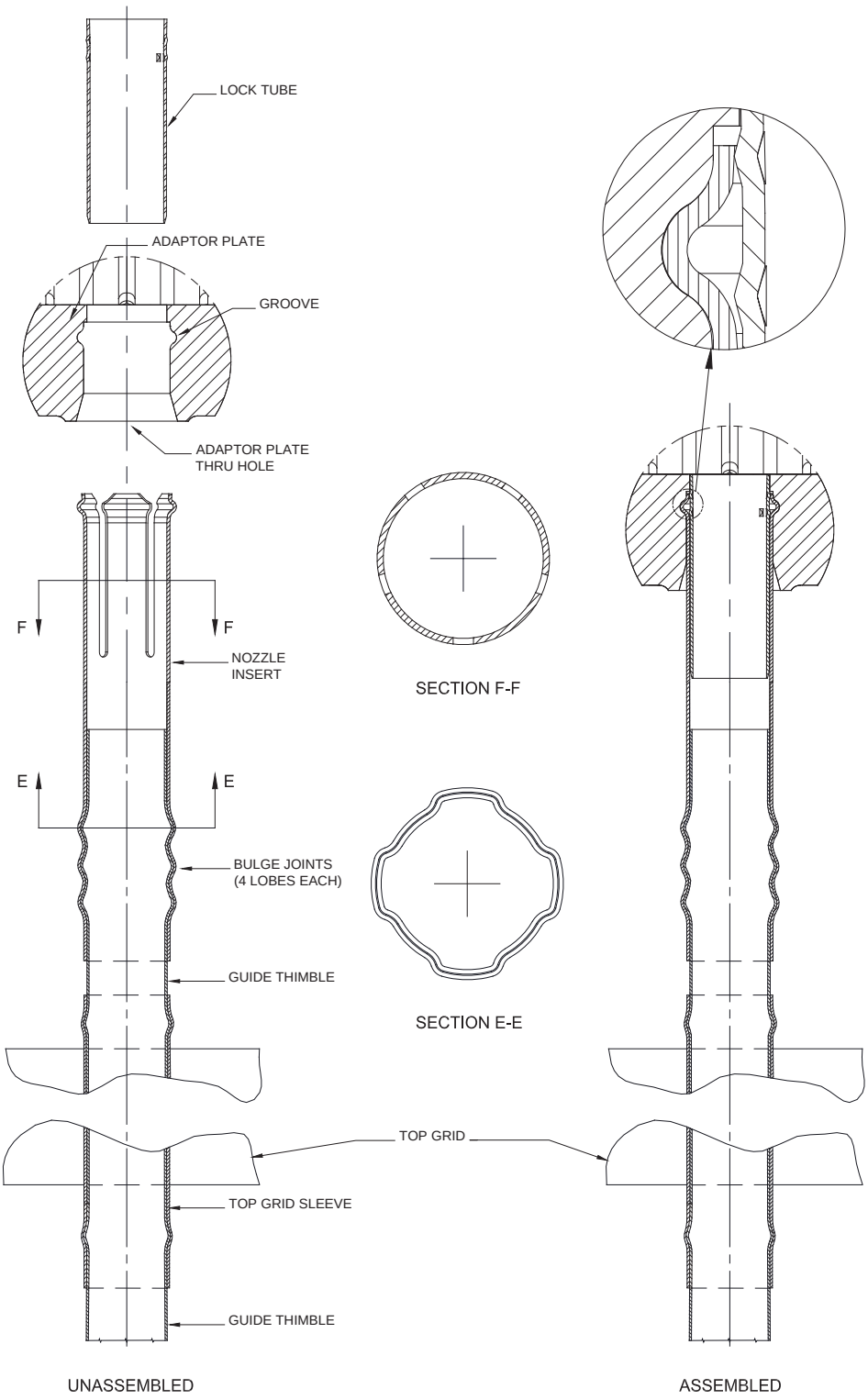


Figure 22-5. Top Nozzle Sleeve Detail

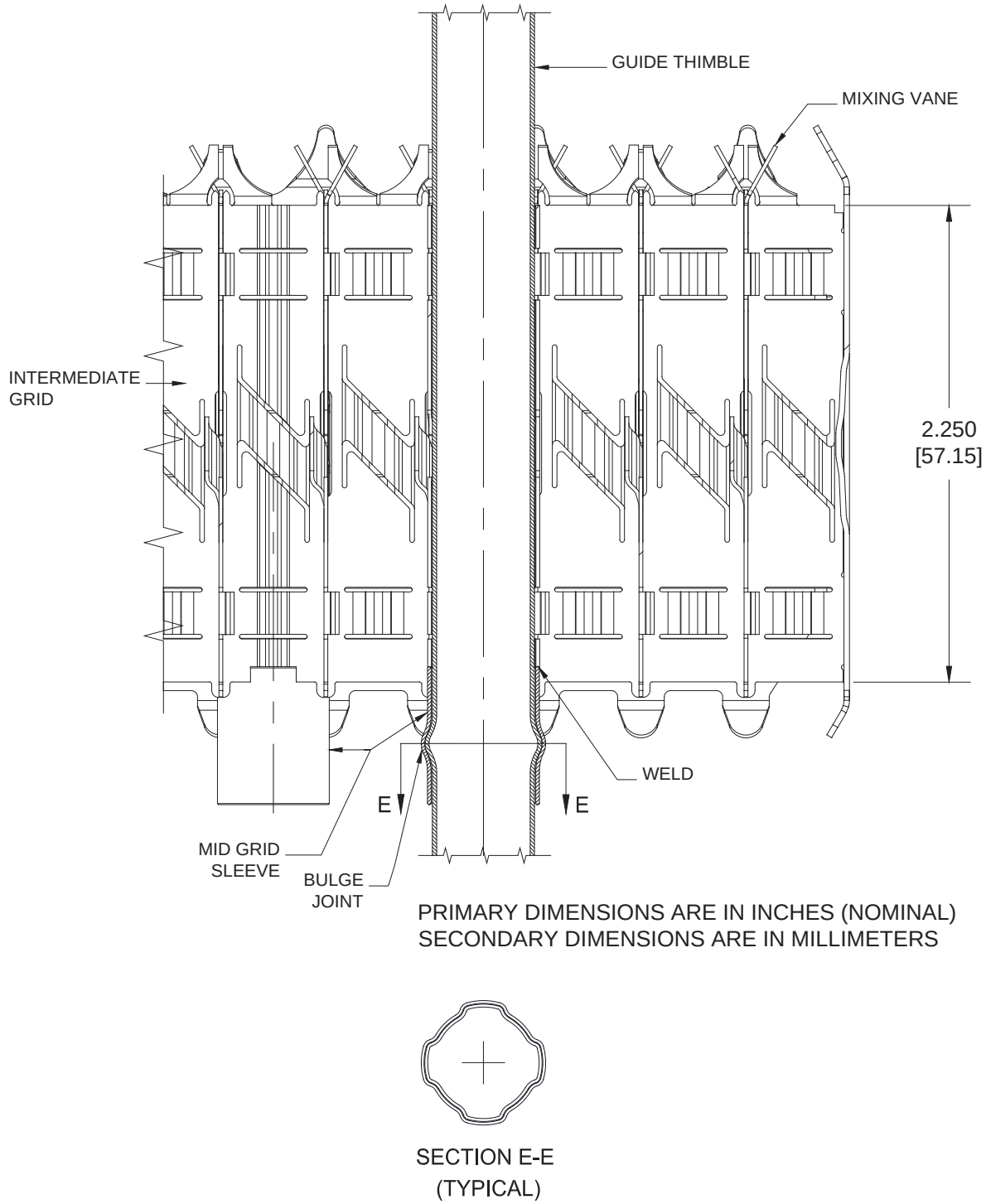


Figure 22-6. Intermediate Grid-to-Thimble Attachment Joint

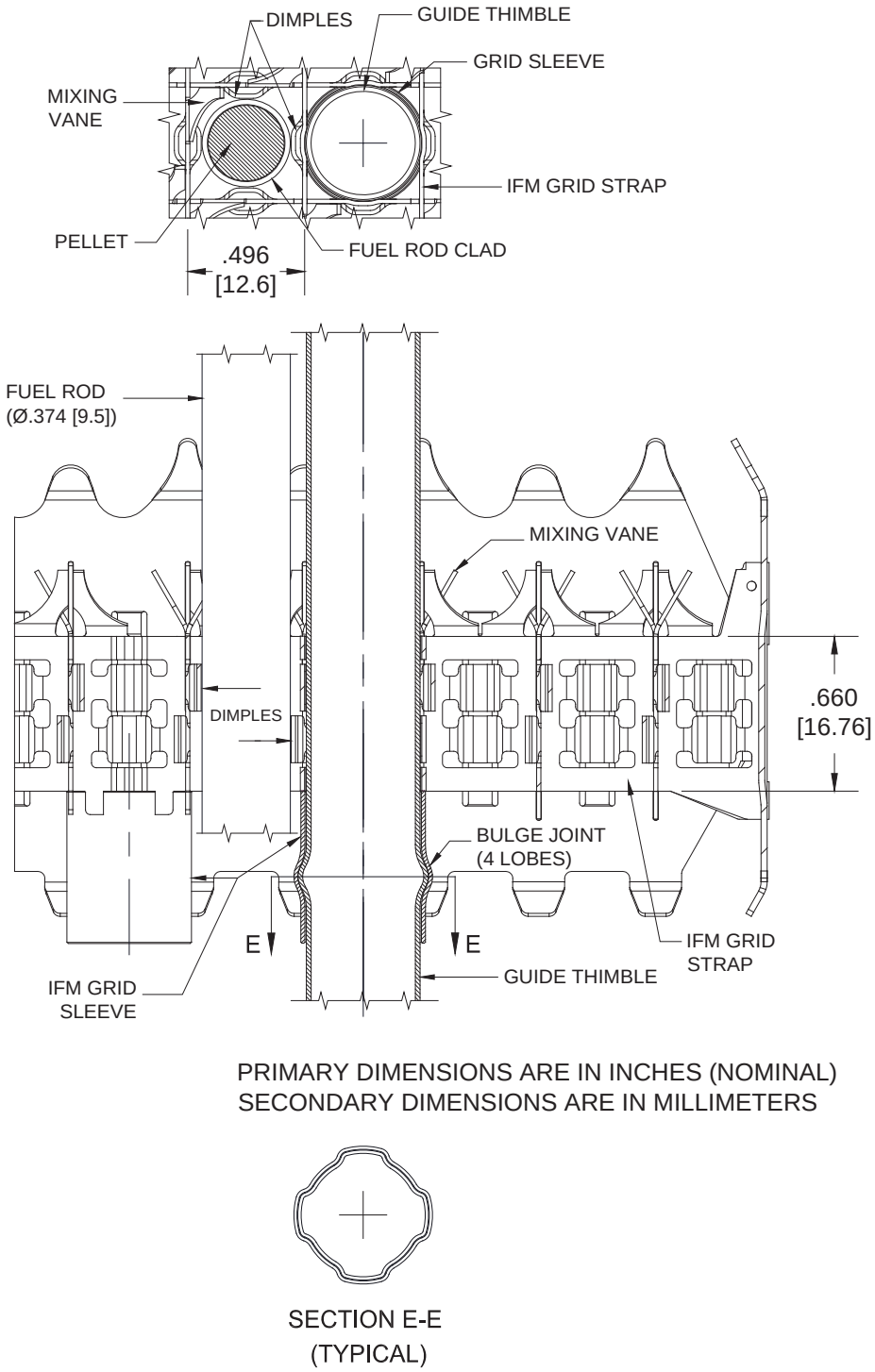


Figure 22-7. Intermediate Flow Mixer Grid-to-Thimble Attachment

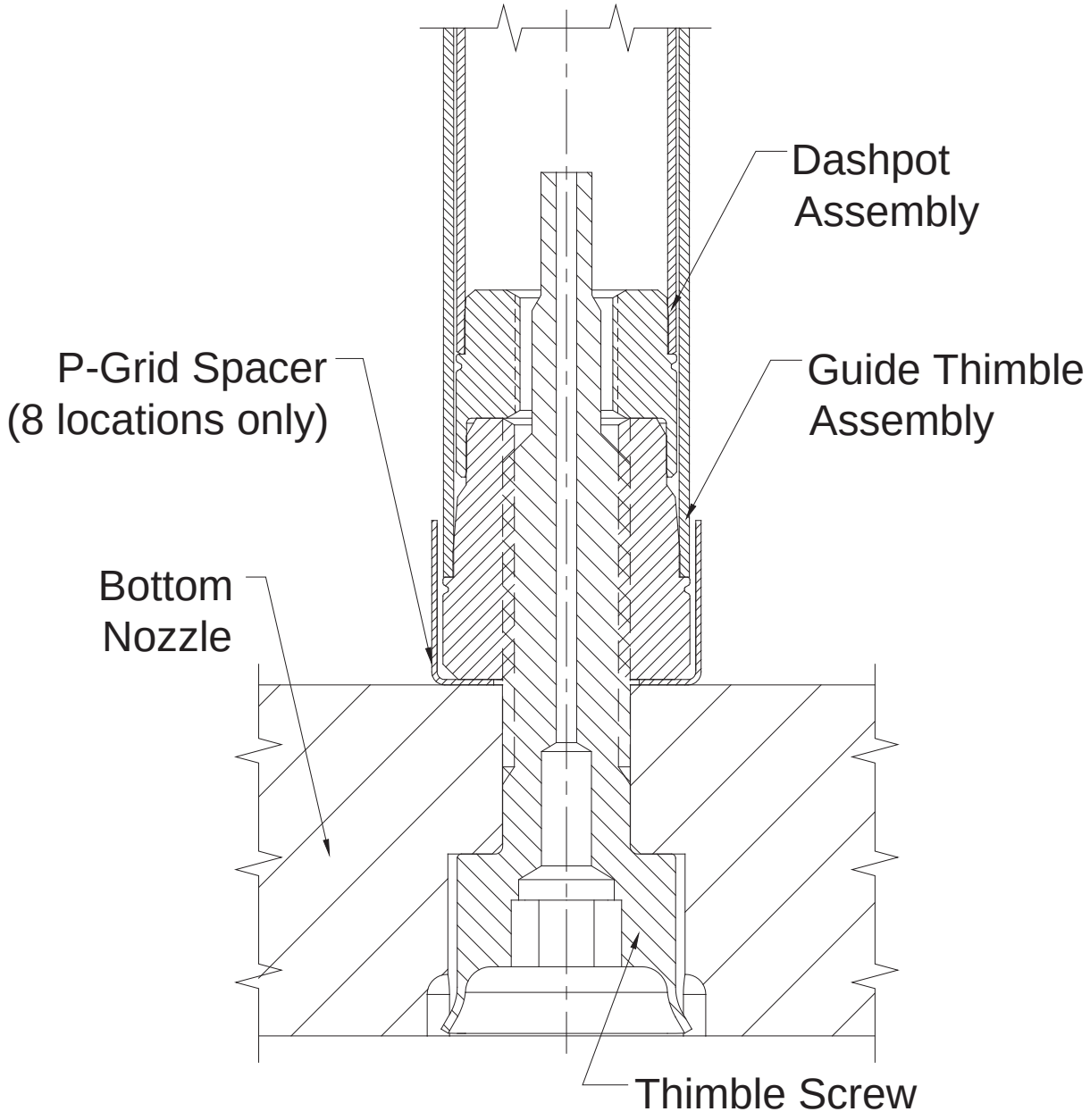


Figure 22-8. Guide Thimble-to-Nozzle Joint (Protective Grid is omitted for clarity)

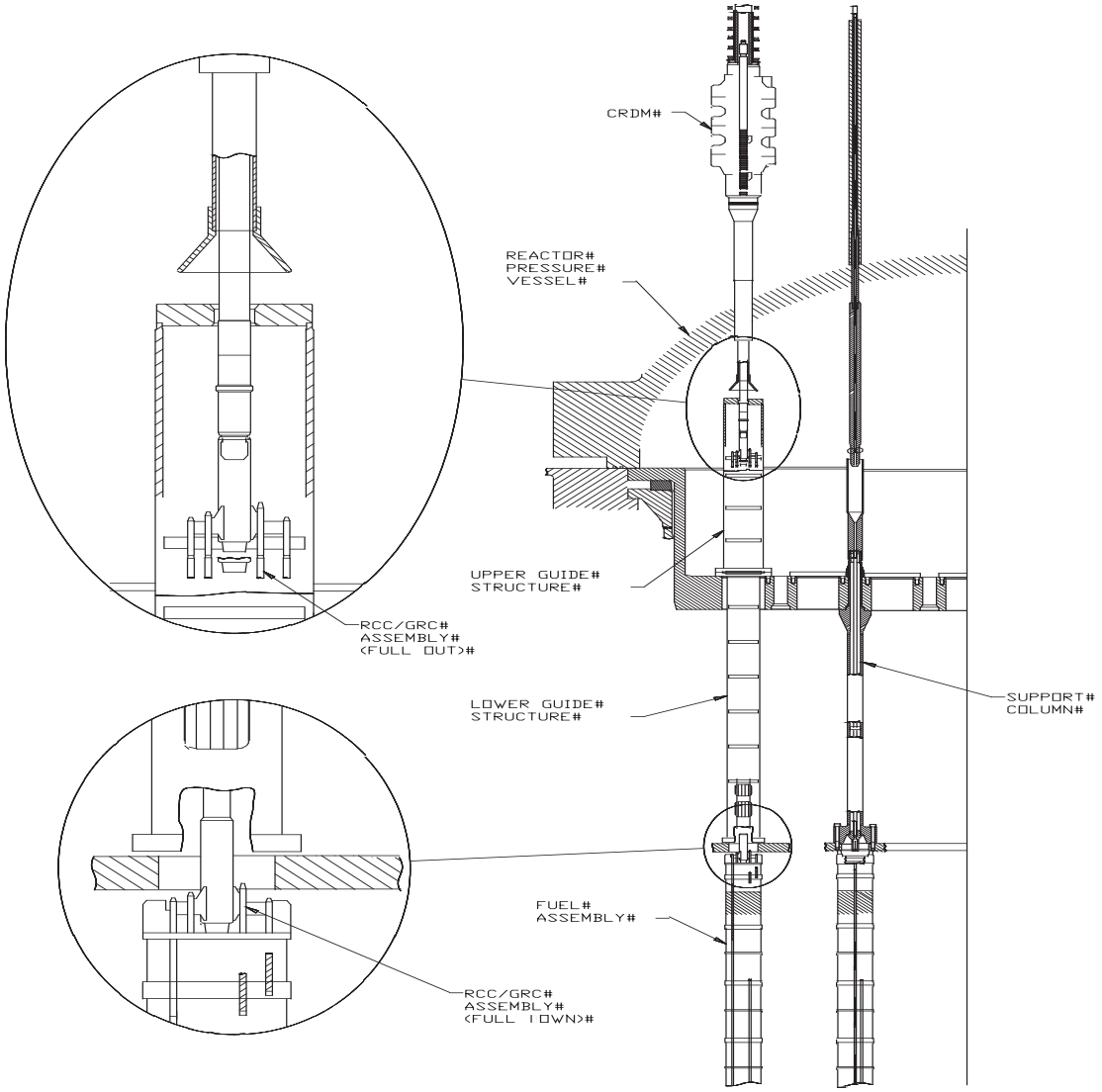


Figure 22-9. Rod Cluster Control and Drive Rod Assembly with Interfacing Components

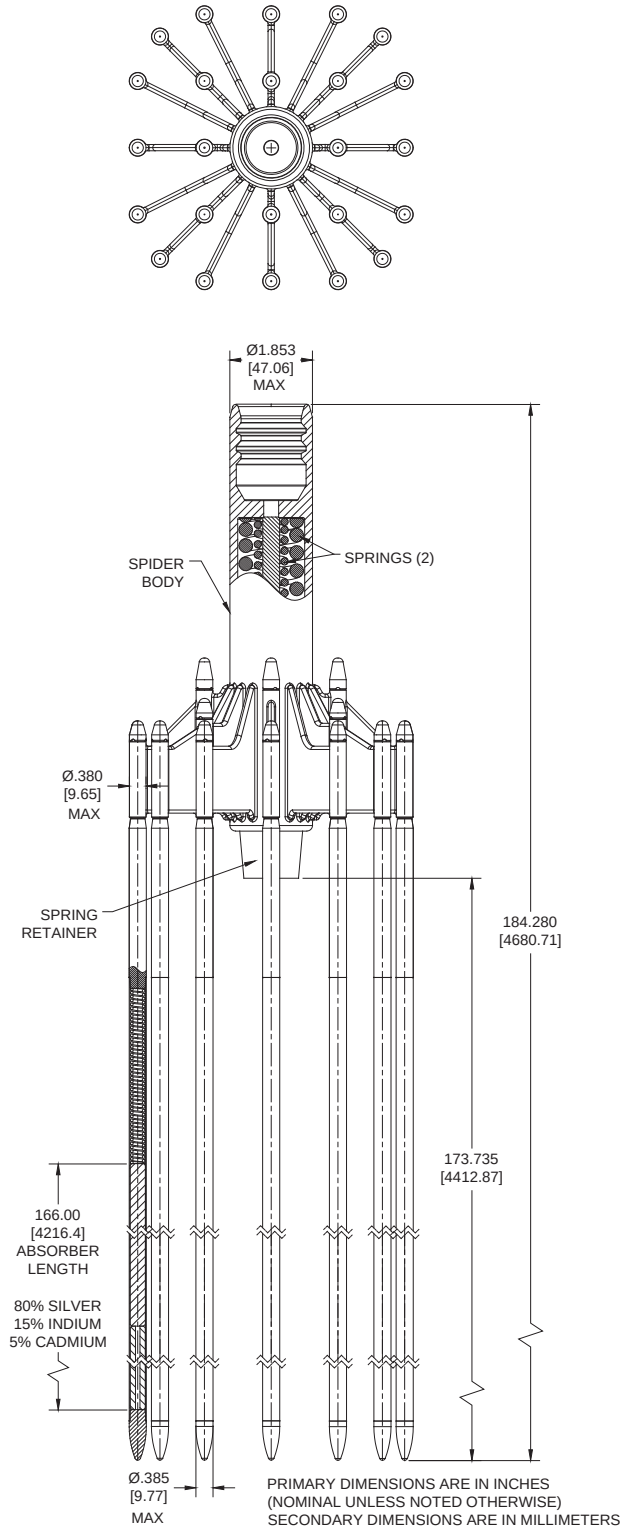
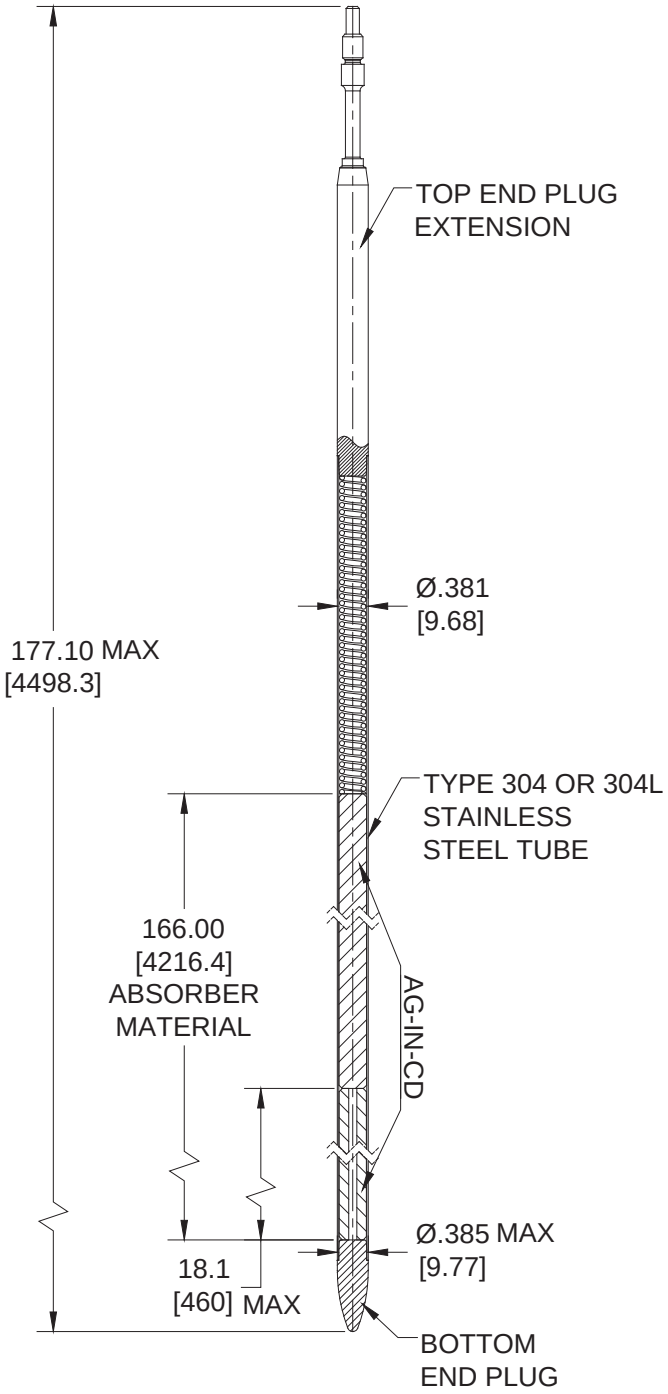


Figure 22-10. RCCA



PRIMARY DIMENSIONS ARE IN INCHES
(NOMINAL UNLESS NOTED OTHERWISE)
SECONDARY DIMENSIONS ARE IN MILLIMETERS

Figure 22-11. Absorber Rod Detail

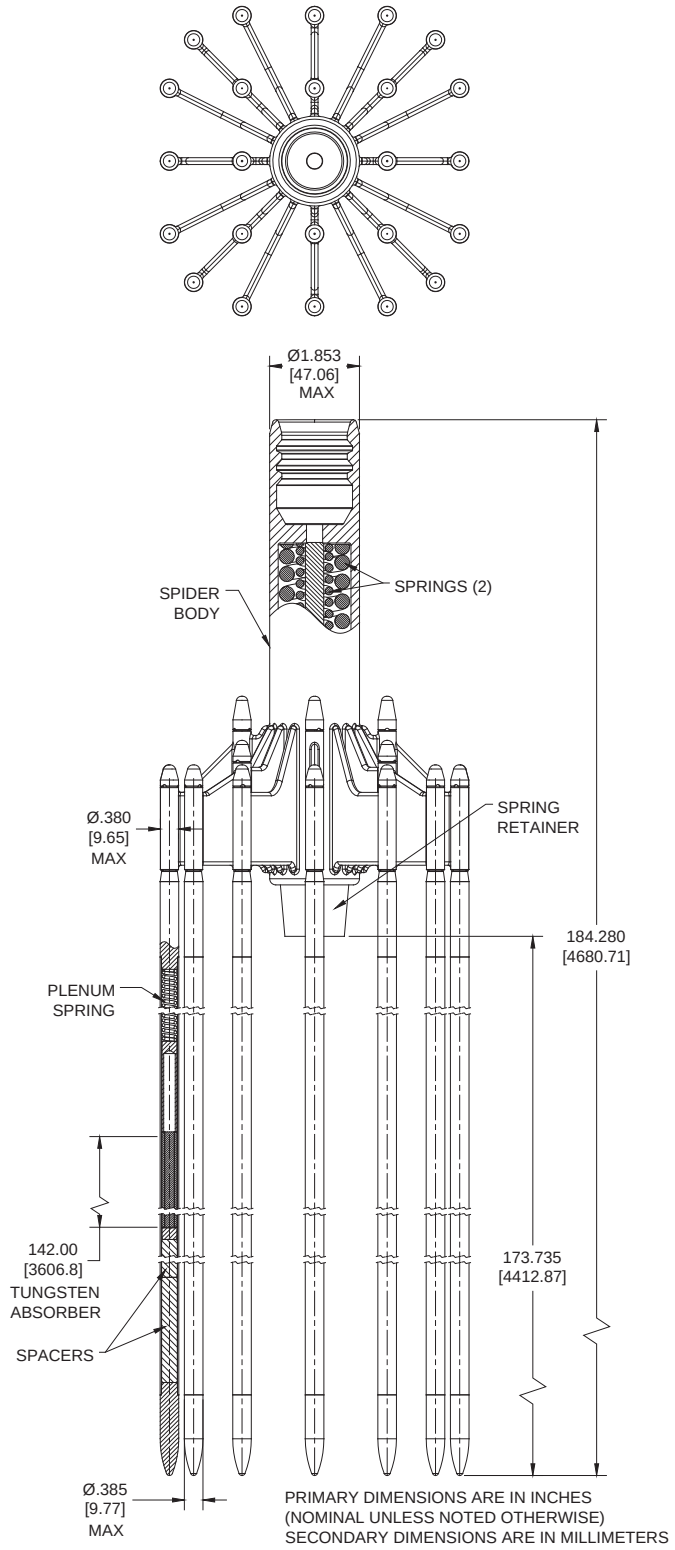


Figure 22-12. Gray Rod Cluster Assembly

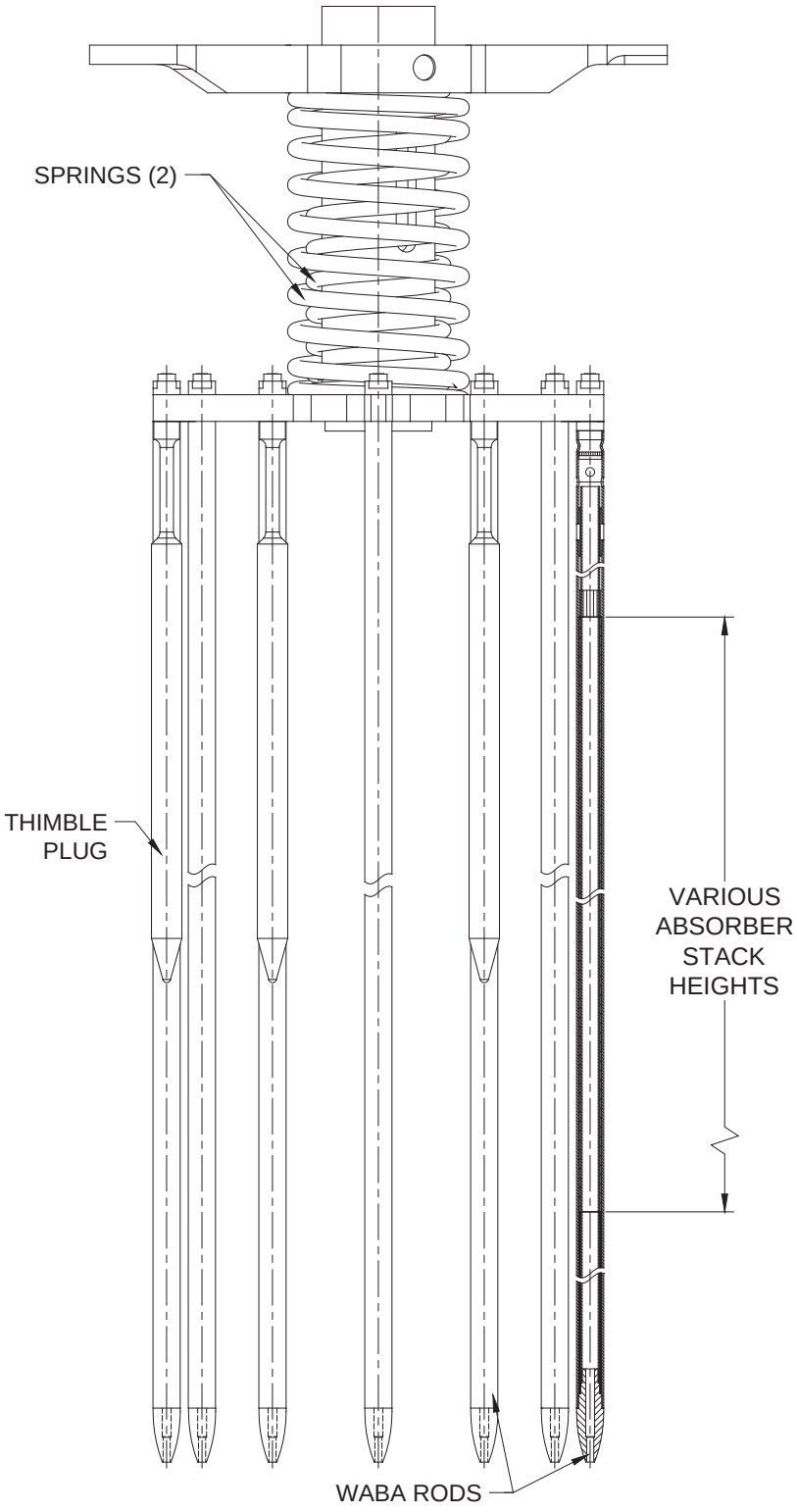


Figure 22-13. Wet Annular Burnable Absorber Assembly

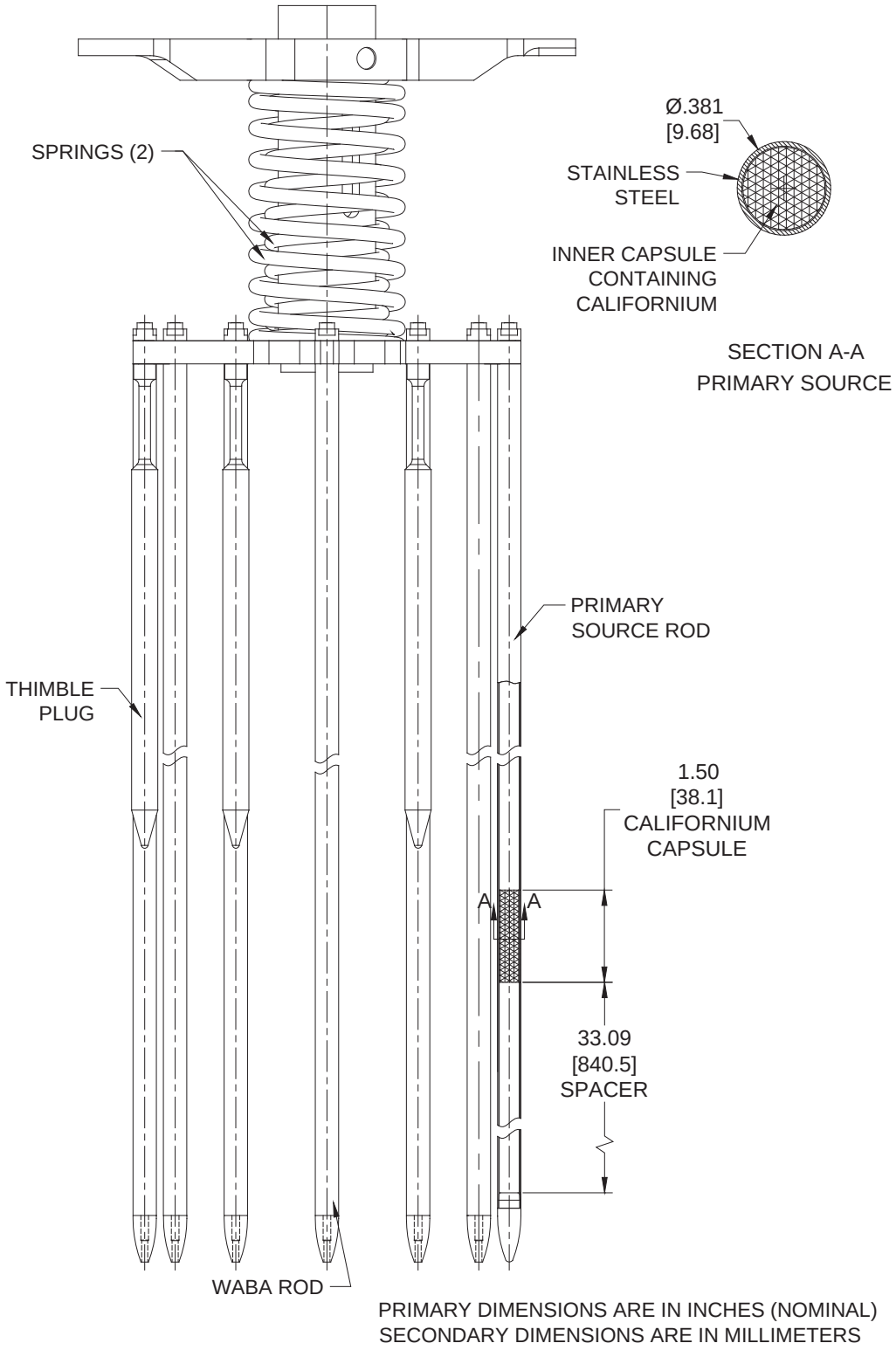


Figure 22-14. Primary Source Assembly

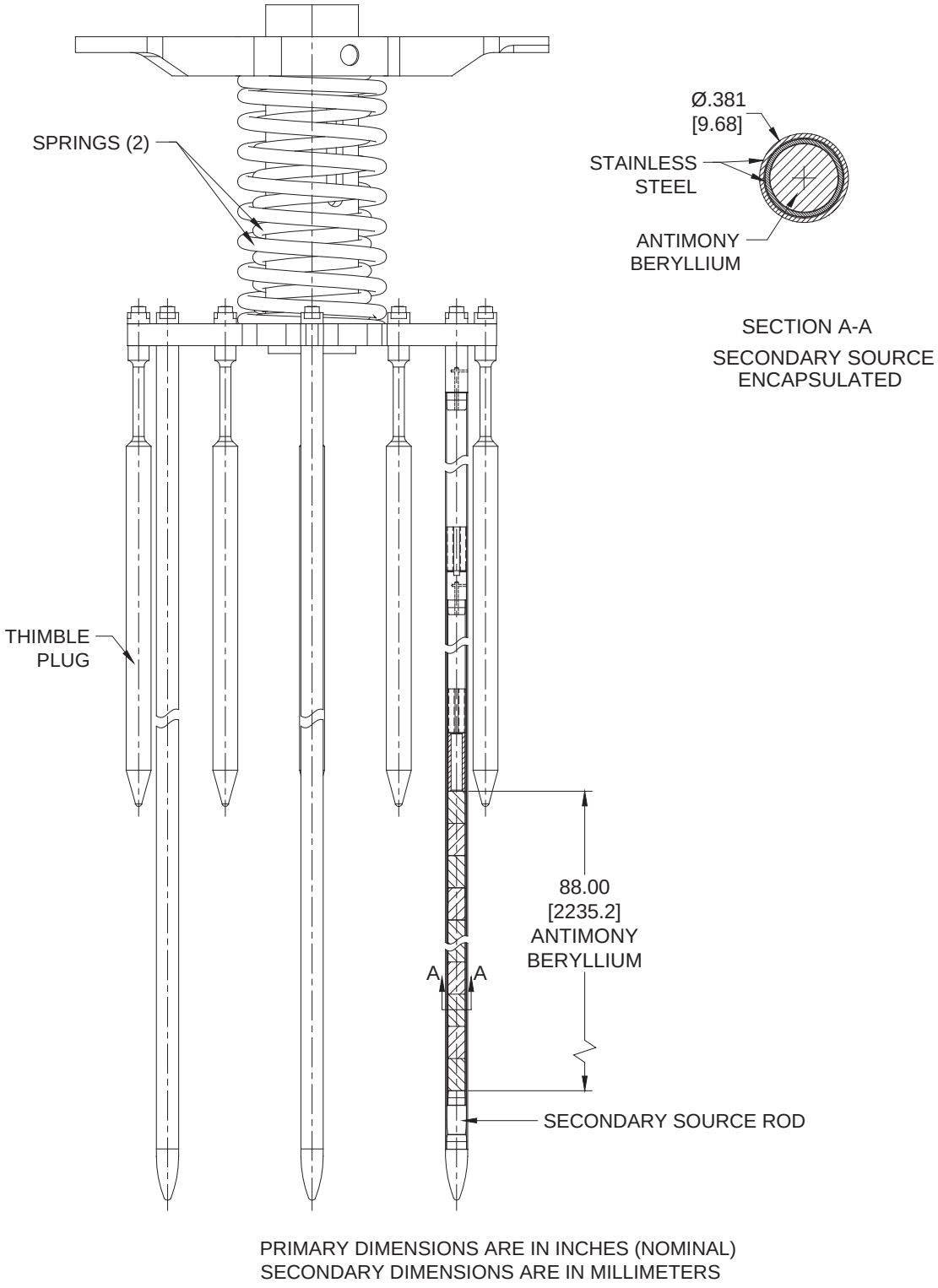


Figure 22-15. Secondary Source Assembly

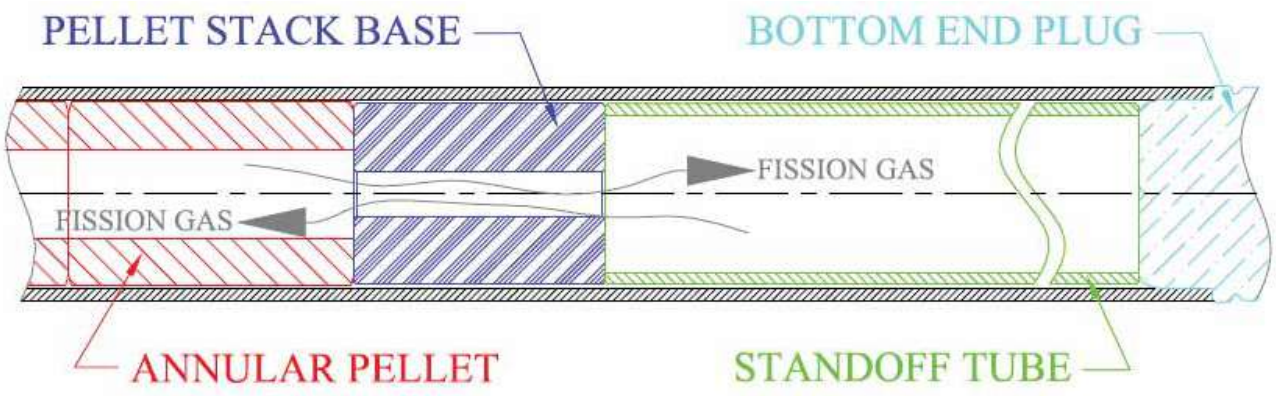
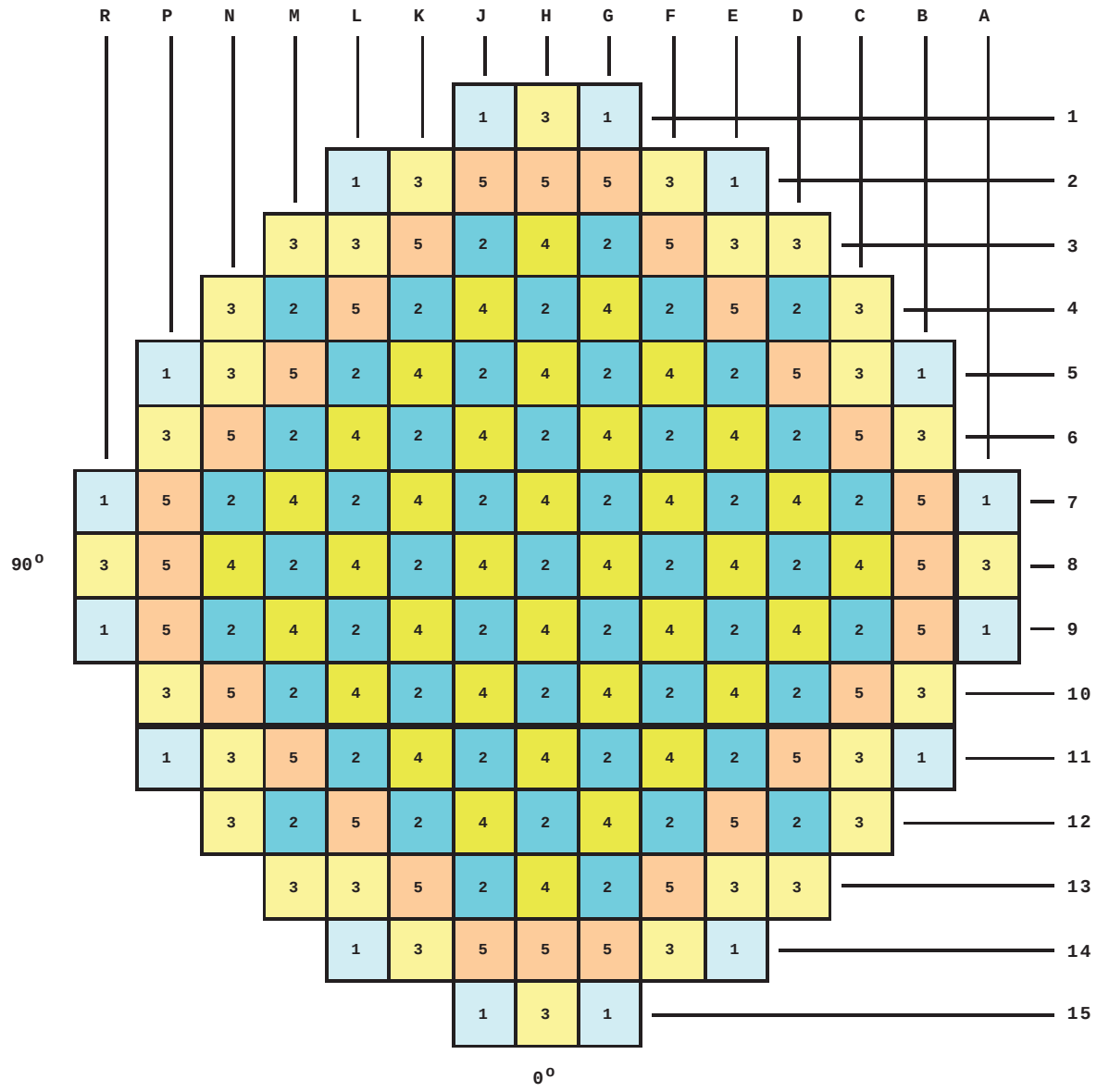


Figure 22-16. Cross-Section View of the Lower Plenum Region



Region	Enrichment
1	0.74 w/o
2	1.58 w/o
3	3.20 w/o
4	3.776 w/o
5	4.376 w/o

Figure 22-17. Fuel Loading Arrangement

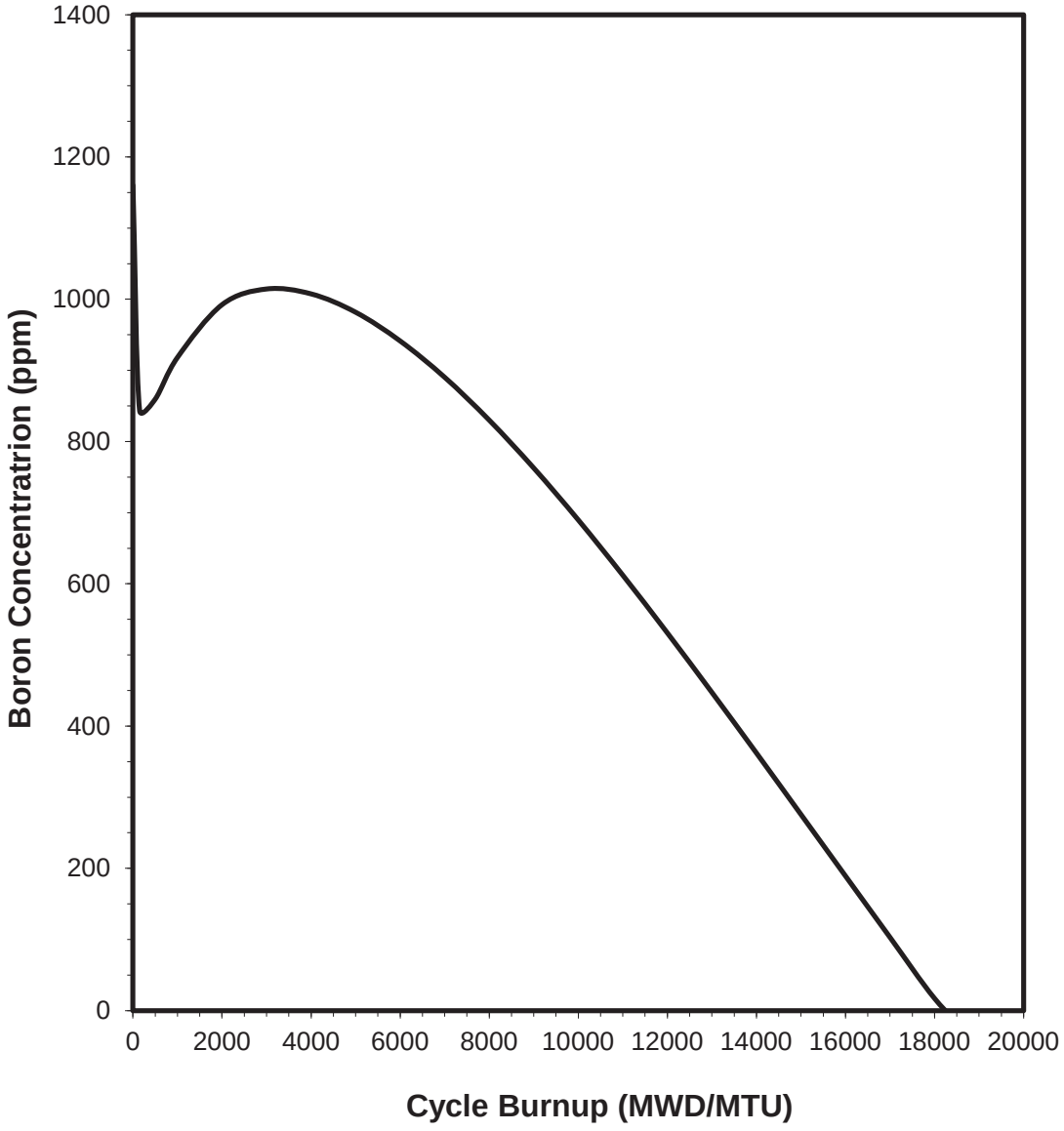
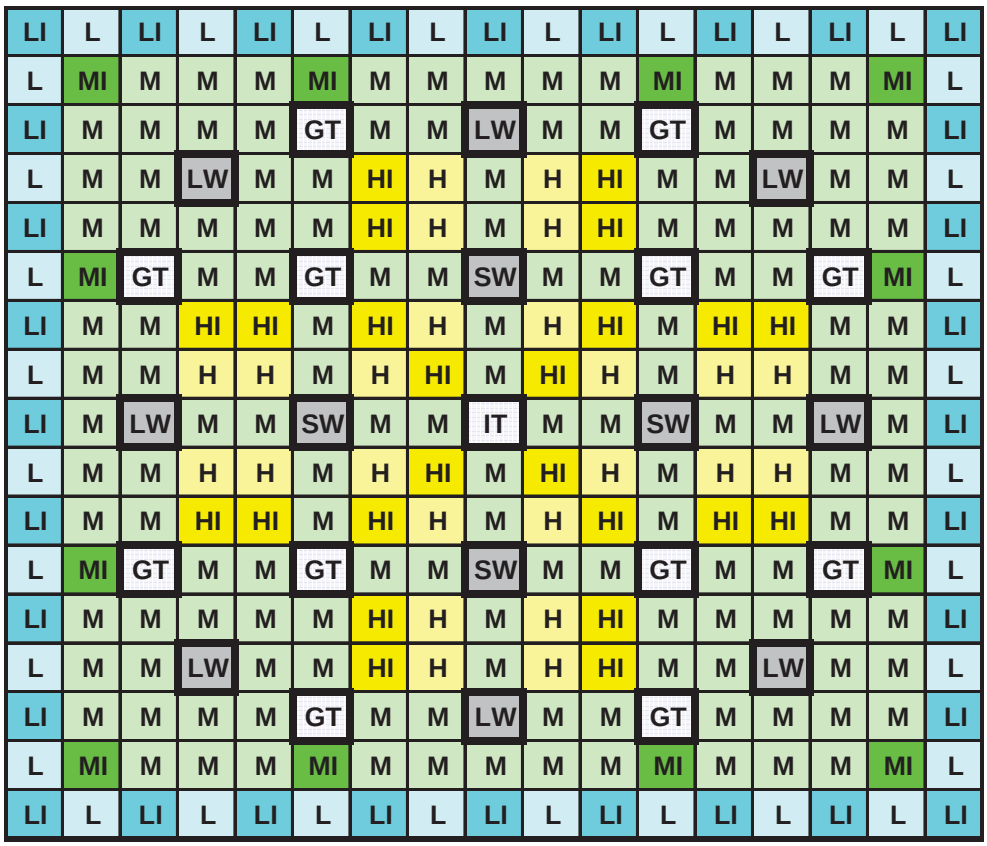
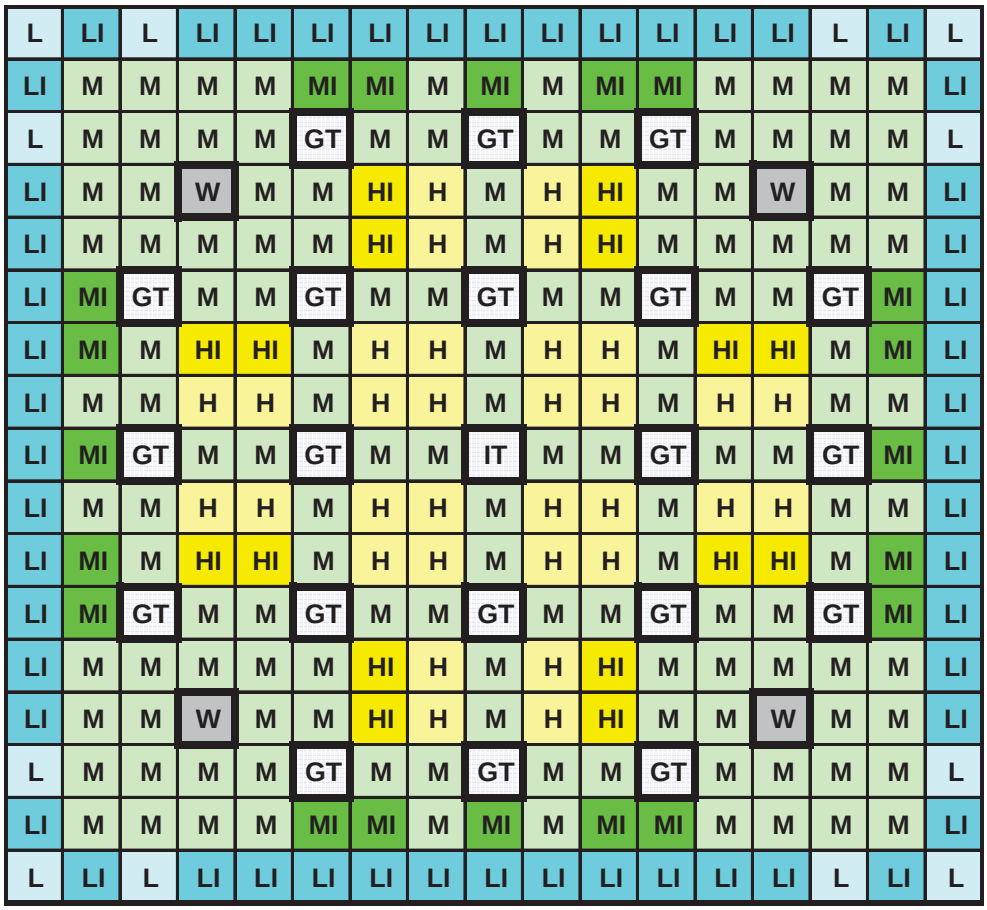


Figure 22-18. Soluble Boron Concentration versus Burnup



Region D 68 IFBA + 12 WABA			
	No. Pins	Enr.	BA
L	32	3.40	No BA
LI	32	3.40	IFBA
M	140	3.80	No BA
MI	12	3.80	IFBA
H	24	4.20	No BA
HI	24	4.20	IFBA
SW	4		WABA
LW	8		WABA
GT	12		
IT	1		

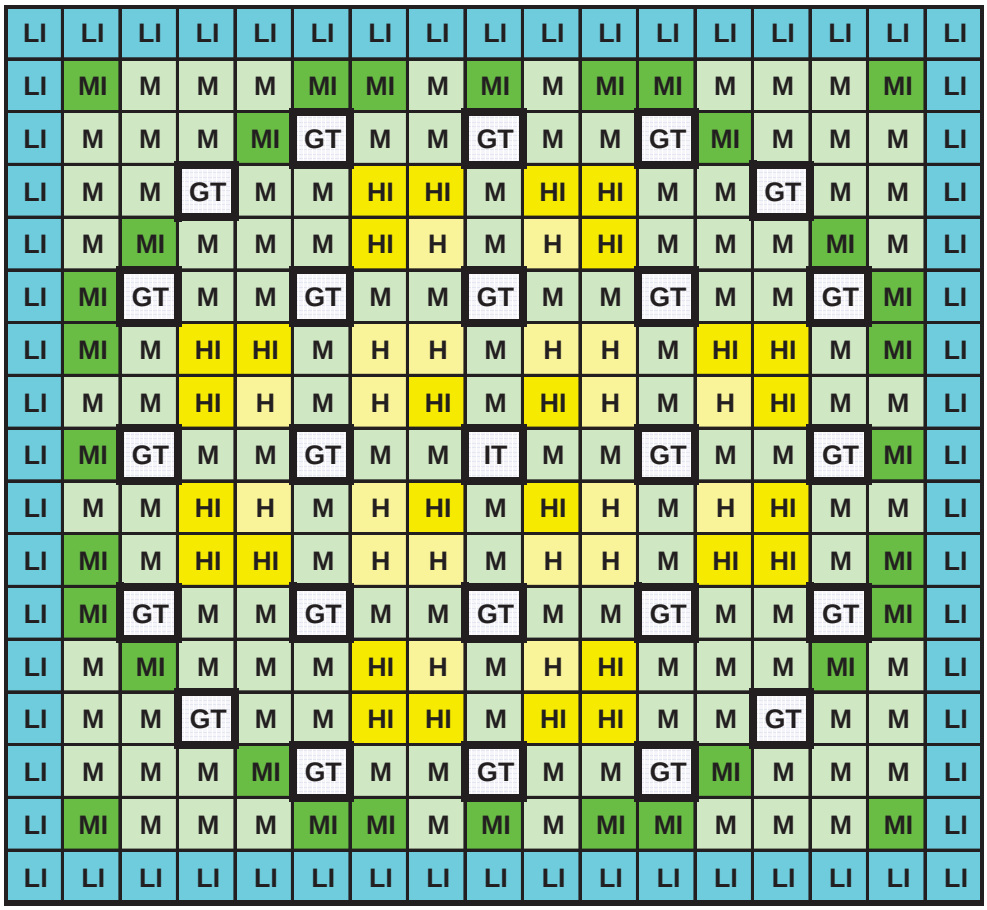
Figure 22-19. Cycle 1 Assembly Integral and Wet Annular Burnable Absorber Rod Patterns



Region E 88 IFBA + 4 WABA

	No. Pins	Enr.	BA
L	12	4.00	No BA
LI	52	4.00	IFBA
M	132	4.40	No BA
MI	20	4.40	IFBA
H	32	4.80	No BA
HI	16	4.80	IFBA
W	4		WABA
GT	20		
IT	1		

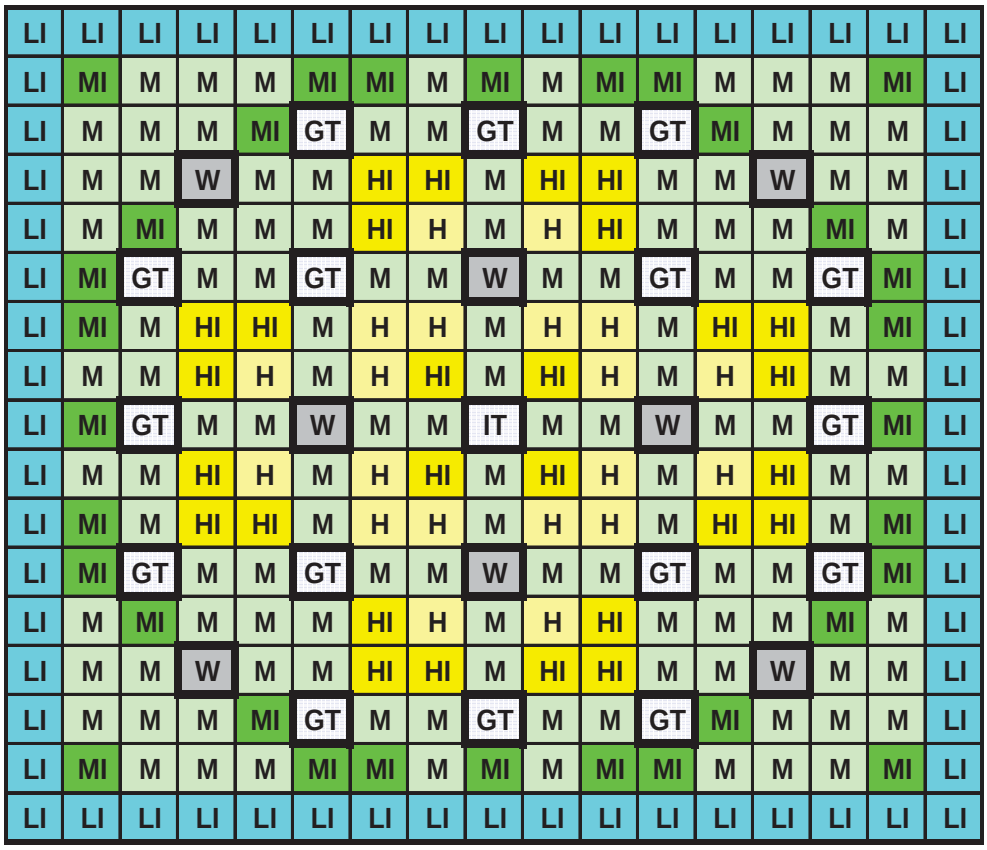
Figure 22-19. Cycle 1 Assembly Integral and Wet Annular Burnable Absorber Rod Patterns (cont.)



Region E 124 IFBA

	No. Pins	Enr.	BA
L	0	4.00	No BA
LI	64	4.00	IFBA
M	120	4.40	No BA
MI	32	4.40	IFBA
H	20	4.80	No BA
HI	28	4.80	IFBA
W	0		WABA
GT	24		
IT	1		

Figure 22-19. Cycle 1 Assembly Integral and Wet Annular Burnable Absorber Rod Patterns (cont.)



Region E 124 IFBA + 8 WABA

	No. Pins	Enr.	BA
L	0	4.00	No BA
LI	64	4.00	IFBA
M	120	4.40	No BA
MI	32	4.40	IFBA
H	20	4.80	No BA
HI	28	4.80	IFBA
W	8		WABA
GT	16		
IT	1		

Figure 22-19. Cycle 1 Assembly Integral and Wet Annular Burnable Absorber Rod Patterns (cont.)

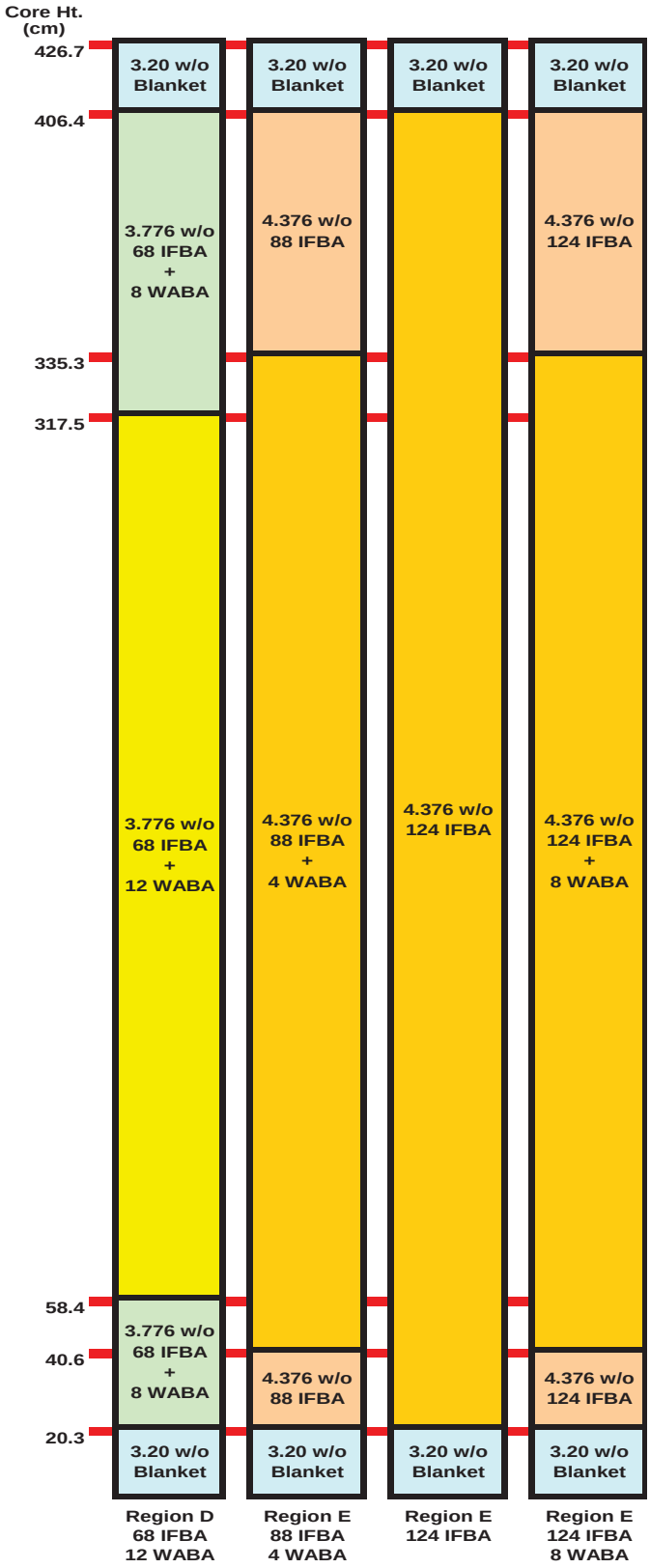
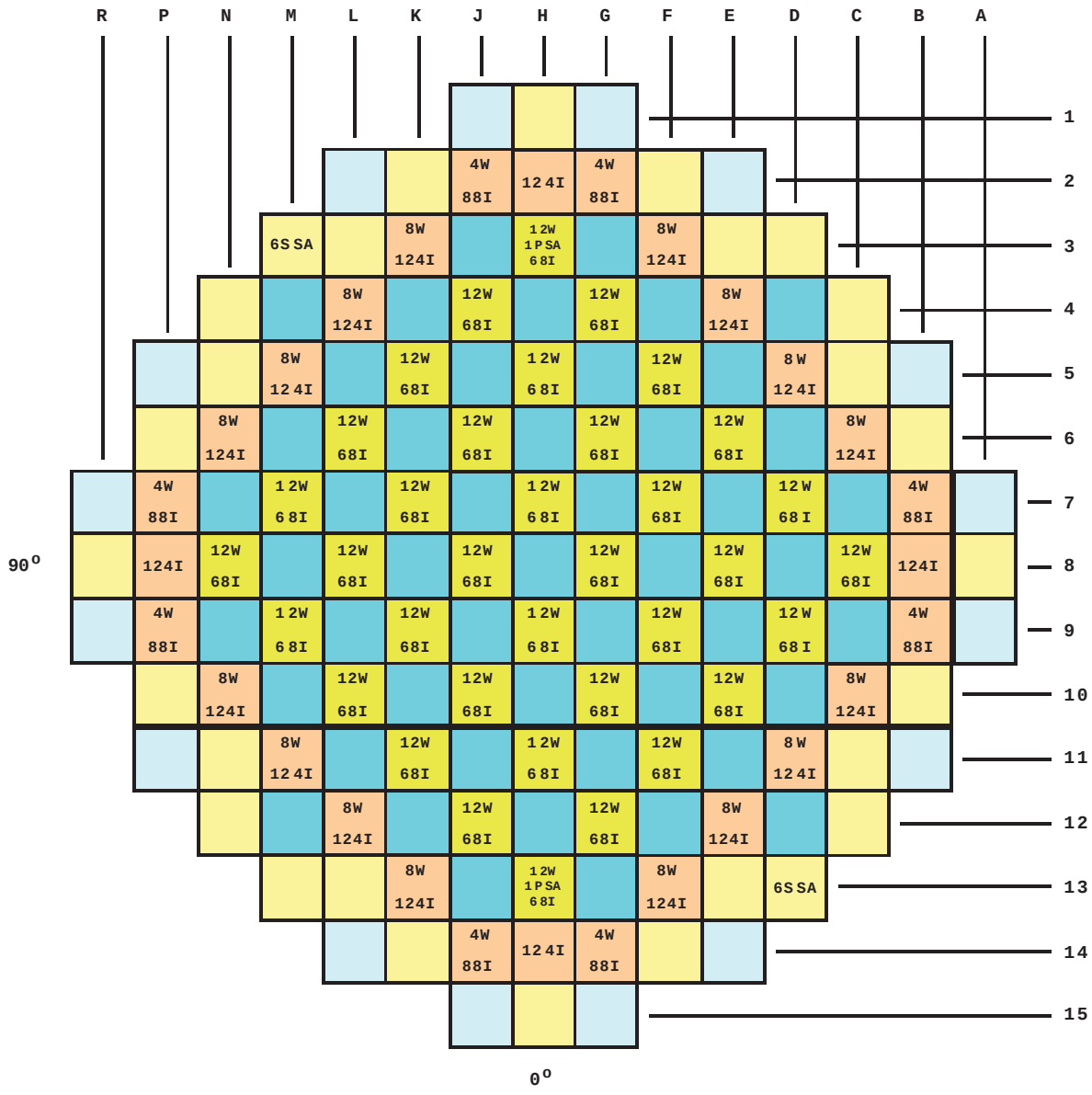


Figure 22-20. Cycle 1 Assembly Integral and Wet Annular Burnable Absorber Axial Configurations



TYPE	TOTAL
##W...(NUMBER OF WABA RODLETS).....	592
##I...(TOTAL NUMBER OF FRESH IFBA RODS).....	5632
#SSA..(NUMBER OF SECONDARY SOURCE RODLETS)...	12
#PSA..(NUMBER OF PRIMARY SOURCE RODLETS).....	2

Figure 22-21. Cycle 1 Burnable Absorber, Primary and Secondary Source Assembly Locations

0.962	1.296	0.964	1.299	0.966	1.277	1.205	0.653
1.296	0.963	1.299	0.967	1.301	0.947	1.149	0.201
0.964	1.299	0.967	1.307	0.970	1.290	0.874	
1.299	0.967	1.307	0.963	1.348	1.164	0.232	
0.966	1.301	0.970	1.348	0.829	0.765		
1.277	0.947	1.290	1.164	0.765			
1.205	1.149	0.874	0.232				
0.653	0.201						

Calculated $F^N_{\Delta H} = 1.460$

Key: Values Represent Assembly Relative Power

Figure 22-22. Cycle 1 Normalised Power Density Distribution Near Beginning of Life, Unrodded Core, Hot Full Power, No Xenon

1.002	1.327	0.998	1.316	0.982	1.258	1.171	0.647
1.327	1.001	1.323	0.992	1.300	0.947	1.119	0.207
0.998	1.323	0.996	1.314	0.977	1.262	0.856	
1.316	0.992	1.314	0.974	1.326	1.136	0.238	
0.982	1.300	0.977	1.326	0.829	0.752		
1.258	0.947	1.262	1.136	0.752			
1.171	1.119	0.856	0.238				
0.647	0.207						

Calculated $F^{N}_{\Delta H} = 1.441$

Key: Values Represent Assembly Relative Power

Figure 22-23. Cycle 1 Normalised Power Density Distribution Near Beginning of Life, Unrodded Core, Hot Full Power, Equilibrium Xenon

1.029	1.348	1.009	1.338	1.004	1.224	0.928	0.566
1.348	1.001	1.283	0.997	1.330	0.949	1.063	0.191
1.009	1.283	0.794	1.288	1.013	1.306	0.874	
1.338	0.997	1.288	0.995	1.391	1.204	0.253	
1.004	1.330	1.013	1.391	0.888	0.808		
1.224	0.949	1.306	1.204	0.808			
0.928	1.063	0.874	0.253				
0.566	0.191						

Calculated $F^{N}_{\Delta H} = 1.505$

Key: Values Represent Assembly Relative Power

Figure 22-24. Cycle 1 Normalised Power Density Distribution Near Beginning of Life, Gray Bank MA+MB Inserted, Hot Full Power, Equilibrium Xenon

1.017	1.350	1.017	1.349	1.014	1.339	1.260	0.660
1.350	1.017	1.349	1.014	1.338	0.979	1.144	0.275
1.017	1.349	1.013	1.338	0.991	1.269	0.790	
1.349	1.014	1.338	0.987	1.303	0.963	0.267	
1.014	1.338	0.991	1.303	0.756	0.599		
1.339	0.979	1.269	0.963	0.599			
1.260	1.144	0.790	0.267				
0.660	0.275						

Calculated $F_{\Delta H}^{N} = 1.428$

Key: Values Represent Assembly Relative Power

Figure 22-25. Cycle 1 Normalised Power Density Distribution Near Middle of Life, Unrodded Core, Hot Full Power, Equilibrium Xenon

0.984	1.253	0.990	1.266	1.006	1.293	1.263	0.738
1.253	0.987	1.260	0.997	1.278	0.998	1.170	0.366
0.990	1.260	0.995	1.272	1.001	1.266	0.832	
1.266	0.997	1.272	0.998	1.287	0.981	0.346	
1.006	1.278	1.001	1.287	0.814	0.645		
1.293	0.998	1.266	0.981	0.645			
1.263	1.170	0.832	0.346				
0.738	0.366						

Calculated $F^{N}_{\Delta H} = 1.378$

Key: Values Represent Assembly Relative Power

Figure 22-26. Cycle 1 Normalised Power Density Distribution Near End of Life, Unrodded Core, Hot Full Power, Equilibrium Xenon

1.017	1.284	1.006	1.296	1.027	1.253	0.989	0.645
1.284	0.993	1.234	1.006	1.310	0.997	1.106	0.335
1.006	1.234	0.802	1.258	1.039	1.312	0.848	
1.296	1.006	1.258	1.023	1.356	1.041	0.366	
1.027	1.310	1.039	1.356	0.872	0.695		
1.253	0.997	1.312	1.041	0.695			
0.989	1.106	0.848	0.366				
0.645	0.335						

Calculated $F^N_{\Delta H} = 1.431$

Key: Values Represent Assembly Relative Power

Figure 22-27. Cycle 1 Normalised Power Density Distribution Near End of Life, Gray Bank MA+MB Inserted, Hot Full Power, Equilibrium Xenon

1.215	1.187	1.200	1.215	1.228	1.234	1.239	1.258	1.265	1.273	1.265	1.269	1.269	1.261	1.251	1.250	1.310
1.139	1.194	1.279	1.296	1.312	1.277	1.248	1.345	1.310	1.355	1.267	1.304	1.348	1.341	1.338	1.272	1.263
1.133	1.258	1.260	1.255	1.246		1.347	1.360		1.368	1.362		1.273	1.295	1.317	1.350	1.274
1.143	1.270	1.250		1.283	1.343	1.281	1.281	1.322	1.287	1.290	1.360	1.307		1.305	1.364	1.293
1.159	1.288	1.245	1.286	1.317	1.356	1.287	1.339	1.258	1.343	1.294	1.369	1.336	1.317	1.293	1.381	1.311
1.170	1.261		1.353	1.363		1.341	1.266		1.269	1.347		1.378	1.380		1.345	1.320
1.181	1.239	1.359	1.298	1.301	1.349	1.396	1.365	1.278	1.367	1.400	1.355	1.311	1.317	1.402	1.315	1.325
1.203	1.339	1.378	1.304	1.359	1.279	1.371	1.309	1.354	1.311	1.374	1.284	1.369	1.321	1.417	1.417	1.342
1.213	1.307		1.348	1.280		1.287	1.358		1.361	1.292		1.290	1.366		1.378	1.345
1.220	1.354	1.392	1.317	1.372	1.291	1.383	1.319	1.364	1.321	1.384	1.293	1.377	1.329	1.425	1.424	1.349
1.213	1.269	1.389	1.325	1.327	1.374	1.421	1.388	1.299	1.388	1.420	1.374	1.328	1.333	1.418	1.329	1.338
1.217	1.306		1.397	1.405		1.379	1.300		1.300	1.377		1.406	1.405		1.367	1.340
1.218	1.350	1.302	1.343	1.373	1.411	1.337	1.389	1.303	1.388	1.335	1.409	1.373	1.350	1.324	1.412	1.338
1.212	1.345	1.323		1.353	1.413	1.344	1.342	1.382	1.342	1.342	1.411	1.353		1.346	1.404	1.329
1.208	1.344	1.347	1.341	1.329		1.431	1.440		1.440	1.429		1.329	1.348	1.368	1.399	1.319
1.217	1.284	1.381	1.400	1.416	1.376	1.341	1.440	1.398	1.441	1.341	1.376	1.418	1.407	1.401	1.330	1.320
1.294	1.282	1.305	1.326	1.341	1.346	1.348	1.362	1.364	1.365	1.351	1.349	1.345	1.334	1.322	1.322	1.388

Figure 22-28. Rodwise Power Distribution in a Typical Assembly (M-5) Near Beginning of Life, Hot Full Power, Equilibrium Xenon, Unrodded Core

1.115	1.080	1.078	1.095	1.120	1.148	1.167	1.187	1.213	1.217	1.224	1.232	1.232	1.235	1.244	1.269	1.319
1.085	1.108	1.126	1.153	1.188	1.234	1.222	1.246	1.284	1.276	1.277	1.318	1.300	1.293	1.291	1.296	1.286
1.076	1.119	1.144	1.208	1.233		1.271	1.282		1.312	1.327		1.343	1.347	1.307	1.304	1.275
1.081	1.134	1.195		1.255	1.268	1.289	1.297	1.295	1.326	1.344	1.350	1.365		1.359	1.318	1.277
1.091	1.154	1.205	1.240	1.230	1.269	1.291	1.308	1.296	1.337	1.345	1.350	1.337	1.376	1.366	1.336	1.285
1.103	1.183		1.238	1.253		1.279	1.289		1.318	1.333		1.361	1.373		1.366	1.296
1.107	1.156	1.212	1.242	1.260	1.264	1.298	1.312	1.304	1.341	1.353	1.344	1.368	1.378	1.373	1.335	1.299
1.113	1.166	1.210	1.237	1.263	1.260	1.299	1.308	1.314	1.337	1.353	1.341	1.372	1.372	1.370	1.346	1.303
1.123	1.188		1.220	1.237		1.277	1.300		1.329	1.331		1.345	1.355		1.368	1.312
1.113	1.166	1.210	1.237	1.263	1.260	1.299	1.308	1.314	1.337	1.353	1.341	1.372	1.372	1.370	1.346	1.303
1.107	1.156	1.212	1.242	1.260	1.264	1.298	1.312	1.304	1.341	1.353	1.344	1.368	1.378	1.373	1.335	1.299
1.103	1.183		1.238	1.253		1.279	1.289		1.318	1.333		1.361	1.373		1.366	1.296
1.091	1.154	1.205	1.240	1.230	1.269	1.291	1.308	1.296	1.337	1.345	1.350	1.337	1.376	1.366	1.336	1.285
1.081	1.134	1.195		1.255	1.268	1.288	1.297	1.295	1.326	1.344	1.350	1.365		1.359	1.318	1.277
1.076	1.119	1.144	1.208	1.233		1.271	1.282		1.312	1.327		1.343	1.347	1.307	1.304	1.275
1.085	1.108	1.126	1.153	1.188	1.234	1.222	1.246	1.284	1.276	1.277	1.318	1.300	1.293	1.291	1.296	1.286
1.115	1.080	1.078	1.095	1.120	1.148	1.167	1.187	1.213	1.217	1.224	1.232	1.232	1.235	1.244	1.269	1.319

Figure 22-29. Rodwise Power Distribution in a Typical Assembly (P-8) Near End of Life, Hot Full Power, Equilibrium Xenon, Unrodded Core

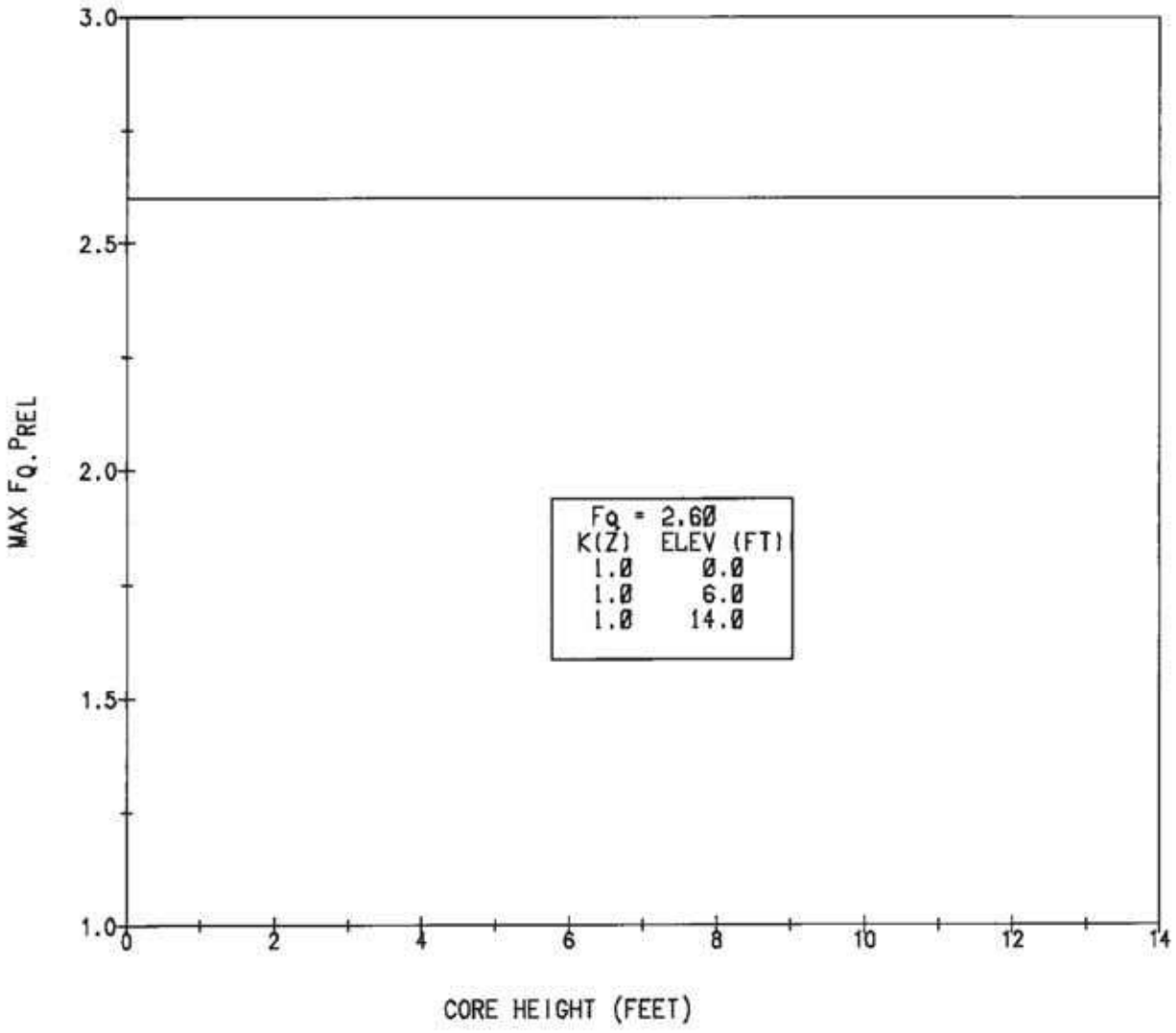


Figure 22-30. Maximum F_Q x Power Versus Axial Height During Normal Operation

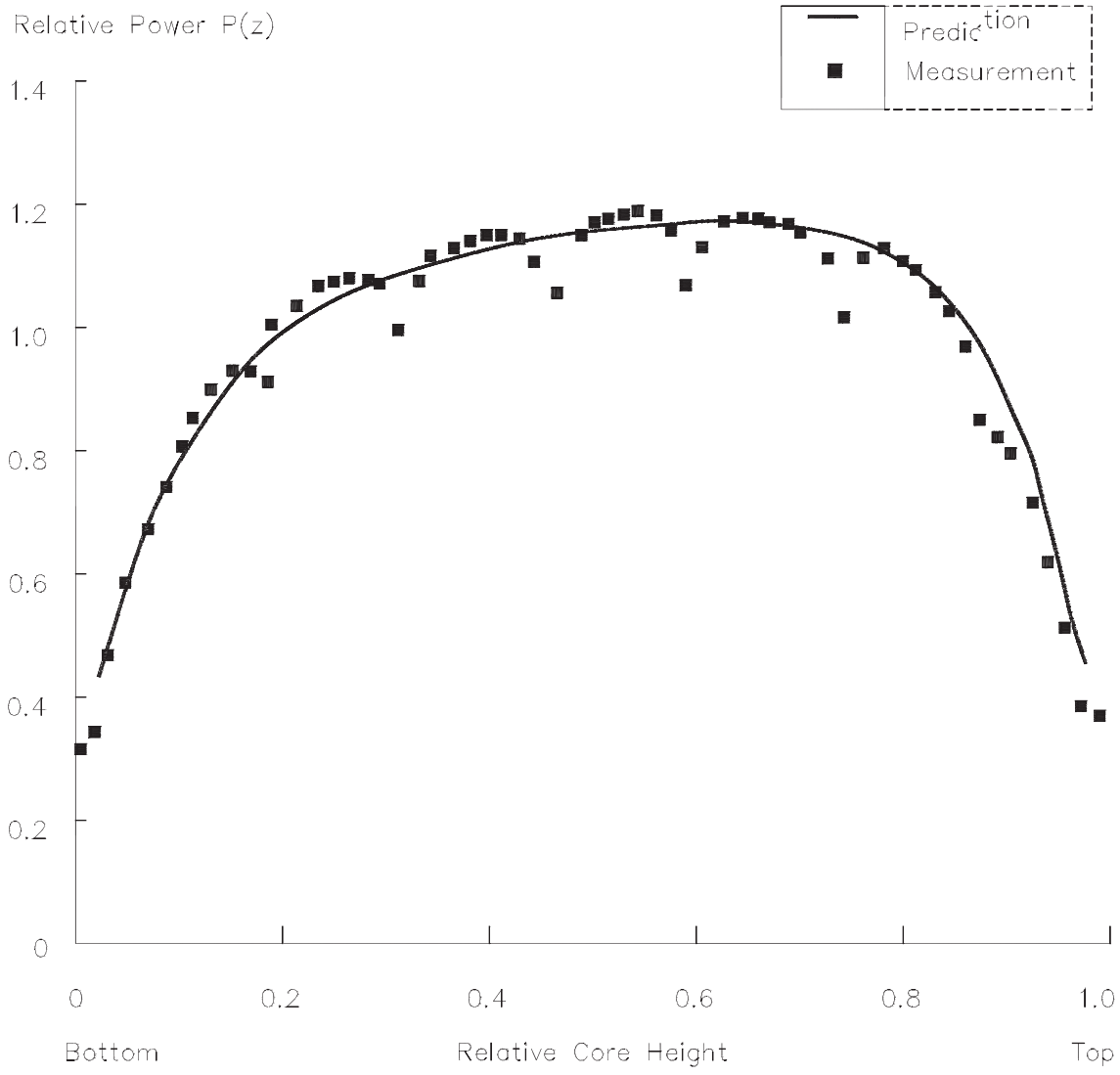


Figure 22-31. Typical Calculated versus Measured Axial Power Distribution

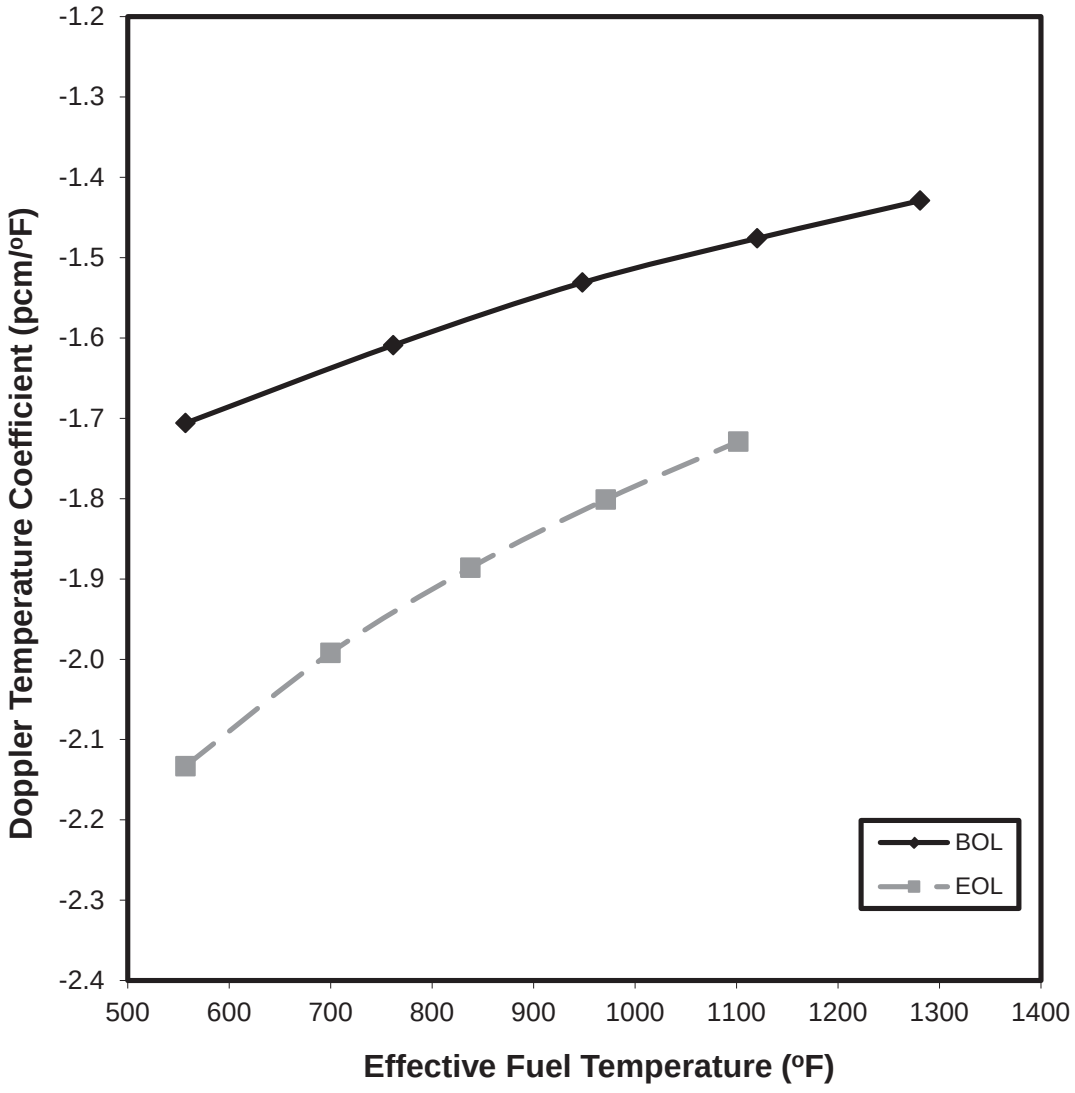


Figure 22-32. Typical Doppler Temperature Coefficient at Beginning and End of Life

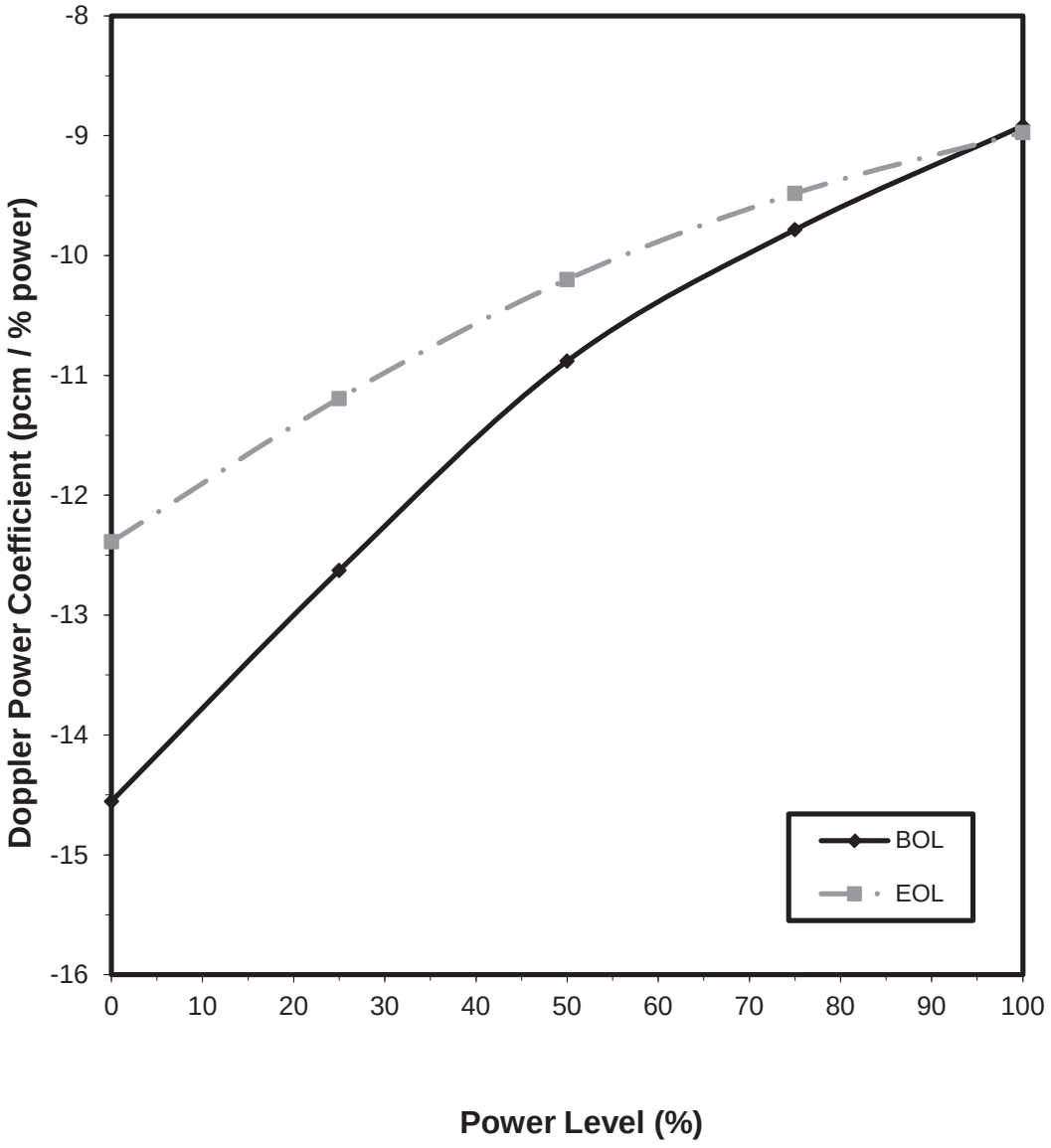


Figure 22-33. Typical Doppler-Only Power Coefficient at Beginning and End of Life

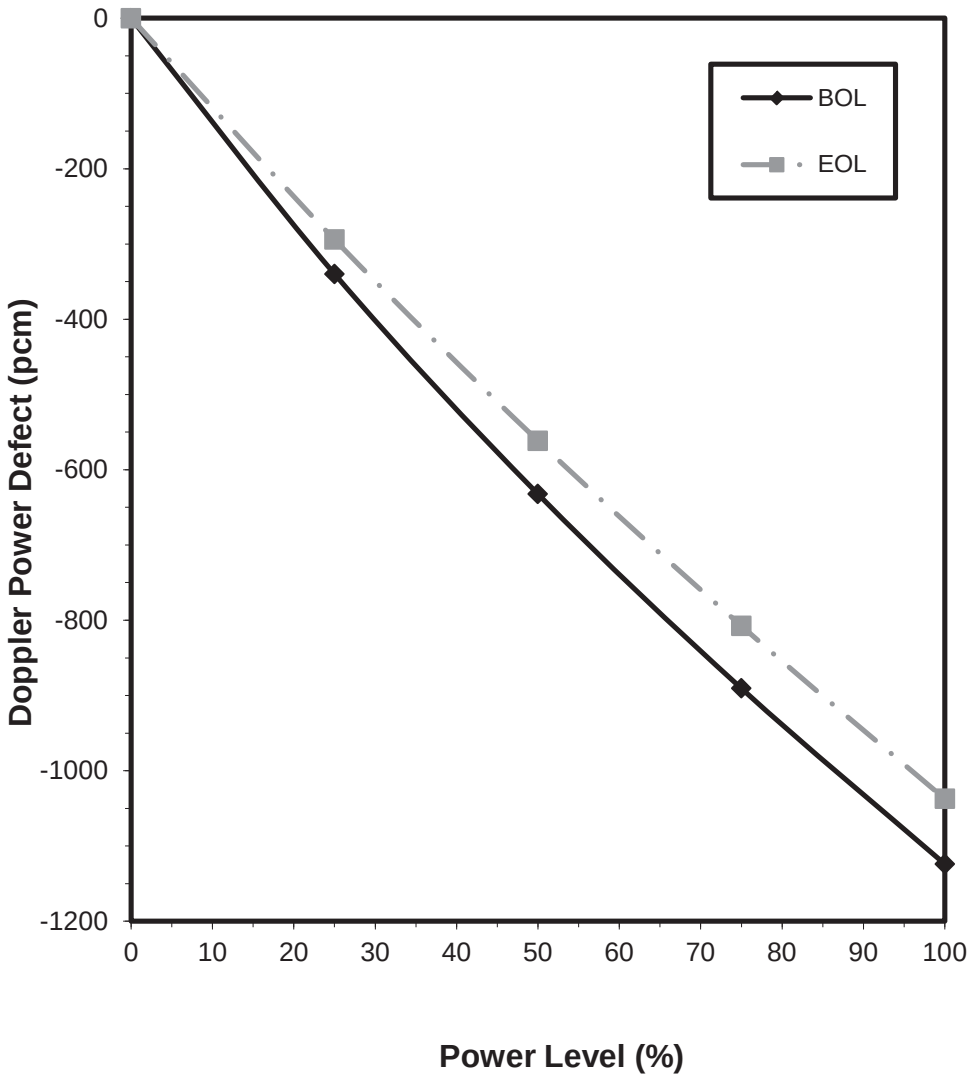


Figure 22-34. Typical Doppler-Only Power Defect at Beginning and End of Life

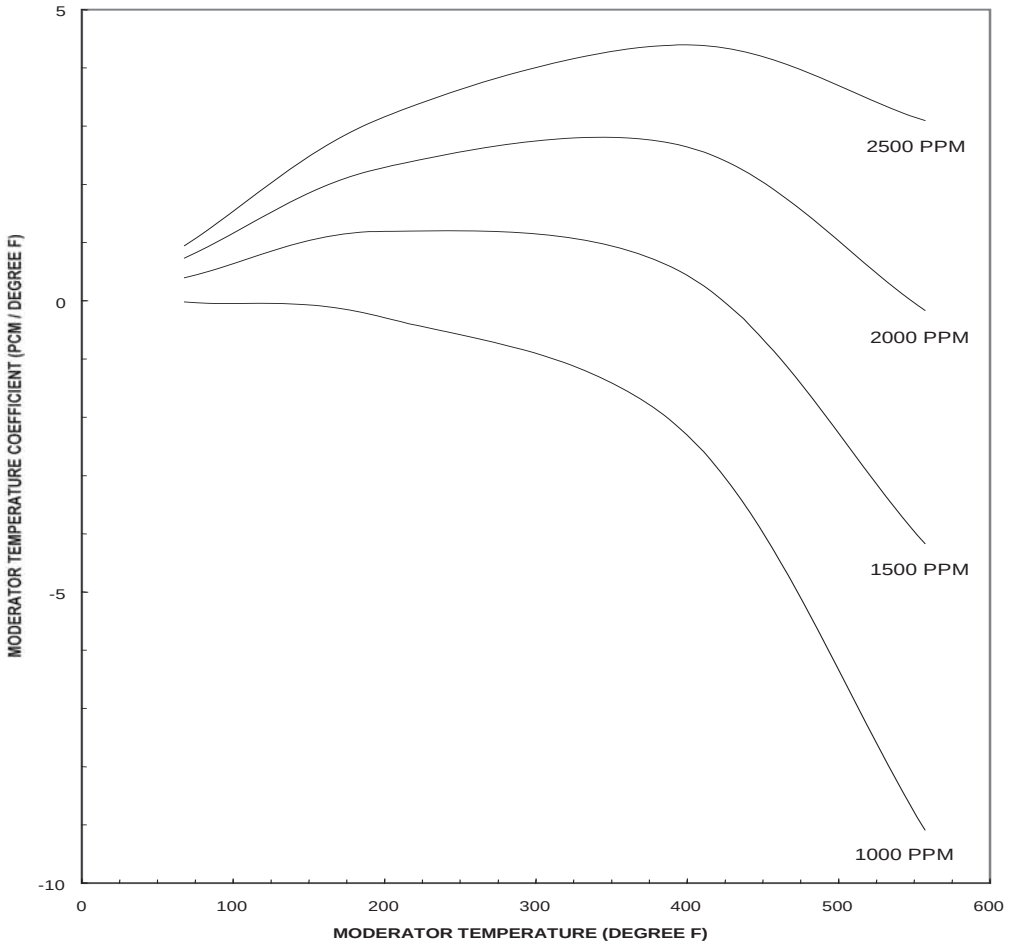


Figure 22-35. Typical Moderator Temperature Coefficient at Beginning of Life – Unrodded

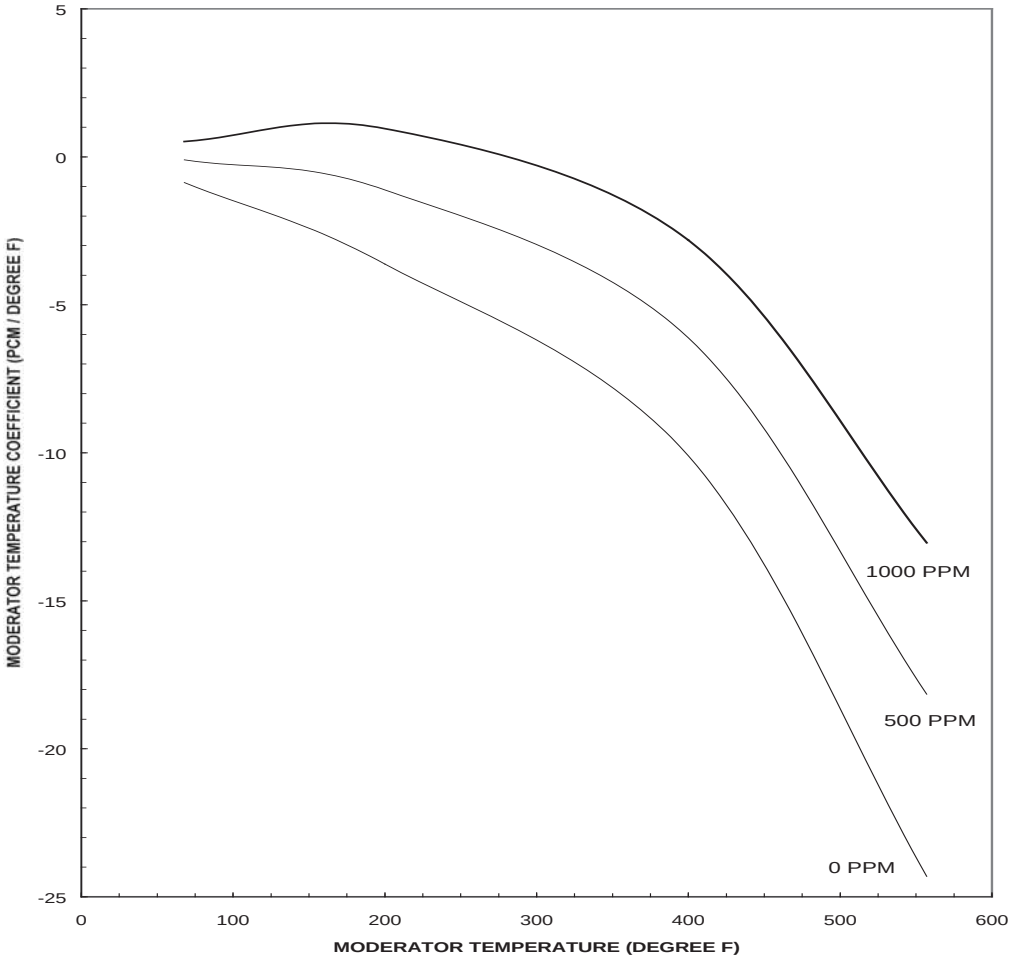


Figure 22-36. Typical Moderator Temperature Coefficient at End of Life – Unrodded

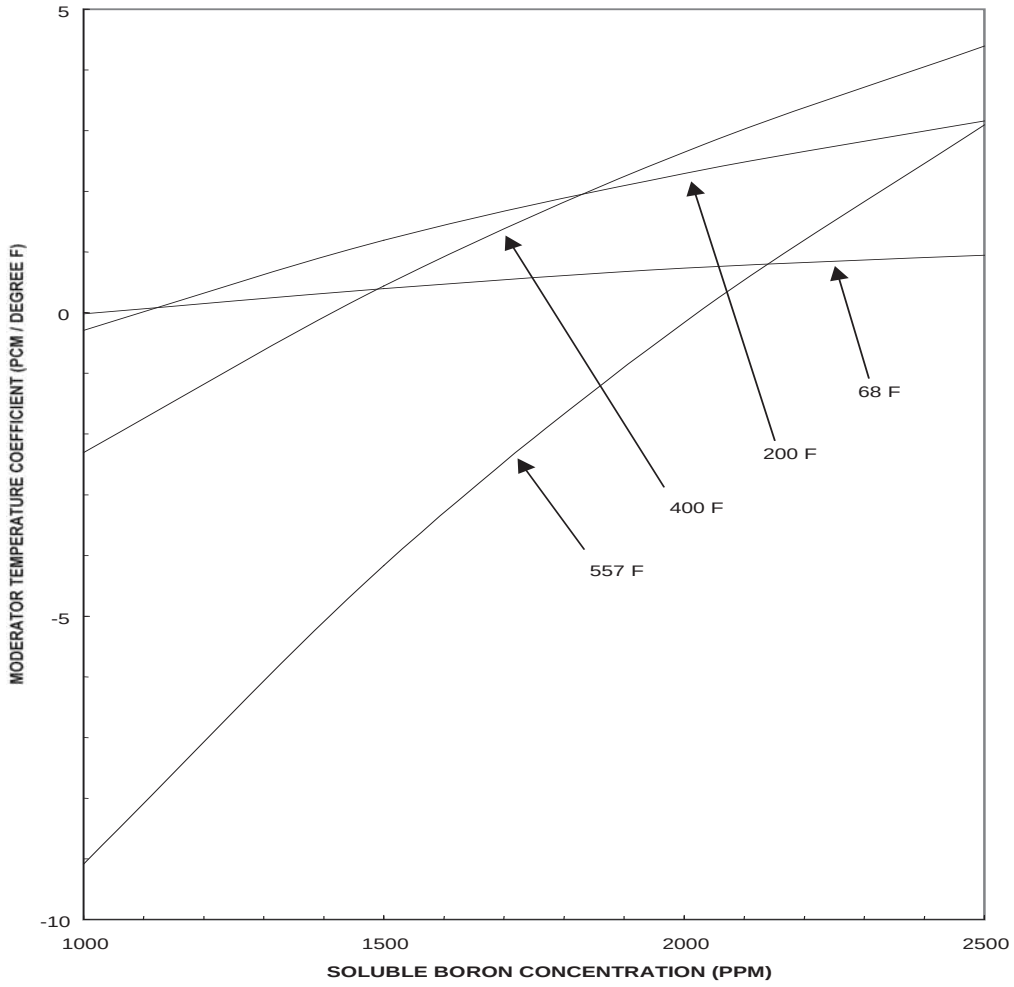


Figure 22-37. Typical Moderator Temperature Coefficient as a Function of Boron Concentration at Beginning of Life – Unrodded

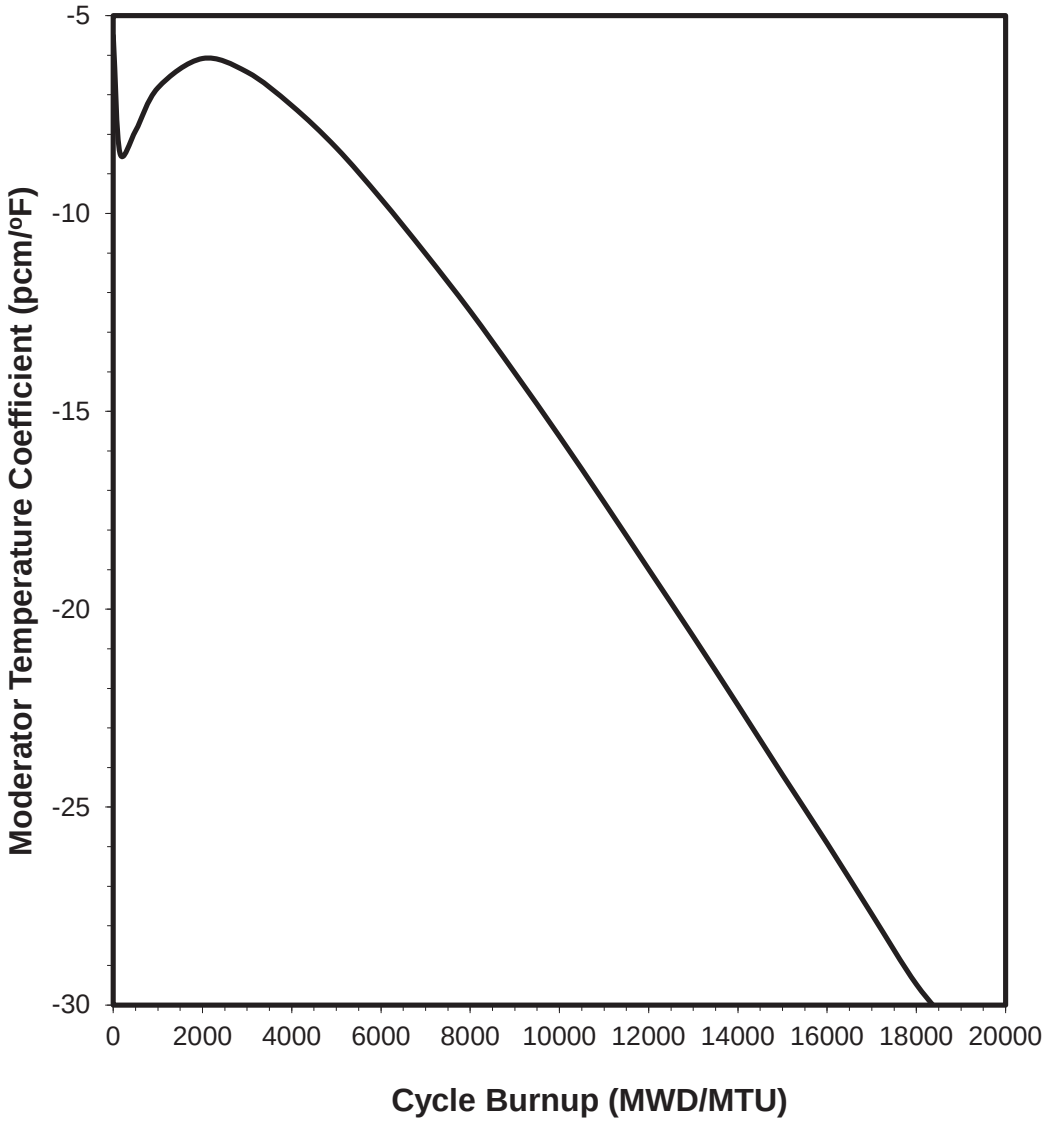


Figure 22-38. Typical Hot Full Power Temperature Coefficient versus Cycle Burnup

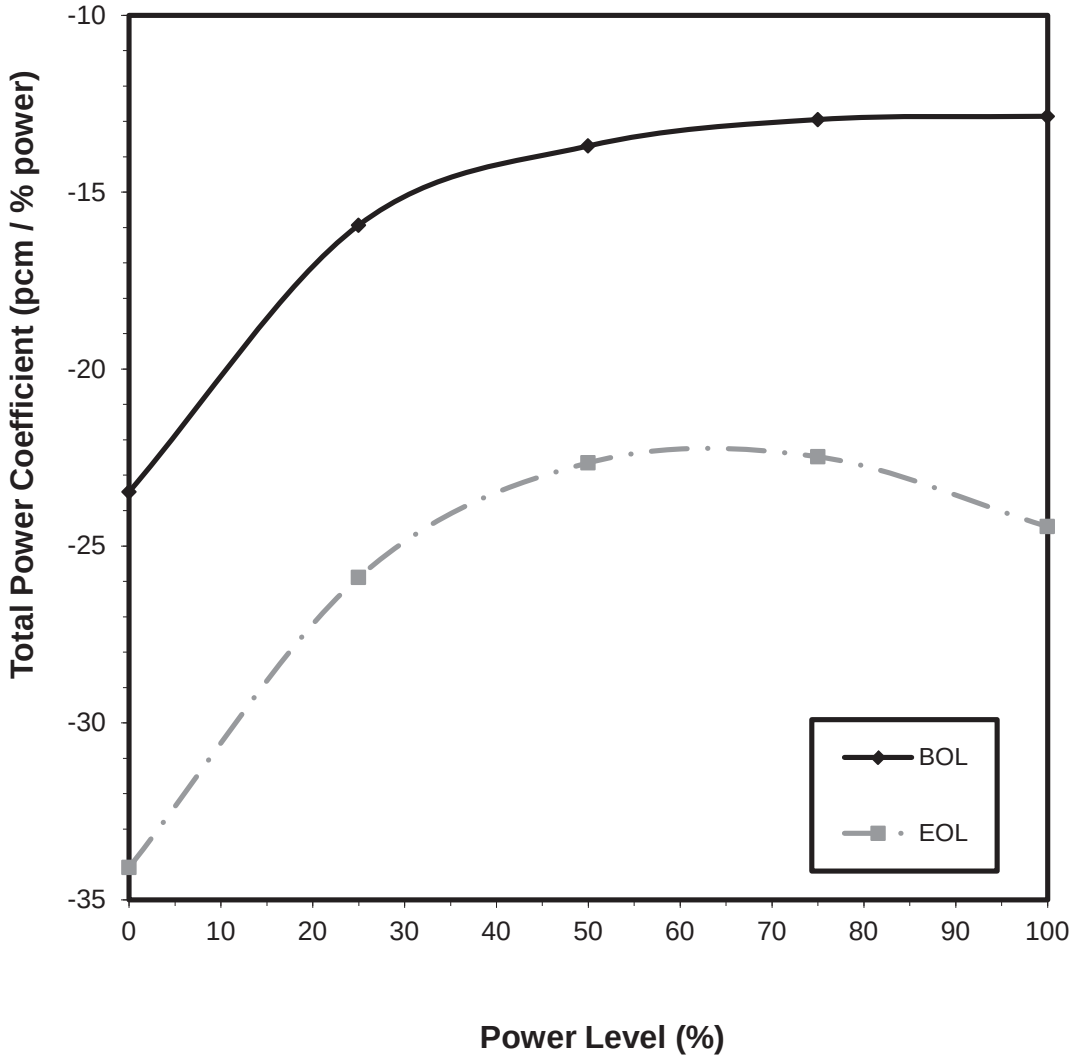


Figure 22-39. Typical Total Power Coefficient at BOL and EOL

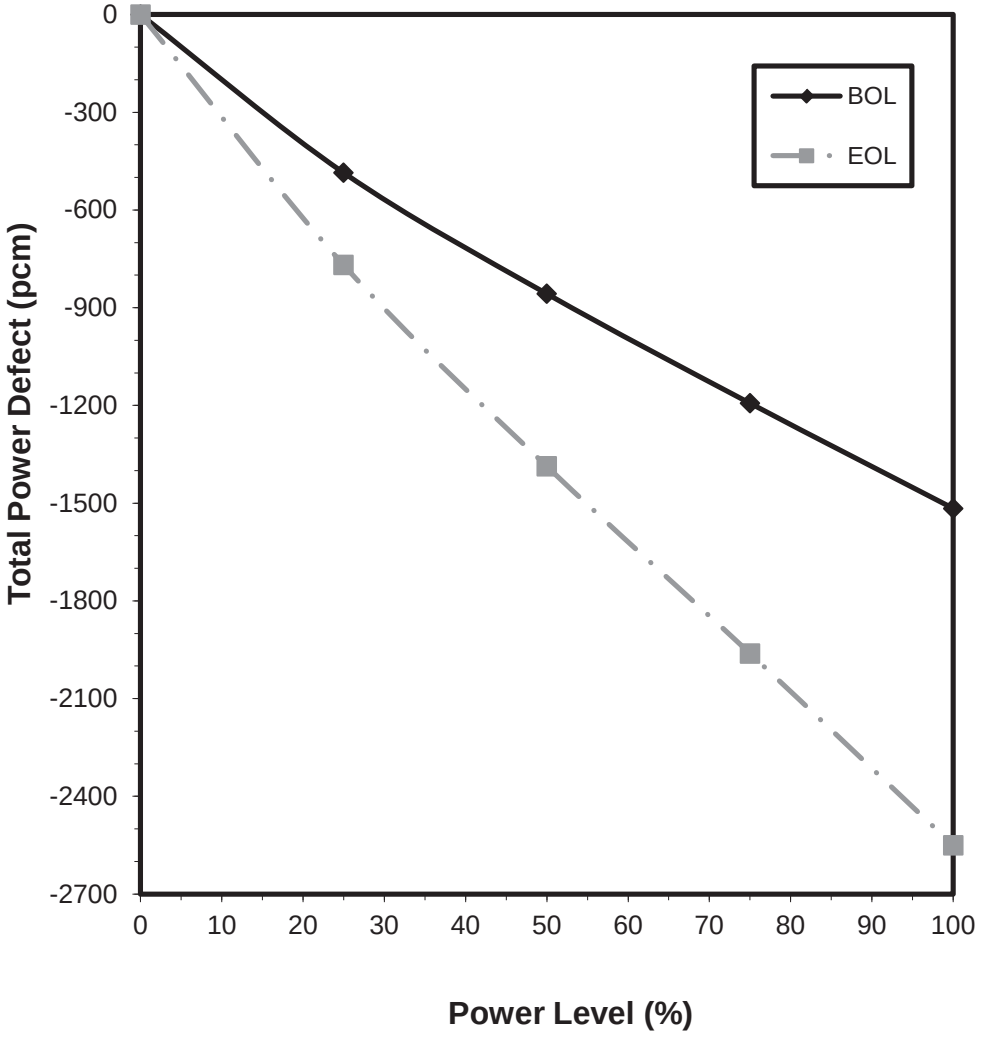
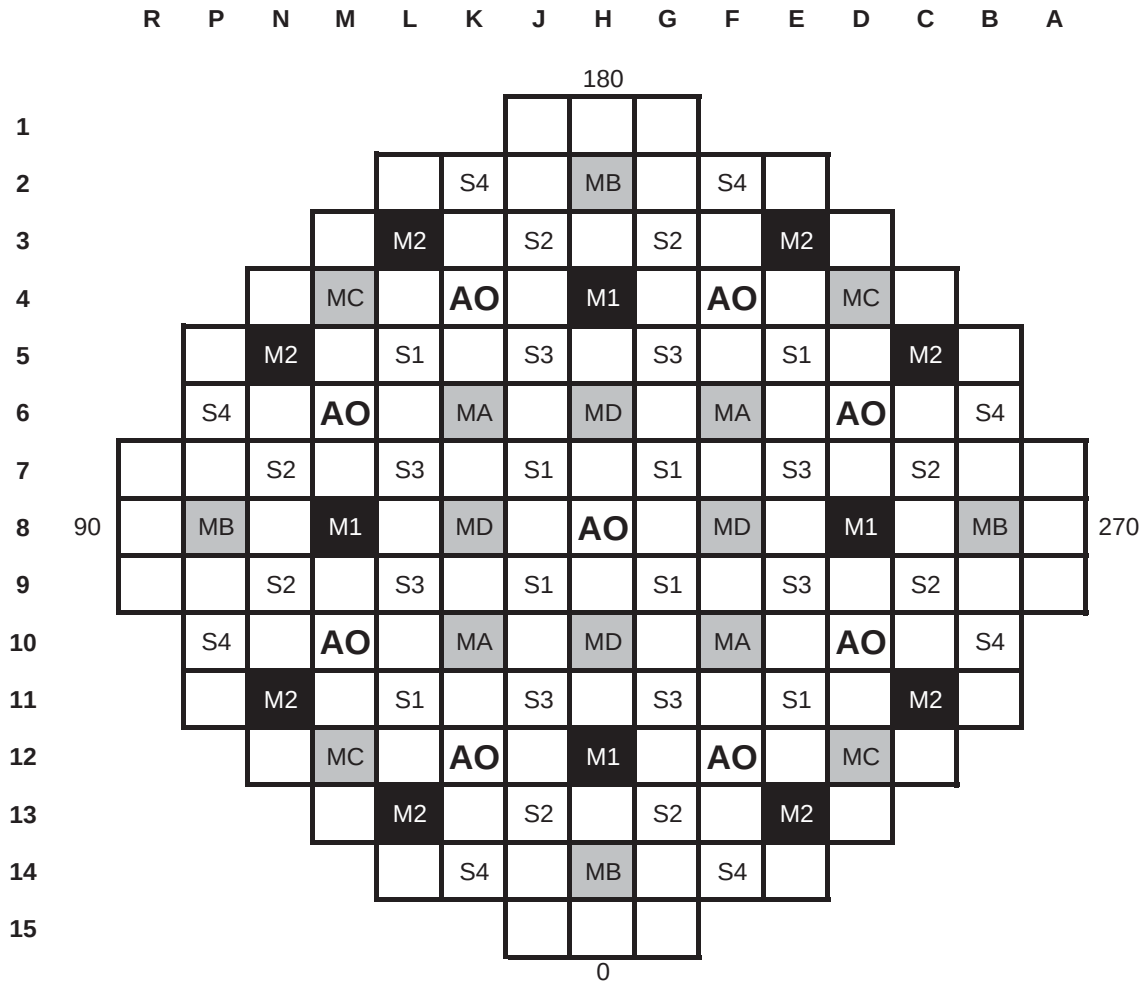


Figure 22-40. Typical Total Power Defect at BOL and EOL



Bank ID	Group Association	Cluster Design Type	# of Clusters
MA	MSHIM Control	Gray	4
MB	MSHIM Control	Gray	4
MC	MSHIM Control	Gray	4
MD	MSHIM Control	Gray	4
M1	MSHIM Control	Black	4
M2	MSHIM Control	Black	8
AO	Axial Offset Control	Black	9
S1	Shutdown	Black	8
S2	Shutdown	Black	8
S3	Shutdown	Black	8
S4	Shutdown	Black	8
Total			**69**

Figure 22-41. Rod Cluster Control Assembly Pattern

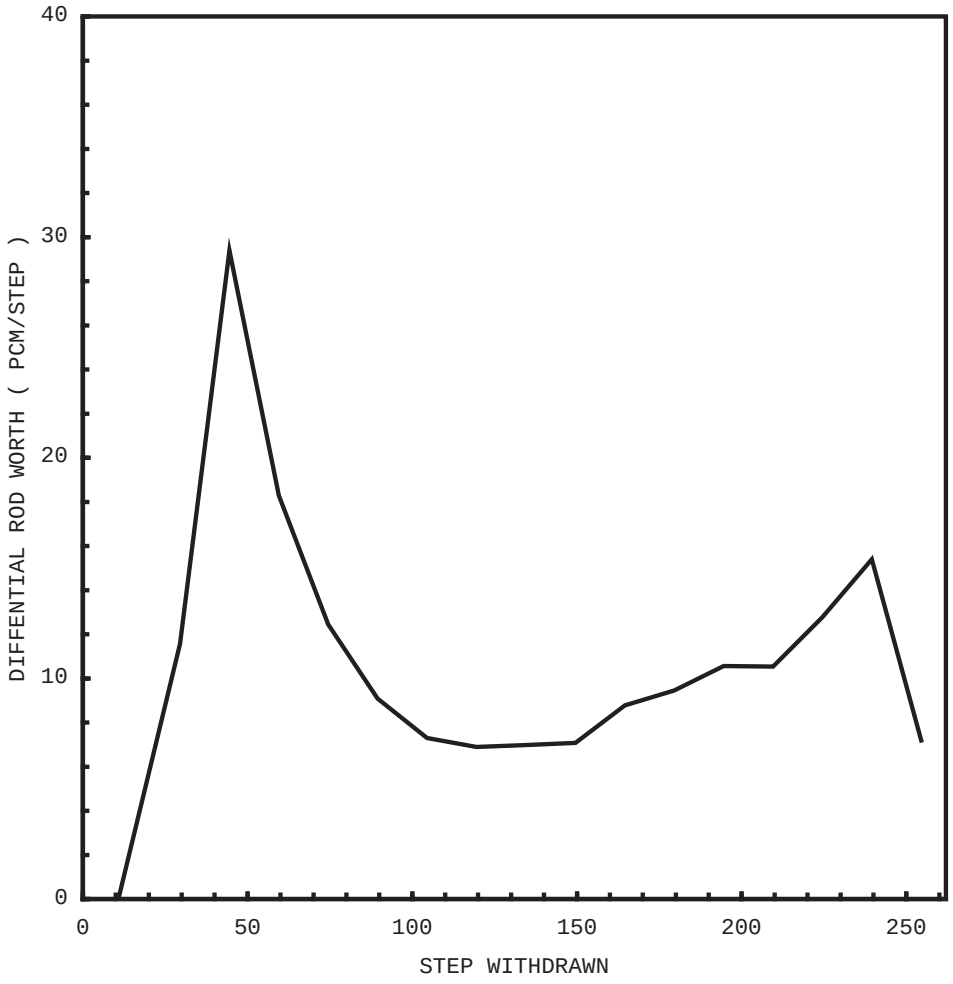


Figure 22-42. Typical Accidental Simultaneous Withdrawal of Two Control Banks at End of Life, Hot Zero Power, Moving in the Same Plane

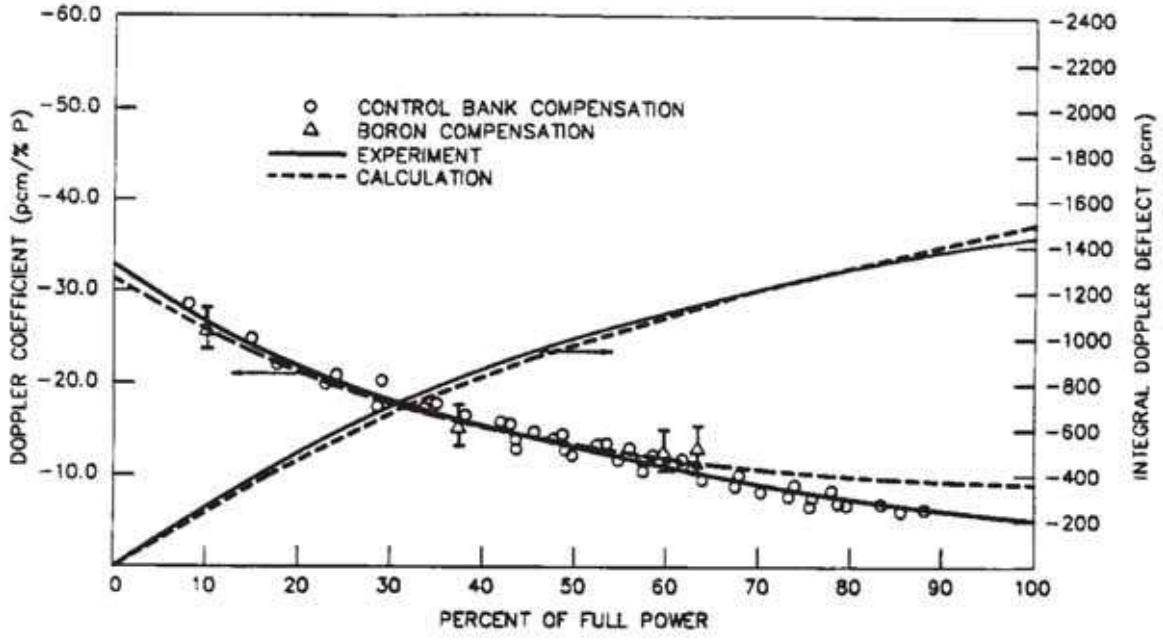


Figure 22-43. Calculated and Measured Doppler Defect and Coefficient at Beginning of Life

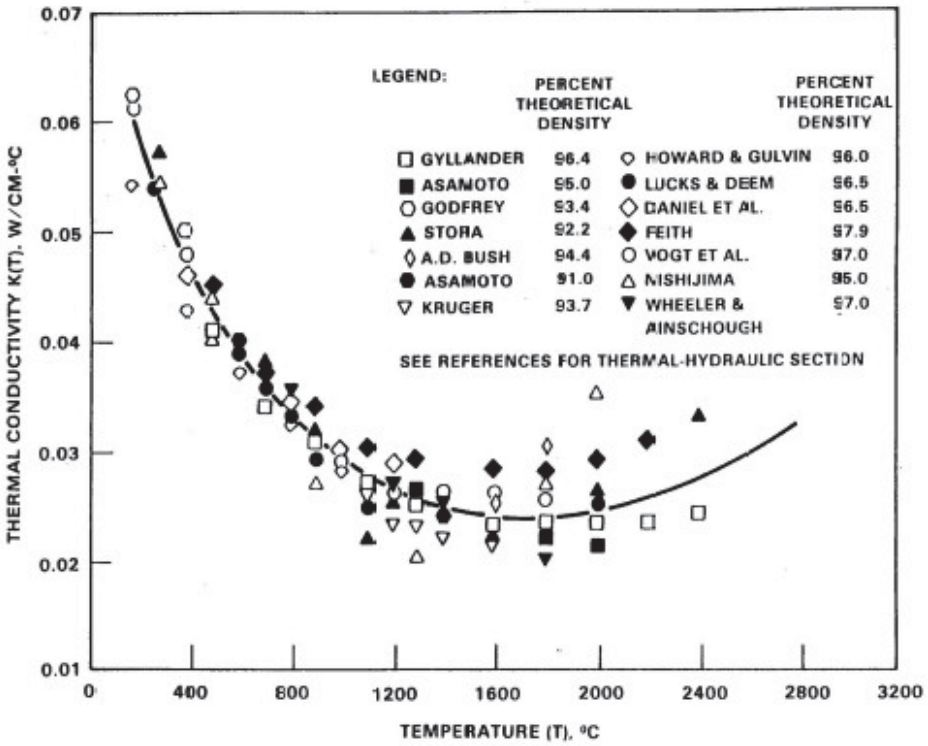


Figure 22-44. Thermal Conductivity of Uranium Dioxide

TABLE OF CONTENTS

TABLE OF CONTENTS (cont.)

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

None.

LIST OF ABBREVIATIONS AND ACRONYMS

AHU	air handling unit
ALARP	as low as reasonably practicable
AMCA	Air Movement and Control Association
ANSI	American National Standards Institute
AOV	air-operated valve
ARI	Air Conditioning and Refrigeration Institute
ASHRAE	American Society of Heating, Refrigerating, and Air Conditioning Engineers
ASME	American Society of Mechanical Engineers
BAT	best available technology
BDS	steam generator blowdown system
C&I	control and instrumentation
CAS	compressed air system
CCS	component cooling water system
C-I	Category I
C-II	Category II
CIV	containment isolation valve
CSA	control support area
CV	containment vessel
CVS	chemical and volume control system
DAS	diverse actuation system
DBA	design basis accident
DOP	dispersed oil penetration
DOS	standby diesel and auxiliary boiler fuel oil system
ECS	main ac power system
EDS	Class 2 dc and uninterruptible power supply system
EMIT	examination, maintenance, inspection, and testing
EPRI	Electric Power Research Institute
FCU	fan coil unit
FPS	fire protection system
GNS	general non-safety
HEPA	high-efficiency particulate air
HHISO	half-height ISO (containers)
HVAC	heating, ventilation, and air conditioning
IDS	essential electrical supply system
ILRT	Integrated Leak Rate Test
ILW	Intermediate Level Waste
ISO	International Organisation for Standardisation
IST	in-service testing
LLW	low-level waste
LLWR	low-level waste repository
LOCA	loss-of-coolant accident
MCR	main control room
MSIV	main steam line isolation valve
MSS	Manufacturers Standardisation Society
P&ID	piping and instrumentation diagram
PAR	passive autocatalytic recombiner
PCS	passive containment cooling system
PCSR	Pre-Construction Safety Report
PLS	plant control system
PMS	protection and safety monitoring system
PSA	probabilistic safety assessment

LIST OF ABBREVIATIONS AND ACRONYMS (cont.)

PWR	pressurised water reactor
RCA	radiologically controlled area
RCS	Reactor Coolant System
RMS	radiation monitoring system
RNS	normal residual heat removal system
RSR	remote shutdown room
SFP	spent fuel pool
SFS	spent fuel pool cooling system
SG	steam generator
SGS	steam generator system
SMACNA	Sheet Metal and Air Conditioning Contractors' National Association
SSC	systems, structures, and components
SSD	system specification document
Tech Spec	technical specification
UK	United Kingdom
UL	Underwriters Laboratories
URD	Utility Requirements Document
US	United States
VAS	radiologically controlled area ventilation system
VBS	nuclear island nonradioactive ventilation system
VCS	containment recirculation cooling system
VES	main control room emergency habitability system
VFS	containment air filtration system
VHS	health physics and hot machine shop HVAC system
VLS	containment hydrogen control system
VRS	radwaste building HVAC system
VTS	turbine building ventilation system
VUS	containment leak rate test system
VWS	central chilled water system
VXS	annex/auxiliary building nonradioactive ventilation system
VYS	hot water heating system
VZS	diesel generator building heating and ventilation system
WLS	liquid radwaste system
ZOS	onsite standby power system

23 CONTAINMENT AND NUCLEAR VENTILATION SYSTEMS

23.1 Introduction

This chapter provides the evidence that the design of the containment and nuclear ventilation systems in the AP1000 design is adequate to meet the safety claims placed upon these systems in other parts of the safety case, both for normal operations and under fault conditions. System Specification Documents (SSD) are referenced for each relevant mechanical system. The SSD provides addition details and evidence for the safety claims placed upon systems, structures, and components (SSCs). Each SSD identifies the specific design requirements for the system and documents the system design that satisfies the requirements. SSD delineate the following:

- Summarises the functions, design criteria, and design data of system
- Describes system layout, instrumentation and control, interfacing systems, and environmental requirements.
- Describes system operations and identifies examination, maintenance, inspection, and testing (EMIT) guidelines.
- Listing of the pertinent Piping and Instrumentation Diagrams for the system.
- Lists supporting references

The containment and nuclear ventilation systems largely support the primary safety functions of the containment of radioactive substances, heat transfer/residual heat removal and provide environmental support to SSCs that, in turn contribute to primary safety functions. Analysis of the containment and ventilation systems has therefore been carried out to review their requirements against the primary safety functions. The intention of the justification against these safety functions is to demonstrate how the risks have been reduced to a level that can be considered as low as reasonably practicable (ALARP).

Generic component failure data parameters for the SSCs discussed in Chapter 23 are shown in Table 10-34 and Table 10-35. The component failure data is used as an input to the AP1000 plant Probabilistic Safety Assessment (PSA) discussed in Chapter 10. Justification against the containment primary safety function considers how the mechanical design of plant systems ensures that the containment provided by the containment vessel (CV) and other SSCs is protected.

Justification against the heat transfer/residual heat removal primary safety function considers the way in which the mechanical design of plant systems influences the management of decay heat within the CV.

Justification of the support provided by the ventilation systems to other SSCs considers how the ventilation systems maintain the internal building conditions within design limits with regards to temperature, hydrogen concentrations, and other factors.

The report against each of the relevant systems is structured in the following way:

- Its role in normal and abnormal operation is discussed and the primary safety functions to which the system contributes are identified and discussed.

- A description of the relevant SSCs that contribute to provision of the system function is provided.

- Classification and categorisation of these components and identification of what they must do to meet any safety requirements.

- A justification to support the claims that are made.

Plant response to loss of heating, ventilation, and air conditioning (HVAC) events are discussed in Chapter 6 and Chapter 8 respectively. Section 6.6.3 describes design features to maintain the Main Control Room habitable if normal HVAC is lost. Chapter 8 describes the design basis for loss of normal HVAC to the balance of auxiliary building. Active HVAC is not required for containment during a design basis accident.

The contribution of the ventilation systems to radiation protection is discussed further in Chapter 24 of this Pre-Construction Safety Report (PCSR).The AP1000 plant ventilation systems are designed to United States (US) codes and standards. The design satisfies the with United Kingdom (UK) practice as described in References 23.1 and 23.2. This is discussed further in Appendix 23A. A justification for the acceptability of United States standards for use in the UK is provided in UKP-GW-GL-045 (Reference 23.44).

23.2 SCOPE

23.2.1 Scope of Ventilation Systems

The CV is supported in its containment function by the following ventilation systems:

- Containment air filtration system (VFS)
- Containment recirculation cooling system (VCS)
- Containment leak rate test system (VUS)
- Containment hydrogen control system (VLS)

The passive containment cooling system (PCS), which provides the principal post-accident means of removing decay heat from the containment to the ultimate heat sink, the atmosphere, is not discussed in this chapter, but a detailed discussion of the safety claims and supporting evidence is provided in Section 17.6.1.

The support of other SSCs is provided outside the CV by the following:

- Main control room emergency habitability system (VES)
- Radiologically controlled area ventilation system (VAS)
- Radwaste building HVAC system (VRS)
- Health physics and hot machine shop HVAC system (VHS)
- Nuclear island nonradioactive ventilation system (VBS)
- Annex/auxiliary building nonradioactive ventilation system (VXS)
- Turbine building ventilation system (VTS)
- Diesel generator building heating and ventilation system (VZS)

The AP1000 design safety case presented in this PCSR makes a number of claims on the containment and ventilation systems. These claims in Chapter 14 are detailed in the relevant parts of this chapter.

23.2.2 Maritime Weather Conditions

The hardening of ventilation external features in respect to the maritime climate is a site-specific design change, while the standard design ventilation (assessed in the generic design assessment) is not salt-hardened. However, Westinghouse recognises that if the AP1000 design is selected for construction in the UK, it will be most likely for a coastal site. In that case, the following changes may be necessary depending on the sea salt aerosol concentrations:

- The majority of AP1000 plant ventilation systems includes filtration of air intakes and will remove any sea salt aerosols or particulates at the first, coarse filter and the higher efficiency second filter. Air passing through the remainder of the HVAC system will be essentially salt-free. It is only the portions of the HVAC components and structures upstream of the filters that will be exposed to potential salt corrosion, Therefore, salt-resistant materials will be added to ducts and air handling units so that all material upstream of high-efficiency filters is salt-hardened.

- The remaining HVAC systems are portions of the VTS, VBS (PCS valve room), and VZS. The aforementioned systems do not provide any air conditioning. At coastal sites, the portions of the turbine building served by the unfiltered VTS ventilation subsystem will be exposed to unmodified outside salt air. Those portions of the building, all of the HVAC ducting, components, and structures are exposed to salt, therefore:

  – Salt-resistant coatings will be added for equipment, components, piping, and exposed structural steel located in the nonconditioned areas of the turbine building, including ducts and equipment.

  – Fan-ventilated electrical cabinets in nonconditioned areas will be required to have inlet air filters to remove salt spray and particles. This additional cabinet filtration will add to the normal maintenance inspection and replacement schedule.

The VCS, VES, and the VLS are not affected by coastal site conditions because they are not exposed to salt-laden air.

23.3 CONTAINMENT AIR FILTRATION SYSTEM

23.3.1 Role

The VFS contributes to the containment primary safety function by providing containment isolation and filtered extract from the fuel handling area, the radiologically controlled area (RCA) of the annex/auxiliary buildings and the hot machine shop, and other areas served by the VHS following detection of high radiation by the VAS or VHS. Further design details of this system and its constituent components are delineated in Reference 23.5. This system is also discussed in Chapter 6.

The plant design makes provision for two supply air handling units (AHUs) and two air filtration exhaust units and fans. The filtration units include high-efficiency particulate air (HEPA) filters and charcoal adsorbers. Containment isolation valves (CIVs) are provided on either side of the containment penetrations for the supply and extract air pipework.

During normal intermittent purge operation, only one supply and exhaust system is required to operate. The standby supply and exhaust units can be started manually by the operator if the operating train fails. Prior to and during plant shutdown, one or both exhaust filtration trains can be operated to remove airborne radioactivity for personnel access.

A number of systems support the function of the VFS. These include, but are not limited to the following:

- Compressed air system (CAS)
- VCS recirculation coolers.
- Protection and safety monitoring system (PMS)
- Diverse actuation system (DAS)
- Plant control system (PLS)
- Fire protection system (FPS)

The PMS and radiation monitoring system (RMS) are supported by the VFS through the provision of appropriate sensors within the system.

23.3.2 System Components and Equipment Contributing to Safety Function[2]

The following components provide key contributions to the ability of the VFS to perform its safety function.

- **CIVs (VFS-PL-V003, V004, V009, V010)** – The CIVs are metal seated butterfly valves. The valves are designed and constructed to American Society of Mechanical Engineers (ASME) Code, Section III-2 (Reference 23.4) and are Seismic Category I (C-I) as detailed in the VFS system specification document (Reference 23.5, Appendix F2). Each valve is provided with a pneumatically operated spring return actuator that fails safe in a closed position on a loss of electrical power or instrument air. The isolation valves have manual manipulation devices to verify proper operation of the valves and/or to override their fail safe position.

  Automatic closure of the CIVs in response to the DAS or PMS is necessary to maintain the leaktight integrity of the CV. The CIVs are designed to Class 1 as they are the principal means of Containment Isolation which is a Category A safety function.

  CIVs (VFS-PL-V800A, V800B, V803A, 803B) – The vacuum relief portion of the VFS provides a relief path into containment to relieve excessive negative pressure caused by cold weather. Containment isolation valves (VFS-PL-V800A and V800B) are metal seated butterfly valves. The valves are designed and constructed to ASME Code III-2 (Reference 23.4) and are Seismic C-I. Containment isolation valves VFS-PL-V803A and V803B are check valves. The valves are designed and constructed to ASME Code, Section III-2 (Reference 23.4) and are Seismic C-I. The CIVs are designed to Class 1 as they are the principal means of Containment Isolation which is a Category A safety function.

  Manual CIV (V007, V008, V101, V202, V587) – The Integrated Leak Rate Test (ILRT) test connection valves (VFS-PL-V008, V101) are manual globe valves. The containment isolation block valves **(**VFS-PL-V202, V587) are manual butterfly valves. The Reactor Coolant System (RCS) vacuum ejector discharge air isolation valve (VFS-PL-V007) is a manual butterfly valve. The valves are designed and constructed to ASME Code, Section III-2 (Reference 23.4) and are Seismic C-I. The CIVs are designed to Class 1 as they are the principal means of Containment Isolation which is a Category A safety function.

- **HEPA filter** – HEPA filters are constructed, qualified, and tested in accordance with the nuclear air and gas treatment code (Reference 23.6, Section FC). Each HEPA filter cell is individually shop tested to verify an efficiency of at least 99.97 percent using a

monodisperse 0.3-µm (1.18e-5 inch) aerosol in accordance with Reference 23.6, Section TA.

The HEPA filters in the VFS work to remove particulate present in extract air from the containment, fuel handling area and auxiliary/annex buildings to minimise the offsite release of contamination to a level that is ALARP and within the regulatory limits.

HEPA filters are passive components, and as such, no actuation signal is required. Ensuring a particulate filtration efficiency of 99.97 percent of 0.3-µm (1.18e-5 inch) particles is a Category B safety function and thus the component is designed to Class 3.

- **Charcoal adsorber** – Each charcoal adsorber is designed, constructed, qualified, and tested in accordance with ASME AG-1 (Reference 23.6, Section FE) and Regulatory Guide 1.140 (Reference 23.7). This guide describes the design, inspection, and testing criteria for air filtration and adsorption units of normal atmosphere cleanup systems in light-water-cooled nuclear power plants. Each charcoal adsorber is a single assembly with welded construction and 102 mm (4 inches) deep Type III rechargeable adsorber cell. Reference 23.7 indicates that a charcoal adsorber of this type should have a decontamination efficiency of 99 percent using the appropriate test methodology.

  The charcoal adsorbers in the VFS work to remove radiation present in extract air from the containment, fuel handling area and auxiliary/annex buildings to minimise the offsite release of radiation to a level that is ALARP and within the regulatory limits.

  Charcoal adsorbers are passive components, and as such, no actuation signal is required. Ensuring a decontamination efficiency of 99 percent is a Category B safety function and is designed to Class 3.

- **Supply and exhaust fans** – The supply and exhaust air fans are centrifugal type, single-width single-inlet, with high-efficiency wheels and backward-inclined blades to produce non-overloading characteristics. Fan performance is rated in accordance with American National Standards Institute (ANSI)/Air Movement and Control Association (AMCA) Standards 210 [1] (Reference 23.9), 211 (Reference 23.10), and 300 (Reference 23.11).

  Operation of the supply and exhaust fans ensures that a suitable airflow can be achieved through the containment during purge operations to reduce the radiation levels in the containment environment. The exhaust fans also provide a filtered exhaust route from the fuel handling area and annex/auxiliary buildings, maintaining a depression relative to the surrounding areas.

  The supply/exhaust fans operate in response to signals from the PLS. They are manually operated for containment purge functions. The exhaust fans respond automatically to signals that include high/low pressure differential in the fuel handling area, RCAs of the annex/auxiliary buildings, or high radiation in these areas.

  Failure of the supply fans would not result in the VFS being unable to fulfil its primary safety function; therefore, no further analysis is required. Failure of the exhaust fans when demanded to extract from the fuel handling area and annex/auxiliary buildings

1. The AP1000 design ventilation systems are designed to US codes and standards. The design satisfies the UK practice as described in References 23.1 and 23.2. This is discussed further in Appendix 23A. A justification for the acceptability of United States standards for use in the UK is provided in UKP-GW-GL-045 (Reference 23.44).

may prevent the maintenance of a depression in those areas and lead to an unmonitored release of air to the environment or surrounding areas. Therefore, operation of the exhaust fans is a Category C safety function and the component is designed to Class 3.

- **Isolation, balancing, and shutoff dampers** – Isolation dampers are bubble-tight, single- or parallel-blade type. The isolation dampers have spring return actuators that fail closed on loss of electrical power or instrument air. The design and construction of the isolation dampers is in accordance with ANSI/AMCA Standard 500 (Reference 23.12) or ASME AG-1 (Reference 23.6). Multi-blade, two-position, remotely operated shutoff dampers are parallel-blade type. AHU and fan shutoff dampers are designed for maximum fan static pressure at shutoff flow and meet the performance requirements of ANSI/AMCA Standard 500 (Reference 23.12). The containment exhaust air dampers meet the design and construction criteria of ASME AG-1 (Reference 23.6, Section DA). Multi-blade, balancing dampers are of single or opposed-blade type.

  The isolation and shutoff dampers operate in response to signals from the PLS.

  The dampers are manufactured to appropriate industrial or nuclear standards to ensure a high reliability. Balancing dampers are set during commissioning and are not required to actuate during operation. In the main ductwork, active dampers are located in redundant supply/extract lines such that failure of a damper will not prevent the VFS from performing its safety function. The exception to this is on the extract lines from the areas served by the VAS. However, it is considered that the likelihood of coincident failure of an isolation damper and the occurrence of an event leading to a release of contamination is very low. As such, no further analysis is required.

- **Ductwork and accessories** – Ductwork, duct supports, and accessories are constructed of galvanised steel. Ductwork subject to fan shutoff pressures is structurally designed to accommodate these pressures. The system air ductwork inside containment is constructed from pipe, and meets Seismic Category II (C-II) criteria so that it will not fall and damage any safety equipment following a safe shutdown earthquake. Ductwork, supports, and accessories meet the design and construction requirements of the Sheet Metal and Air Conditioning Contractors' National Association (SMACNA) Rectangular and Round Industrial Duct Construction Standards (References 23.13 and 23.14) and HVAC Duct Construction Standard – Metal and Flexible (Reference 23.15). The exhaust air ductwork and supports meet the design and construction requirements of ASME AG-1 (Reference 23.6, Article SA-4500). The ductwork low leakage rate will be tested as necessary in accordance with SMACNA HVAC Duct Leakage Test Manual (Reference 23.16) and/or ASME N510 (Reference 23.17, Section 6) to verify that the leak tightness meets the design requirements (Reference 23.5, Section 5.1).

  The ductwork is required to contain potentially contaminated air within the VFS. It is considered that the tests and standards outlined above are adequate to allow the ductwork to meet its safety function and as such no further analysis is required.

- **Fire dampers** – Fire dampers are provided at duct penetrations through fire barriers to maintain the fire resistance rating of the barriers. The fire dampers are constructed of galvanised carbon steel and actuated by fusible links designed to melt and release the damper blade when the air temperature reaches 74°C (165°F) (Reference 23.5, Section 5.1). The damper blades close via a spring mechanism. Additionally some VFS fire dampers are provided with position indication. The fire dampers meet the design, testing and installation requirements of Underwriters Laboratories (UL) 555 (Reference 23.18).

The fire dampers are passive components operated by temperature and an internal spring mechanism. As such, no actuation signal is required.

The fire damper rating will be at least equal to the fire barrier that it penetrates, up to a maximum 3-hour rating. This is essential to maintain the integrity of fire barriers discussed in the internal fire hazard section of Chapter 11 and is Category B Class 3 equipment.

23.3.3 Claims on Components and Equipment

23.3.3.1 Containment Isolation Valves (VFS-PL-V003, V004, V009, V010, V800A, V800B, V803A, 803B)

Containment isolation maintains the integrity of the CV in the event of a loss-of-coolant accident (LOCA), thus minimising the release of radioactive material from the containment. This is a Category A safety function. The CIVs are fundamental to maintaining the containment boundary, and failure to operate could result in a significant release of radioactive material from the containment. The CIVs are the primary means of fulfilling the containment isolation function and hence are Class 1 components. The UK safety categorisation and classification methodology is discussed in further detail in Chapter 5 and Appendix 15A.

CIVs are provided in series with one valve inside containment and one valve outside containment. It is claimed that at least one CIV will close to successfully isolate the containment.

The design of CIVs are very similar to other air-operated valves (AOVs) installed in pressurised water reactors (PWRs) already operating.

23.3.3.2 High-Efficiency Particulate Air Filter and Charcoal Adsorber

The HEPA filters and charcoal adsorbers in the VFS minimise the radiation released to the environment during containment purging operations and extract from the fuel handling area and annex/auxiliary building. As such, the HEPA filters and charcoal adsorbers provide a Category B safety function. Failure of either the HEPA filters or the charcoal adsorbers will result in the potential for a release of contamination and radioactivity to the environment. The HEPA filters and charcoal adsorbers provide a contribution to the VFS primary safety function and are Class 3 equipment. See Appendix 15A.

There is one HEPA filter bank and one charcoal adsorber in each exhaust air filtration unit, and there are two exhaust air filtration units. Only one filtration unit is required to operate for the VFS to deliver its safety function. Therefore, it is claimed that one HEPA filter bank and one charcoal adsorber will filter the exhaust air to ensure air discharged to atmosphere is below preset radiation limits.

23.3.3.3 Exhaust Fans

The exhaust fans are not required to operate to support the containment following an event. However, they do maintain a depression in the fuel handling area and annex/auxiliary building areas served by the VAS following detection of high radiation. This prevents an unmonitored release of air to the environment and surrounding areas. In doing this, the fans control the level of radioactivity released to the environment, which is a Category C safety

function. The exhaust fans provide a contribution to nuclear safety and are Class 3 equipment. See Appendix 15A.

There are two exhaust fans installed, and it is claimed that one fan will start and operate to extract air from the fuel handling area, the RCA of the annex/auxiliary buildings and the hot machine shop, and other areas served by the VHS following detection of high radiation by the VAS or VHS.

23.3.3.4 Fire Dampers

Fire dampers are installed where ductwork passes through fire barriers.

The fire dampers protect against fire hazards that could, as part of a sequence of failures, result in loss of a safety function. This could compromise normally operating systems and safety systems delivering a specific function. Therefore, this is a Category B safety function. As the fire dampers provide a contribution to achieving this safety function, they are deemed to be Class 3 equipment. See Appendix 15A.

Single fire dampers are provided where the ducts pass through a fire barrier. It is claimed that the fire dampers will close when the air temperature in the duct reaches the design limit.

23.3.4 Justification of Claims on Components and Equipment

23.3.4.1 Containment Isolation Valves (VFS-PL-V003, V004, V009, V010)

The CIVs are of a spring return design such that no external power source is required to close the valve. This passive approach offers a high degree of inherent safety and high reliability.

The CIVs are Seismic C-I and are to be designed and constructed to the ASME Code, Section III-2 (Reference 23.4) design code. This code has been specifically developed to qualify pressure retaining components in safety significant applications on nuclear power stations. The code, with the testing and examination that supports it, provides the foundations for claims made on the CIVs.

The isolation valve design is fail safe such that a loss of pneumatic or electrical power will cause the valve to fail closed. The valves are very similar to those already in service to provide the same function on many operating power stations. As a result, the information from testing of these in-service valves offers a high degree of confidence about the reliability to be expected from the valves proposed for the AP1000 design. The AOV component boundary includes the valve, valve operator (including the associated solenoid operated valves), local circuit breaker, and local control and instrumentation (C&I) circuitry (Reference 23.21). It is reasonable to assume that a large proportion of these failures will be associated with moves to an energised position.

The operating mechanism for the valve is simple, and aside from gross mechanical failure, the principal mechanisms for valve failure, is considered to be some form of adhesion preventing the valve closing, or leakage of the valve under pressure when in the closed position. These failures are considered to be unlikely because of a combination of good design and a robust maintenance, inspection, and testing regime. The valve is a metal seated butterfly type with double seals around the periphery of the disk to reduce leakage past the valve. CIVs will be leak tested at a suitable frequency in accordance with the primary containment leakage rate test programme (Reference 23.5, Appendix I-2.2). The materials of the valve have been selected to minimise the risk of corrosion interfering with valve

operation. In-service testing (IST) will include the following (Reference 23.5, Appendix I-2.2):

- Movement of the valve through its full stroke every quarter to verify operation
- Demonstration of valve closure times and valve position sensor testing by cycling and monitoring valve position every 2 years
- Containment isolation leak testing

23.3.4.2 Containment Isolation Valves (VFS-PL-V800A, V800B, V803A, V803B)

CIVs VFS-PL-803A/B are of a check valve design such that no external power source is required to close the valve. This passive approach offers a high degree of inherent safety and high reliability.

CIVs 803A/B are Seismic C-I and are to be designed and constructed to the ASME Code, Section III-2 (Reference 23.4) design code. The code, with the testing and examination that supports it, provides the foundations for claims made on the CIVs.

The operating mechanism for the valve is simple, and aside from gross mechanical failure, the principal mechanisms for valve failure, are considered to be some form of adhesion preventing the valve from closing, or leakage of the valve under pressure when in the closed position. These failures are considered to be unlikely because of a combination of good design and a robust maintenance, inspection, and testing regime. The valve is a metal seated butterfly type with double seals around the periphery of the disk to reduce leakage past the valve. CIVs will be leak tested at a suitable frequency in accordance with the primary containment leakage rate test programme (Reference 23.5, Appendix I-2.2). The materials of the valve have been selected to minimise the risk of corrosion interfering with valve operation. IST) will include the following (Reference 23.5, Appendix I-2.2):

- Movement of the valve through its full stroke every refuelling outage to verify operation
- Containment isolation leak testing

CIVs VFS-PL-800A/B are of a motor operated butterfly valve design. The valves are powered by the Class 1 electrical system. They are fail-as-is since both opening and closing is a safety function.

CIVs 800A/B are Seismic C-I and are to be designed and constructed to the ASME Code, Section III-2 (Reference 23.4). The code, with the testing and examination that supports it, provides the foundations for claims made on the CIVs.

The operating mechanism for the valve is simple, and aside from gross mechanical failure, the principal mechanisms for valve failure, are considered to be some form of adhesion preventing the valve from closing, or leakage of the valve under pressure when in the closed position. These failures are considered to be unlikely because of a combination of good design and a robust maintenance, inspection, and testing regime. The valve is a metal seated butterfly type with double seals around the periphery of the disk to reduce leakage past the valve. CIVs will be leak tested at a suitable frequency in accordance with the primary containment leakage rate test programme (Reference 23.5, Appendix I-2.2). The materials of the valve have been selected to minimise the risk of corrosion interfering with valve operation. IST will include the following (Reference 23.5, Appendix I-2.2):

- Movement of the valve through its full stroke every refuelling outage to verify operation
- Demonstration of valve closure times and valve position sensor testing by cycling and monitoring the valve position every 2 years
- Containment isolation leak testing

23.3.4.3 High-Efficiency Particulate Air Filter and Charcoal Adsorber

HEPA filters and charcoal adsorbers are passive components with a high degree of inherent safety. They will meet their claimed efficiency through being constructed, qualified, and tested in accordance with appropriate standards (detailed in Section 23.3.2). There is a large amount of experience with using HEPA filters and charcoal adsorbers designed to these codes in operating nuclear power stations around the world, which gives confidence in their ability to meet their safety function.

A pressure differential sensor is installed across the HEPA filter to measure the pressure drop across it as an indication of its performance. Upon detection of a high-pressure drop across the HEPA filter, an indicator and alarm are activated.

A particle penetration of the HEPA filter unit (including through any bypass routes) that is greater than the design limit will be detected by the radiation sensor downstream of the filter bank. This would enable operator action to take place, such as shutting down the exhaust filtration system or switching to the alternative exhaust filtration unit, if it is not in operation.

The claimed efficiency of the HEPA filters and charcoal adsorbers will be demonstrated in situ upon installation of a new filter/adsorber and through periodic testing in accordance with ASME N510 throughout the plant life (Reference 23.17, Table 1).

23.3.4.4 Exhaust Fans

Primary containment of radioactive substances is provided by the building structure, and the VFS provides a defence in depth function. The fan design includes backward-inclined blades to produce nonoverloading characteristics. This will prevent overpressurisation of the ventilation distribution system if a damper in the system closes. This is an inherently safe design feature and provides a high degree of confidence in maintaining the integrity of the ventilation system.

The exhaust fans are to be designed and constructed to normal industrial standards that are suitable for Class 3 equipment.

Redundant fans are provided in the design to further reduce the risk of a total failure of the VFS extract from the fuel handling area and annex/auxiliary building areas.

Conceivable failure modes for this type of fan include, for example, a failed bearing, failed drive belt, etc. These types of mechanical failures are avoidable with appropriate maintenance and can be readily detected and rectified.

Maintenance will be carried out in line with the manufacturer’s information. There is extensive experience of operating this type of fan, designed and constructed to similar standards, to give confidence that if they are adequately maintained they will have a good reliability in service and be able to meet their safety functions.

23.3.4.5 Fire Dampers

The design of fire damper used in the VFS does not require any external power source or actuation signals. Actuation is achieved by heat from the air in the duct melting the fusible link and a spring mechanism closing the damper. Additionally some VFS fire dampers are provided with position indication. This provides a high degree of inherent safety and high reliability. The fire load in the served areas will be kept to a minimum to reduce the risk and potential size of a fire. This also contributes to the inherent safety of the system.

The highest classification of fire dampers is Class 3. The dampers are to be designed and manufactured to normal industrial standards that are suitable for Class 3 equipment.

Any failure that causes the fire damper to close is a failure to safety because the fire barrier will be maintained. The only conceivable failure to an unsafe position is if the damper was to seize or jam in the open position.

Maintenance will be carried out in line with the manufacturer's information. There is extensive experience of operating this type of damper to give confidence that if they are adequately maintained, they will not seize or jam and will move to the closed position when the temperature rises above the specified point.

23.4 CONTAINMENT RECIRCULATION COOLING SYSTEM

23.4.1 Role

The primary safety function of the VCS is heat transfer/residual heat removal. The safety function of the system is to support the containment structure and equipment by maintaining the containment thermal environment within appropriate limits for normal operation (below 49°C (120°F)) and during refuelling and shutdown (10° to 21°C (50° to 70°F)). The VCS also makes a contribution to the containment primary safety function with the provision of a steam generator (SG) maintenance space ventilation subsystem. This is for use during shutdown designed to protect maintenance personnel and control the spread of airborne contamination from the SG compartments to the other containment areas. Further design details of this system and its constituent components are delineated in Reference 23.3. This system is also discussed in Chapter 6.

The VCS makes provision for four 50-percent-capacity skid-mounted fan coil unit (FCU) assemblies to a common supply duct ring header and distribution system. The SG maintenance space ventilation subsystem consists of permanently installed exhaust ductwork with flexible hose connectors in the vicinity of the SG channel heads. The other end of the ductwork can be connected to a portable exhaust air filtration unit. During operation of the subsystem, flexible hosing can be used to exhaust localised contaminated air from the SG.

Cooling water is supplied to the FCUs by the central chilled water system (VWS). During cold weather conditions, while the plant is in an outage, the Hot Water Heating System (VYS) can be manually aligned to supply hot water to the VCS for containment heating purposes to keep piping and components from freezing as well as for personnel comfort. Control of the VCS is provided by the PLS with flow and temperature sensors. The FCUs are powered from the main ac power system (ECS) with redundant supply coming from the onsite standby power system (ZOS).

The VCS supports the VFS by helping to mix and distribute the VFS supply air within the containment. The VCS includes three containment atmosphere temperature sensors that provide input to the DAS for actuation of the PCS.

23.4.2 System Components and Equipment Contributing to Safety Function

Ductwork, accessories, and duct supports are constructed of galvanised steel and are structurally designed to accommodate fan shutoff pressures. The ductwork meets the design, testing, and construction requirements of SMACNA HVAC Duct Construction Standards – Metal and Flexible (Reference 23.15). Ductwork and connectors are the only components in the SG space ventilation subsystem that contribute to the containment primary safety function. The standards described above are adequate to ensure that the subsystem will deliver its safety function, and no further analysis is required.

The following components provide key contributions to the ability of the VCS to perform its safety functions.

- **Fan coil units** – Each FCU has a return air mixing plenum for each assembly and cooling coils for each FCU. The cooling coils are counterflow finned tubular type. The cooling coils are rated and meet the performance requirements in accordance with ANSI/Air Conditioning and Refrigeration Institute (ARI) 410 (Reference 23.22) for forced-circulation air cooling and air heating coils and the American Society of Heating, Refrigerating and Air Conditioning Engineers (ASHRAE) 33 (Reference 23.23) for the testing methods for rating of forced circulation air cooling and air heating coils. Each FCU includes a recirculation fan. The fans are a vane axial upblast type, direct driven with high-efficiency wheel, adjustable blades, and an inlet bell. The fans are designed with a nonoverloading, two-speed motor. The fans are designed, factory-tested and rated for performance in accordance with ANSI/AMCA Standards 210 (Reference 23.9), 211 (Reference 23.10), and 300 (Reference 23.11).

  The initiating signal for each FCU is from the PLS. The FCUs are required to operate to maintain the temperature in the containment within preset limits, and correct operation is therefore a safety function.

23.4.3 Claims on Components and Equipment

The VCS recirculation FCU assemblies and ductwork are classified as Seismic C-II such that it cannot adversely affect operation of Class 1 equipment inside containment. See Chapter 5 and Appendix 15A.

23.4.3.1 Fan Coil Units

The FCUs provide an alternative containment heat removal path for heat released to containment by the primary equipment. This is a Category B safety function. The FCUs provide an alternative role as the primary system for containment cooling is the PCS. As such, the FCUs are Category B Class 3 equipment. See Appendix 15A.

Two FCUs are required to start and operate to remove nuclear heat from the containment atmosphere during normal operation.

23.4.4 Justification of Claims on Components and Equipment

23.4.4.1 Fan Coil Units

The FCUs are standard components designed and manufactured to normal industrial codes that are appropriate for Class 3 equipment.

Redundant FCUs are provided in the VCS (4x50 percent).

FCU assemblies. They are connected to the ECS with backup supply from the ZOS. This redundancy provides further confidence that the FCUs will be able to meet the required reliability.

The Technical Specification (Tech Spec) surveillance requirement associated with the VCS is SR 3.6.5.1, which requires verification every 24 hours that the containment average air temperature is within limits (Reference 23.46). Specific maintenance requirements for the FCUs will be taken from the component manufacturer's information. There is extensive experience of operating this type of FCU to give confidence that if they are adequately maintained, they will have a good reliability in service.

23.5 CONTAINMENT LEAK RATE TEST SYSTEM

23.5.1 Role

The reactor containment, containment penetrations, and isolation barriers are designed to permit periodic leak rate testing. The VUS is designed to verify that leakage from the containment remains within limits established in the Tech Specs. Containment isolation is discussed further in Chapter 17.

The VUS verifies that containment isolation components are capable of performing their safety functions. It does not in itself perform a safety function. Any faults associated with the VUS will not result in the loss of function of other equipment. Therefore, substantiation of the system is not required.

Further design details of this system and its constituent components are delineated in Reference 23.19. This system is also discussed in Chapter 6.

23.5.2 System Components and Equipment Contributing to Safety Function

- **Manual CIV (V015, V016, Personnel Hatch Test Connections, V023 Electrical Penetration Test Isolation Valves Spare Penetration Test Connection) –** The ILRT test connection valves are manual globe valves. These valves are ASME III seismic C-I.

23.5.3 Claims on Components and Equipment

- **Manual CIV (V015, V016, Personnel Hatch Test Connections, V023 Electrical Penetration Test Isolation Valves Spare Penetration Test Connection) –** The ILRT test connection valves are manual globe valves. These valves are Category A Class 1 because they form part of the containment boundary.

23.5.4 Justification of Claims on Components and Equipment

Not applicable.

23.6 CONTAINMENT HYDROGEN CONTROL SYSTEM

23.6.1 Role

The VLS supports the containment primary safety function. Detonation of hydrogen is a hazard that could challenge containment integrity. The VLS acts to limit the hydrogen concentration in the containment so that containment integrity is not endangered.

The system consists of the following three subsystems:

- Hydrogen concentration monitoring
- Hydrogen recombination
- Hydrogen ignition

The hydrogen concentration monitoring subsystem consists of three hydrogen monitors to inform personnel of hydrogen levels in the containment building. The hydrogen recombination subsystem makes provision for two passive autocatalytic recombiners (PARs) inside the containment building to accommodate hydrogen released following a LOCA. The hydrogen ignition subsystem makes provision for 66 hydrogen igniters to accommodate the potential for release of large quantities of hydrogen during and following a degraded core or core melt scenarios.

The hydrogen ignition elements are supported by the ECS, ZOS, and Class 2 dc and uninterruptible power supply system (EDS) for electrical supplies.

The VLS supports the containment system by preventing the build-up of a hazard.

Further design details of this system and its constituent components are delineated in Reference 23.24. This system is also discussed in Chapter 6.

23.6.2 System Components and Equipment Contributing to Safety Function

There are construction and layout features to enhance the atmospheric natural circulation within containment and prevent the buildup of hydrogen pockets. All compartments below deck include openings through the top of the compartments to prevent dead-pockets of high hydrogen concentration.

The following components provide key contributions to the ability of the VLS to perform its safety function.

- **PARs** – The PARs consist of a stainless steel enclosure containing the catalyst material. There is space between the catalyst material to permit through flow of air and a chimney to the top of the enclosure to enhance the efficiency and ventilation of the device. The PARs are passive devices with no moving parts and no requirement for electrical supply or other support systems. The PARs are effective over a wide range of temperatures and hydrogen levels. The safety function of the PARs is to prevent the buildup of hydrogen within the containment building.

- **Hydrogen igniters** – The hydrogen igniters are of the heated coil type that is designed to maintain a minimum surface temperature of 927°C (1700°F) in the anticipated containment environment following a severe accident. The igniters burn hydrogen in the vicinity once the gas concentration reaches flammability conditions. The igniters are normally de-energised and are energised manually from the main control room (MCR)

when required via the PLS or DAS. The safety function of the hydrogen igniters is to burn off hydrogen in a controlled fashion if the containment hydrogen concentration exceeds flammability limits.

23.6.3 Claims on Components and Equipment

23.6.3.1 Passive Autocatalytic Recombiners

The PARs prevent the build-up of a hazard that could compromise the integrity of the containment for design basis accidents. Functions provided to reach and maintain safe state for design basis are Category B safety functions. The PARs provide a defence in depth function to protect containment against the build-up of hydrogen following a LOCA. Therefore, the PARs are Category B Class 3 equipment. See Appendix 15A.

Two PARs are provided in the VLS, and it is claimed that at least one will operate to prevent the build-up of hydrogen in the containment, as identified in the VLS system specification document (Reference 23.24, Section 3.1.2).

23.6.3.2 Hydrogen Igniters

The igniters prevent the build-up of a hazard that could compromise the integrity of the containment for severe accidents (see Section 10). Functions provided to reach and maintain safe state for beyond design basis are Category B safety functions. The igniters provide protection against a build-up of hydrogen following a degraded core or core melt accident (severe accident scenario) and therefore are Class 2 equipment. See Appendix 15A.

A total of 66 hydrogen igniters are provided in the VLS, and it is claimed that only 33 are needed to be operable to prevent the buildup of hydrogen in the containment (Chapter 10).

23.6.4 Justification of Claims on Components and Equipment

23.6.4.1 Passive Autocatalytic Recombiners

The PARs are passive components with no moving parts and no requirement for electrical power or other support systems. As such, they offer a high degree of inherent safety and high reliability.

The PARs are designed and constructed to the manufacturer’s standards in line with good engineering practice. This is suitable for Class 3 equipment.

The PARs are very similar to those already in service to provide the same function on many operating power stations. As a result, the information from testing these in-service recombiners offers a high degree of confidence about the reliability to be expected from the components proposed for the AP1000 design.

Redundant PARs are provided in the VLS. Since the PARs are passive devices with no moving parts or power supplies, there are no active failures associated with them. One possible failure mechanism is blockage of the airflow route through the device; however, the location of the PARs is such that the units are not susceptible to debris blockage.

There are Operating Rules associated with the PARs. Periodic inspection and testing of a sample of the catalytic material will be carried out to provide further confidence in the reliability of the PARs and their ability to perform their safety function.

23.6.4.2 Hydrogen Igniters

The hydrogen igniters are designed and constructed to the manufacturer's standards in line with good engineering practice. There are no nuclear-specific standards available for the design of hydrogen igniters, which is what would usually be expected for Class 2 equipment. Therefore, these are the most suitable standards to use.

The igniters are very similar to those already in service to provide the same function on many operating power stations. As a result, the information from testing these in service igniters offers a high degree of confidence about the reliability to be expected from the components proposed for the AP1000 design.

A total of 66 hydrogen igniters are provided in the VLS, and these are divided into two groups. Each group is normally powered by offsite power, with standby power supplied by a separate nonessential diesel generator. If the diesels fail, igniter operation is supported by Class 2 batteries. These three power supply sources provide the confidence that the VLS is able to maintain operation of at least 33 hydrogen igniters to meet the claim. The grouping of the igniters has been defined so that each containment compartment and hydrogen pathway has igniter coverage provided by at least one igniter in each group.

The hydrogen igniters provide the primary protection against the build-up of hydrogen in the containment following degraded core or core melt scenarios (severe accident). A hazardous concentration of hydrogen will not develop immediately, and in the unlikely event that the three electrical supplies available to the igniters fail, there would be time available to reinstate them. For this reason, it is appropriate for the hydrogen igniters not to be supplied by the essential electrical system.

The igniters are actuated manually, by MCR personnel, on receiving an elevated core exit temperature in excess of 649°C (1200°F). This will occur well in advance of the hydrogen concentration reaching the flammability limit (Reference 23.24, Section 3.1.3) and provides further assurance that a dangerous containment atmosphere will not develop.

Periodic inspection and testing is to be performed to confirm the continued operability of the hydrogen ignition system. Operability testing consists of energising the igniters and confirming the surface temperature exceeds 927°C (1700°F).

23.7 MAIN CONTROL ROOM EMERGENCY HABITABILITY SYSTEM

23.7.1 Role

The safety function of the VES is to maintain the MCR environment such that it is suitable for prolonged occupancy throughout the duration of a postulated accident involving the release of radioactivity. A maximum of 11 people can be accommodated for up to 72 hours. This is achieved by providing ventilation, pressurisation, filtration, and cooling to the MCR.

In the unlikely event that the VBS is still unavailable after 72 hours, there are provisions for supplying the required cooling of the MCR by operating one of the two VBS MCR ancillary fans to supply outside air to the MCR. A Class 1 connection provides means to supply air to VES for continued operation.

The VES supplies air to the MCR from four banks of compressed air storage tanks (32 tanks in total) using the stored energy of the compressed air. This provides fresh breathing air and maintains the positive pressure in the MCR envelope. The flow of compressed air passes

through an eductor, which induces a recirculating flow of the MCR air through HEPA filtration and charcoal adsorption. The pressure and flow rate of compressed air is controlled by pressure-regulating valves and flow metering orifices located in the main and eductor-bypass supply lines. Air delivery main isolation valves are remotely operated valves arranged in parallel and located in the main supply line inside the MCR envelope. A manual isolation valve is provided within the MCR to open the alternate supply line.

The VES operates upon detection of high particulate or iodine radioactivity in the MCR supply air duct of the VBS or upon loss of ac power for more than 10 minutes. The VBS also supports the VES by providing isolation of the MCR from the surrounding areas and outside environment.

The PMS provides control of specific VES components following certain accidents and abnormal events. The CAS is used to refill the air storage tanks when required, and the VAS maintains the VES air storage/operating deck staging area within temperature limits.

Further design details of this system and its constituent components are delineated in Reference 23.27. This system is also discussed in Chapter 6.

23.7.2 System Components and Equipment Contributing to Safety Function

The following components provide key contributions to the ability of the VES to perform its safety function.

- **Emergency air storage tanks** – There are a total of 32 air storage tanks. The air storage tanks are constructed of forged, seamless pipe, with no welds, and conform to the ASME Boiler and Pressure Vessel Code, Section VIII (Reference 23.25) and Appendix 22 (Reference 23.26). The design pressure of the air storage tanks is 28 MPa (4000 psi). The storage tanks collectively contain a minimum storage capacity of 9,276 m^3 (327,574 scf). The tanks are Seismic C-I. See Appendix 15A.

  The air storage tanks are required to maintain and deliver a store of breathing air to the MCR. The air storage tanks are simple pressure vessels, and their structural integrity is a Category A safety function and are thus Category A Class 1 equipment.

- **Pressure-regulating valves (VES-PL-V002A/B)** – These are 25-mm DN (1-inch) normally open, pressure-reducing, process-controlled globe valves designed to ASME Code III-3 (Reference 23.4) as detailed in the VES system specification document (Reference 23.27, Section 5.2.2, Appendix B-4.2). Each self-contained pressure-regulating valve is located downstream of the common header for the associated compressed air tanks.

  The valves maintain a constant pressure in their outlet line upstream of the eductor or the eductor bypass flow orifice in order to ensure a constant airflow rate to the MCR.

  The valve operates by its internal mechanism, and no external actuation or control signal is required. Correct operation of the pressure-regulating valves is a Category A safety function and are thus Category A Class 1 equipment.

- **Eductor bypass flow orifice (VES-PY-R02)** – An orifice designed to ASME Code, Section III-3 (References 23.4 and 23.27, Appendix F-1) is placed downstream of the pressure-regulating valves to control the airflow rate delivered to the MCR following a passive single failure in the passive air filtration line. No initiating signal is required. The combination of pressure-regulating valve and flow control orifice provides a

constant air addition flow rate regardless of the air pressure in the tanks (Reference 23.27). Correct flow control is a Category A function and thus the component is Category A Class 1 equipment.

- **Air delivery main isolation valves (VES-PL-V005A/B)** – These 25 mm DN (1 inch), normally closed, fail-open, solenoid-operated globe valves are designed to ASME III-3 (Reference 23.4) and have a soft elastomeric seat material to have a low leak rate (Reference 23.27, Appendix B-4.2). These valves are equipped with manual isolation capability to allow manual valve stem closure operation in the event of solenoid operator malfunction.

  The valves are located downstream of the pressure-regulating valve and orifice in the main supply line and are actuated by signals from the PMS or PLS. The valves are designed to Class 1 as they are the principal means to isolate the compressed emergency air supply lines from the MCR when the VES is not in operation and to permit airflow to the MCR when the VES is activated which is a Category A safety function.

- **Main airflow path isolation valve (VES-PL-V044)** – This is a 25-mm DN (1-inch), normally open, manual globe valve designed to ASME Code, Section III-3 (References 23.4 and 23.27, Appendix F-2). The valve is located within the MCR pressure boundary, downstream of the remotely operated air delivery main isolation valves.

  The actuation of the valve isolates the main air supply path and preserves the air storage tanks' contents if the pressure regulator in the main path malfunctions. This valve is Category A Class 1 equipment.

  As it is a manual valve no actuation signal is required. The main air flow path isolation valve is required to be able to be manually closed to isolate the main air supply line in the event of failure of the pressure-regulating valve. As this is a simple manual globe valve that is to be designed to an appropriate code (ASME Code, Section III-3) no further analysis or justification is required.

- **Air delivery alternate isolation valve (VES-PL-V001)** – This is a 25-mm DN (1-inch), normally closed, manual globe valve designed to ASME Code, Section III-3 (References 23.4 and 23.27, Appendices B-4.1, F-2). The valve is located within the MCR and is required to manually activate the alternate delivery airflow path in the event the main delivery airflow path is inoperable.

  As it is a manual valve no actuation signal is required. The air delivery alternate isolation valve is required to have a low leak rate when closed to prevent depletion of the emergency air storage tanks and must also be able to be manually opened to activate the alternate air supply line in the event of failure of the main line pressure-regulating valve. As this is a simple manual globe valve that is to be designed to an appropriate code (ASME Code, Section III-3) no further analysis or justification is required. This valve Category A Class 1 equipment.

- **MCR Eductor/Air Amplifier** – The eductor is a passive component that has no electrical or C&I power requirements, contains no moving parts, and requires no maintenance such as adjusting set points or lubricating bearings. It directs the compressed air from the VES makeup line through a nozzle that contains a flow control orifice to generate a vacuum that draws air from the MCR through connected ductwork into the passive air filtration line. The eductor must generate a sufficient vacuum to draw

the appropriate flow into the passive air filtration system. This is a Category A safety function and thus these components are Category A Class 1 equipment.

- **HEPA filters** – HEPA filters are constructed, qualified, and tested in accordance with UL 586 (Reference 23.28) and ASME AG-1 (Reference 23.6, Section FC). Each HEPA filter cell is individually shop tested to verify an efficiency of at least 99.97 percent using a mono-disperse 0.3-micron aerosol in accordance with ASME AG-1 (Reference 23.6, Section TA). The HEPA filter is in the MCR passive filtration flow path and works to remove particulate from the air to reduce potential control room dose during VES operation. HEPA filters are passive components, and as such, no actuation signal is required. The HEPA filters is designed to Class 1 as it is the principal means of ensuring a particulate filtration efficiency of 99.97 percent or 0.3-micron particles which is a Category A safety function. The VES air filtration unit includes a shield plate underneath to provide radiation attenuation to minimize accident condition radiation emissions in the break room. The shield plate is a Class 1 component.

- **Charcoal adsorber** – The charcoal adsorber is designed, constructed, qualified, and tested in accordance with ASME AG-1 (Reference 23.6, Section FD) and Regulatory Guide 1.52 (Reference 23.29). Each charcoal adsorber is an assembly with 51 mm (2 inch) deep Type II adsorber cells. Reference 23.29 indicates that a charcoal adsorber of this type should have a decontamination efficiency of 99 percent using the appropriate test methodology.

  The charcoal adsorber in the MCR passive filtration flow path works to remove iodine from the air to reduce potential control room dose during VES operation. The charcoal adsorber is a passive component; therefore, no actuation signal is required. The charcoal adsorber is designed to Class 1 as it is the principal means of ensuring a decontamination efficiency of 99 percent is a Category A safety function.

- **Passive Filtration Ducting and Components** – The components that make up the passive filtration ducting and components (dampers, registers, silencers) that provide flow through the HEPA filters and charcoal adsorber are designed in accordance with ASME N509 or ASME N509/N510 as delineated in Appendix 15A.

- **Manual and Tank Pressure Relief Valves** – The various manual valves and tank pressure relief valves are designed in accordance with ASME III. These valves allow for isolation of portions of the system for operation and maintenance. The pressure relief precludes over pressure of the system.

23.7.3 Claims on Components and Equipment

All the components and equipment in the VES act to maintain the habitability of the MCR. This is identified as a Category A safety function. See Appendix 15A.

23.7.3.1 Emergency Air Storage Tanks

The emergency air storage tanks provide the principal means of fulfilling the safety function of the system and therefore are Category A Class 1 equipment. See Appendix 15A.

It is claimed that the air storage tanks will contain a sufficient quantity of air to accommodate up to 11 people for 72 hours in the MCR and that this air can be delivered to the MCR.

23.7.3.2 Pressure-Regulating Valves (VES-PL-V002A/B)

The pressure-regulating valves in the air supply lines provide the principal means of fulfilling the safety function of the system and therefore are Category A Class 1 equipment. See Appendix 15A. It is claimed that the pressure-regulating valves will modulate appropriately to maintain a constant air pressure downstream of the valve. This will ensure that the correct airflow is provided to the MCR.

23.7.3.3 Eductor Bypass Flow Control Orifice (VES-PY-R02)

The eductor bypass flow control orifice, located in the alternate air supply, provides the principal means of fulfilling the safety function of the system and therefore is Category A Class 1 equipment. See Appendix 15A.

It is claimed that the flow control orifice will control the flow rate of air supplied to the MCR to the design flow. The orifice works together with the pressure-regulating valve to preserve the air storage tanks' contents such that they will be able to support the MCR for 72 hours at the design flow rate.

23.7.3.4 Air Delivery Main Isolation Valves (VES-PL-V005A/B)

The air delivery main isolation valves provide the principal means of fulfilling the safety function of the system and therefore are Category A Class 1 equipment. See Appendix 15A.

Two isolation valves are provided in parallel in the main air supply line, and it is claimed that at least one of these valves will open upon receipt of a signal to operate the VES. There is also an implied claim that the valves will have a low leak rate when closed to prevent depletion of the emergency air storage tanks.

23.7.3.5 MCR Eductor/Air Amplifier

The eductor provides the principal means of controlling the flow rate with an internal flow control orifice and inducing a flow through the passive air filtration line in the VES and therefore is Category A Class 1 equipment. See Appendix 15A.

It is claimed that the eductor will induce a vacuum sufficient to draw the designed flow rate of air from the MCR through the passive air filtration line.

23.7.3.6 High-Efficiency Particulate Air Filters

The HEPA filters provide the principal means of removing particulate from the MCR atmosphere and therefore are Category A Class 1 equipment.

It is claimed that the HEPA filters will have an efficiency of not less than 99.97 percent using a mono-disperse 0.3-micron aerosol (the most penetrating particle size).

23.7.3.7 Charcoal Adsorber

The charcoal adsorber provides the principal means of removing radioactive iodine from the MCR atmosphere and therefore is Category A Class 1 equipment.

It is claimed that the charcoal adsorber will have a decontamination efficiency of not less than 99 percent.

23.7.3.8 Passive Filtration Ducting and Components

The components that make up the passive filtration ducting and components (dampers, registers, silencers) that provide flow through the HEPA filters and charcoal adsorber maintain the habitability of the MCR and are thus Category A Class 1 Components.

23.7.3.9 Manual and Tank Pressure Relief Valves

The various manual valves and tank pressure relief valves maintain MCR habitability in the event of an accident and are thus Category A Class 1.

23.7.4 Justification of Claims on Components and Equipment

23.7.4.1 Emergency Air Storage Tanks

The emergency air storage tanks are simple components and have a high degree of inherent safety. The tanks are Class 1 equipment and have been designed to an appropriate ASME standard for pressure vessels (Reference 23.25). Class 1 equipment is normally constructed to nuclear-specific standards; initially, it may be thought that ASME Code, Section III would be a more appropriate standard to use for the emergency air storage tanks, but there is a vast amount of experience to support the reliability of air cylinders designed to ASME Code, Section VIII. This allows the evidence for the emergency air storage tanks to be based on the service experience of other air tanks in operation. As such, it is not considered that construction to ASME Code, III would ensure that the risk of failure was ALARP.

There are 32 tanks arranged in four banks. The emergency air storage tanks have been sized to ensure the volume of air stored is sufficient and the capacity is to be verified during preoperational testing.

Surveillance Requirement SR 3.7.6.2 requires verification that the compressed air storage tanks contain more than 9276 m^3 (327,574 scf) of compressed air every 24 hours. This ensures the air storage tanks will contain sufficient air to support 11 people in the MCR for 72 hours.

23.7.4.2 Pressure-Regulating Valves (VES-PL-V002A/B)

The pressure-regulating valves rely on their internal mechanisms and not on any external powered actuation to perform their function, providing a high degree of inherent safety. Pressure-regulating valves are common components in pressurised gas systems and as such a lot of knowledge exists about their design and operation. The valves have been designed to the ASME Code, Section III-3 design code (Reference 23.4), which has been specifically developed to qualify components suitable for nuclear power stations. The code, with the testing and examination that support it, provides the foundations for claims made on the pressure-regulating valves.

Pressure-regulating valves are present in the main and alternative supply lines, thus providing redundancy if one valve fails. Also, the valves have two stages that reduce the chance of a total valve failure. The pressure-regulating valves could either fail open or fail closed. If the main pressure-regulating valve fails open, airflow greater than the design value would result. Air supplies would not last for the required 72 hours, but the main supply line could be manually isolated and the alternative line manually activated. If the main pressure-regulating valve fails closed, the alternative line could be manually activated and the minimum flow rate would be met.

Surveillance Requirement (SR) 3.7.6.9 requires periodic verification that the self-contained pressure-regulating valve in each VES delivery airflow path is operable in accordance with the IST programme.

23.7.4.3 Eductor Bypass Flow Control Orifice (VES-PY-R02)

The flow control orifice is a simple component with no moving parts and is inherently safe. The orifice has been designed to the ASME Code, Section III-3 design code (Reference 23.4), which has been specifically developed to qualify components suitable for nuclear power stations. The code, with the testing and examination that support it, provides the foundations for claims made on the flow control orifice.

It is expected that the VES will operate very infrequently, and as such, wear should not be a significant failure mechanism. Preoperational testing will verify that the design flow rate of 110.4 ±8.5 m^3/hr (65 ±5 scfm) is achieved.

There is extensive experience of operating flow metering orifices, designed and constructed to similar standards, to give confidence that they will have a good reliability in service.

23.7.4.4 Air Delivery Main Isolation Valves (VES-PL-V005A/B)

The air delivery main isolation valves have been designed and manufactured to the ASME Code, Section III-3 design code (Reference 23.4), which has been specifically developed to qualify components suitable for nuclear power stations. The code, with the testing and examination that support it, provides the foundations for claims made on the air delivery main isolation valves.

The isolation valves are normally closed but designed to fail open. Redundant air delivery main isolation valves are provided in parallel on the main supply line and are sized such that one valve is allowed to fail closed and the other will still allow the required flow rate to pass. If both isolation valves fail closed, the alternative supply line provides a redundant route for supplying air to the MCR.

Surveillance requirement SR 3.7.6.3 requires periodic verification that each VES air delivery isolation valve is operable in accordance with the IST programme. There is extensive experience of operating this type of valve, designed and constructed to similar standards, to give confidence that if they are adequately maintained they will have a good reliability in service.

23.7.4.5 MCR Eductor/Air Amplifier

The eductor is a passive component with no moving parts, no electrical power requirements and no requirement for maintenance such as adjusting set points or lubricating bearings. Its function relies solely on the design of the eductor and an adequate flow of compressed air. This approach offers a high degree of inherent safety and high reliability.

As this is a passive component that will be called on very infrequently over the life of the AP1000 Plant, there is no credible mechanism for failure. Additionally, there is extensive experience on operating eductors designed and constructed to similar standards. This gives confidence that it will have good reliability in service. Preoperational testing will verify that the eductor is capable of inducing the design flow rate into the passive air filtration line.

23.7.4.6 High-Efficiency Particulate Air Filters and Charcoal Adsorbers

HEPA filters and charcoal adsorbers are passive components. They will meet their claimed efficiency through being constructed, qualified, and tested in accordance with appropriate standards (detailed in Section 23.7.2). There is a large amount of experience in using HEPA filters and charcoal adsorbers designed to these codes in operating nuclear power stations around the world, which gives confidence in their ability to meet their safety function.

HEPA filter damage could occur during installation. However, in situ penetration testing is to be carried out after every filter change to demonstrate that the filter is achieving the correct efficiency.

The claimed efficiencies will be demonstrated through periodic testing under the ventilation filter testing programme.

23.8 RADIOLOGICALLY CONTROLLED AREA VENTILATION SYSTEM

23.8.1 Role

The primary safety functions of the VAS are the containment of radioactive substances and the provision of support to other safety systems.

The VAS consists of the following two subsystems:

- Auxiliary/annex building ventilation
- Fuel handling area ventilation

Further design details of this system and its constituent components are delineated in Reference 23.30. This system is also discussed in Chapter 6.

23.8.1.1 Auxiliary/Annex Building Ventilation Subsystem

The safety function of the auxiliary/annex building ventilation subsystem is to control the spread of any potential contamination through maintaining appropriate negative pressures with respect to surrounding spaces, maintaining contamination levels below set limits, and monitoring the radiation in the extract air from the served areas. Upon detection of high radiation levels the VAS subsystem is isolated and the VFS is initiated to provide a charcoal and HEPA filtered extract route from the area.

HEPA filtration is provided for the spent fuel pool relief panel. In the unlikely case of spent fuel pool boiling, the HEPA filters ducted to the relief panel will remove particulates from the discharged air-steam mixture.

The served areas are split into two zones and each zone can be isolated independently of the other upon detection of high radiation. The subsystem also extracts from the radwaste effluent holdup tanks to prevent the potential build-up of airborne radioactivity or hydrogen gas.

An additional safety function of the auxiliary/annex building ventilation subsystem is to provide cooling to plant rooms that contain equipment contributing to the safety functions of other systems.

The auxiliary/annex building ventilation subsystem makes provision for two 50-percent-capacity supply AHUs, two 50-percent-capacity exhaust air fans and standalone unit coolers in the normal residual heat removal system (RNS) and chemical and volume control system (CVS) pump rooms. Isolation dampers provide isolation of the subsystem upon detection of high radiation.

The subsystem is supported by the PLS, VWS, and ZOS.

The auxiliary/annex building ventilation subsystem of the VAS supports the CVS through heat removal from the CVS makeup pump rooms, the RNS through heat removal from the RNS pump rooms, and the spent fuel pool cooling system (SFS) through heat removal from the SFS pump rooms. The subsystem maintains the VES air storage/operating deck staging area within design temperature limits during normal plant operation to ensure that the storage capacity of the VES pressurised air storage tanks is unaffected. The subsystem supports the RMS through the provision of radiation monitors in the extract ductwork and provides high radiation signals to the VFS filtered exhaust subsystem when high airborne radioactivity is detected in the VAS exhaust ducts or in the rooms served by the subsystem (using area monitors). The use of the exhaust radiation monitor and local area monitors to detect high levels of radiation ensures a rapid containment of the radiation (in less than 15 seconds).

23.8.1.2 Fuel Handling Area Ventilation Subsystem

The safety function of the fuel handling area ventilation subsystem is to control the spread of any potential contamination through maintaining appropriate depressions, diluting any contamination to maintain the concentration below set limits and monitoring the radiation in the extract air from the served areas. HEPA filtration is included in the VAS extract subsystem serving the fuel handling area. Upon detection of high radiation levels, the VAS subsystem is isolated and the VFS is initiated to provide a charcoal and HEPA filtered extract route from the area.

HEPA filtration is provided for the spent fuel pool relief panel. In the unlikely case of spent fuel pool boiling for a time sufficient to actuate the relief panel, the HEPA filters ducted to the relief panel will remove particulates from the discharged air stream.

The supply and exhaust ductwork is arranged to exhaust the spent fuel pool (SFP) area and to provide directional airflow from the rail car bay/filter storage area into the spent resin equipment rooms.

The fuel handling area ventilation subsystem makes provision for two 50-percent-capacity supply AHUs and two 50-percent-capacity exhaust air fans. Isolation dampers provide isolation of the subsystem upon detection of high radiation.

The subsystem's safety function is supported by the PLS and ZOS.

The subsystem supports the RMS through the provision of radiation monitors in the extract ductwork and provides high radiation signals to the VFS filtered exhaust subsystem when high airborne radioactivity is detected in the VAS exhaust ducts or in the rooms served by the subsystem (using area monitors). The use of the exhaust radiation monitor and local area monitors to detect high levels of radiation ensures a rapid containment of the radiation (in less than 15 seconds).

23.8.2 System Components and Equipment Contributing to Safety Function

Ductwork, duct supports, and accessories are constructed of galvanised steel. Ductwork subject to fan shutoff pressure is structurally designed for fan shutoff pressures. Ductwork, supports and accessories meet the design and construction requirements of SMACNA Rectangular and Round Industrial Duct Construction Standards (References 23.13 and 23.14) and SMACNA HVAC Duct Construction Standard – Metal and Flexible (Reference 23.15).

The following components make key contributions to the ability of the VAS to perform its safety function.

- **Passive Filtered Relief –** a passive damper is provided in the fuel handling building area to provide a path for steam during spent fuel pool boiling. The damper is constructed of stainless steel or suitable material and actuated by fusible links designed to melt and release the damper when the air temperature reaches 74°C (l65°F). HEPA filtration of the exhaust flow path is provided.

- **Supply and exhaust air fans and CVS and RNS pump room coolers** – The supply and exhaust air fans are centrifugal type, single-width single-inlet, or double-width double-inlet, with high-efficiency wheels and backward-inclined blades to produce nonoverloading characteristics. The fans are designed and rated in accordance with ANSI/AMCA Standards 210 (Reference 23.9), 211 (Reference 23.10), and 300 (Reference 23.11).

  The supply fans in the supply AHUs are required to operate to dilute any contamination maintaining the concentration below set limits, and to meet the cooling requirements of areas containing safety equipment not supplied with unit coolers, e.g., the SFS pump rooms and the VES air storage/operating deck staging area.

  The supply fans in the unit coolers are required to operate to meet the cooling requirements of areas containing safety equipment, i.e., the CVS makeup pump rooms and the RNS pump rooms.

  The exhaust fans are required to operate to control the spread of any potential contamination by maintaining appropriate depressions and to provide a constant airflow in the extract duct, which is monitored for radiation. They are also required to prevent the potential build-up of hydrogen gas in the radwaste effluent holdup tanks.

  The fans operate in response to signals from the PLS, which include flow rate, temperature, and shutoff damper positions.

  Detection of radiation in the exhaust ductwork will result in the exhaust fans being shut down and initiation of the VFS. Failure of the exhaust fans and an increase or decrease in differential pressure in the served areas will also isolate the VAS subsystem and initiate the VFS extract system. This is a safe condition; therefore, no further analysis is required for the exhaust fans (see Section 23.3 for justification of the VFS).

  The supply fans are designed to Class 3 as they are the principal means of generation of the required airflows which is a Category B safety function.

  The CVS and RNS Pump Room Coolers are designed to Class 3 as they are the principal means of maintaining the rooms within their design temperature range which is a Category C safety function.

- **Cooling coils** – The chilled water cooling coils are counterflow, finned tubular type. Each cooling coil is constructed with copper tubes and fins and a galvanised steel casing. Large cooling coil banks that are constructed from multiple cooling coils are provided with coil holding racks designed to allow each coil to be independently removed (side pull) from the housing. The cooling coils are designed and rated in accordance with ASHRAE 33 (Reference 23.23) and ANSI/ARI 410 (Reference 23.22). The cooling capacity of the coils includes a 15 percent margin. This 15-percent margin accounts for uncertainties in the calculated cooling loads, as detailed in the VAS system specification document (Reference 23.30, Section 5.1). Coils are designed to withstand a working pressure of 1.03 MPa (150 psig) at 93.3°C (200°F) and are leak tested with 2.07 MPa (300 psig) air under water (Reference 23.30, Section 5.1).

  The cooling coils in the auxiliary/annex building ventilation subsystem AHUs and unit coolers obtain a flow of cooling water through activation of the chilled water control valves in response to signals from the PLS. The cooling coils are designed to Class 3 as it is the principal means to permit the flow of cooling water through the copper tubes and maintain an adequate surface for heat transfer between the air and cooling water in order to meet air temperature control requirements for the Air Handling Units which is a Category B safety function.

- **Isolation dampers** – Isolation dampers are bubble-tight, single- or parallel-blade type. The isolation dampers have spring return actuators that fail closed on loss of electrical power or loss of air pressure. The isolation dampers are constructed, qualified, and tested in accordance with ANSI/AMCA Standard 500 (Reference 23.12).

  The isolation dampers are required to operate to prevent the unfiltered release of potentially contaminated air from the served areas to the environment.

  Actuation of the isolation dampers is via the PLS in response to signals such as high radiation, high/low pressure differential, or one of the VFS dampers opening. The isolation dampers are designed to Class 3 as it is the principal means of isolation of individual airflows which is a Category B safety function.

- **Fire dampers** – Fire dampers are provided at duct penetrations through fire barriers to maintain the fire resistance rating of the barriers. Additionally some VAS fire dampers are provided with position indication. The fire dampers are constructed of galvanised carbon steel and actuated by fusible links designed to melt and release the damper blade when the air temperature reaches 74°C (165°F) (Reference 23.30, Section 5). The damper blades close via a spring mechanism. The fire dampers meet the design, testing, and installation requirements of UL 555 (Reference 23.18).

  The fire dampers are passive components operated by temperature and an internal spring mechanism. As such, no actuation signal is required.

  The fire damper rating will be at least equal to the fire barrier that they penetrate, up to a maximum UL 555 3-hour rating. This is essential to maintain the integrity of fire barriers discussed in the internal fire hazard section of Chapter 11 and the dampers are Category B Class 3 equipment.

- **HEPA filters –** HEPA filtration is located on the VAS subsystem serving the fuel handling area to capture potential airborne particulates containing radioactivity. HEPA filters are constructed, qualified, and tested in accordance with ANSI N509.

23.8.3 Claims on Components and Equipment

23.8.3.1 Passive Filtration

Although not credited in the dose analysis, the passive filtration flow path is designed to remove particulate material from steam generated during spent fuel pool boiling.

23.8.3.2 Supply Air Fans and CVS and RNS pump room coolers

The supply fans make a minor contribution to the containment of radioactive substances through diluting the concentration of contamination in the air. The more significant function is providing cooling to equipment important to the safety functions of other systems. The RNS, CVS, and SFS pumps and the VES air storage area are all supported by the VAS supply air fans.

Failure of the fans supplying the VES air storage area could potentially lead to an increase in temperature of the air storage tanks and consequently a reduction in the mass of air stored within them. However, unlike the pump rooms, there is no significant heat load in this area, and the supply fans would have to be inoperable for a prolonged period of time to have an effect on the stored mass of air. This time period would be sufficient for operator intervention.

Failure of the supply fans will only be an issue after at least 8 hours of operation and until that time will be certain not to prevent the RNS, CVS, and SFS from providing their safety functions. Table 8A-4 identifies the need for HVAC to support these systems functionality. The RNS pumps provide a Category A safety function and are Class 2 equipment (see Chapter 17), the CVS pumps provide a Category A safety function and are Class 2 equipment and the SFS pumps provide a Category A safety function and are Class 2 equipment (see Chapter 17).

- RNS pump room unit cooler fans – Category C safety function, Class 3
- CVS pump room unit cooler fans – Category C safety function, Class 3
- Auxiliary/annex building ventilation subsystem supply AHU fans (which support the SFS pumps) – Category B safety function, and are thus Class 3 equipment

One supply fan is installed in each supply AHU of the auxiliary/annex building ventilation subsystem. The subsystem makes provision for 2- x 50-percent supply AHUs. Therefore, it is claimed that both fans will continue to operate to meet the VAS safety functions. However, as maintenance will be required on the system, the VAS is designed such that:

- The radiation chemistry laboratory and security rooms are provided with sufficient ventilation that design room temperatures can be maintained while one 50-percent-capacity supply air subsystem is shut down for maintenance.
- The system provides sufficient ventilation airflow to plant areas enclosing Class 1 qualified CIVs so that the ambient design temperatures can be maintained while one 50-percent-capacity supply air subsystem is shut down for maintenance.
- The auxiliary/annex building and fuel handling area will be ventilated with two, 50-percent-capacity supply and exhaust air subsystems so that a single train may be

taken out of service while the operating train maintains a negative pressure differential and ALARP airflow directions.

It is desirable to perform routine maintenance of the fuel handling area building isolation dampers and radiation monitors while there are no refuelling activities so that VAS isolation capability is available during fuel handling activities.

It is desirable to perform routine maintenance of the auxiliary building isolation dampers and radiation monitors while the plant is in cold shutdown so that VAS isolation capability is available during normal plant operation, when the probability for an abnormal release of airborne radioactivity is greatest.

Isolation dampers located at the inlet to the exhaust fans are designed to be closed to isolate the equipment from the process flow during maintenance activities. The damper blades will be repositioned to their normal open position when restoring equipment operation.

One supply fan is installed in each unit cooler in the RNS pump rooms, and one unit cooler is located in each of the two RNS pump rooms. It is claimed that each unit cooler will start on demand to meet the cooling requirements of the associated RNS pump.

One supply fan is installed in each of the two unit coolers in the CVS pump room. The CVS pump room contains two CVS pumps, and only one pump is required to operate at any time. Therefore, it is claimed that one unit cooler fan will start on demand to meet the cooling requirements of the CVS pump.

23.8.3.3 Cooling Coils

As with the fans, the cooling coils provide the primary means of cooling the areas that contain safety equipment. The cooling coils should have the same classification as their associated fans. Therefore, the following equipment categorisation and classifications apply to the cooling coils in the VAS:

- RNS pump room unit cooler chilled water cooling coils – Category C safety function, Class 3
- CVS pump room unit cooler chilled water cooling coils – Category C safety function, Class 3
- Auxiliary/annex building ventilation subsystem supply AHU chilled water cooling coils – Category B safety function, and are thus Class 3 equipment

Each RNS pump room unit cooler includes two chilled water cooling coil banks: one supplied from train A of the chilled water system and the other supplied from train B. Only one cooling coil bank on each unit cooler is required to operate to meet the 100 percent cooling demand of the RNS pump associated with each unit cooler. Both pumps and therefore both unit coolers may operate at the same time.

Each unit cooler in the CVS pump room makes provision for a single cooling coil bank. One cooling coil bank is supplied by train A of the chilled water system and the other bank is supplied by train B. One unit cooler can meet 100 percent of the cooling demand from a CVS pump. Only one CVS pump is in operation at any time; therefore, it is claimed that one CVS pump room unit cooler and cooling coil bank will operate on demand.

Each auxiliary/annex building ventilation subsystem supply AHU makes provision for a single chilled water cooling coil bank. The AHUs are 2- x 50-percent duty; therefore, it is claimed that both AHUs and both cooling coil banks will operate to meet the cooling demand.

23.8.3.4 Isolation Dampers

The VAS isolation dampers operate to prevent an unfiltered release of contamination when high levels of radiation are detected in the extract duct. Failure of the isolation dampers will not result in a design basis accident (DBA); therefore, this is a Category B safety function, and the dampers are Class 3 equipment. See Appendix 15A.

Single isolation dampers are provided in the duct branches where isolation is required. It is claimed that the isolation dampers will close on demand.

23.8.3.5 Fire Dampers

Fire dampers are installed where ductwork passes through fire barriers.

The fire dampers protect against fire hazards that could, as part of a sequence of failures, result in loss of a safety function. This could compromise normally operating systems and safety systems delivering a specific function. Therefore, this is a Category B safety function. As the fire dampers provide a contribution to achieving this safety function they are deemed to be Class 3 equipment. See Appendix 15A.

Single fire dampers are provided where the ducts pass through a fire barrier. It is claimed that the fire dampers will close when the air temperature in the duct reaches the design limit.

23.8.3.6 HEPA Filters

HEPA filtration is located on the VAS subsystem serving the fuel handling area to capture potential airborne particulates containing radioactivity and thus are Category B Class 3 equipment.

23.8.4 Justification of Claims on Components and Equipment

23.8.4.1 Passive Filtered Filtration

The design of damper used in the VAS does not require any external power source or actuation signals. Actuation is achieved by heat from the air melting the fusible link and a gravity opening the damper. This provides a high degree of inherent safety and high reliability.

The flow path components are designed and manufactured to standards that are suitable for Class I equipment, but some components are Class 2.

At least on redundant path is provided to prevent impact from the failure of a single path. Maintenance will be carried out in line with the manufacturer's information. There is extensive experience of operating similar dampers to give confidence that if they are adequately maintained they will not seize or jam and will move to the closed position when the temperature rises above the specified point.

23.8.4.2 Supply Air Fans

The fan design includes backward-inclined blades to produce nonoverloading characteristics. This will prevent overpressurisation of the ventilation distribution system if a damper in the system closes. This is an inherently safe design feature and provides a high degree of confidence in maintaining the integrity of the ventilation system.

The highest classification of supply air fan in the VAS is Class 3. The supply fans are to be designed and manufactured to normal industrial standards that are suitable for Class 3 equipment.

The fans are very similar to those already in service to provide the same function on many operating power stations. As a result, the information from testing these in service fans offers a high degree of confidence about the reliability to be expected from the fans proposed for the AP1000 design.

Conceivable failure modes for this type of fan include, for example, a failed bearing or failed drive belt. These types of mechanical failures are avoidable with appropriate maintenance and can be readily detected and rectified.

Maintenance will be carried out in line with the manufacturer's information. There is extensive experience of operating this type of fan, designed and constructed to similar standards, to give confidence that if they are adequately maintained they will have a good reliability in service.

23.8.4.3 Cooling Coils

The highest classification of cooling coil in the VAS is Class 3. The coils are to be designed and manufactured to normal industrial standards that are suitable for Class 3 equipment.

Redundant cooling coils are included in the RNS pump room unit coolers and these are supplied from diverse trains of the chilled water system. Redundant unit coolers are provided in the CVS pump room, and the cooling coil in each unit cooler is supplied from diverse trains of the chilled water system. This redundancy and diversity provides further confidence that the cooling coils will be able to deliver the reliability required to ensure the VAS meets its safety functions.

Possible failure mechanisms include the following:

- Failure of the chilled water control valves. If the control valves on the unit coolers fail and the supply temperature start to rise, sensors will activate the redundant coil or unit cooler. If the valves fail on the cooling coils in one of the AHUs, the other AHU will continue to provide cooling. Depending on ambient temperatures, this may be sufficient to maintain the area temperatures within the design limits. If it is not, then a temperature rise in the served areas would be detected and allow operator intervention.

- Failure of the complete chilled water system. If chilled water is lost to both AHUs of the auxiliary/annex building ventilation subsystem, the AHU may not be capable of maintaining design indoor temperatures, based on the outdoor temperature. Operator intervention may be required.

  Chilled water is supplied to the unit coolers in the RNS and CVS pump rooms from redundant VWS trains. As such, loss of a single train should ensure that one CVS pump and the RNS pumps can be supported.

- Structural failure of the coils. The use of suitable design standards and appropriate in service maintenance is deemed sufficient to reduce the risk of structural failure of the cooling coils.

In addition, the RNS pump motors could operate for at least 8 hours without room cooling . This would provide sufficient time for operator intervention following total failure of cooling in that area.

Maintenance will be carried out in line with the manufacturer's information. There is extensive experience of operating this type of cooling coil to give confidence that if they are adequately maintained they will have a good reliability in service.

23.8.4.4 Isolation Dampers

The isolation dampers are designed such that they fail safe. The spring return pneumatic design ensures that a loss of electrical power or pneumatic air will cause the dampers to close, isolating the ductwork and preventing any unfiltered release of air from the supplied areas. This provides a high degree of inherent safety. Spurious operation of the isolation damper in the supply duct serving the auxiliary building will prohibit the flow of cooling air to the SFS pump rooms. This will raise an alarm in the MCR and allow operator intervention to occur before the pump room temperature rises to a level that would prevent operation of the SFS pumps. The probability of spurious failure is considered to be sufficiently low based on the design and maintenance requirements of the damper. In addition, diverse cooling is available to the SFP via the RNS pumps, which are not affected by spurious operation of an isolation damper.

The dampers are to be designed and manufactured to normal industrial standards that are suitable for Class 3 equipment. The dampers are of a low leakage design to minimise the passing of any air when the dampers are shut. This in turn prevents leakage of contamination from the area when the VAS is isolated.

Maintenance will be carried out in line with the manufacturer's information. There is extensive experience of operating this type of damper to give confidence that if they are adequately maintained they will not seize or jam and will move to the closed position if demanded.

23.8.4.5 Fire Dampers

The design of fire damper used in the VAS does not require any external power source or actuation signals. Actuation is achieved by heat from the air in the duct melting the fusible link and a spring mechanism closing the damper. This provides a high degree of inherent safety and high reliability. The fire load in the areas served by VAS will be kept to a minimum to reduce the risk and potential size of a fire. This also contributes to the inherent safety of the system.

The dampers are to be designed and manufactured to normal industrial standards that are suitable for Class 3 equipment.

Any failure that causes the fire damper to close is a failure to safety because the fire barrier will be maintained. The only conceivable failure to an unsafe position is if the damper was to seize or jam in the open position.

Maintenance will be carried out in line with the manufacturer's information. There is extensive experience of operating this type of damper to give confidence that if they are

adequately maintained they will not seize or jam and will move to the closed position when the temperature rises above the specified point.

23.8.4.6 HEPA Filters

HEPA filters are passive components. They will meet their claimed efficiency through being constructed, qualified, and tested in accordance with appropriate standards. There is a large amount of experience in using HEPA filters designed to these codes in operating nuclear power stations around the world, which gives confidence in their ability to meet their safety functions. HEPA filter damage could occur during installation. However, in situ penetration testing is to be carried out after every filter change to demonstrate that the filter is achieving the correct efficiency.

The claimed efficiencies will be demonstrated through periodic testing under the ventilation filter testing programme.

23.9 RADWASTE BUILDING HEATING, VENTILATION, AND AIR CONDITIONING SYSTEM

23.9.1 Role

The VRS contributes to the containment primary safety function by controlling the spread of airborne contamination within the radwaste building and preventing the unmonitored release of potentially contaminated air. The VRS provides cooling to a number of processes in the radwaste building, but if the ventilation system is unavailable, the processes can be suspended. This does not impact on safe operation of the plant; therefore, cooling is not considered a safety function of the VRS.

The VRS is a once-through ventilation system that consists of two integrated subsystems: the radwaste building supply air system and the radwaste building exhaust air system.

The VRS makes provision for two 50-percent-capacity supply AHUs and two 50-percent-capacity exhaust fans. A radiation monitor is included in the exhaust duct to detect radioactivity. Exhaust connection points are provided to allow the direct exhaust of equipment located on the mobile systems. Mobile systems are where potential for significant airborne release exists; mobile systems include HEPA filtration. Backdraft dampers are provided at each mobile system connection to prevent blowback through the equipment in the event of exhaust system trip.

If a single component in either one of the supply AHUs or an exhaust fan is inoperable due to maintenance, failure, or repair, the VRS can operate with one supply AHU in conjunction with its associated exhaust fan, reducing the overall system capacity to 50 percent. In this mode of operation, airflow directions and building negative pressure still can be maintained. However, design indoor temperature may or may not be maintained within limits depending on the levels of radwaste process activities taking place and the outdoor conditions at the time.

The VRS operates continuously. It is recommended that filter replacement or other routine maintenance activities that require VRS components to be shut down be scheduled when radwaste activities are not required. Maintenance on unit heaters should be performed during warm weather. This will minimise temperature transients that will occur when VRS equipment is temporarily shut down for maintenance.

There is a low risk of airborne contamination being present within the radwaste building. HEPA filters are provided in the radwaste building exhaust system. Upon detection of radiation in the extract duct the operator in the MCR is alerted and can take appropriate action, such as sending maintenance personnel to investigate and shutting down the VRS.

Fire dampers are provided at duct penetrations through fire barriers to maintain the fire resistance ratings of the barriers.

The VRS is supported by the PLS for control functions and the FPS, which trips fans in the VRS on detection of fire in the served areas.

The VRS supports the RMS through the provision of radiation monitors in the exhaust ductwork and supports processes carried out by the gaseous and solid radwaste systems.

Further design details of this system and its constituent components are delineated in Reference 23.31. This system is also discussed in Chapter 6.

23.9.2 System Components and Equipment Contributing to Safety Function

Ductwork, duct supports, and accessories are constructed of galvanised steel. Ductwork subject to fan shutoff pressures is structurally designed to accommodate fan shutoff pressures. Ductwork, supports, and accessories meet the design and construction requirements of SMACNA Industrial Rectangular and Round Duct Construction Standards (References 23.13 and 23.14) and SMACNA HVAC Duct Construction Standards – Metal and Flexible (Reference 23.15).

Multi-blade, two-position remotely operated shutoff dampers are parallel-blade type. Multi-blade, control and balancing dampers are opposed-blade type. AHU and fan shutoff dampers are designed for maximum fan static pressure at shutoff flow. Dampers meet the performance requirements of ANSI/AMCA Standard 500 (Reference 23.12).

The following components make key contributions to the ability of the VRS to perform its safety function.

- **Radwaste building exhaust radiation package –** Provides radiation monitoring of all potentially contaminated exhaust air prior to release to the plant vent. This monitoring is a Category C Class 3 function.

- **Fire dampers** – Fire dampers are provided at duct penetrations through fire barriers to maintain the fire resistance rating of the barriers. The fire dampers are constructed of galvanised carbon steel and actuated by fusible links designed to melt and release the damper blades when the air temperature reaches 74°C (165°F), as detailed in the VRS system specification document (Reference 23.31, Section 5.2.1.3). The fire damper design has parallel blades and uses a spring mechanism to close. The fire dampers meet the design, testing, and installation requirements of UL555 (Reference 23.18).

- **HEPA filters** – HEPA filters are provided in the VRS extract. The filters provide protection to minimise particulate releases. The filters remove 99.97% of all particles 0.3 microns in diameter from the exhaust.

  A pressure differential sensor is installed across the HEPA filter to measure the pressure drop across it as an indication of its performance. Upon detection of a high pressure drop across the HEPA filter, an indicator and alarm are activated. They are designed per ANSI N509.

The fire damper rating will be at least equal to the fire barrier that they penetrate, up to a maximum UL 555 3-hour rating. Fire dampers are passive components operated by temperature and a spring mechanism. As such, no actuation signal is required. The fire dampers are essential to maintain the integrity of fire barriers discussed in the internal fire hazard section in Chapter 11. These fire dampers are Category B Class 3 equipment.

23.9.3 Claims on Components and Equipment

23.9.3.1 Fire Dampers

Fire dampers are installed where ductwork passes through fire barriers.

The fire dampers protect against fire hazards that could, as part of a sequence of failures, result in loss of a safety function. This could compromise normally operating systems and safety systems delivering a specific function. Therefore, this is a Category B safety function. See Appendix 15A. As the fire dampers assist in achieving this safety function, they are deemed to be Class 3 equipment. See Appendix 15A.

Single fire dampers are provided where the ducts pass through a fire barrier. It is claimed that the fire dampers will close when the air temperature in the duct reaches the design limit and maintain the integrity of the fire barrier.

23.9.3.2 High-Efficiency Particulate Air Filters

HEPA filters are passive components with a high degree of inherent safety. They will meet their claimed efficiency through being constructed, qualified and tested in accordance with appropriate standards (detailed in Section 23.3.2 above). There is a large amount of experience in using HEPA filters designed to these codes in operating nuclear power stations around the world, which gives confidence in their ability to meet their safety function.

A particle penetration of the HEPA filter unit (including through any bypass routes) that is greater than the design limit will be detected by the radiation sensor downstream of the filter bank. This would enable operator action to take place, such as shutting down the exhaust filtration system.

The claimed efficiency of the HEPA filters will be demonstrated in situ upon installation of a new filter and through periodic testing.

The HEPA filters in the VRS minimise the radiation released to the environment during operation. As such, the HEPA filters provide a Category B safety function. Failure of either the HEPA filters will result in the potential for a release of contamination and radioactivity to the environment. The HEPA filters provide a contribution to the VRS's primary safety function and are Class 3 equipment. See Appendix 15A.

23.9.4 Justification of Claims on Components and Equipment

23.9.4.1 High-Efficiency Particulate Air Filters

HEPA filters are passive components. They will meet their claimed efficiency through being constructed, qualified, and tested in accordance with appropriate standards (detailed in Section 23.7.2). There is a large amount of experience in using HEPA filters designed to these codes in operating nuclear power stations around the world, which gives confidence in their ability to meet their safety functions.

HEPA filter damage could occur during installation. However, in situ penetration testing is to be carried out after every filter change to demonstrate that the filter is achieving the correct efficiency.

The claimed efficiencies will be demonstrated through periodic testing under the ventilation filter testing programme.

23.9.4.2 Fire Dampers

The design of fire damper used in the VRS does not require any external power source or actuation signals. Actuation is achieved by heat from the air in the duct melting the fusible link and a spring mechanism closing the damper. This provides a high degree of inherent safety and high reliability. The fire load in the radwaste building will be kept to a minimum to reduce the risk and potential size of a fire. This also contributes to the inherent safety of the system.

The highest classification of fire dampers in the system is Class 3. The dampers are to be designed and manufactured to normal industrial standards that are suitable for Category B Class 3 equipment.

Any failure that causes the fire damper to close is a failure to safety because the fire barrier will be maintained. The only conceivable failure to an unsafe position is if the damper was to seize or jam in the open position.

Maintenance will be carried out in line with the manufacturer's information. There is extensive experience of operating this type of damper to give confidence that if they are adequately maintained they will not seize or jam and will move to the closed position when the temperature rises above the specified point.

23.10 HEALTH PHYSICS AND HOT MACHINE SHOP HEATING, VENTILATION, AND AIR CONDITIONING SYSTEM

23.10.1 Role

The safety function of the VHS in support of the containment of radioactive substances is to control the spread of airborne contamination within the served areas and provide for radiation monitoring of the exhaust air prior to discharge. The VHS is designed to operate continuously.

The areas served by the VHS are the annex building stairwell, personnel decontamination area, frisking and monitoring facilities, containment access corridor, health physics facility, and hot machine shop in the annex building.

The plant design makes provision for two 100-percent-supply AHUs and two 100-percent-centrifugal exhaust fans. An additional exhaust fan and HEPA filter provide extract from machine tools and other localised areas in the hot machine shop. Radiation monitoring is installed in the exhaust ductwork.

The VHS is capable of maintaining a negative pressure in the health physics/controlled access area and hot machine shop with one active component out of service for maintenance or repair.

There is a low risk of airborne contamination being present within the areas served by the VHS. Upon detection of high radiation levels the VHS subsystem is isolated, and the VFS is initiated to provide a charcoal and HEPA filtered extract route from the area. The use of the exhaust radiation monitor and local area monitors to detect high levels of radiation ensures a rapid containment of the radiation (in less than 15 seconds).

The airflow pattern is controlled to minimise the spread of airborne contamination. Signals from differential pressure sensors in the served rooms modulate control dampers in the supply system to maintain an appropriate depression. The differential pressure sensor in the health physics area modulates the inlet vane dampers of the supply fans and the sensor in the hot machine shop modulates the control damper in the supply line to that area (VHS-MD-D008).

Low flow signals from the PLS for either the supply or extract fan will trip both the operating supply and extract fans. In addition, control signals from the PLS will close the outside air inlet damper of the operating AHU, the supply isolation damper and the extract isolation damper.

The VHS supports the RMS through the provision of the radiation monitor in the exhaust ductwork and is supported by the PLS through the control of the differential pressure in the served areas and the fan and damper controls.

Further design details of this system and its constituent components are delineated in Reference 23.45. This system is also discussed in Chapter 6.

23.10.2 System Components and Equipment Contributing to Safety Function

Ductwork, duct supports, and accessories are constructed of galvanised steel. Ductwork subject to fan shutoff pressure is structurally designed for fan shutoff pressures. Ductwork, supports, and accessories meet the design and construction requirements of SMACNA Rectangular and Round Industrial Duct Construction Standards (References 23.13 and 23.14) and SMACNA HVAC Duct Construction Standards – Metal and Flexible (Reference 23.15).

The following components provide contributions to the ability of the VHS to perform its function.

- **Annex building exhaust radiation package –** Provides radiation monitoring of all potentially contaminated exhaust air prior to release to the plant vent. This monitoring is a Category C Class 3 function.

- **Fire dampers** – Fire dampers are provided at duct penetrations through fire barriers to maintain the fire resistance rating of the barriers. The fire dampers are constructed of galvanised carbon steel and actuated by fusible links designed to melt and release the damper blades when the air temperature reaches 74°C (165°F). The fire damper design has parallel blades and uses a spring mechanism to close. The fire dampers meet the design, testing, and installation requirements of UL555 (Reference 23.18).

- **HEPA filters** – HEPA filters are provided in the VHS extract from individual machine tools. The filters provide protection to minimise particulate releases. The filters remove 99.97 percent of all particles 0.3 microns in diameter from the exhaust. They are designed in accordance with ANSI N509.

  A pressure differential sensor is installed across the HEPA filter to measure the pressure drop across it as an indication of its performance. Upon detection of a high-pressure drop

across the HEPA filter, an indicator and alarm are activated.

- **Shutoff dampers** – These are low leakage, gasket, parallel-blade dampers with manual manipulation devices to verify proper operability of the dampers and to manipulate the blade from its fail safe closed position. The shutoff damper actuators are of the spring return pneumatic type complete with solenoid valves that close the damper when there is a loss of pneumatic air or electrical power. The dampers meet the performance requirements of ANSI/AMCA Standard 500 [Reference 23.12]. The outside air inlet dampers of the AHUs, the supply isolation dampers, and the extract isolation dampers are of this type and act to isolate the supply and extract line upon failure of the operating system. The control signal comes from the PLS. Isolation of air supplies is does not contribute to maintaining nuclear safety as determined by the safety case and are thus classified as general non-safety (GNS).

23.10.3 Claims on Components and Equipment

Components and equipment in the VHS control and monitor the level of radioactivity released to the environment. As such, they provide a contribution to nuclear safety, but failure to maintain the safety function does not have the potential to result in a DBA.

23.10.3.1 Fire Dampers

Fire dampers are installed where ductwork passes through fire barriers. The fire dampers protect against fire hazards that could, as part of a sequence of failures, result in loss of a safety function. This could compromise normally operating systems and safety systems delivering a specific function. Therefore, this is a Category B safety function. See Appendix 15A. Because the fire dampers assist in achieving this safety function, they are deemed to be Class 3 equipment. See Appendix 15A.

Single fire dampers are provided where the ducts pass through a fire barrier. It is claimed that the fire dampers will close when the air temperature in the duct reaches the design limit and will maintain the integrity of the fire barrier.

23.10.3.2 High-Efficiency Particulate Air Filters

HEPA filters are passive components with a high degree of inherent safety. They will meet their claimed efficiency through being constructed, qualified, and tested in accordance with appropriate standards (detailed in Section 23.3.2 above). There is a large amount of experience with using HEPA filters designed to these codes in operating nuclear power stations around the world, which gives confidence in their ability to meet their safety function.

A particle penetration of the HEPA filter unit (including through any bypass routes) that is greater than the design limit will be detected by the radiation sensor downstream of the filter bank. This would enable operator action, such as shutting down the exhaust filtration system, to take place.

The claimed efficiency of the HEPA filters will be demonstrated in situ upon installation of a new filter and through periodic testing.

The HEPA filters in the VHS minimise the radiation released to the environment during operation. As such, the HEPA filters provide a Category B safety function. Failure of either the HEPA filters will result in the potential for a release of contamination and radioactivity to

the environment. The HEPA filters provide a contribution to the VHS's primary safety function and are Category B Class 3 equipment. See Appendix 15A.

23.10.3.3 Shutoff Dampers

Operation of the shutoff dampers provides a non-safety function.

It is claimed that they will close on demand from the PLS to prevent an unmonitored release of air from the supplied areas when the VHS has failed. If they do not close, the VFS will still be capable of maintaining a negative pressure in the VHS area.

23.10.4 Justification of Claims on Components and Equipment

23.10.4.1 High-Efficiency Particulate Air Filters and Charcoal Adsorbers

HEPA filters are passive components. They will meet their claimed efficiency through being constructed, qualified, and tested in accordance with appropriate standards (detailed in Section 23.7.2). There is a large amount of experience in using HEPA filters designed to these codes in operating nuclear power stations around the world, which gives confidence in their ability to meet their safety function.

HEPA filter damage could occur during installation. However, in situ penetration testing is to be carried out after every filter change to demonstrate that the filter is achieving the correct efficiency.

The claimed efficiencies will be demonstrated through periodic testing under the ventilation filter testing programme.

23.10.4.2 Fire Dampers

The design of fire damper used in the VHS does not require any external power source or actuation signals. Actuation is achieved by heat from the air in the duct melting the fusible link and a spring mechanism closing the damper. This provides a high degree of inherent safety and high reliability. The fire load in the radwaste building will be kept to a minimum to reduce the risk and potential size of a fire. This also contributes to the inherent safety of the system.

The highest classification of fire dampers in the system is Category B Class 3. The dampers are to be designed and manufactured to normal industrial standards suitable for Class 3 equipment.

Any failure that causes the fire damper to close is a failure to safety because the fire barrier will be maintained. The only conceivable failure to an unsafe position is if the damper were to seize or jam in the open position.

Maintenance will be performed in line with the manufacturer's information. The extensive experience of operating this type of damper gives confidence that if adequately maintained, they will not seize or jam and will move to the closed position when the temperature rises above the specified point.

23.10.4.3 Shutoff Dampers

The shutoff dampers are designed such that they fail to safety. The spring return pneumatic design ensures that a loss of electrical power or pneumatic air will cause the dampers to close, isolating the ductwork and preventing any unmonitored release of air from the supplied areas. This provides a high degree of inherent safety. If they do not close, and there is a radioactive release, the VFS will actuate to maintain a negative pressure in the VHS area, even if the dampers fail to close.

The shutoff dampers are to be designed to normal industrial standards. The dampers are of a low leakage design to minimise the passing of any air when the dampers are shut. This in turn prevents leakage of contamination from the area when the VHS is isolated.

Periodic inspection of the dampers will be undertaken to ensure that they have not seized or jammed and maintenance will be carried out in line with the manufacturer's information. There is extensive experience of operating this type of damper to give confidence that if they are adequately maintained they will not seize or jam and will move to the closed position if demanded.

23.11 NUCLEAR ISLAND NONRADIOACTIVE VENTILATION SYSTEM

23.11.1 Role

The VBS contributes to the containment primary safety function and provides support to other safety systems. The VBS consists of the following three subsystems:

- MCR/control support area (CSA), HVAC
- Essential electrical system equipment room, remote shutdown room (RSR) HVAC
- PCS valve room heating and ventilation

If complete ac power is lost, in the post-72-hour period, division B and C C&I room temperature is maintained by operating their respective ancillary fans to supply outside air to the C&I rooms. The air flow rate design basis is to maintain the C&I rooms below the qualification temperature of the C&I equipment (below 48.8°C (120°F)). Loss of normal HVAC is discussed in Chapter 8.

If complete ac power is lost, in the post-72-hour period, MCR habitability is maintained by operating one of the two MCR ancillary fans to supply outside air to the MCR.

Further design details of this system and its constituent components are delineated in Reference 23.33 and Chapter 6.

23.11.1.1 Main Control Room/Control Support Area Heating, Ventilation, and Air Conditioning Subsystem

The safety function of the MCR/CSA HVAC subsystem is to contribute to maintaining the MCR environment in a habitable condition. This is achieved through monitoring the MCR supply air for radioactive particles and iodine concentrations and maintaining the space at a positive pressure to prevent unmonitored infiltration of air. The subsystem isolates the HVAC penetrations upon detection of high-high particulate or iodine concentrations in the MCR supply air or upon loss of ac power for more than 10 minutes or low MCR differential pressure with respect to the surrounding rooms for 10 minutes. This supports the function of the VES described in Chapter 6. In addition, the MCR/CSA HVAC subsystem provides a

defence in depth safety function through the filtration of MCR/CSA air during conditions of high airborne radioactivity in the supply air. The subsystem maintains the VES passive cooling heat sink below its initial design temperature and can operate in a recirculation mode when smoke is detected outside or provide smoke removal capabilities from the supplied areas.

The MCR/CSA HVAC subsystem makes provision for two 100-percent-capacity supply AHUs, return/exhaust air fans, supplemental air filtration units, associated dampers, C&I, and common ductwork. The supply AHUs and return/exhaust air fans are connected to common ductwork, which distributes air to the MCR and CSA areas. Each supplemental air filtration unit includes a supply fan, HEPA filter bank, and charcoal adsorber. Ancillary fans provide post-72-hour ventilation to the MCR and C&I rooms.

The MCR pressure boundary penetrations include isolation valves and isolation dampers. These are provided to isolate the normal outside air intake such that the outside air passes through the supplemental air filtration. Combination fire/smoke dampers are provided at duct penetrations through fire barriers to maintain the fire resistance ratings of the barriers and prevent the migration of smoke.

Stairwell pressurisation fans are provided where required to prevent smoke from entering stairwells during a fire.

The subsystem is supported by the PMS for MCR pressure boundary isolation and actuation of supplemental air filtration and the PLS for other control functions, the FPS for activation signals to the fire/smoke dampers, the VWS to supply the AHU cooling coils, and the ZOS for the standby power supply.

The MCR/CSA HVAC subsystem supports the FPS through the provision of smoke detection and deluge connections on the supplemental filtration units, the RMS through the provision of radiation monitors and the VES through the maintenance of the MCR passive heat sink initial design temperature and isolation of the MCR pressure boundary.

23.11.1.2 Essential Electrical System Equipment Room Heating, Ventilation, and Air Conditioning Subsystem

The safety function of the essential electrical system equipment room HVAC subsystem is to maintain the essential electrical system equipment room passive cooling heat sink below its initial design ambient air temperature limit and provide post-72-hour cooling to the room. It is also required to exhaust air from the essential electrical system battery rooms to prevent the buildup of hydrogen gas and provide smoke removal capabilities from the essential electrical system equipment rooms and battery rooms.

The A and C electrical divisions, spare battery room, and reactor coolant pump trip switchgear rooms are served by one ventilation subsystem; the B and D electrical divisions and remote shutdown room are served by a second ventilation subsystem. Each subsystem makes provision for two 100-percent-supply AHUs that include both supply and return/exhaust fans and a chilled water cooling coil bank. Ancillary fans provide post-72-hour ventilation to the division B and C C&I room. Each subsystem for the essential electrical system battery rooms is provided with two 100-percent-capacity exhaust fans. Combination fire/smoke dampers are provided for essential electrical system equipment rooms, including the remote shutdown room, to isolate each fire area and block the migration of smoke and hot gases to or from adjacent fire areas.

The subsystem is supported by the PLS for control functions, the FPS for activation signals to the fire/smoke dampers, the VWS to supply the AHU cooling coils and the ZOS.

The main essential electrical system room HVAC subsystem supports the FPS through the provision of smoke detection. It also supports the essential electrical supply system (IDS) through the provision of battery room and electrical equipment room ventilation.

23.11.1.3 Passive Containment Cooling System Valve Room Heating and Ventilation Subsystem

The safety function of the PCS valve room heating and ventilation subsystem is to maintain the temperature of the valve room within predefined limits.

The subsystem includes one 100-percent-ventilation fan, two 100-percent-capacity electric unit heaters, and an air intake louver damper. The PCS valve room is not expected to exceed its upper temperature limit based on maximum ambient conditions and internal heat sources. Therefore, the ventilation fan does not provide a safety function.

The subsystem is supported by the PLS and ZOS.

The PCS valve room heating and ventilation subsystem supports the PCS through maintaining the PCS valve room temperature within pre-defined limits.

23.11.2 System Components and Equipment Contributing to Safety Function

Ductwork, duct supports, and accessories are constructed of galvanised steel. Ductwork subject to fan shutoff pressures is structurally designed to accommodate fan shutoff pressures. Ductwork, supports, and accessories meet the design and construction requirements of SMACNA Industrial Rectangular and Round Duct Construction Standards (References 23.13 and 23.14) and SMACNA HVAC Duct Construction Standards – Metal and Flexible (Reference 23.15). The MCR/CSA HVAC subsystem's ductwork, including the air filtration units and the portion of the ductwork located outside of the MCR envelope that maintains the integrity of the MCR/CSA pressure boundary, are designed in accordance with ASME AG-1 (Reference 23.6, Article SA-4500). This ensures the ductwork is of a low leakage construction to maintain MCR/CSA habitability.

The ancillary fans provide post 72-hour cooling to the MCR and Division B and C C&I rooms with power from the ancillary diesel generators. They are centrifugal type with nonoverloading characteristics. Each can provide a minimum of 2718 m^3/hr (1600 cfm). The fans are designed and rated in accordance with ANSI/AMCA Standards 210 (Reference 23.9), 211 (Reference 23.10), and 300 (Reference 23.11).

Multi-blade, two-position remotely operated shut off dampers are parallel-blade type. Multi-blade, balancing dampers are opposed-blade type. AHU and fan shutoff dampers are designed for maximum fan static pressure at shutoff flow and meet the performance requirements in accordance with ANSI/AMCA Standard 500 (Reference 23.12). The supplemental air filtration subsystem dampers are constructed, qualified, and tested in accordance with ANSI/AMCA Standard 500 or ASME AG-1 (Reference 23.6, Section DA).

The following components make key contributions to the ability of the VBS to perform its safety function.

- **Air handling units supply and return/exhaust fans** – These are centrifugal type, single-width single-inlet or double-width double-inlet, with high-efficiency wheels and backward-inclined blades to produce nonoverloading characteristics. The fans are

designed and rated in accordance with ANSI/AMCA Standards 210 (Reference 23.9), 211 (Reference 23.10), and 300 (Reference 23.11).

The supplemental air filtration unit fans are provided with fan shaft seals to reduce external leakage as identified in the VBS system specification document (Reference 23.33, Section 5.1.2.1). This is to be done in accordance with requirements of the Utility Requirements Document (URD) (Reference 23.34, Chapter 9, Paragraph 8.2.1.1.13) and Information Notice 93-06[2] regarding potential bypass leakage paths in ventilation systems (Reference 23.35).

The essential electrical system battery room exhaust fans are of a spark proof design.

The supply and return/exhaust air fans in the MCR/CSA HVAC subsystem AHUs are required to operate to provide cooling to the MCR passive heat sink.

The supplemental air filtration unit fans are required to operate to provide the MCR/CSA with filtered air and prevent the ingress of unfiltered air.

The supply and return/exhaust air fans in the essential electrical system equipment room HVAC subsystem AHUs are required to operate to provide cooling to the essential electrical system equipment room emergency passive heat sink.

The essential electrical system battery room exhaust fans are required to operate to prevent the build-up of hydrogen in the battery rooms.

The fans all operate in response to signals from the PLS that include flow rate, temperature, and shutoff damper positions.

The Battery Exhaust Fans are designed to Class 2 as they are the principal means of proper airflow in the battery rooms to prevent hydrogen accumulation above the design limit during battery charging which is a Category B safety function.

The MCR/CSA Supplemental Air Filtration Units are designed to Class 2 as they are the principal means to provide supplementary ventilation function to preserve the habitability of MCR/CSA which is a Category A safety function.

The Other Air Handling Units are designed to Class 2 as they are the principal means to maintain design temperatures in the Class 1 electrical and C&I rooms which is a Category A safety function.

- **HEPA filters and charcoal adsorbers** – HEPA filters are constructed, qualified, and tested in accordance with UL 586 (Reference 23.28) and ASME AG-1 (Reference 23.6, Section FC). Each HEPA filter cell is individually shop tested to verify an efficiency of at least 99.97 percent using a monodisperse 0.3-micron aerosol in accordance with ASME AG-1 (Reference 23.6, Section TA). The HEPA filters in the supplemental air filtration units work to remove particulate from the outside supply air to reduce potential control room dose during high radiation levels. They also filter a proportion of recirculation air from the served areas. This is a Class 2 safety requirement.

2. Information Notice 93-06 represents good industry practice to prevent potential bypass leakage paths in ventilation systems and is therefore applicable to UK power stations.

Each charcoal adsorber is designed constructed, qualified, and tested in accordance with ASME AG-1 (Reference 23.6, Section FE) and Regulatory Guide 1.140 (Reference 23.7). Each charcoal adsorber is a single assembly with welded construction and 102 mm (4 inch) deep Type III rechargeable adsorber cell, conforming to IE Bulletin 80-03 (Ref. 23.8). Reference 23.7 indicates that a charcoal adsorber of this type should have a decontamination efficiency of 99 percent using an appropriate test methodology. The charcoal adsorbers in the supplemental air filtration units work to remove radiation from the outside supply air to reduce potential control room dose during high radiation levels. They also treat a proportion of recirculation air from the served areas. This is a Class 2 safety requirement.e HEPA filters and charcoal adsorbers are designed to Class 2 as they are the principal means to provide supplementary ventilation function to preserve the habitability of MCR/CSA which is a Category A safety function.

- **Electric unit heaters** – The electric unit heaters are forced-air, finned-tubular type, factory assembled, integral package units with single-stage or two-stage heating. Electric unit heater casings will be constructed of heavy gauge steel with a fan section and electric heating coil section. The electric unit heaters are UL-listed and meet the requirements of UL 1996 (Reference 23.36) and the National Electrical Code (Reference 23.37).

  The electric unit heaters operate in response to temperature signals from the PLS to maintain the temperature in the PCS valve room above the predefined lower limit in order to support valve operation. The PCS Room Heaters are designed to Class 3 as they are the principal means to maintain the temperature of the PCS valve room above freezing during normal operation which is a Category C safety function.

- **Cooling coils** – The chilled water cooling coils are counterflow, finned-tubular type. Each cooling coil is constructed with copper tubes and fins. Large cooling coil banks that are constructed from multiple cooling coils are provided with coil holding racks designed to allow each coil to be independently removed (side pull) from the housing. The cooling coils are designed and rated in accordance with ASHRAE 33 (Reference 23.23) and ANSI/ARI 410 (Reference 23.22). The cooling capacity of the coils includes a 15 percent margin. Coils are designed to withstand a working pressure of 1.03 MPa (150 psig) at 7.2°C (45°F) and leak tested with 2.07 MPa (300 psig) of air under water (Reference 23.33, Section 5.1.1.4.2).

  The cooling coils obtain a flow of cooling water through activation of the chilled water control valves in response to signals from the PLS. The cooling coils are designed to Class 2 as they are the principal means to permit the flow of cooling water through the copper tubes and maintain an adequate surface for heat transfer between the air and cooling water in order to meet air temperature control requirements which is a Category A safety function.

- **Isolation valves** – The MCR envelope isolation valves are rotary, double-seat, butterfly valves. The valves are designed to ASME Code, Section III, Class 3, and Seismic C-I (References 23.4 and 23.33, Appendix F2). The valve actuators are motor operated. The actuators are two-position type and fail in place upon electrical and control power failures. The actuators are designed to provide at least 1.5 times the torque required to meet the specific dynamic requirements and leakage rates. The actuators are designed with position switches to verify proper operation of the valves and manual manipulation devices to move the valve position, if necessary. The allowable leakage rate of the

isolation valves meets the testing and performance requirements of the Manufacturers Standardisation Society (MSS) SP-61 (References 23.38 and 23.33, Section 5.2.1).

The valves are required to operate to maintain the low leak rate integrity of the MCR envelope when the MCR emergency habitability system is operating. The valves operate in response to manual actuation signals from the PLS or automatic signals from the PMS. These MCR Isolation Valves are designed to Class 1 as they are the principal means for MCR isolation which is a Category A safety function.

- **Isolation dampers** – Isolation dampers are bubble-tight, single- or parallel-blade type. The isolation dampers have spring return actuators that fail closed on loss of electrical or control power. The isolation dampers are constructed, qualified and tested in accordance with ANSI/AMCA Standard 500 (Reference 23.12) or ASME AG-1 (Reference 23.6, Section DA).

  The isolation dampers are required to operate in response to signals from the PLS to prevent the infiltration of unfiltered supply air into the MCR/CSA AHU when high radiation has been detected. These Isolation Dampers are designed to Class 2 as they are the principal means for MCR/CSA isolation which is a Category A safety function.

- **Combination fire/smoke dampers** – Combination fire/smoke dampers are all galvanised construction, low leakage with parallel blades, suitable for vertical or horizontal mounting, and listed for dynamic closure. Damper blades are designed to close against the subsystem pressure and flow condition at the duct section in which they are located. The fire damper frame is continuously welded into a galvanised steel sleeve to minimise air leakage when the damper is closed. Combination fire/smoke dampers meet the requirements of UL 555 (Reference 23.18) and UL 555S (Reference 23.39) and bear a UL label. UL 555S is suitable for leakage rated dampers for use in smoke control systems. The fire rating of the combination fire/smoke damper is at least equal to the fire barrier that it protects, up to a maximum of three hours. The combination fire/smoke dampers are installed in accordance with the manufacturer's recommendations (Reference 23.33, Section 5.2.6). The fire/smoke damper closes under the action of a spring mechanism. The design includes a hold-open actuator, which releases and closes the damper in response to a control signal to prevent smoke migration.

  The combination fire/smoke dampers are required to operate to maintain the integrity of a fire barrier within which they are located and prevent the spread of smoke to other fire compartments. They respond to either the air temperature in the duct where no actuation signal is required or a smoke detection signal via the PLS. These combination fire/smoke dampers are Category A Class 2 equipment.

- **Ancillary fan –** Reduces the probability of requiring the use of offsite SSCs to maintain Category A safety functions after 72 hours following an accident. The ancillary fans provide ventilation beginning 72 hours after an accident. They are required to operate to provide cooling to essential equipment. They are designed to meet the requirements of ANSI/AMCA standards.

- **VBS radiation package –** VBS contains two skid mounted MCR radiation monitoring packages consisting of radiation detectors, local radiation processors, and sampling components to continuously measure and record the radioactive materials in the MCR main supply air duct and actuate VBS supplemental air filtration and VES operation. They are designed to meet the requirements of applicable manufacturing standards and are seismic C-I.

23.11.3 Claims on Components and Equipment

23.11.3.1 Supply and Return/Exhaust Air Fans

- The supply and return/exhaust air fans in the MCR/CSA HVAC subsystem AHUs and the supplemental air filtration unit fans maintain the MCR habitability, and as such provide a Category A safety function. See Appendix 15A. They provide a defence in depth function as the primary system to maintain the MCR habitability is the VES. Therefore, the fans are Category A Class 2 equipment. See Appendix 15A.

  There are two 100-percent-capacity AHUs in the MCR/CSA HVAC subsystem with one supply and one return/exhaust air fan in each AHU. It is claimed that the fans in one of the AHUs will start on demand and continue to operate to provide cooling to the MCR passive heat sink and supply recirculation air to the supplemental air filtration units.

  There are two supplemental air filtration unit fans, and it is claimed that at least one of the fans will start on demand to supply the MCR/CSA with filtered air preventing the infiltration of potentially contaminated air. It is also claimed that they will recirculate air from the MCR/CSA through the filtration units.

- The essential electrical system battery room exhaust fans, in the essential electrical system equipment room HVAC subsystems, prevent the build-up of hydrogen in the battery rooms, which would directly and inevitably result in loss of other Category A safety functions. As such, the battery room exhaust fans provide a Category B safety function. See Appendix 15A. Hydrogen detectors in the battery rooms provide additional protection against hydrogen build-up. Also, the volume of air in the battery rooms effectively provides a delay between the failure of the exhaust fans and the hazard developing. The essential electrical system equipment room emergency passive heat sink controls the battery room temperature ensure that the batteries maintain their design capacity. The exhaust fans provide a significant contribution to preventing the build-up of hydrogen and are therefore Category B Class 3 equipment.

  There are two 100-percent-capacity essential electrical system battery room exhaust fans in each subsystem, and it is claimed that one fan from each battery room will start and continue to operate to prevent the build-up of hydrogen in the battery rooms.

- The supply and return/exhaust air fans in the essential electrical system equipment room HVAC subsystem AHUs support the essential electrical system equipment, including supplying the essential electrical system battery rooms. Failure of the ventilation system will not inevitably lead to the loss of the essential electrical system equipment room emergency passive heat sinks. Temperature sensors in the essential electrical system equipment rooms would alert MCR personnel if the room temperatures started to rise and allow them to take appropriate action to ensure that the passive heat sink temperatures did not rise above a predefined limit. The ancillary fans support the Category A safety functions provided by the essential electrical system equipment after 72 hours following an accident, and that is a Category B safety function. See Appendix 15A.The fans in the AHUs are required to operate to ventilate the battery rooms and failure of the supply will start the standby air handling unit fans. The fans in the AHUs should be of the same categorisation as the exhaust fans. Therefore, the supply and return/exhaust air fans in the essential electrical system equipment room HVAC subsystem AHUs provide a Category A safety function. See Appendix 15A. The fans provide a significant contribution to nuclear safety and are Class 2 equipment. See Appendix 15A.

There are two 100-percent-capacity AHUs in each essential electrical system equipment room HVAC subsystem with one supply and one return/exhaust air fan in each AHU. The fans in one of the AHUs in each subsystem are required to start on demand and continue to operate to provide cooling to the essential electrical system equipment rooms and ventilation to the battery rooms.

23.11.3.2 High-Efficiency Particulate Air Filters and Charcoal Adsorbers

HEPA filters and charcoal adsorbers in the MCR/CSA HVAC subsystem maintain the MCR habitability and as such provide a Category A safety function. See Appendix 15A. They provide a defence in depth function, as the primary system to maintain the MCR habitability is the VES. Therefore, the HEPA filters and charcoal adsorbers are Category A Class 2 equipment. See Appendix 15A.

There are two 100-percent-capacity supplemental air filtration units each containing a HEPA filter bank and charcoal adsorber. Only one unit is required to operate.

It is claimed that the HEPA filter banks and charcoal adsorbers will filter the supply and recirculation air to maintain the atmosphere in the MCR below pre-defined radiation limits.

23.11.3.3 Electric Unit Heaters

The electric unit heaters in the PCS valve room heating and ventilation subsystem support the PCS valves by ensuring that the temperature does not fall below a pre-determined limit. However, failure of the heaters will not inevitably lead to the loss of function of the PCS valves. Temperature sensors in the PCS valve room would alert MCR personnel if the room temperature started to fall below pre-set limits and allow them to take appropriate action to ensure the room temperature did not compromise PCS valve function. Failure of the electric unit heaters may reduce safety margins but would not lead to a DBA; therefore, the heaters provide a Category C safety function. See Appendix 15A. The electric unit heaters provide a minor contribution to nuclear safety and are Class 3 equipment. See Appendix 15A.

There are two 100-percent-capacity electric unit heaters, and it is claimed that one will start on demand to maintain the temperature in the PCS valve room.

23.11.3.4 Cooling Coils

The cooling coils in the MCR/CSA HVAC subsystem AHUs maintain the temperature in the MCR. Failure of the ventilation system will not inevitably lead to the loss of the MCR passive heat sink. Temperature sensors in the MCR would alert personnel if the room temperature started to rise and allow them to take appropriate action to ensure that the passive heat sink temperature did not rise above a predefined limit. The cooling coils support the Category A safety function of maintaining MCR habitability after 72 hours following an accident. They also function to maintain the room temperature at or below the set point temperature to support the VES. It is therefore concluded that the cooling coils in the MCR/CSA HVAC subsystem AHUs provide a Category A safety function. See Appendix 15A. The cooling coils provide a significant contribution to nuclear safety and are Class 2 equipment. See Appendix 15A.

There are two 100-percent-capacity AHUs in the MCR/CSA HVAC subsystem, with one cooling coil bank in each AHU. It is claimed that the cooling coil in one of the AHUs will continue to operate to provide cooling to the MCR passive heat sink.

The cooling coils in the essential electrical system equipment room HVAC subsystem AHUs support the essential electrical system equipment. Failure of the ventilation system will not inevitably lead to the loss of the essential electrical system equipment room emergency passive heat sinks. Temperature sensors in the essential electrical system equipment rooms would alert MCR personnel if the room temperatures started to rise and allow them to take appropriate action to ensure the passive heat sink temperatures did not rise above a predefined limit. It is therefore concluded that the cooling coils in the essential electrical system equipment room HVAC subsystem AHUs provide a Category A safety function. See Appendix 15A. The cooling coils provide a contribution to nuclear safety and are Class 2 equipment. See Appendix 15A.

There are two 100-percent-capacity AHUs in each essential electrical system equipment room HVAC subsystem, with one cooling coil bank in each AHU. It is claimed that the cooling coils in one of the AHUs will continue to operate to provide cooling to the essential electrical system equipment rooms.

23.11.3.5 Isolation Valves

The isolation valves in the MCR/CSA HVAC subsystem supply and extract ductwork close upon activation of the VES. They maintain the habitability of the MCR by preventing the ingress of potentially contaminated air into the MCR. This is a Category A safety function. See Appendix 15A. The isolation valves provide the principal means of ensuring the integrity of the MCR envelope therefore they are deemed to be Category A Class 1 equipment. See Appendix 15A.

Two isolation valves are provided in series for each of the penetrations. It is claimed that one valve will close to form a low leak rate seal.

23.11.3.6 Isolation Dampers

The VBS dampers in lines isolating radioactive contamination close to prevent an unfiltered supply of air into the MCR/CSA AHUs following detection of high radiation levels in the supply air. They act to maintain the MCR habitability and as such provide a Category A safety function. See Appendix 15A. They provide a secondary function, because primary isolation of the MCR is provided by the isolation valves. Therefore, the VBS isolation dampers are Category A Class 2 equipment. See Appendix 15A.

Two isolation dampers are provided in series in the MCR/CSA HVAC subsystem AHU normal outside air intake duct. It is claimed that one damper will close to form a low leak rate seal and prevent the supply of unfiltered outside air to the MCR/CSA AHUs.

23.11.3.7 Combination Fire/Smoke Dampers

Combination fire/smoke dampers are installed in the VBS where ductwork passes through fire barriers. Some VBS dampers are provided with position indication.

The fire/smoke dampers protect against fire hazards that could, as part of a sequence of failures, result in loss of a safety function. This could compromise normally operating systems and safety systems delivering a specific function. Therefore, this is a Category A safety function. See Appendix 15A. As the fire/smoke dampers provide a contribution to achieving this safety function, they are deemed to be Class 2 equipment. See Appendix 15A.

23.11.3.8 Ancillary Fans – Reduces the probability of requiring the use of offsite SSCs to maintain Category A safety functions after 72 hours following an accident. Therefore, this component is Category B Class 2 equipment.

23.11.3.9 VBS Radiation Package – VBS contains two skid mounted MCR radiation monitoring packages consisting of radiation detectors, local radiation processors, and sampling components to continuously measure and record the radioactive materials in the MCR main supply air duct and actuate VBS supplemental air filtration and VES operation. Therefore, this component is Category A Class 1.

23.11.4 Justification of Claims on Components and Equipment

23.11.4.1 Supply and Return/Exhaust Air Fans

The fan design includes backward-inclined blades to produce nonoverloading characteristics. This will prevent overpressurisation of the ventilation distribution system if a damper in the system closes. This is an inherently safe design feature and provides a high degree of confidence in maintaining the integrity of the ventilation system.

Hydrogen detectors in the battery rooms and redundant fans provide additional protection against hydrogen build-up. Also, the volume of air in the battery rooms provides a delay between the failure of the exhaust fans and the hazard developing to permit operator intervention. The essential electrical system equipment room emergency passive heat sink controls the battery room temperature to maintain battery capacity.

The supply and return/battery exhaust air fans in the VBS are Class 2 equipment. The fans are to be designed and manufactured to normal industrial standards that are suitable for Class 2 equipment. The battery room exhaust fans include enhancements to the design to ensure they are spark proof. This protects against the risk of ignition of any hydrogen in the rooms.

Redundant fans are included with the provision of standby supply AHUs for both the MCR/CSA HVAC subsystem and the essential electrical system equipment room HVAC subsystem and standby battery room exhaust fans. This redundancy provides further confidence that the fans will be able to deliver the reliability required to ensure the VBS meets its safety functions.

The fan motors and their lubricants are designed to withstand the environmental effects over the design life of the plant. The battery room fans are provided with direct-driven motors and self-lubricating seal bearings to minimise maintenance efforts (Reference 23.33).

Conceivable failure modes for these types of fans include, for example, a failed bearing, excessive vibration, etc. Such mechanical failures are avoidable with appropriate maintenance and can be readily detected and rectified. MCR operators will be alerted to failure of any of the fans that will enable them to take appropriate action.

Maintenance will be carried out in line with the manufacturer's information. It is recognised that reliability of the battery room exhaust fans is very important, and any further maintenance requirements will be identified in the site-specific PCSR. There is extensive experience of operating these types of fans to give confidence that if adequately maintained they will have good reliability in service.

23.11.4.2 High-Efficiency Particulate Air Filters and Charcoal Adsorbers

HEPA filters and charcoal adsorbers are passive components and have a high reliability in service. They are Category A Class 2 equipment and will meet their claimed efficiency through being constructed, qualified, and tested in accordance with appropriate standards (detailed in Section 23.11.2 above). There is a large amount of experience in using HEPA filters and charcoal adsorbers designed to these codes in operating nuclear power stations. This gives confidence in their ability to meet their safety function.

A pressure differential sensor is installed to measure the pressure drop across the filter as an indication of its performance. Upon detection of a high pressure drop across the HEPA filter, an indicator and alarm are activated.

A filtration/adsorption efficiency lower than or approaching the design limit will be detected by periodic testing. The radiation sensors in the MCR supply duct will sense any high radiation level, and automatically actuate the supplemental AHU and if necessary the VES.

The claimed efficiency of the HEPA filters and charcoal adsorbers will be demonstrated in situ through periodically testing each operating cycle and after each replacement of a HEPA filter or charcoal adsorber (Reference 23.33, Table 9-2).

23.11.4.3 Electric Unit Heaters

The electric unit heaters are classified as Class 3. The heaters are to be designed and manufactured to normal industrial standards that are suitable for Class 3 equipment.

Redundant electric unit heaters are included with the provision of two 100-percent-heaters in the PCS valve room. This redundancy provides further confidence that the electric unit heaters will be able to deliver the reliability required to ensure the VBS meets its safety functions.

Failure of the unit heaters will not lead to an immediate loss of PCS valve function. The operators would be alerted to unit heater failure and a reduction in temperature below pre-set limits. This would enable them to take appropriate action to ensure the PCS valves can maintain their safety function.

Maintenance will be carried out in line with the manufacturer's information. There is extensive experience of operating this type of electric unit heater to give confidence that if they are adequately maintained, they will demonstrate good reliability in service.

23.11.4.4 Cooling Coils

The highest classification of cooling coil in the VBS is Class 2. The coils are to be designed and manufactured to normal industrial standards that are suitable for Class 2 equipment.

Redundant cooling coils are included with the provision of standby supply AHUs for both the MCR/CSA HVAC subsystem and the essential electrical system equipment room HVAC subsystem. This redundancy provides further confidence that the cooling coils will be able to deliver the reliability required to ensure the VBS meets its safety functions.

Possible failure mechanisms include:

- Failure of the chilled water control valves. If the chilled water control valves on the operating AHU fail, leading to an increase in supply air temperature, then an alarm would annunciate in the MCR. The temperature in the served area can be maintained by operation of the standby AHU.

- Failure of the complete chilled water system. If chilled water is lost to both AHUs in each subsystem, leading to an increase in supply air temperature, then an alarm would annunciate in the MCR. It may, in these circumstances, not be possible to maintain design indoor temperatures, based on the outdoor temperature. Thermal inertia will provide a time delay before room temperature exceeds design limits, and this would enable operator intervention to occur.

- Structural failure of the coils. The use of suitable design standards and appropriate in service maintenance is deemed sufficient to reduce the risk of structural failure of the cooling coils.

Maintenance will be carried out in line with the manufacturer's information. There is extensive experience of operating this type of cooling coil to give confidence that if they are adequately maintained, they will have good reliability in service.

23.11.4.5 Isolation Valves

The MCR isolation valves are battery operated and fail in place. This offers a high degree of inherent safety and high reliability because each redundant valve is connected to a different battery.

The MCR isolation valves are Seismic C-I and are to be designed and constructed to the ASME Code, Section III-3 design code (Reference 23.33, Appendix F2). This code has been specifically developed to qualify components in safety significant applications on nuclear power stations. The code, with the testing and examination that supports it, provides the foundation for claims made on the MCR isolation valves.

The valves are very similar to those already in service, providing the same function on many operating power stations. As a result, the information from the testing of these in service valves offers a high degree of confidence regarding the reliability of the valves proposed for the AP1000 design.

The operating mechanism for the valve is relatively simple, and aside from gross mechanical failure, the principal mechanisms for valve failure are considered to be some form of adhesion preventing the valve closing, or leakage of the valve under pressure when in the closed position. These failures are considered to be unlikely because of a combination of good design and a robust maintenance, inspection, and testing regime. The valve is of a double-seat butterfly type. The materials of the valve have been selected to minimise the risk of corrosion interfering with valve operation.

IST of the VBS MCR isolation valves is included in surveillance requirement SR 3.7.6.6. This requires verification that all VBS MCR isolation valves are operable and will close upon receipt of an actual or simulated actuation signal every 24 months. Periodic pneumatic leakage testing is also performed.

23.11.4.6 Isolation Dampers

The isolation dampers are designed such that they fail safe to the closed position. The spring-return actuator design ensures that a loss of electrical or control power will cause the dampers to close, isolating the ductwork and preventing any unfiltered supply of air to the MCR AHUs. This provides a high degree of inherent safety. Spurious operation of the isolation dampers in the AHU supply duct puts the ventilation system in a safe condition and can be manually reset.

The dampers in lines isolating radioactive contamination are to be designed and manufactured to normal industrial standards that are suitable for Class 3 equipment. The dampers are of a low leakage design to minimise the passing of any air when the dampers are shut. This in turn prevents the supply of unfiltered air when the main AHU supply duct is isolated.

Redundant isolation dampers are included in the design such that only one is required to operate. This gives further assurance that the isolation dampers will be able to meet their safety function.

Periodic inspection of the dampers will be undertaken to ensure that they have not seized or jammed and maintenance will be carried out in line with the manufacturer's information. There is extensive experience of operating this type of damper to give confidence that if they are adequately maintained, they will not seize or jam and will return to the closed position if demanded.

23.11.4.7 Combination Fire/Smoke Dampers

The design of the combination fire/smoke damper used in the VBS actuates in response to one of two signals: direct heat from a fire or upon receipt of a smoke signal from one of the area smoke detectors. For the damper to close in response to heat from a fire, it does not require any external power source or actuation signals. This provides a high degree of inherent safety and high reliability. The fire load in the served areas will be kept to a minimum to reduce the risk and potential size of a fire. This also contributes to the inherent safety of the system. Some VBS dampers are provided with position indication.

The fire/smoke dampers are to be designed and manufactured to normal industrial standards that are suitable for Class 2 equipment.

The combination fire/smoke dampers fail closed using a spring mechanism. Any failure that causes the fire/smoke damper to close is a failure to safety because the fire barrier will be maintained. The only conceivable failure to an unsafe position is if the damper was to seize or jam in the open position.

Maintenance will be carried out in line with the manufacturer's information. There is extensive experience of operating this type of damper to give confidence that if they are adequately maintained, they will not seize or jam and will move to the closed position when required.

23.12 ANNEX/AUXILIARY BUILDING NONRADIOACTIVE HEATING, VENTILATION, AND AIR CONDITIONING SYSTEM

23.12.1 Role

The VXS consists of the following six subsystems:

- General area HVAC
- Mechanical equipment areas HVAC
- Switchgear room HVAC
- Equipment room HVAC
- Main steam line isolation valve (MSIV) compartment HVAC
- Valve/piping penetration room HVAC
- Annex building offices (area 4)

The general area and annex building offices HVAC subsystems do not provide a contribution to nuclear safety and, therefore, are not discussed in this section.

The mechanical equipment areas HVAC subsystem serves the ancillary diesel generator room, demineralised water deoxygenating room, boric acid batching room, upper south air handling equipment room, and air handling equipment room in the annex building. Ventilation and cooling for the ancillary diesel generator room when the ancillary diesel generators operate is provided by means of manually operated dampers and opening doors to allow radiator discharge air to be exhausted direct to outdoors. The equipment in the other rooms does not perform a safety function. The mechanical equipment areas HVAC subsystem does not perform a safety function and is not discussed further in this section.

The other subsystems of the VXS make a contribution to nuclear safety with their primary safety function being the provision of support to other safety systems.

To protect the power generation design basis, the VXS is provided with redundant equipment to limit temperature excursions in mechanical and electrical equipment areas resulting from the failure or the shutdown of HVAC equipment for maintenance.

Further design details of this system and its constituent components are delineated in Reference 23.40 and Chapter 6.

23.12.1.1 Switchgear Room Heating, Ventilation, and Air Conditioning Subsystem

The safety function of the switchgear room HVAC subsystem is to support the diesel bus switchgear in the electrical switchgear rooms 1 and 2 through the provision of ventilation cooling and maintaining a minimum temperature during cold ambient conditions.

The subsystem consists of two 100-percent AHUs with integral supply and exhaust fans, cooling and heating coils. Mixing dampers are used to control the proportion of exhaust air that is recirculated. Combination fire/smoke dampers are installed at ductwork penetrations through fire barriers to the switchgear rooms.

The switchgear room HVAC subsystem is supported by the FPS that shuts the fire/smoke dampers on detection of fire in the served areas, the PLS that provides control functions, the ZOS to provide standby power to the VXS in the event of loss of offsite power, and the VWS and VYS for chilled and hot water, respectively.

The switchgear room HVAC subsystem supports operation of the ZOS through the provision of ventilation and cooling of the diesel bus switchgear.

23.12.1.2 Equipment Room Heating, Ventilation, and Air Conditioning Subsystem

The safety function of the equipment room HVAC subsystem is to support equipment in the electrical and mechanical rooms. These rooms include the standby electrical system battery charger rooms 1 and 2, the standby electrical system battery rooms 1 and 2, the reactor trip switchgear rooms 1 and 2, and the standby electrical system penetration rooms. The equipment is supported by the provision of ventilation cooling and maintaining a minimum temperature during cold ambient conditions. In addition, the subsystem prevents the build-up of hydrogen through the continuous exhaust of the battery rooms.

The subsystem consists of two 100-percent-capacity AHUs with integral supply and exhaust fans, cooling and heating coils. Mixing dampers are used to control the proportion of exhaust air that is recirculated. An exhaust fan serves each of the standby electrical system battery rooms. Fire dampers or combination fire/smoke dampers are installed at ductwork penetrations through fire barriers.

The equipment room HVAC subsystem is supported by the FPS, which trips the fans on detection of fire in the served areas; the PLS, which provides control functions; the ZOS, which provides standby power to the VXS in the event of loss of offsite power; and the VWS and VYS, which provide chilled and hot water, respectively.

The equipment room HVAC subsystem supports operation of the ECS, the EDS, and the reactor trip switchgear.

23.12.1.3 Main Steam Isolation Valve Compartment Heating, Ventilation, and Air Conditioning Subsystem

The safety function of the MSIV compartment HVAC subsystem is to support the MSIVs through the provision of ventilation cooling. Operation of the MSIVs will be required when the steam legs are hot; therefore, heating is not required to maintain safe operation of the valves.

The subsystem consists of separate heating and cooling equipment for each MSIV compartment. Two 100-percent-capacity AHUs are included within each MSIV compartment. Each AHU includes a fan and cooling coil.

The MSIV compartment HVAC subsystem is supported by the PLS for control functions, the VWS for chilled water, and the ZOS for standby power to the VXS in the event of loss of offsite power.

The MSIV compartment HVAC subsystem supports operation of the steam generator system (SGS) through the provision of heating and cooling of the MSIV compartment.

23.12.1.4 Valve/Piping Penetration Room Heating, Ventilation, and Air Conditioning Subsystem

The safety function of the valve/piping penetration room HVAC subsystem is to support equipment in the valve/piping penetration room through the provision of cooling and maintaining a minimum temperature during cold ambient conditions.

The subsystem consists of two 100-percent-capacity AHUs with integral supply fans, heating and cooling coils. Fire dampers are installed at ductwork penetrations through fire barriers.

The valve/piping penetration room HVAC subsystem is supported by the FPS, which trips the fans on detection of fire in the served areas; the PLS, which provides control functions; the ZOS, which provides standby power to the VXS in the event of loss of offsite power; and the VWS and VYS, which provide chilled and hot water, respectively.

The valve/piping penetration room HVAC subsystem supports equipment in the valve/piping penetration room.

23.12.2 System Components and Equipment Contributing to Safety Function

Ductwork, duct supports and accessories are constructed of galvanised steel. Ductwork subject to fan shutoff pressure is structurally designed for fan shutoff pressures. Ductwork, supports, and accessories meet the design and construction requirements of SMACNA Rectangular and Round Industrial Duct Construction Standards (References 23.13 and 23.14) and SMACNA HVAC Duct Construction Standards – Metal and Flexible (Reference 23.15).

Isolation dampers are single- or parallel-blade type. The isolation dampers have spring return actuators, which fail closed on loss of electrical power or loss of air pressure. The isolation dampers are constructed, qualified, and tested in accordance with ANSI/AMCA Standard 500 (Reference 23.12).

The following components make key contributions to the ability of the VXS to perform its safety function.

- **Supply and exhaust air fans** – The supply and exhaust fans are centrifugal type, single-width single-inlet, or double-width double-inlet. Most of the fans have backward-inclined blades to produce nonoverloading characteristics. However, those fans installed in AHUs that have little or no ductwork may utilise forward curved blades. The fan operating conditions will be selected to ensure smooth stable operation over the specified operating range without fan surging or instability. The fans are isolated from the AHU casing with spring-type vibration isolators. The fans are designed and rated in accordance with ANSI/AMCA Standards 210 (Reference 23.9), 211 (Reference 23.10), and 300 (Reference 23.11).

  In addition, the exhaust fans from the battery rooms in the equipment room HVAC subsystem have nonsparking wheels.

  The supply and exhaust air fans in the switchgear room HVAC subsystem AHUs are required to operate to provide long-term cooling to the diesel bus switchgear.

  The supply and exhaust air fans in the equipment room HVAC subsystem AHUs are required to operate to provide long-term cooling to the electrical equipment including the reactor trip switchgear.

The battery room exhaust air fans in the equipment room HVAC subsystem are required to operate to prevent the build-up of hydrogen in the battery rooms in the long term.

The supply fans in the MSIV compartment room HVAC subsystem AHUs are required to operate to provide long-term cooling to the MSIVs.

The supply fans in the valve/piping penetration room HVAC subsystem AHUs are required to operate to provide long-term cooling to components in the valve/piping penetration room.

All the fans operate in response to signals from the PLS that include flow rate, temperature, and fire protection signals. These supply and exhaust fans which provide required supply and extract airflows are Category C Class 3 equipment.

- **Cooling coils** – The chilled water cooling coils are counterflow, finned-tubular type. Each cooling coil is constructed with finned tubes. Large cooling coil banks that are constructed from multiple cooling coils are provided with coil holding racks designed to allow each coil to be independently removed (side pull) from the housing. The cooling coils are designed and rated in accordance with ASHRAE 33 (Reference 23.23) and ANSI/ARI 410 (Reference 23.22).

  The cooling coils in the ventilation subsystems obtain a flow of cooling water through activation of the chilled water control valves in response to signals from the PLS. The cooling coils are designed to Class 3 as they are the principal means to permit the flow of cooling water through the tubes and maintain an adequate surface for heat transfer between the air and cooling water which is a Category C safety function.

- **Heating coils** – The hot water heating coils are of the face and bypass type with counterflow, finned tubes. Large heating coil banks that are constructed from multiple heating coils are provided with coil holding racks designed to allow each coil to be independently removed (side pull) from the housing. The heating coils are designed and rated in accordance with ASHRAE 33 (Reference 23.23) and ANSI/ARI 410 (Reference 23.22).

  The heating coils in the valve/piping penetration room HVAC subsystem are required to permit the flow of hot water through the tubes and maintain an adequate surface for heat transfer between the air and hot water. Also, the face and bypass dampers operate to control the temperature of the supply air.

  The heating coil dampers operate in response to temperature signals from the PLS. Thes heating coils are designed to Class 3 as they are the principal means to maintain a minimum temperature in the served areas which is a Category C safety function.

- **Combination fire/smoke dampers** – Combination fire/smoke dampers are all galvanised construction, low leakage with parallel blades, suitable for vertical or horizontal mounting and listed for dynamic closure. Damper blades are designed to close against the subsystem pressure and flow condition at the duct section in which they are located. The fire/smoke damper frame is continuously welded into a galvanised steel sleeve to minimise air leakage when the damper is closed. Combination fire/smoke dampers meet the requirements of UL 555 and UL 555S and bear a UL label (References 23.18 and 23.39). The fire rating of the combination fire/smoke damper is at least equal to the fire barrier that it protects up to a maximum of three hours. The combination fire/smoke dampers are installed in accordance with the manufacturer's recommendations. The fire/smoke damper closes under the action of a spring

mechanism. The design includes a hold-open actuator, which releases and closes the damper in response to a control signal to prevent smoke migration.

The combination fire/smoke dampers respond to either the air temperature in the duct where no actuation signal is required or a smoke detection signal via the PLS. These dampers are designed to Class 3 as they are the principal means to operate in order to maintain the integrity of a fire barrier within which they are located and prevent the spread of smoke to other fire compartments which is a Category B safety function.

- **Fire dampers** – The fire dampers are constructed of galvanised carbon steel and actuated by fusible links designed to melt and release the damper blades when the air temperature reaches 74°C (165°F). The damper blades close via a spring mechanism. Additionally some VXS fire dampers are provided with position indication. The fire dampers meet the design, testing, and installation requirements of UL 555 (Reference 23.18).

  The fire dampers are passive components operated by temperature and a spring mechanism. As such, no actuation signal is required. There is a Category B safety function that the fire damper rating will be at least equal to the fire barrier that they penetrate, up to a maximum 3-hour rating. These dampers are Category B Class 3 equipment.

23.12.3 Claims on Components and Equipment

23.12.3.1 Supply and Exhaust Air Fans and Dampers

- AHUs and dampers that support operation of ZOS by maintaining the diesel bus switchgear rooms and battery charger rooms (containing dc switchgear) within their design temperature range. The supply and exhaust air fans in the switchgear room HVAC subsystem AHUs support operation of the diesel bus switchgear. The onsite diesel generator system, including the diesel bus switchgear, supports a number of Category A safety functions and therefore provide a Category C safety function (see Appendix 15A). The diesel generators have a defence in depth role and are classified as Class 2 equipment. The switchgear ventilation system is therefore a Category C safety function system and is classified as Class 3 equipment.

  There are two 100-percent-capacity AHUs in the switchgear room HVAC subsystem with one supply and one exhaust air fan in each AHU. It is claimed that the fans in one of the AHUs will start on demand and continue to operate to provide cooling to the diesel bus switchgear.

- The standby electrical system battery room exhaust fans in the equipment room HVAC subsystem prevent the build-up of hydrogen in the battery rooms. Significant build-up can only occur during charging, when ac electrical power is available. At that point in time, the batteries are not required to operate. As such, the battery room exhaust fans provide a Category C safety function. Hydrogen detectors are used in battery rooms to protect against hydrogen build-up by alerting operators that hydrogen levels are building. Also, the volume of air in the battery rooms provides a delay between the failure of the exhaust fans and the hazard developing. The exhaust fans provide a minor contribution to nuclear safety and are therefore Class 3 equipment. See Appendix 15A.

There is one standby electrical system battery room exhaust fan extracting from each battery room. It is claimed that each fan will continue to operate to help prevent the build-up of hydrogen in the battery rooms when the batteries are being charged.

- The supply and exhaust air fans in the equipment room HVAC subsystem AHUs support electrical equipment, including the reactor trip switchgear and the nonessential electrical system battery rooms. The fans provide long-term support for the reactor trip switchgear. Failure of the ventilation system will not inevitably lead to the loss of reactor trip switchgear function. Low flow sensors in the ductwork would alert MCR personnel if the ventilation failed and allow them to take appropriate action to ensure that the room temperatures did not rise above a predefined limit. The fans contribute to delivering this safety function and are Class 3 equipment. See Appendix 15A.

  There are two 100-percent-capacity AHUs in the equipment room HVAC subsystem, with one supply and one exhaust air fan in each AHU. It is claimed that the fans in one of the AHUs will start on demand and continue to operate to provide cooling to the equipment, including the reactor trip switchgear, and ventilation to the battery rooms.

- The supply air fans in the MSIV compartment HVAC subsystem AHUs support operation of the MSIVs. The MSIVs provide a number of Category A safety functions and are classified as Class 1 equipment (see Chapter 17 for details). The fans support the Category A safety functions provided by the MSIVs. The AP1000 has the capability of using natural ventilation to cool these spaces. Therefore, the MSIV fans provide a Category C safety function. Failure of the ventilation system will not inevitably lead to the loss of MSIV function. Low flow sensors in the ductwork would alert MCR personnel if the ventilation failed and allow them to take appropriate action to ensure the compartment temperatures did not rise above a predefined limit. The fans contribute to delivering this safety function and are Class 3 equipment. See Appendix 15A.

  There are two 100-percent-capacity AHUs in each MSIV compartment, with one supply fan in each AHU. It is claimed that the fan in one of the AHUs in each compartment will start on demand and continue to operate to provide cooling to the MSIVs.

- The supply air fans in the valve/piping penetration room HVAC subsystem AHUs support the safety equipment in the valve/piping penetration room. Failure of the ventilation system will not inevitably lead to the loss of safety equipment function. Temperature sensors in the room will alert MCR personnel if the ventilation failed and allow them to take appropriate action to ensure that the room temperatures did not rise above a predefined limit. The fans support the pumps and piping that refill and heat the passive cooling water storage tank. This is a Category C function. The fans provide a minor contribution to delivering the safety function and are Class 3 equipment. See Appendix 15A.

  There are two 100-percent-capacity AHUs in the valve/piping penetration room HVAC subsystem, with one supply air fan in each AHU. It is claimed that the fan in one of the AHUs will start on demand and continue to operate to provide cooling to the room.

- Exhaust fan providing ancillary diesel room ventilation within their design temperature range. The supply and exhaust air fans in the switchgear room HVAC subsystem AHUs support operation of the ancillary diesel generator. The ancillary diesel generator supports a number of Category B safety functions. Therefore, the exhaust fan is Category C Class 3 equipment (see appendix 15A).

23.12.3.2 Cooling Coils

The cooling coils provide the same contribution to safety as the AHU supply and exhaust fans discussed above (Section 23.12.3.1). For the same reasons, the cooling coils in the subsystems of the VXS under discussion provide a Category C safety function. Similarly, all the cooling coils are Class 3 equipment. See Appendix 15A.

In each subsystem there are two 100-percent-capacity AHUs, with one cooling coil bank in each AHU. It is claimed that the chilled water control valves in one of the AHUs per subsystem will modulate to control the flow of chilled water and will therefore provide the cooling required to the served areas.

23.12.3.3 Heating Coils

The heating coils provide the same contribution to safety as the AHU supply and exhaust fans in the switchgear room, equipment room, and valve/piping penetration room HVAC subsystems discussed in Section 23.12.3.1. For the same reasons, the heating coils in the switchgear room, equipment room, and valve/piping penetration room HVAC subsystems provide a Category C safety function and are classified as Class 3 equipment.

In each subsystem there are two 100-percent AHUs, with one heating coil in each AHU. It is claimed that the heating coil dampers in one of the AHUs per subsystem will modulate to control the flow of air across the heating coil and hence provide the heating required to the served areas.

23.12.3.4 Combination Fire/Smoke Dampers

Fire dampers or combination fire/smoke dampers are installed in the VXS where ductwork passes through fire barriers.

The combination fire/smoke dampers protect against fire hazards that could, as part of a sequence of failures, result in loss of a safety function. This could compromise normally operating systems and safety systems delivering a specific function. Therefore, this is a Category B safety function. See Appendix 15A. As the fire/smoke dampers contribute to achieving this safety function, they are deemed to be Class 3 equipment. See Appendix 15A.

Single combination fire/smoke dampers are provided where the ducts pass through a fire barrier. It is claimed that the fire/smoke dampers will close when the air temperature in the duct reaches the design limit or upon a fire detection signal from the PLS to maintain the integrity of the fire barrier.

23.12.3.5 Fire Dampers

Included in discussion of “Combination Fire/Smoke Dampers” in section 23.12.3.4.

23.12.4 Justification of Claims on Components and Equipment

23.12.4.1 Supply and Exhaust Air Fans

The fan design for subsystems with a significant amount of ductwork includes backward-inclined blades to produce nonoverloading characteristics. This will prevent overpressurisation of the ventilation distribution system if a damper in the system closes. This

is an inherently safe design feature and provides a high degree of confidence in maintaining the integrity of the ventilation system.

Hydrogen detectors protect against hydrogen build-up by alerting operators that hydrogen concentrations are increasing. Also, the volume of air in the battery rooms effectively provides a delay between the failure of the exhaust fans and the hazard developing to permit operator intervention.

The highest classification of supply and return/exhaust air fans in VXS AHUs is Class 3. The fans are to be designed and manufactured to normal industrial standards that are suitable for Class 3 equipment.

The battery room exhaust fans are also Class 3 equipment. They are designed and manufactured to normal industrial standards with enhancements to the design such as nonsparking wheels and motors. This protects against the risk of ignition of any hydrogen in the room.

Redundant fans are included with the provision of standby AHUs in the switchgear room, equipment room, MSIV compartment, and valve/piping penetration room HVAC subsystems. This redundancy provides further confidence that the fans will be able to deliver the reliability required to ensure that the VXS meets its safety functions. No redundancy is provided for the standby electrical system battery room exhaust fans. This is appropriate because the fans provide a Category C safety function, and the hydrogen levels are monitored.

The fan motors and their lubricants are designed to withstand the environmental effects over the design life of the plant. The battery room fans are provided with direct-driven motors, as are the AHU fans and self-lubricating seal bearings, to minimise maintenance effort.

Conceivable failure modes for these types of fans include, for example, a failed bearing, excessive vibration, etc. Such mechanical failures are avoidable with appropriate maintenance and can be readily detected and rectified. MCR operators will be alerted to failure of any of the fans, which will enable them to take appropriate action.

Maintenance will be carried out in line with the manufacturer's information. There is extensive experience of operating this type of fan, which gives confidence that if they are adequately maintained, they will have good reliability in service.

23.12.4.2 Cooling Coils

The highest classification of cooling coils is Class 3. The coils are to be designed and manufactured to normal industrial standards that are suitable for Class 3 equipment.

Redundant cooling coils are included with the provision of standby AHUs in the switchgear room, equipment room, MSIV compartment and valve/piping penetration room HVAC subsystems. This redundancy provides further confidence that the cooling coils will be able to deliver the reliability required to ensure the VXS meets its safety functions.

Possible failure mechanisms include:

- Failure of the chilled water control valves. If the control valves on a cooling coil fails and the room temperature start to rise, this would be detected by the room temperature sensor and the standby AHU would be started.

- Failure of the complete chilled water system. If chilled water is lost to both AHUs of the switchgear room and equipment room HVAC subsystems, the subsystems may be operated in a once-through mode to maintain air circulation. The VXS system specification document (Reference 23.40, Section 4.3) identifies that, in this mode of operation, design indoor temperatures may not be capable of being maintained, based on the outdoor temperature. Some operations may have to be suspended in the affected areas.

  If chilled water is lost to both AHUs in each MSIV compartment HVAC subsystem and the valve/piping penetration room HVAC subsystem, then the design indoor temperatures may not be capable of being maintained. The operators will be notified of a rise in room temperature. Temporary ventilation or cooling may be required to control area temperature until heat loads in the areas can be reduced or chilled water is restored (Reference 23.40, Section 4.3).

- Structural failure of the coils resulting in a significant leak of chilled water. The use of suitable design standards and appropriate in service maintenance is deemed sufficient to reduce the risk of structural failure of the cooling coils.

Maintenance will be carried out in line with the manufacturer's information. There is extensive experience of operating this type of cooling coil to give confidence that if they are adequately maintained, they will have a good reliability in service.

23.12.4.3 Heating Coils

The highest classification of heating coils is Class 3. The coils are to be designed and manufactured to normal industrial standards that are suitable for Class 3 equipment.

Redundant heating coils are included with the provision of standby AHUs in the switchgear room, equipment room, and valve/piping penetration room HVAC subsystems. This redundancy provides further confidence that the heating coils will be able to deliver the reliability required to ensure the VXS meets its safety functions.

Possible failure mechanisms include:

- Failure of the heating coil dampers. Each AHU has a low temperature controller located in its discharge ductwork or in the area served. A fall in discharge temperature would be detected if the heating coil damper fails. The MCR would be notified and the standby AHU could be started.

- Failure of the complete hot water system. If hot water is lost to both AHUs of the switchgear room and equipment room HVAC subsystems and the room temperature was above the minimum room design temperature, the system may be operated in a normal manner; however, design area temperatures may not be maintained. In extreme ambient conditions, if the room temperature fell below the minimum room design temperature, the subsystems would have to be shut down and operations in the area served may need to be suspended (Reference 23.40, Section 4.3).

  If hot water is lost to the valve/piping penetration room HVAC subsystem and the temperature stays above the minimum room temperature, the subsystem can continue to operate normally. In extreme ambient conditions, if the room temperature falls below the minimum room temperature, the MCR will be notified and temporary heating may be required (Reference 23.40, Section 4.3).

- Structural failure of the coils resulting in a significant leak of hot water. The use of suitable design standards and appropriate in service maintenance is deemed sufficient to reduce the risk of structural failure of the heating coils.

Maintenance will be carried out in line with the manufacturer's information. There is extensive experience of operating this type of heating coil to give confidence that if they are adequately maintained, they will have good reliability in service.

23.12.4.4 Combination Fire/Smoke Dampers

The design of combination fire/smoke damper used in the AP1000 Design actuates in response to one of two signals: direct heat from a fire, or upon receipt of a smoke signal from one of the area smoke detectors. For the damper to close in response to heat from a fire, it does not require any external power source or actuation signals. This provides a high degree of inherent safety and high reliability. The fire load in the served areas will be kept to a minimum to reduce the risk and potential size of a fire. This also contributes to the inherent safety of the system.

The highest classification of fire/smoke dampers is Class 3. The dampers are to be designed and manufactured to normal industrial standards that are suitable for Class 3 equipment.

The combination fire/smoke dampers fail closed using a spring mechanism. Any failure that causes the fire/smoke damper to close is a failure to safety because the fire barrier will be maintained. The only conceivable failure to an unsafe position is if the damper was to seize or jam in the open position.

Maintenance will be carried out in line with the manufacturer's information. There is extensive experience of operating this type of damper to give confidence that if they are adequately maintained, they will not seize or jam and will move to the closed position when required.

23.12.4.5 Fire Dampers

The design of fire damper used in the AP1000 design does not require any external power source or actuation signals. Actuation is achieved by heat from the air in the duct melting the fusible link and the spring mechanism closing the damper. Additionally some VXS fire dampers are provided with position indication. This provides a high degree of inherent safety and high reliability. The fire load in the served areas will be kept to a minimum to reduce the risk and potential size of a fire. This also contributes to the inherent safety of the system.

The highest classification of fire dampers is Class 3. The dampers are to be designed and manufactured to normal industrial standards that are suitable for Class 3 equipment.

Any failure that causes the fire damper to close is a failure to safety because the fire barrier will be maintained. The only conceivable failure to an unsafe position is if the damper was to seize or jam in the open position.

Maintenance will be carried out in line with the manufacturer's information. There is extensive experience of operating this type of damper to give confidence that if they are adequately maintained, they will not seize or jam and will move to the closed position when the temperature rises above the specified point.

23.13 TURBINE BUILDING VENTILATION SYSTEM

23.13.1 Role

The VTS consists of the following subsystems:

- General area heating and ventilation
- Local area heating and ventilation
- Electrical equipment, south bay equipment, and personnel work area HVAC

The general area and local area heating and ventilation subsystems do not provide a primary nuclear safety function and, therefore, are not discussed in this section. The electrical equipment, south bay equipment, and personnel work area HVAC subsystem are subdivided into three independent HVAC systems. The south bay HVAC subsystem is the only VTS subsystem that supports Class 2 systems.

The south bay equipment HVAC system serves the component cooling water system (CCS) pumps, SG blowdown system (BDS) pumps, reactor coolant pumps' variable frequency drive power converter areas, the EDS battery room and the PLS through the provision of cooling and ventilation to equipment/components.

The VTS is supported by the ECS for electrical power, the PLS for control signals, the VWS and the VYS for chilled and hot water, respectively.

Further design details of this system and its constituent components are delineated in Reference 23.41 and Chapter 6.

23.13.1.1 South Bay Equipment Subsystem

The safety function of the south bay equipment HVAC subsystem is to support the CCS system through the provision of ventilation cooling and exhausting potential hydrogen build-ups in the battery room.

The subsystem consists of two 50-percent AHUs with integral supply fans, and cooling and heating coils. Fire dampers are installed at ductwork penetrations through fire barriers to the CCS rooms.

The south bay equipment HVAC subsystem is supported by the FPS that shuts the fire/smoke dampers on detection of fire in the served areas, the PLS that provides control functions, the ZOS to provide standby power to the VXS in the event of loss of offsite power, and the VWS and VYS for chilled and hot water, respectively.

23.13.2 System Components and Equipment Contributing to Safety Function

- **Supply and exhaust air fans** – The supply and exhaust fans are centrifugal type, single-width single-inlet, or double-width double-inlet, with high-efficiency wheels. Most of the fans have backward-inclined blades to produce nonoverloading characteristics. However, those fans installed in AHUs that have little or no ductwork may utilise forward curved blades. The fan operating conditions will be selected to ensure smooth stable operation over the specified operating range without fan surging or instability. The fans are isolated from the AHU casing with spring-type vibration isolators. The fans are designed and rated in accordance with SMACNA, ANSI/AMCA Standards 210 (Reference 23.9), 211 (Reference 23.10), and 300 (Reference 23.11).

  In addition, the exhaust fans from the battery rooms in the equipment room HVAC subsystem have nonsparking wheels.

  The fans in the south bay equipment HVAC subsystem AHUs are required to operate to provide long-term cooling to the CCS equipment.

  The battery room exhaust air fan in the south bay equipment room HVAC subsystem is required to operate to prevent the build-up of hydrogen in the battery rooms in the long term.

  All the fans operate in response to signals from the PLS that include flow rate, temperature, and fire protection signals. Provision of the required supply and extract airflows do not contribute to maintaining nuclear safety as determined by the safety case and the supply and exhaust fans are class GNS equipment.

- **Cooling coils** – The chilled water cooling coils are counterflow, finned-tubular type. Each cooling coil is constructed with tubes and fins. Large cooling coil banks that are constructed from multiple cooling coils are provided with coil holding racks designed to allow each coil to be independently removed (side pull) from the housing. The cooling coils are designed and rated in accordance with ASHRAE 33 (Reference 23.23) and ANSI/ARI 410 (Reference 23.22).

  The cooling coils in the ventilation subsystems obtain a flow of cooling water through activation of the chilled water control valves in response to signals from the PLS. The flow of cooling water through the tubes and maintain an adequate surface for heat transfer between the air and cooling water do not contribute to maintaining nuclear safety as determined by the safety case and the cooling coils are class GNS equipment.

- **Fire dampers** – The fire dampers are constructed of galvanised carbon steel and actuated by fusible links designed to melt and release the damper blades when the air temperature reaches 74°C (165°F). The damper blades close via a spring mechanism. The fire dampers meet the design, testing, and installation requirements of UL 555 (Reference 23.18).

  The fire dampers are passive components operated by temperature and a spring mechanism. As such, no actuation signal is required. The fire dampers are essential to maintain the integrity of fire barriers discussed in the internal fire hazard section in Chapter 11. The functional requirement is that they are rated to be at least equal to the fire barrier that they penetrate, up to a maximum 3-hour rating.

23.13.3 Claims on Components and Equipment

23.13.3.1 Supply and Exhaust Air Fans

- The supply and exhaust air fans in the south bay equipment HVAC subsystem AHUs support operation of the CCS. The CCS supports a number of Category A safety functions and therefore provides a Category A safety function (see Chapter 17 and Appendix 15A). The CCS pumps and equipment have a defence in depth role and are classified as Class 2 equipment. The south bay equipment HVAC system does not contribute to maintaining nuclear safety as determined by the safety case and thus is classified as class GNS equipment.

  There are two 50-percent-capacity AHUs in the south bay equipment HVAC subsystem. The AHUs are sized so that one of the AHUs can cool both operating pumps. It is claimed that the fan in one of the AHUs will start on demand and continue to operate to provide cooling to the CCS equipment.

- The battery room exhaust fan in the south bay equipment HVAC subsystem prevents the build-up of hydrogen in the battery room. Significant build-up can only occur during charging, when ac electrical power is available. At that point in time, the batteries are not required to operate. As such, the battery room exhaust fans do not contribute to maintaining nuclear safety as determined by the safety case. Hydrogen detectors are used in battery rooms to protect against hydrogen build-up by alerting operators that hydrogen levels are building. Also, the volume of air in the battery rooms provides a delay between the failure of the exhaust fans and the hazard developing. The exhaust fans do not contribute to maintaining nuclear safety as determined by the safety case and are therefore GNS equipment. See Appendix 15A. The fans will operate to help prevent the build-up of hydrogen in the battery rooms when the batteries are being charged.

23.13.3.2 Cooling Coils

The cooling coils provide the same contribution to safety as the AHU fans discussed above (Section 23.12.3.1). For the same reasons, the cooling coils in the subsystems of the VTS under discussion do not contribute to maintaining nuclear safety as determined by the safety case. Thus, all the cooling coils are class GNS equipment. See Appendix 15A.

There are two 50-percent-capacity AHUs, with one cooling coil bank in each AHU. Only one AHU is required to operate to cool the CCS equipment. It is claimed that the chilled water control valves in one of the AHUs per subsystem will modulate to control the flow of chilled water and will, therefore, provide the cooling required to the served areas.

23.13.3.3 Fire Dampers

The fire dampers protect against fire hazards that could, as part of a sequence of failures, result in loss of a safety function. This could compromise normally operating systems and safety systems delivering a specific function. Therefore, this is a Category B safety function. See Appendix 15A. As the fire dampers provide a contribution to achieving this safety function, they are deemed to be Category B Class 3 equipment. See Appendix 15A.

Single fire dampers are provided where the ducts pass through a fire barrier. It is claimed that the fire dampers will close when the air temperature in the duct reaches the design limit and maintain the integrity of the fire barrier.

23.13.4 Justification of Claims on Components and Equipment

23.13.4.1 Supply and Exhaust Air Fans

The fan design for subsystems with a significant amount of ductwork includes backward-inclined blades to produce nonoverloading characteristics. This will prevent overpressurisation of the ventilation distribution system if a damper in the system inadvertently closes. This is an inherently safe design feature and provides a high degree of confidence in maintaining the integrity of the ventilation system.

A hydrogen detector protects against hydrogen build-up by alerting operators that hydrogen concentrations are increasing. Also, the volume of air in the battery room effectively provides a delay between the failure of the exhaust fans and the hazard developing to permit operator intervention.

The highest classification of supply and return/exhaust air fans in the VTS AHUs is Class GNS equipment. The fans are to be designed and manufactured to normal industrial standards that are suitable for Class GNS equipment.

The battery room exhaust fan is also Class GNS equipment. It is designed and manufactured to normal industrial standards with enhancements to the design such as nonsparking wheels. This protects against the risk of ignition of any hydrogen in the room.

Multiple fans are included with the provision of pairs of AHUs in the south bay equipment area. This provides further confidence that the fans will be able to deliver the reliability required to ensure that the VTS meets its safety functions. No redundancy is provided for the electrical system battery room exhaust fan. This is appropriate because the fans do not contribute to maintaining nuclear safety as determined by the safety case, and the hydrogen levels are monitored.

The fan motors and their lubricants are designed to withstand the environmental effects over the design life of the plant. The battery room fan is provided with a direct-driven motor.

Conceivable failure modes for these types of fans include, for example, a failed bearing, excessive vibration. Such mechanical failures are avoidable with appropriate maintenance and can be readily detected and rectified. MCR operators will be alerted to failure of any of the fans, which will enable them to take appropriate action.

Maintenance will be carried out in line with the manufacturer’s information. There is extensive experience in operating these fans, which gives confidence that if they are adequately maintained, they will have good reliability in service.

23.13.4.2 Cooling Coils

The highest classification of cooling coils is Class GNS equipment. The coils are to be designed and manufactured to normal industrial standards that are suitable for Class 3 equipment.

Multiple cooling coils are included with the provision of multiple AHUs in the south bay equipment HVAC subsystems. This redundancy provides further confidence that the cooling coils will be able to deliver the reliability required to ensure the VTS meets its safety functions.

Possible failure mechanisms include:

- Failure of the chilled water control valves. If the control valve on a cooling coil fails and the room temperature starts to rise, this would be detected by the room temperature sensor.

- Failure of the complete chilled water system. If chilled water is lost to both AHUs of the south bay HVAC subsystem, the subsystems may be operated to maintain air circulation. The VTS system specification document (Reference 23.41, Section 4.3) identifies that, in this mode of operation, design indoor temperatures may not be capable of being maintained, based on the outdoor temperature. CCS pump operation will be maintained because the pump motor will operate at temperatures well above the room design temperature.

- Structural failure of the coils resulting in a significant leak of chilled water. The use of suitable design standards and appropriate in-service maintenance is deemed sufficient to reduce the risk of structural failure of the cooling coils.

Maintenance will be carried out in line with the manufacturer's information. There is extensive experience in operating this type of cooling coil to give confidence that if they are adequately maintained, they will have a good reliability in service.

23.13.4.3 Fire Dampers

The design of the fire damper used in the AP1000 design does not require any external power source or actuation signals. Actuation is achieved by heat from the air in the duct melting the fusible link and the spring mechanism closing the damper. This provides a high degree of inherent safety and high reliability. The fire load in the served areas will be kept to a minimum to reduce the risk and potential size of a fire. This also contributes to the inherent safety of the system.

The highest classification of fire dampers is Class 3. The dampers are to be designed and manufactured to normal industrial standards that are suitable for Class 3 equipment.

Any failure that causes the fire damper to close is a failure to safety because the fire barrier will be maintained. The only conceivable failure to an unsafe position is if the damper were to seize or jam in the open position.

Maintenance will be carried out in line with the manufacturer's information. There is extensive experience in operating this type of damper to give confidence that if the dampers are adequately maintained, they will not seize or jam and will return to the closed position when the temperature rises above the specified point.

23.14 DIESEL GENERATOR BUILDING HEATING AND VENTILATION SYSTEM

23.14.1 Role

The primary safety function of the VZS is in support of the safety systems housed within the diesel generator building through maintaining appropriate temperature ranges and removing combustible vapours.

The system consists of the following four subsystems:

- Normal heating and ventilation
- Standby exhaust ventilation
- Fuel oil day tank vault exhaust
- Diesel oil transfer module enclosures ventilation and heating

Further design details of this system and its constituent components are delineated in Reference 23.42 and Chapter 6.

23.14.1.1 Normal Heating and Ventilation Subsystem

The safety function of the normal heating and ventilation subsystem is to maintain the ambient temperature of the diesel generator rooms within appropriate limits when the diesel generators are not operating. This is to ensure that the diesel generators will be able to start on demand. The subsystem also supports the equipment in the electrical equipment service module through maintenance of the ambient temperature during normal operation and when the diesel generators are operating.

There are two diesel generator rooms, and the system makes provision for one AHU per engine room. Cooling is provided by the supply of outside air (there are no cooling coils in the AHUs), while heating is provided by two electric unit heaters in each engine room. This allows the maintenance of the design minimum room temperature with a single heater operating except at extremely low design temperatures. The minimum design room temperature is based on personnel comfort for maintenance operations and higher than temperatures that will affect diesel generator operation.

One supply AHU is provided for each electrical equipment service module. Cooling is provided by the supply of outside air (there are no cooling coils in the AHUs), and heating is provided by an electric heating coil in the AHU.

The normal heating and ventilation subsystem is supported by the PLS.

The normal heating and ventilation subsystem supports the ZOS by maintaining the initial temperature of the diesel generators at start-up and maintaining the temperature of the ZOS electrical equipment.

23.14.1.2 Standby Exhaust Ventilation Subsystem

The safety function of the standby exhaust ventilation subsystem is to maintain the ambient temperature of the diesel generator rooms within appropriate limits when the diesel generators are operating.

The subsystem consists of two 50-percent-capacity roof mounted exhaust fans per engine room, and one or both fans are required to operate to maintain the room temperature

depending on outdoor ambient temperatures. The subsystem also includes motor-operated air intake dampers mounted in the exterior walls of the rooms.

The standby exhaust ventilation subsystem is supported by the PLS.

The standby exhaust ventilation subsystem supports the ZOS by maintaining the temperature of the diesel generators during operation.

23.14.1.3 Fuel Oil Day Tank Vault Exhaust Subsystem

The safety function of the fuel oil day tank vault exhaust subsystem is to prevent the build-up of a hazard by continuously exhausting combustible vapour from the fuel oil day tank vault.

The subsystem consists of one centrifugal exhaust fan for each vault, with the openings into and out of the vault protected by fire dampers.

The fuel oil day tank vault exhaust subsystem is supported by the PLS.

The fuel oil day tank vault exhaust subsystem supports the ZOS by preventing the build-up of combustible vapours that could affect operation of the ZOS.

23.14.1.4 Diesel Oil Transfer Module Enclosures Ventilation and Heating Subsystem

The safety function of the diesel oil transfer module enclosures ventilation and heating subsystem is to maintain the ambient temperature of the enclosures within appropriate limits.

The system consists of one roof fan and one electric unit heater per enclosure.

The diesel oil transfer module enclosures ventilation and heating subsystem is supported by the PLS.

The diesel oil transfer module enclosures ventilation and heating subsystem supports the standby diesel and auxiliary boiler fuel oil system (DOS) by maintaining the temperature of the diesel oil transfer module enclosures.

23.14.2 System Components and Equipment Contributing to Safety Function

Ductwork, duct supports, and accessories are constructed of galvanised steel. Ductwork subject to fan shutoff pressure is structurally designed for fan shutoff pressures. Ductwork, supports, and accessories meet the design and construction requirements of SMACNA Rectangular and Round Industrial Duct Construction Standards (References 23.13 and 23.14) and SMACNA HVAC Duct Construction Standards – Metal and Flexible (Reference 23.15).

Multi-blade, two-position shutoff remotely operated dampers are parallel-blade type. Multi-blade, control and balancing dampers are opposed-blade type. Backdraft dampers are provided to prevent backflow through shut down exhaust fans and to relieve pressure from the service module and diesel generator building. Dampers meet the performance requirements of ANSI/AMCA Standard 500 (Reference 23.12).

The following components make key contributions to the ability of the VZS to perform its safety function.

- **Supply and exhaust fans** – These are centrifugal type, single-width single-inlet, or double-width double-inlet, with high-efficiency wheels and backward-inclined blades to

produce nonoverloading characteristics. The fans are designed and rated in accordance with ANSI/AMCA Standards 210 (Reference 23.9), 211 (Reference 23.10), and 300 (Reference 23.11). In addition, the VZS system specification document identifies that the fuel oil day tank vault exhaust fans will have nonsparking wheels and motors (Reference 23.42, Section 5.1).

The electrical equipment service room AHU supply fans and fuel oil day tank vault exhaust fans operate in response to manual signals from the PLS and are required to operate to maintain the temperature in the electrical equipment service rooms and prevent the build-up of combustible vapours. These fans are Category C Class 3 equipment.

Failure of the fans in the engine room AHUs would only lead to an increase in temperature if there were very warm ambient conditions. If this happens, the standby exhaust fans would be initiated when the temperature reached a preset upper limit thus maintaining the temperature in the engine room. As such, no further analysis is required for the engine room AHU supply fans.

- **Electric heating coils** – These are finned tubular type with wire heating element embedded within a protective metal sheath. Coils will be wired for multiple stages, with each stage arranged across the full face of the coils (Reference 23.42, Section 5.1). The electric heating coils meet the requirements of UL 1995 for heating and cooling equipment (Reference 23.43).

  The heating coils operate in response to room temperature and fan operation status signals from the PLS. The heating coils are required to operate to maintain the temperature in the electrical equipment service modules within the preset limits. These electric heating coils are Category C Class 3.

- **Roof exhaust fans** – The roof exhaust fans in the standby exhaust ventilation subsystem are roof mounted, direct drive upblast ventilators. The diesel oil transfer module enclosure exhaust fans are direct driven fan roof ventilators. Both fan types are equipped with gravity dampers that open when the fan operates and close when the fan is shut down. The standby exhaust ventilation subsystem fans' dampers provide weather-tight closures when the fan is shut down to prevent the entry of rain or snow.

  The standby exhaust ventilation subsystem fans operate in response to temperature or diesel generator operation signals from the PLS. The diesel oil transfer module enclosure exhaust fans operate in response to temperature signals from the PLS. The roof exhaust fans in both subsystems are designed to Class 3 as they are the principal means to maintain the temperature in the engine rooms and diesel oil transfer module enclosures below the predetermined upper limit which is a Category C safety function.

- **Electric unit heaters** – these are horizontal single-stage or two-stage finned tubular type with adjustable louvers to direct discharge air down. Heating coils will consist of aluminium-finned copper-clad steel sheath elements. The electric unit heaters are UL-listed and meet the requirements of UL 1996 (Reference 23.36) and the National Electric Code (Reference 23.37). Unit heaters are of conventional, commercially available construction. (Reference 23.42, Section 5.1).

  Local space thermostats turn the unit heaters on and off as required for temperature control. The electric unit heaters therefore have a safety function to operate to maintain the temperature in the diesel oil transfer module enclosures above the predetermined

lower limit. The engine room unit heaters are non-safety since they are not required to support the diesel engine starting or operation.

- **Fire dampers** – these are provided at duct penetrations through fire barriers to maintain the fire resistance rating of the barriers. The fire dampers are constructed of galvanised carbon steel and are actuated by fusible links designed to melt and release the damper blade when the air temperature reaches 74°C (165°F). The damper blades close via a spring mechanism. The fire dampers meet the design, testing, and installation requirements of UL 555 (Reference 23.18).

  The fire dampers are essential to maintain the integrity of fire barriers discussed in the internal fire hazard section in Chapter 11. The fire dampers are passive components operated by temperature and a spring mechanism. As such, no actuation signal is required. The fire dampers are designed to Class 3 as they are the principal means of a fire damper rating will be at least equal to the fire barrier that they penetrate, up to a maximum 3-hour rating which is a Category B safety function.

23.14.3 Claims on Components and Equipment

23.14.3.1 Supply and Exhaust Fans

- The fuel oil day tank vault exhaust fans support the operation of the diesel generators. Failure of the fuel oil day tank vault exhaust fans does not directly affect operation of the diesel generators; they do reduce the chance of a fuel fire, so they provide a Category C safety function. Similarly, the fuel oil day tank vault exhaust fans are classified as Category C Class 3 equipment. See Appendix 15A.

  There is one exhaust fan provided for each fuel oil day tank vault. It is claimed that each exhaust fan will continue to operate to prevent the build-up of combustible vapours.

- The electrical equipment service module AHU supply fans support operation of the diesel generators. However, failure of the fans will not lead to the loss of function of the diesel generators. Temperature sensors in the service module would alert MCR personnel if the room temperature started to rise above pre-set limits. This would allow them to take appropriate action to ensure that the room temperatures did not compromise diesel generator operation. Failure of the electrical equipment service module AHU supply fans may reduce electrical cabinet safety margins but would not lead to a DBA and, therefore, the supply fans provide a Category C safety function. The electrical equipment service module AHU supply fans provide a minor contribution to nuclear safety and are Category C Class 3 equipment.

  There is one supply fan provided for each electrical equipment service module. It is claimed that each supply fan will continue to operate to maintain the electrical equipment within its design temperature limits.

23.14.3.2 Electric Heating Coils

The electric heating coil in the electrical equipment service module AHU supports the operation of the diesel generators. However, failure of the heating coil will not lead to the loss of function of the electrical equipment and diesel generators. Temperature sensors in the service module would alert MCR personnel if the room temperature started to fall below pre-set limits and allow them to take appropriate action to ensure the room temperature did not compromise electrical equipment and diesel generator operation. Failure of the electric

heating coil will not reduce safety margins and would not lead to a DBA. Therefore, the heating coil provides a Category C safety function. See Appendix 15A. The electric heating coil provides a contribution to nuclear safety and is Class 3 equipment. See Appendix 15A.

One electric heating coil is provided in the electrical equipment service module AHU. It is claimed that the electric heating coil will start on demand and continue to operate to maintain the electrical equipment within its design temperature limits.

23.14.3.3 Roof Exhaust Fans

- The standby exhaust ventilation subsystem fans support the operation of the diesel generators. Failure of the standby exhaust fans may affect operation of the diesel generators. Therefore, they support the diesel generator and provide a Category C safety function and are Category C Class 3 equipment. See Appendix 15A.

  There are two standby exhaust ventilation subsystem fans in each engine room. Both standby exhaust fans may be required to operate depending on the outside air temperature. It is claimed that each standby exhaust fan will start on demand and continue to operate to maintain the maximum temperature in the engine rooms within the design limits during diesel generator operation.

- The diesel oil transfer module enclosure exhaust fans support operation of the diesel generators. However, failure of the fans will not lead to the loss of function of the diesel generators. Temperature sensors in the diesel oil transfer module enclosures would alert MCR personnel if the room temperature started to rise above pre-set limits. This would allow them to take appropriate action to ensure that the room temperatures did not compromise diesel generator operation. Failure of the diesel oil transfer module enclosure exhaust fans will not reduce safety margins; therefore, the exhaust fans provide a Category C safety function. See Appendix 15A. The diesel oil transfer module enclosure exhaust fans provide a minor contribution to nuclear safety and are Category C Class 3 equipment. See Appendix 15A.

  There is one roof exhaust fan provided in the each diesel oil transfer module enclosure. It is claimed that each roof exhaust fan will start on demand and continue to operate to deliver its safety function.

23.14.3.4 Electric Unit Heaters

The electric unit heaters in the diesel oil transfer module enclosures support operation of the diesel generators. However, failure of the unit heaters will not inevitably lead to the loss of function of the diesel generators. Temperature sensors in the engine rooms and diesel oil transfer module enclosures would alert MCR personnel if the room temperature started to fall below pre-set limits. This would allow them to take appropriate action to ensure the room temperatures did not compromise diesel generator operation. Failure of the electric unit heaters will not reduce safety margins; therefore, the unit heaters provide a Category C safety function. See Appendix 15A. The electric unit heaters provide a minor contribution to nuclear safety and are Category C Class 3 equipment. See Appendix 15A.

One electric unit heater is provided in each diesel oil transfer module enclosure. It is claimed that each diesel oil transfer electric unit heater will start on demand and continue to operate to deliver its safety function.

23.14.3.5 Fire Dampers

The fire dampers protect against fire hazards that could, as part of a sequence of failures, result in loss of a safety function. This could compromise normally operating systems and safety systems delivering a specific function. Therefore, this is a Category B safety function (Reference 23.17). As the fire dampers provide contribute to achieving this safety function, they are deemed to be Category B Class 3 equipment. See Appendix 15A.

Single fire dampers are provided where the ducts pass through a fire barrier. It is claimed that the fire dampers will close when the air temperature in the duct reaches the design limit and maintain the integrity of the fire barrier.

23.14.4 Justification of Claims on Components and Equipment

23.14.4.1 Supply and Exhaust Fans

The fan design includes backward-inclined blades to produce non-overloading characteristics. This will prevent over pressurisation of the ventilation distribution system if a damper in the system closes. This is an inherently safe design feature and provides a high degree of confidence in maintaining the integrity of the ventilation system.

The highest classification of supply and exhaust air fans is Class 3. The fans are to be designed and manufactured to normal industrial standards that are suitable for Class 3 equipment. In addition, the fuel oil day tank vault exhaust fans will have nonsparking wheels and motors to minimise the risk of ignition in the vaults.

Conceivable failure modes for this type of fan include, for example, a failed bearing, failed drive belt, etc. These types of mechanical failures are avoidable with appropriate maintenance and can be readily detected and rectified. Also, the fan design will require grease fittings for rotating equipment to be located outside the equipment casing to avoid temporary shutdown of equipment to lubricate bearings or self-lubricating sealed bearings to be used. Operators will be notified of any fan failure by the system to allow them to take appropriate action.

Maintenance will be carried out in line with the manufacturer's information. There is extensive experience of operating this type of fan, providing confidence that if they are adequately maintained, they will have good reliability in service.

23.14.4.2 Electric Heating Coils

The electric heating coil is classified as Class 3 equipment. The heating coil is to be designed and manufactured to normal industrial standards that are suitable for Class 3 equipment.

Failure of the electric heating coil will not lead to an immediate loss of diesel generator function. The operators would be alerted to heating coil failure and a reduction in temperature of the electrical equipment service module below pre-set limits. This would enable them to take appropriate action to ensure the electrical equipment and diesel generators can maintain their safety function.

Maintenance will be carried out in line with the manufacturer's information. There is extensive experience of operating this type of electric heating coil to give confidence that if they are adequately maintained they will have a good reliability in service.

23.14.4.3 Roof Exhaust Fans

The standby exhaust ventilation subsystem fans and the diesel oil transfer module enclosure exhaust fans are classified as Class 3. The fans are to be designed and manufactured to normal industrial standards that are suitable for Class 3 equipment.

2- x 50-percent standby exhaust ventilation subsystem fans are included in each engine room such that a degree of cooling will still be provided if one fan fails. The requirement for operation of both fans is dependent on ambient air temperatures. This provides further confidence that the standby ventilation subsystem exhaust fans will be able to deliver the cooling required ensuring the VZS meets its safety functions. Redundancy is not included with the diesel oil transfer module enclosure exhaust fans. This is appropriate as they provide a Category C safety function.

Conceivable failure modes for this type of fan include, for example, a failed bearing or excessive vibration. These types of mechanical failures are avoidable with appropriate maintenance and can be readily detected and rectified. Also, the standby exhaust ventilation subsystem fan design will require extended lube lines to be provided for bearing lubrication wherever applicable or self-lubricating sealed bearings to be used. Operators will be notified of any fan failure by the system to allow them to take appropriate action.

Maintenance will be carried out in line with the manufacturer's information. There is extensive experience of operating these types of fans, designed and constructed to similar standards, to give confidence that if they are adequately maintained, they will have good reliability in service.

23.14.4.4 Electric Unit Heaters

The electric unit heaters in the engine rooms and the diesel oil transfer module enclosures are classified as Class 3 equipment. The heaters are to be designed and manufactured to normal industrial standards that are suitable for Class 3 equipment.

Failure of the diesel oil transfer unit heaters will not lead to an immediate loss of diesel generator function. The operators would be alerted to unit heater failure and a reduction in temperature of a diesel oil transfer module enclosure below pre-set limits. This would enable them to take appropriate action to ensure that the diesel generators can maintain their safety function.

Maintenance will be carried out in line with the manufacturer's information. There is extensive experience of operating this type of electric unit heaters to give confidence that if they are adequately maintained, they will have good reliability in service.

23.14.4.5 Fire Dampers

The design of fire damper used in the VZS does not require any external power source or actuation signals. Actuation is achieved by heat from the air in the duct melting the fusible link and the spring mechanism closing the damper. This provides a high degree of inherent safety and high reliability. The ignition sources in the fuel oil day tank vaults are minimised with the requirement for the exhaust fans to have nonsparking wheels and motors. This also contributes to the inherent safety of the system.

The highest classification of fire dampers is Class 3. The dampers are to be designed and manufactured to normal industrial standards that are suitable for Class 3 equipment.

Any failure that causes the fire damper to close is a failure to safety because the fire barrier will be maintained. The only conceivable failure to an unsafe position is if the damper was to seize or jam in the open position.

Maintenance will be carried out in line with the manufacturer's information. There is extensive experience of operating this type of damper to give confidence that if they are adequately maintained, they will not seize or jam and will move to the closed position when the temperature rises above the specified point.

23.15 REFERENCES

23.1 NVF/DG001, Issue 1, "An Aid to the Design of Ventilation of Radioactive Areas," Nuclear Industry Safety Directors Forum, January 2009.

23.2 IAEA NS-G-1.13, "Radiation Protection Aspects of Design for Nuclear Power Plants," International Atomic Energy Agency, November 2005.

23.3 Westinghouse Report APP-VCS-M3-001, Rev. 0, "Containment Recirculation Cooling System (VCS); System Specification Document," August 2015.

23.4 ASME Boiler and Pressure Vessel Code, Section III, Div. 1, "Rules for Construction of Nuclear Facility Component," American Society of Mechanical Engineers, 1998, 2000 Addenda.

23.5 Westinghouse Report APP-VFS-M3-001, Rev. 1, "Containment Air Filtration System, System Specification Document," September 2015.

23.6 ASME/ANSI AG-1, "Code on Nuclear Air and Gas Treatment," American Society of Mechanical Engineers/American National Standards Institute, December 1997.

23.7 NRC Regulatory Guide 1.140, Rev. 2, "Design, Inspection, and Testing Criteria for Air Filtration and Adsorption Units of Normal Atmosphere Cleanup Systems in Light-Water-Cooled Nuclear Power Plants," U.S. Nuclear Regulatory Commission, June 2001.

23.8 NRC IE Bulletin 80-03, "Loss of Charcoal from Standard Type II, 2 inch, Tray Adsorber Cells," U.S. Nuclear Regulatory Commission, February 1980.

23.9 ANSI/AMCA Standard 210, "Laboratory Method of Testing Fans for Certified Aerodynamic Performance Rating," American National Standards Institute/Air Movement and Control Association, 1985.

23.10 ANSI/AMCA Standard 211, "Certified Ratings Program, Air Performance," American National Standards Institute/Air Movement and Control Association, 1987.

23.11 ANSI/AMCA Standard 300, "Reverberant Room Method for Sound Testing of Fans," American National Standards Institute/Air Movement and Control Association, 1985.

23.12 ANSI/AMCA Standard 500, "Methods of Testing Heavy Duty Dampers for Rating," American National Standards Institute/Air Movement and Control Association, 1989.

23.13 "Rectangular Industrial Duct Construction Standards," Sheet Metal and Air Conditioning Contractors' National Association, 1980.

23.14 "Round Industrial Duct Construction Standards," Sheet Metal and Air Conditioning Contractors' National Association, 1999.

23.15 "HVAC Duct Construction Standards – Metal and Flexible," Sheet Metal and Air Conditioning Contractors' National Association, 1985.

23.16 "HVAC Duct Leakage Test Manual," Sheet Metal and Air Conditioning Contractors' National Association, 1985.

23.17 ASME N510, "Testing of Nuclear Air-Treatment Systems," American Society of Mechanical Engineers, 1989.

23.18 ANSI/UL 555, "Fire Dampers," American National Standards Institute/ Underwriters Laboratories, 1999.

23.19 Westinghouse Report APP-VUS-M3-001, Rev. 3, "**AP1000** Containment Leak Rate Test System - System Specification Document," August 2015.

23.20 Not Used.

23.21 NUREG/CR-6928, "Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants," U.S. Nuclear Regulatory Commission, February 2007.

23.22 ANSI/ARI 410, "Forced-Circulation Air-Cooling and Air-Heating Coils," American National Standards Institute/Air Conditioning and Refrigeration Institute, 1991.

23.23 ASHRAE 33, "Methods of Testing Forced Circulation Air Cooling and Air Heating Coils," American Society of Heating, Refrigeration and Air Conditioning Engineers, 1978.

23.24 Westinghouse Report APP-VLS-M3-001, Rev. 4, "Containment Hydrogen Control System: System Specification Document," February 2014.

23.25 ASME Boiler and Pressure Vessel Code, Section VIII, "Pressure Vessels," American Society of Mechanical Engineers, 2001, 2003 Addenda.

23.26 ASME Boiler and Pressure Vessel Code, Appendix 22, "Rules for Reinforcement of Cone-to-Cylinder Junction Under External Pressure," American Society of Mechanical Engineers, 2001, 2003 Addenda.

23.27 Westinghouse Report APP-VES-M3-001, Rev. 4, "Main Control Room Emergency Habitability System, System Specification Document," November 2014.

23.28 UL 586, "High-Efficiency, Particular, Air Filter Units," Underwriters Laboratories, 1996.

23.29 NRC Regulatory Guide 1.52, Rev. 3, "Design, Inspection, and Testing Criteria for Air Filtration and Adsorption Units of Post-Accident Engineered-Safety-Feature Atmosphere Cleanup Systems in Light-Water-Cooled Nuclear Power Plants," U.S. Nuclear Regulatory Commission, June 2001.

23.30 Westinghouse Report APP-VAS-M3-001, Rev. 0, "Radiologically Controlled Area Ventilation System, System Specification Document," March 2016.

23.31 Westinghouse Report APP-VRS-M3-001, Rev. 0, "Radwaste Building HVAC System, System Specification Document," October 2015.

23.32 Not Used.

23.33 Westinghouse Report APP-VBS-M3-001, Rev. D, "Nuclear Island Nonradioactive Ventilation System, System Specification Document," May 2008.

23.34 EPRI "Advanced Light Water Reactor Utilities Requirements Document," Volume III, Rev. 8, Electric Power Research Institute, March 1999.

23.35 NRC Information Notice 93-06, "Potential Bypass Leakage Paths Around Filters Installed in Ventilation Systems," U.S. Nuclear Regulatory Commission, January 1993.

23.36 UL 1996, "Electric Duct Heaters," Underwriters Laboratories, 1996.

23.37 NFPA 70, "National Electrical Code," National Fire Protection Association, 1999.

23.38 MSS SP-61, "Pressure Testing of Steel Valves," Manufacturers Standardisation Society, January 2003.

23.39 UL 555S, "Smoke Dampers," Underwriters Laboratories, 1999.

23.40 Westinghouse Report APP-VXS-M3-001, Rev. D, "Annex/Auxiliary Building Nonradioactive HVAC System, System Specification Document," May 2008.

23.41 Westinghouse Report APP-VTS-M3-001, Rev. 0, "Turbine Building Ventilation System (VTS) System Specification Document," July 2012.

23.42 Westinghouse Report APP-VZS-M3-001, Rev. B, "Diesel Generator Building HVAC System, System Specification Document," January 2009.

23.43 UL 1995, "Heating and Cooling Equipment," Underwriters Laboratories, 1995.

23.44 Westinghouse Report UKP-GW-GL-045, Rev. 2, "AP1000 Equivalence/Maturity Study of the U.S. Codes and Standards," September 2011.

23.45 Westinghouse Report APP-VHS-M3-001, Rev. B, "Health Physics and Hot Machine Shop HVAC System (VHS), System Specification Document," January 2009.

23.46 Westinghouse Report UKP-GW-GL-500, Rev. 0, "AP1000 Limits and Conditions Process Description," December 2015.

APPENDIX 23A
AP1000 NUCLEAR VENTILATION – COMPARISON WITH UK PRACTICE AND BEST AVAILABLE TECHNOLOGY ASSESSMENT

23A.1 COMPARISON WITH UK PRACTICE

The AP1000 plant ventilation systems are designed to US codes and standards. The design satisfies the UK practice as described in References 23.1 and 23.2. This is discussed further in Appendix 23A. A justification for the acceptability of United States standards for use in the UK is provided in UKP-GW-GL-045 (Reference 23.44).

The extracts from areas with the potential for radioactive discharges are individually continuously monitored and alarmed. In addition, the plant vent combined discharge is monitored and alarmed.

Reference 23.1 defines a classification scheme for working areas according to the potential for radioactive contamination, whether surface or airborne:

- White means a clean area free from radioactive contamination, whether surface or airborne.
- Green means an area that is substantially clean. Only in exceptional circumstances is airborne contamination such that provisions must be made for its control.
- Amber means an area in which some surface contamination is expected. In some cases, there will be a potential for airborne contamination such that provision must be made for its control.
- Red means an area in which contamination levels are so high that there is normally no access without appropriate respiratory protection.

While the detailed access controls for each area are meant for individual operators, the classification provides recommendations for the design of the associated ventilation systems.

No HEPA filtration is required on the extract for all white areas. HEPA filtration is expected on the extract for all red areas. For green and amber areas, the need for HEPA filtration must be reviewed as part of the plant hazard assessment, taking into account the potential for airborne release.

Reference 23.1 recognises that in cases where the ventilation discharge has little accidental discharge risk, cleanup systems are not always justified. During normal running, to avoid passing large amounts of air through HEPA filters (which are expensive to install, maintain, and dispose of after use), standby systems serving a number of areas could be brought into use for fault conditions. This is particularly the case when the radioactive materials are contained in high-quality primary containment. In the AP1000 plant, all active liquids and resins are contained within pipework, pumps, and tanks designed to standards suitable for the temperature and pressure involved, and that activity is thus contained.

UK practice is also described in Reference 23.2. Reference 23.2 provides the following guidance: “Particulate material from both the management system for gaseous waste and the ventilation systems should be removed using filters. It is a good practice to ensure that all gas discharged from the plant that may be radioactive passes through high efficiency filters.” Therefore, compliance with Reference 23.2 is only discussed for potentially radioactive

exhausts, i.e., areas classified as green, amber, and red following the guidance provided in Reference 23.1.

The potential for routine and accidental activity in the areas served by each of the AP1000 plant ventilation systems is reviewed below.

23A.1.1 Nuclear Island Nonradioactive Ventilation System

The VBS serves the MCR, control support area, 1E electrical spaces, and the PCS valve room, as described in Section 23.11. These areas do not have sources of activity present during normal operation or fault conditions.

In line with Reference 23.1, the area served by the VBS is classified as white for both normal and fault conditions, and as such there are no provisions made for exhaust HEPA filtration.

23A.1.2 Annex/Auxiliary Building Nonradioactive Ventilation System

The VXS serves the office areas, switchgear rooms, locker rooms, battery rooms, computer rooms, toilets, and other similar spaces, as described in Section 23.12. These areas do not typically have sources of radioactive contamination present during normal operation.

A drain line from the BDS to the liquid radwaste system (WLS) passes through the areas served by the VXS. The drain line can be contaminated by the BDS if there are 1) fuel leaks, 2) steam generator leakage, and 3) a radiation monitor failure or an isolation valve failure. Since the drain system has no valves or connections within the area served by the VXS and it is gravity-drained, the chance of leakage into the VXS area is negligible as there would need to be a pre-existing leak co-incident with a fault.

It is not reasonably foreseeable for activity to be present in the areas served by the VXS and hence, in line with Reference 23.1, the area is classified as white for both normal and fault conditions, and as such no provisions are made for HEPA filtration.

23A.1.3 Diesel Generator Building Heating and Ventilation System

The VZS supplies air to and exhausts from the diesel generator building, as described in Section 23.14. The diesel generator building is a physically separate building.

There is no credible source or fault that would result in a radioactive release from the diesel generator building and thus there is no normal or fault condition where a HEPA filter would reduce radioactive releases; hence, HEPA filtration is not provided. In line with Reference 23.1, the area served by the VZS is classified as white for both normal and fault conditions, and as such there are no provisions made for HEPA filtration.

23A.1.4 Containment Recirculation System

The VCS recirculates and cools air within the containment during power operations and shutdown, as described in Section 23.4. The recirculation of the containment air results in an energy savings and a reduction in waste generated in the form of used filters when compared with what would arise from the level of once-through HVAC ventilation system. The air recirculated by this system is expected to contain some activity (mostly noble gases and some iodine), although it does not penetrate the containment boundary and thus does not give rise to any discharges to atmosphere.

During shutdown operations in the containment, local, filtered extract systems are available for particular operations where airborne activity may be generated. This reduces the potential for airborne activity to be released into the general containment atmosphere, which the recirculation system could spread to other parts of the containment building.

The extracted air is continuously monitored for airborne activity that would give early warning to workers in the containment of the presence of airborne activity.

There is no path to discharge the VCS to the environment and hence HEPA filtration is not provided.

23A.1.5 Containment Air Filtration System

The VFS purges the containment by providing fresh air from outside and exhausting air to plant vent. The VFS also exhausts from areas served by the VAS and the VHS after receipt of a High radiation signal in the VAS or the VHS exhaust respectively, or from one of the area radiation monitors.

Each VFS train is equipped with HEPA filtration and charcoal filters for removal of particulate and iodine vapour respectively. A high-efficiency filter (80 percent ASHRAE) is installed before the HEPA filter to increase operational life and reduce the quantity of low-level waste (LLW). A high-efficiency filter has a greater capacity and therefore will require less frequent changing and thus potentially reduce volumes of LLW produced. A high-efficiency filter is also installed after the charcoal filter to ensure that discharges are ALARP. Continuous monitoring of airborne discharges is provided to detect deterioration in the performance of either ventilation train. These provisions represent good industry practice for ensuring that discharges to the atmosphere and doses to members of the public are ALARP.

In line with Reference 23.1, the containment is an amber area with a potential for occasional releases. It is therefore provided with full-time filtration on the exhaust. The design of the VFS complies also with the guidance provided in Reference 23.2.

23A.1.6 Health Physics and Hot Machine Shop HVAC System

The VHS supply air system consists of two 100-percent-capacity air handling units, consisting of a low-efficiency and a high-efficiency filter bank, heating and cooling coils, and a supply fan with automatic inlet valves. The exhaust air system consists of two 100-percent-capacity exhaust fans sized to allow the system to maintain negative pressure, as described in Section 23.10.

The hot machine shop provides a location within the controlled area for repair and refurbishment of items of equipment from within the controlled area, i.e., they may not actually be contaminated or activated but it is easier to have a dedicated workshop rather than undertaking clearance monitoring, which may not be possible. Operations in the hot machine shop are conventional hands-on work, i.e., there is no provision for remote handling. The routine arisings of airborne contamination from machining operations are not expected to be significant because equipment that can be repaired will be decontaminated beforehand. Equipment that is too active to handle manually and cannot be decontaminated will be packaged and disposed of as radioactive waste.

Airborne contamination from the remaining space extract from the hot machine shop and other areas served by this system is not expected to be significant during either normal or fault conditions.

The facility has a dedicated decontamination facility that has HEPA filtration and a glovebox that also has HEPA filtration. The HEPA filters on the decontamination chamber and glovebox are typically ported so that a dispersed oil penetration (DOP) test can be performed. The portable decontamination units are also capable of DOP testing although equipment is not specified to date.

Individual machine tools have local exhaust ventilation arrangements that include HEPA filters. The HEPA filters on the individual machine tools are ported so that a DOP test can be performed.

HEPA filtration is not provided on the HVAC system; however, the VHS fans shut down on a High radiation signal and the exhaust is then directed through the VFS, thus reducing the airflow from the served spaces but allowing for the exhaust to be filtered.

The filtration system is in line with Reference 23.1 as follows:

- Gloveboxes are red areas, and therefore HEPA filtration is provided.
- Individual machine tools are amber areas with significant potential for low level of activity release, hence HEPA filtration is provided.
- Airborne contamination from the remaining space of the hot machine shop and other areas served by this system is not expected to be significant during either normal or fault conditions. Therefore, the remaining space is a green area with low risk; hence, no constant HEPA filtration is provided but the extract is directed to a VFS after receipt of a High radiation signal in the VHS exhaust.

The design of the VHS also complies with the guidance provided in Reference 23.2: HEPA filtration is provided on all exhausts that may be radioactive, whether as full-time filtration when there is a significant potential for activity release or using a stand-by filtered system if necessary when the release of activity is very unlikely.

It is further demonstrated in Section 23A.2 that the VHS design for the radiologically controlled part of the auxiliary and annex represent the best available technology (BAT).

23A.1.7 Radwaste Building Heating, Ventilation, and Air Conditioning System

The VRS supplies and exhausts air from the radwaste building, as described in Section 23.9.

The radwaste building has three potential sources of radioactive contamination, which are the following:

- Tanks for low-level liquid effluent for monitoring and sentencing. The monitor tanks contain water that has the potential of having radiological contamination. The water in the monitoring tanks is not expected to contain significant contamination and will typically be below environmental discharge limits.
- An area for loading packaged solid LLW into containers for dispatch to a LLW Repository (LLWR). Packaged solid radwaste is stored in the radwaste building. This

material is bagged or loaded into storage containers at the point where it is generated and processed, so the chance of a significant release is low. All LLW will have been prepackaged. Currently, primary circuit resins are classified as intermediate-level waste (ILW). Condensate polishing resins might be LLW in the event of SG tube failures and are encapsulated at the spent resin tank. Other LLW is not encapsulated. LLW processing equipment is currently expected to be permanently installed. ILW processing equipment is mobile if it is subjected to further treatment such as low or high force compaction in the radwaste building; then the equipment used will be self-contained with integral ventilation and HEPA filtration. The equipment may be permanently located at each site or may be transportable to undertake campaigns at more than one site. All of the AP1000 plant standard radwaste equipment located in the radwaste building is portable.

- Portable or permanently installed equipment for packaging ILW and/or compacting LLW and ILW. The current AP1000 design has provisions for portable radwaste processing equipment. This equipment will connect to the railcar bay auxiliary building HVAC systems; therefore, the risk of contamination from equipment and processing equipment is small. In addition, all potential sources are filtered at the component level.

The VRS general extract may contain significant airborne activity during either normal operation or fault conditions if the portable radwaste equipment is not properly operated.

In line with Reference 23.1, the radwaste building is classified as an amber area with the potential for significant airborne activity release. Because there is a possibility of a release in the unlikely event of a serious equipment failure, the VRS extract is passed through HEPA filters. The design of the VRS also complies with the guidance provided in Reference 23.2.

23A.1.8 Turbine Building HVAC System

The VTS serves all areas of the turbine building, as described in Section 23.13. The HVAC systems serving the switchgear rooms, rectifier room, security rooms, and plant control system cabinet rooms do not have a credible source of radioactive contamination. The general area of the turbine building is ventilated using about 850 m^3/s (1,800,000 cfm) exhausted through roof ventilators. This part of the AP1000 plant does not have a likely source of radioactive contamination. These areas do not have HEPA filtration because they do not offer a significant protection benefit.

The Bay 1 area of the turbine building contains the reactor coolant pump variable speed drives, CCS equipment (a nonradioactive system), and the BDS. The BDS may be contaminated in the very unlikely event of concurrent fuel defects, SG leak, radiation monitor or BDS isolation failure, and a BDS leak.

In line with Reference 23.1, the turbine building, except for the Bay 1 area, is a white area. The Bay 1 area is a green area with a very limited potential for airborne release, hence, no HEPA filtration is provided.

23A.1.9 Radiologically Controlled Area Ventilation System

The AP1000 plant VAS serves the RCA of the auxiliary and annex buildings, as described in Section 23.3. The VAS consists of two separate subsystems, the fuel handling area ventilation subsystem and the auxiliary/annex building ventilation subsystem combined to a single extract. Both of these subsystems are once-through-type ventilation systems.

The supply airflow rate is modulated to maintain the areas served at a slightly negative pressure differential with respect to the outside environment. The HEPA filtered exhaust air is directed to the plant vent for discharge and monitoring of offsite gaseous release.

23A.1.9.1 Fuel Handling Area

The fuel handling area ventilation subsystem supply and exhaust ductwork is arranged to exhaust the spent fuel pool area separately from the auxiliary building. It provides directional airflow from the rail car/bay filter storage area into the spent resin equipment rooms. The exhaust fans discharge the exhaust air through HEPA filters into the plant vent for monitoring of offsite airborne gaseous and other radiological releases.

All spent fuel handling operations are performed under borated water to provide radiation protection. Activity levels in the SFP are controlled by Technical Specification. The activity level in the SFP is reduced, if necessary, by transferring a portion of the SFP water to the WLS for discharge and replacing it with clean water. The SFP water is constantly filtered and purified by the SFS to remove radioactive corrosion products, fission product and other impurities to maintain low SFP radioactivity levels and water clarity.

Routine releases for the fuel handling area are low. The potential for accidental release is low; however, if the radiation monitors detect a high level of radiation, the fuel handling extract is diverted to the VFS, which contains both HEPA filters and charcoal filters. It can also be diverted manually if particular operations are being undertaken that could result in release of activity.

HEPA filtration is provided for the exhaust from the fuel handling areas as follows:

- The AP1000 plant fuel handling area is similar to other UK and European modern plant fuel handling areas, and it is common practice at those plants is to have HEPA filtration on the exhaust of the ventilation system serving the fuel handling area.

- The corrosion product crud that has accumulated on the spent fuel assemblies is highly radioactive. Crud slowly dissolves in the spent fuel water, which is cleaned up by the SFS twice every 24 hours using the purification loop. There is no accumulation of crud in the SFP thanks to good mixing achieved by the SFS. There is some uncertainty, however, about the potentiality of the crud to become airborne as the SFP water evaporates. In case of equipment failure, therefore, there is a potential for airborne crud to be released through the VAS exhaust.

HEPA filtration is provided for the spent fuel pool relief panel. In the unlikely case of spent fuel pool boiling, the HEPA filters ducted to the relief panel will remove particulates from the discharged air-steam mixture.

In line with Reference 23.1, the fuel handling area is classified amber with low risk for activity release, hence HEPA filtration is provided. This design is in line with the guidance provided in Reference 23.2.

23A.1.9.2 Auxiliary/Annex Building

The remainder of the radiologically controlled part of the auxiliary and annex building exhaust air ductwork is routed to minimise the spread of airborne contamination by directing the supply airflow from the low radiation access areas into the radioactive equipment and piping rooms with a greater potential for airborne radioactivity. In addition, the exhaust air ductwork is connected to the radwaste effluent holdup tanks to prevent the potential build-up of gaseous radioactivity or hydrogen gas within these tanks. The exhaust fans discharge the exhaust air into the plant vent for monitoring of offsite airborne radiological releases.

The supply and exhaust ducts are configured so that two building zones may be independently isolated. The annex building staging and storage area, containment air filtration exhaust rooms, containment access corridor, and adjacent auxiliary building staging, equipment areas, middle annulus, middle annulus access room, and security rooms are aligned with one zone. The other zone includes the remaining rooms and corridors, including but not limited to the radiation chemistry laboratory, primary sample room, SFP cooling water pump and heat exchanger rooms, normal residual heat removal pump and heat exchanger rooms, CVS makeup pump room, and lower annulus; and various radwaste equipment rooms, pipe chases, and access corridors. A radiation monitor is located in the exhaust air duct from each zone.

All active liquids and resins are contained within the system piping and equipment. Routine discharges are low; no single fault will result in higher discharge levels. If, however, the radiation monitors detect a high level of radiation, the fuel handling extract is diverted to the VFS, which contains HEPA filters. It can also be diverted manually if particular operations are being undertaken that could result in release of activity.

In line with Reference 23.1, the radiologically controlled part of the auxiliary and annex building served by the VAS is classified amber with low risk for activity release.

Reference 23.2 recommends providing HEPA filtration on all exhausts that may be radioactive. It is also the practice at UK and European plants to HEPA-filter the exhaust from the RCA of the annex and auxiliary buildings, however:

- The AP1000 design has greatly minimised, when compared with UK and European plants, the potential for release of activity in the general RCA, so that routine discharge is low and HEPA filters would have very little benefit.

- Some infrequent events (such as small break outside containment) will result in higher discharge level, but the use of the HEPA filters and charcoal filters in the VFS provide adequate filtration. Both the local area and ductwork exhaust monitors are used to actuate the extract through the VFS extract to ensure rapid detection and response time.

It is further demonstrated in Section 23A.2 that the VAS design for the radiologically controlled part of the auxiliary and annex represent the BAT.

23A.1.10 Duct Monitors

Beta scintillation monitors set up to detect the principal noble gases present (Kr-85 and Xe-133) are located in the VAS extract duct from the fuel handing area , the VRS radwaste building extract , the VHS health physics and hot machine shop extract , and the VFS containment purge extract ; and in each of the VAS main extract ducts from the annex building and the auxiliary building (Reference 23A.1). (Their approximate sensitivity is specified in the range 3.7e-3 Bq/m^3 (10^{-12}μCi/cc) to 3.7 kBq/m^3 (10^{-7}μCi/cc).

Releases from fuel or primary coolant will include releases of noble gas. The VAS and VHS monitors will stop the associated supply and exhaust systems and start the VFS extract to filter all extract from the impacted area. The VFS maintains the impacted area at a negative pressure with respect to atmosphere so that there is no unfiltered release to atmosphere during or after an abnormal release into the areas served by the VAS.

The VFS and VRS duct monitors alarm on a High signal.

23A.1.11 Area Monitors

Area gamma monitors are provided to measure the radiation intensities in specific areas of the AP1000 plant. The range of the area monitors is such that the normal and anticipated zone dose rate and any anticipated operational occurrences that would increase the zone dose rate are detected. Area monitors are located so as to provide warning of uncontrolled or inadvertent movement of radioactive material in the AP1000 plant.

Selected area monitors are used to actuate the VFS filtration. Using area monitors in addition to the duct radiation monitors to actuate the VFS has a high probability of reducing the filtration actuation time.

Area monitors that provide VFS actuation signals and the monitor locations are delineated in Reference 23A.1.

23A.2 BEST AVAILABLE TECHNOLOGY ASSESSMENT

23A.2.1 Radiologically Controlled Area Ventilation System – General Area of the Auxiliary Building/Annex Building

The AP1000 plant VAS consists of two separate subsystems, the fuel handling area ventilation subsystem and the auxiliary/annex building ventilation subsystem combined into a single extract. As detailed in Section 23A.1.9, the fuel handling area exhaust is HEPA-filtered, however, for the general area of the auxiliary building/annex building HVAC subsystem, the following different design options were considered:

- Option 1: the exhaust air goes to the plant vent without filtration but is directed to the VFS upon detection of a high level of radiation by the exhaust radiation monitor. The VFS system has both HEPA filters and charcoal filters on the exhaust.

- Option 2: the Regulators have asked Westinghouse to add HEPA filtration to the exhaust going to the plant vent. Westinghouse believes that the addition of HEPA filters to the plant vent exhaust is not the BAT for this part of the VAS area, which is considered to have a low risk of radiological contamination. As described below in option 3, Westinghouse proposes to improve the original system by linking more radiation detectors to the VFS switching signal to improve the system response time from

~30 seconds to less than 15 seconds. The linking of additional detectors both improves the reliability of the switching system and reduces the duration of potentially untreated atmospheric releases.

- Option 3 (AP1000 design): the exhaust air goes to the plant vent without filtration but is directed to the VFS upon detection of a high level of radiation by the exhaust radiation monitor or the local area monitors. The use of local and exhaust radiation monitors provides a system response of less than 15 seconds, and ensures good reliability as well. The VFS system has both HEPA filters and charcoal filters on the exhaust.

Options 1 and 3 present the same disadvantages, but Option 3 provides a more rapid containment of radiation and is thus a better option.

Table 23A-1 provides a BAT assessment to compare the benefits and costs of implementing Option 2 versus the Option 3 (AP1000 plant VAS design).

A number of assumptions have been made to generate quantitative data to facilitate comparison of the two options. These assumptions are as follows;

- 54 HEPA and 54 pre-filters required on VAS general area ventilation exhaust
- HEPA filters changed every 2 years
- Pre-filters changed every 4 months
- Cost of HEPA filters is £420 each
- Cost of pre-filters is £30 each
- Cost of electricity is 7.5p/kWh
- Waste filter compaction volume reduction factor is 3.6.
- Six compacted filters will fit into a 210-litre (55.47 gallons) drum.
- Cost of disposal of LLW to Drigg is £27,500 per half height International Organisation for Standardisation (ISO) container (includes cost of container, delivery of container, cost of transportation to Drigg, and cost of disposal at Drigg).
- LLW drums are 100-percent filled

As can be seen in Table 23A-1, the total cost of adding HEPA filtration to the general area of the auxiliary building/annex building ventilation is estimated to be ~£4,968,700 over the 60-year plant operating life + engineering costs + operating, maintenance, and decommissioning costs. The implementation of this option will also lead to the generation, handling, and disposal of 357 m^3 (9.4e4 gallons) of LLW.

It is thus concluded that the cost of adding continuous HEPA filtration is not justified given the implementation of improved reliability and speed of the VFS switching system.

It should be noted that adding filters to the VAS (Option 2) would not be possible without significant impact on building layout and significant cost. This additional cost has not been considered in the present BAT assessment.

23A.2.2 Health Physics and Hot Machine Shop HVAC System – Health Physics and Hot Machine Shop

The VHS includes localised HEPA filtration of potential radioactive sources (e.g., gloveboxes' exhausts and machine shop tools). However, different design options were considered for the area exhaust as follows:

- Option 1: the area ventilation could be discharged directly to the main plant vent at all times.
- Option 2: a first option to comply with the guidance provided in References 23.1 and 23.2 is to add HEPA filtration to the exhaust going to the plant vent.
- Option 3 (AP1000 design): the area ventilation could be discharged directly to the main plant vent but the exhaust is directed to the VFS carbon bed and HEPA filtration system in the event of detection of radiological contamination. The use of local and exhaust radiation monitors provides a system response of less than 15 seconds, and ensures a good reliability as well.

Option 1 is not acceptable based on the guidance provided in References 23.1 and 23.2. Table 23A-2 provides a BAT assessment to compare the benefits and costs of implementing Option 2 versus Option 3 (the AP1000 VHS design 3).

A number of assumptions have been made to generate quantitative data to facilitate comparison of the two options. These assumptions are as follows:

- 18 HEPA and 18 pre-filters required on VHS general area ventilation
- HEPA filters changed every 2 years
- Pre-filters changed every 4 months
- Cost of HEPA filters is £420 each
- Cost of pre-filters is £30 each
- Cost of electricity is 7.5p/kWh
- Waste filter compaction volume reduction factor is 3.6.
- Six compacted filters will fit into a 210-litre drum (55.47 gallons).
- Cost of disposal of LLW to Drigg is £27,500 per half height ISO container (includes cost of container, delivery of container, cost of transportation to Drigg, and cost of disposal at Drigg).
- LLW drums 100-percent filled

Table 23A-2 shows that over the 60-year plant operating life, the total cost of adding HEPA filtration to the health physics and hot machine shop ventilation is estimated at £1,656,200 + engineering costs + operating, maintenance and decommissioning costs. The implementation of this option will also lead to the generation, handling, and disposal of 119 m^3 (3.1435 gallons) of LLW.

In addition, the main source of radiological contamination is already treated by local HEPA filtration and the area is considered to have a low risk of radiological contamination.

It is thus concluded that the cost of adding continuous HEPA filtration to the health physics and hot machine shop is not justified given the local HEPA filtration and the connection of the VHS to the VFS switching system.

23A.2.3 Nuclear Ventilation Design Guidance

A number of clauses in the UK nuclear ventilation design guide (Reference 23.1), support the argument against adding HEPA filters to the plant vent exhaust in areas with a low risk of radiological contamination:

1. Clauses 2.4.1b) and 2.5.1b) outline measures that should be taken to minimise the creation of radioactive waste as far as practicable:

   2.4.1b) states that "for environmental protection (and also cost reasons) it is now accepted policy to minimise radioactive waste arisings as far as practicable; in particular, contaminated HEPA filters, being of low density are very expensive to store or dispose of as radioactive waste."

   2.5.1b) states that "total air flow through the system from inlet to discharge into the atmosphere should be minimised. This will result in the number of filters to be disposed of as radioactive waste also being minimized."

   It is estimated that adding HEPA filtration to the general area of the auxiliary building/annex building and to the health physics and hot machine shop ventilation will increase radioactive waste arisings by 476m^3 (1.25e4 gallons) with an associated LLW disposal cost of £1,776,900 (see Tables A-1 and A-2 for cost breakdown). The total cost of the filter addition over the plant life would be £6,624,000.

2. Clause 2.6.3 states that "the degree of containment, including the number of barriers required, for the particular plant must be determined by a risk assessment, taking account of the design safety principals for the project. This will take into consideration the severity and likely frequency of potential accidents."

   The infrequency of potential radioactive releases in the auxiliary/annex building is a major factor to be considered when assessing the benefits and costs of adding HEPA filters to the plant vent exhaust. The release of radiation above acceptable levels in the auxiliary/annex building is a highly unlikely occurrence and Westinghouse estimated a maximum of one or two discharges exceeding the VFS detector switching points during the 60-year lifespan of the plant. In this situation, the exhaust will be switched to the VFS system, which has HEPA filtration and carbon beds, in less than 15 seconds so that the potential release will be minimal.

3. Clauses 3.7.6 and 3.7.10 specifically refer to the option of using a standby cleanup plant for use with areas that are expected to be clean and that have low accident potential for loss of containment.

   Clause 3.7.6 states that "other extracted areas are cells usually incorporating shielding, which house active plant … Such items are in high quality primary containment. The extract from these cells will be clean if there has been no containment breach. The clean up requirements are usually dependent upon the accident potential of the system as assessed by hazard assessment, and single or double HEPA filtration may be required. An

option on these systems is to keep the clean-up plant on a standby basis, bringing it into use in the event of an accident. This option will have to be justified; it will be necessary to demonstrate that appropriate indication and control functions exist to bring the system into use in sufficient time to control the release to acceptable levels."

Clause 3.7.10 states that "In cases where the ventilation discharge has little accidental discharge risk, clean-up systems are not always justified. During normal running, to avoid passing large amounts of air through HEPA filters (which are expensive to install, maintain and dispose of after use), standby systems serving a number of areas, could be brought into use for fault conditions."

In the AP1000 plant, the operation of the VFS is effectively providing a standby system in the event that areas that are expected to be clean (i.e., the general area of the auxiliary building/annex building and to the health physics and hot machine shop) become contaminated.

23A.2.4 Conclusions of the Best Available Technology Discussion

In conclusion, the AP1000 design for the treatment of ventilation exhaust from the general area of the auxiliary building/annex building and the health physics and hot machine shop represent BAT for these ventilation systems.

23A.3 REFERENCES

23A.1 Westinghouse Report, APP-RMS-J7-001, Rev. 6, "Radiation Monitoring System – System Specification Document," April 2015.

Table 23A-1. BAT Comparison Table – VAS General Area Ventilation

Issue	Option 1	Option 2	AP1000 Design – Option 3	Advantage Option 2	Disadvantage Option 2	Advantage Option 3	Disadvantage Option 3
Filtration/ emissions	Connected added to the VFS to automatically switch to filtered exhaust if a high radiation signal is detected in exhaust duct.	Continuous HEPA filtration of area.	Connection added to the VFS to automatically switch to filtered exhaust if a high radiation signal is detected in exhaust duct or building. Contamination response time less than 15 seconds by linking area and exhaust detectors to initiating switching to VFS.	High level of particulate removal (Efficiency 99.97% on 0.3 micron particles) Reduced environmental emissions of radioactive particulates. Reduced reliance on detection systems. All air filtered, not just air contaminated above detection threshold.	Contaminated air not vented through VFS carbon bed – no radioiodine removal. Radioactive gases not removed by HEPA filters. No measurable reduction in normal emissions (reduction is over two orders of magnitude less than the instrument error range).	Upon detection of contamination, air is vented through VFS HEPA filter and carbon bed (particulate and gaseous contamination removed). Radiation detection response time reduced from ~30 to ~15 s. Reliability of switching improved with more detectors providing switching signal.	Switching to VFS relies on detection system. Contamination may pass out of building unfiltered for up to 15 seconds before system switches to VFS.
Energy use	VAS fans run continuously.	HEPA fans run continuously. Fan horsepower increased by 45-60 hp (33.6-44.7 kW).	VAS fans run continuously.	-	Up to an additional 23.51-GWh power consumption over 60-year operating life of plant.	No change to energy consumption of fans. Energy use of extra detectors negligible.	-
Waste	-	36 – 54 HEPA filters and same number of pre-filters (treated as LLW) HEPA filters will be replaced every 2-3 years. Pre-filters replaced every 4-6 months.	-	-	Total number of filters used = 189 per year and 11,340 over 60-year plant operating life. Volume of each filter is 4 ft^3. Volume of each compacted waste filter is 31.5 litres. Volume of compacted filter waste (LLW) = 5.95 m^3 per year and 357 m^3 over plant operating life. No. of LLW waste packages = 32 drums (210l) per year or 1,890 drums over plant operating life. This equates to 48.5 half-height ISO (HHISO) containers over plant operating life.	No additional HEPA filter waste (above filter usage for VFS system), therefore waste arisings are minimised.	-
Construction	Exhaust fans placed on roof with mounting foundations.	HEPA filtration units placed on roof with mounting foundations.	Exhaust fans placed on roof with mounting foundations. Extra ductwork.	-	HEPA and pre-filtration units placed on roof. Extra ductwork.	-	-
Maintenance	-	HEPA filters would be replaced every 2-3 years. Pre-filters replaced every 4 – 6 months.	-	-	Estimated number of HEPA filter change outs over operating life of plant is 1620. Estimated number of pre-filter change outs over operating life of plant is 9720.	-	-

Table 23A-1. BAT Comparison Table – VAS General Area Ventilation (cont.)

Issue	Option 1	Option 2	AP1000 Design – Option 3	Advantage Option 2	Disadvantage Option 2	Advantage Option 3	Disadvantage Option 3
Dose ALARP	-	Increased risk of maintenance dose.	-	Reduced activity released to atmosphere.	Increased maintenance dose. More ductwork to decontaminate.	No extra maintenance dose. Contamination directed to VFS upon detection rather than released to atmosphere.	Contamination may be released to atmosphere for up to 15 seconds before system switches to VFS.
Decommissioning	-	-	-	-	More equipment to be decontaminated and decommissioned (HEPA/pre-filters, mounting foundations, ductwork).	-	-
Cost	-	Installation of HEPA and pre-filter units and extra ductwork. Cost of filters. Extra energy costs. Maintenance costs. Cost of disposal of filters as LLW.	Programming of radiation detectors.	-	Installation of HEPA and pre filter units and extra ductwork estimated at £600,000-£900,000 + engineering costs. Cost of HEPA filters estimated at £11,340 per year and £680,400 over 60-year plant operating life. Cost of pre-filters estimated at £4,860 per year and £291,600 over 60-year plant operating life. Extra energy costs estimated at £29,400 per year and £1,764,000 over 60-year plant operating life. Cost of disposal of filters as LLW at Drigg estimated at £22,200 per year and £1,332,700 over 60-year plant operating life. Increased operating, maintenance, and decommissioning costs.	Costs are minimal in comparison to cost of HEPA filters.	Programming detectors. Decontamination/decommissioning of detectors and ductwork.

Table 23A-2. BAT Comparison Table – Hot Machine Shop & Health Physics Area Ventilation

Issue	Option 1	Option 2	AP1000 Design – Option 3	Advantage Option 2	Disadvantage Option 2	Advantage Option 3	Disadvantage Option 3
Filtration/emissions	Area exhausts to plant vent without filtration. Machine shop exhaust from tools and glove box exhaust are HEPA filtered.	Continuous HEPA filtration of area.	Connection to the VFS to automatically switch to filtered exhaust if a high radiation signal is detected. Contamination response time less than 15 seconds by linking area and exhaust detectors to initiating switching to VFS.	High level of particulate removal (Efficiency 99.97% on 0.3-micron particles) Reduced environmental emissions of radioactive particulates. Reduced reliance on detection systems. All air filtered, not just air contaminated above detection threshold.	Contaminated air not vented through VFS carbon bed – no radioiodine removal. Radioactive gases not removed by HEPA filters. No measurable reduction in normal emissions (reduction is over two orders of magnitude less than the instrument error range).	HEPA filtration local to potential sources of emissions (machine shop tools and glove box exhausts) to prevent contamination of whole area. Upon detection of contamination, air is vented through VFS HEPA filter and carbon bed (particulate and gaseous contamination removed). Radiation detection response time reduced from ~30 to ~15 s. Reliability of switching improved with more detectors providing switching signal.	Switching to VFS relies on detection system. Contamination may pass out of building unfiltered for up to 15 seconds before system switches to VFS.
Energy use	VHS fans run continuously.	HEPA fans run continuously. Fan horsepower increased by 15-20 hp (11.2-14.9 kW).	VHS fans run continuously.	-	Up to an additional 7.84-GWh power consumption over 60-year plant operating life.	No change to energy consumption of fans. Energy use of extra detectors negligible.	-
Waste	-	18 HEPA filters and same number of pre-filters (treated as LLW) HEPA filters will be replaced every 2-3 years. Pre-filters replaced every 4-6 months.	-	-	Total number of filters used = 63 per year and 3780 over 60-year plant operating life. Volume of each filter is 4 ft^3. Volume of each compacted waste filter is 31.5 litres. Volume of compacted filter waste (LLW) = 1.98 m^3 per year and 119 m^3 over plant operating life. No. of LLW waste packages = 11 drums (210l) per year or 630 drums over plant operating life. This equates to 16.2 HHISO containers over plant operating life.	No additional HEPA filter waste (above filter usage for VFS system).	More ventilation ductwork to decontaminate.
Construction	Exhaust fans placed in annex building with mounting foundations.	HEPA filtration units placed on roof with mounting foundations.	Exhaust fans placed in annex building with mounting foundations. Extra ductwork to connect to VFS.	-	HEPA and pre-filtration units placed on roof. May require extra ductwork.	-	Extra ductwork to connect to VFS.
Maintenance	-	HEPA filters would be replaced every 2-3 years. Pre-filters replaced every 4-6 months.	-	-	Estimated number of HEPA filter change outs over operating life of plant is 540. Estimated number of pre-filter change outs over operating life of plant is 3240.	-	-

Table 23A-2. BAT Comparison Table – Hot Machine Shop & Health Physics Area Ventilation (cont.)

Issue	Option 1	Option 2	AP1000 Design – Option 3	Advantage Option 2	Disadvantage Option 2	Advantage Option 3	Disadvantage Option 3
Dose ALARP	-	Increased risk of maintenance dose.	-	Reduced activity released to atmosphere.	Increased maintenance dose. More ductwork to decontaminate.	No extra maintenance dose. Contamination directed to VFS upon detection rather than released to atmosphere.	Contamination may be released to atmosphere for up to 15 seconds before system switches to VFS.
Decommissioning	-	-	-	-	More equipment to be decontaminated and decommissioned (HEPA/pre-filters, mounting foundations, ductwork).	-	Extra ductwork to decontaminate/decommission.
Cost	-	Installation of HEPA and pre-filter units and extra ductwork. Cost of filters Extra energy costs Maintenance costs Cost of disposal of filters as LLW	Programming and maintenance of detectors. Extra duct work to connect to VFS.	-	Installation of HEPA and pre filter units and extra ductwork estimated at £200,000-£300,000 + engineering costs. Cost of HEPA filters estimated at £3780 per year and £226,800 over 60-year plant operating life. Cost of pre-filters estimated at £1620 per year and £97,200 over 60-year plant operating life. Extra energy costs estimated at £9800 per year and £588,000 over 60-year plant operating life. Cost of disposal of filters as LLW at Drigg estimated at £7400 per year and £444,200 over 60-year plant operating life. Increased operating, maintenance, and decommissioning costs.	Costs are minimal in comparison to cost of HEPA filters.	Programming of detectors. Installation of extra ductwork to connect to VFS system. Decontamination/decommissioning of ductwork.

TABLE OF CONTENTS

TABLE OF CONTENTS (cont.)

LIST OF TABLES

LIST OF TABLES (cont.)

LIST OF FIGURES

LIST OF ABBREVIATIONS, ACRONYMS, AND TRADEMARKS

ALARA	as low as reasonably achievable
ALARP	as low as reasonably practicable
BAT	best available technique
BDS	steam generator blowdown system
BNFL	British Nuclear Fuels Limited
BSL	basic safety level
BSO	basic safety objective
C&I	control and instrumentation
CCS	component cooling water system
CEDE	committed effective dose equivalent
CRDM	control rod drive mechanism
CSA	control support area
CVS	chemical and volume control system
DCF	dose conversion factor
DRPI	digital rod position indicator (system)
EC	eddy current
EPR2010	Environmental Permitting Regulations 2010
GA	general area
GDA	generic design assessment
HEPA	high-efficiency particulate air
HHISO	half-height ISO (container)
HLW	high-level waste
HRGS	high-resolution gamma spectrometer
HSE	Health and Safety Executive
HVAC	heating, ventilation, and air-conditioning
HX	heat exchanger
ICRP	International Commission on Radiological Protection
IHP	integrated head package
IIS	in-core instrumentation system
IITA	in-core instrument thimble assembly
ILW	intermediate-level waste
IRR99	Ionising Radiations Regulations 1999
IRWST	in-containment refuelling water storage tank
ISI	in-service inspection
JEM	job exposure model
LL	legal limit
LLW	low-level waste
LLWR	low-level waste repository
LOCA	loss-of-coolant accident
LRGS	low-resolution gamma spectrometer
MCR	main control room
MEU	mobile encapsulation unit
MSIV	main steam isolation valve
NRC	Nuclear Regulatory Commission
ORE	occupational radiation exposure

LIST OF ABBREVIATIONS, ACRONYMS, AND TRADEMARKS (cont.)

PAD	personal alarming dosimeter
PCS	passive containment cooling system
PCSR	Pre-Construction Safety Report
PPE	personal protective equipment
PSS	primary sampling system
PWR	pressurised water reactor
PXS	passive core cooling system
RCA	radiologically controlled area
RCCA	rod cluster control assembly
RCP	reactor coolant pump
RCS	reactor coolant system
REPPIR	Radiation (Emergency Preparedness and Public Information) Regulations
RM	refuelling machine
RMS	radiation monitoring system
RNS	normal residual heat removal system
RPA	Radiation Protection Adviser
RPI	radiological protection instrumentation
RPS	Radiation Protection Supervisor
RV	reactor vessel
RVCH	reactor vessel closure head
RVLIS	reactor vessel level instrumentation system
RWMD	Radioactive Waste Management Directorate
SAP	safety assessment principle
SCC	stress corrosion cracking
SFAIRP	so far as is reasonably practicable
SFP	spent fuel pool
SFS	spent fuel pool cooling system
SG	steam generator
SSC	system, structure, or component
Tech Spec	technical specification
TLD	thermoluminescent dosimeter
UK	United Kingdom
US	United States
UT	ultrasonic testing
VAS	radiologically controlled area ventilation system
VBS	nuclear island nonradioactive ventilation system
VCS	containment recirculation cooling system
VES	main control room emergency habitability system
VFS	containment ventilation system
VHS	health physics and hot machine shop HVAC system
VRS	radwaste building HVAC system
VTS	turbine building ventilation system
VXS	annex/auxiliary building nonradioactive ventilation system
VZS	diesel generator building heating and ventilation system

LIST OF ABBREVIATIONS, ACRONYMS, AND TRADEMARKS (cont.)

WDC	waste disposal container
WGS	gaseous radwaste system
WLS	liquid radwaste system
WSS	solid radwaste system

TRADEMARKS

Inconel is a registered trademark of Special Metals Corporation.

24 RADIATION PROTECTION

24.1 Introduction

This chapter of the Pre-Construction Safety Report (PCSR) covers the protection of workers and members of the public against exposure to ionising radiation in normal operations and protection of essential workers following a major accident. Potential fault conditions are identified in Volume 3 of the PCSR. The frequency and consequences of accidents and the prevention and mitigation systems are also covered in Volume 3.

Radiation protection from external radiation under normal operating conditions, including routine maintenance, is achieved in the design by reducing, so far as is reasonably practicable (SFAIRP), the sources of radiation. Where sources cannot reasonably be reduced further, exposure to radiation is controlled by means of shielding and by controlling the duration of exposure. Protection from radioactive contamination is achieved by reducing the activity present in dispersible form, and providing suitable containment and ventilation, layout of areas, control of access, monitoring, and personal protective equipment (PPE).

Westinghouse has many years of experience in the design and maintenance of pressurised water reactors (PWRs). Maintenance has included such major operations as replacing steam generators (SGs) and reactor coolant pumps (RCPs) as well as standard refuelling operations. As a result, Westinghouse has developed a considerable understanding of the major sources of radiation exposure during operation and maintenance of its reactor design; it has been able to undertake continuous improvement programmes to reduce sources of external radiation in operating reactors and to reduce doses incurred during operation and refuelling.

The design of the AP1000 reactor has taken into account utility requirements for reliability; safe operation and maintenance; and reduction in operator dose. Experience from the continuing improvements in operating plants has been incorporated into the design (e.g., materials selection, and plant layout) and operating regime (e.g., reactivity control, water chemistry, and zinc addition) to reduce radiation levels from the plant. In areas where high external radiation levels are likely, suitable and sufficient shielding is provided to protect workers from high radiation levels during normal operations, maintenance, and fault conditions. As discussed in section 24.3, the AP1000 design has been simplified when compared to operating PWRs; the AP1000 PWR has fewer valves and less piping which is expected to provide reductions in personnel dose due to reduced maintenance times and activities.

Westinghouse has incorporated features into the design that reduce the outage time for refuelling and, as a result, reduce the duration of worker exposure to radiation. Where applicable in the design, remote inspection and maintenance systems have been allowed for to further reduce exposures during shutdown. This is an ongoing process and in the future, as new techniques become available, backfitting may be considered where reasonably practicable.

Segregation of areas and suitable extract ventilation systems prevent the spread of contamination (including tritiated water) within and outside of the containment and other buildings. Best available techniques (BATs) are used to restrict routine airborne and liquid discharges of radioactive material.

A single personnel entrance is provided for the radiologically controlled areas (RCAs) of the reactor containment, shield building, auxiliary building, annex building, and radwaste building. Non-radiation areas of the auxiliary/annex buildings are completely segregated from

the RCA. The AP1000 design is considered to restrict routine doses to operators and others SFAIRP.

External or internal faults, such as loss of external power or feedwater pump failure, will initiate plant responses that may include operator actions to bring the reactor to a safe state without any abnormal releases or further plant damage. In the unlikely event of coincident failures or operator errors resulting in a severe accident, the use of passive systems for mitigation of major accidents maintains the integrity of the reactor containment for 72 hours without standby systems. However, the main control room (MCR) will continue to be manned and some operations will be undertaken during this period to monitor and prepare to maintain the passive containment water inventory and spent fuel pool (SFP) cooling. The MCR is provided with an uncontaminated supply of air from pressurised cylinders; calculations demonstrate that the dose to workers in the MCR during this period will be limited. If the MCR needs to be evacuated during normal operations (e.g., in the event of a fire in the MCR), the reactor operators will transfer control to the remote shutdown station (Room 12303) but this is not intended for use during a major accident. Predefined routes are provided to locations that need to be accessed in a major emergency and the doses arising from essential actions following a major accident have been assessed.

24.2 Design Targets

An overriding aim in the design of the AP1000 reactor has been to ensure that doses to workers and members of the public are as low as reasonably achievable (ALARA). This is taken to be equivalent to the terms SFAIRP and as low as reasonably practicable (ALARP) as explained in the Health and Safety Executive (HSE) safety assessment principles (SAPs) (Reference 24.1). While regulatory limits provide an upper boundary for individual dose, the emphasis on ALARP ensures that individuals will not be expected to approach any dose limit.

It is therefore reasonable to compare the doses received in normal operations to the numerical targets specified in Reference 24.1 and as shown in Table 24-1.

The design and operating regime of the AP1000 reactor ensures that doses will be kept below the basic safety level (BSL), which, in some cases, is also the legal limit (LL) under the Ionising Radiations Regulations (IRR99) (Reference 24.2) and, in many cases, also show that doses will be at or below the basic safety objective (BSO). The design intent is that doses will be ALARA, which, as noted above, complies with the SFAIRP requirement of the IRR99.

The IRR99 (Reference 24.2) specify a dose limit for members of the public, which is included as the BSL (LL) in the HSE SAPs (Reference 24.1) and shown in Table 24-1. The IRR99 also recommend that a dose constraint of 300 μSv be applied to doses to members of the critical group from a single new source. In the SAPs, the HSE interprets a single source as being a site under a duty holder's control. The Environmental Permitting Regulations 2010 (EPR2010) (Reference 24.3) specify maximum doses to individuals that may result for a defined source of:

1. 0.3 mSv per year from any source from which radioactive discharges are first made on or after 13th May 2000; or

2. 0.5 mSv per year from the discharges from any single site.

It is therefore appropriate to assume a de facto annual dose limit of 300 μSv for members of the public from discharges of radioactive material as noted in Table 24-1, although an objective of 150 μSv has been established for new nuclear power plants.

The AP1000 design process commenced several years ago, and initially, a design target of 1 person-Sv per year was adopted for the annual collective dose to workers to ensure that individual doses are not controlled by dose-sharing among a large group. In addition to this target, the ALARP philosophy was also applied to the design process. At the time, the 1 person-Sv per year target was a challenging goal compared with the annual doses incurred in operating plants. However, as a result of improved practices, the numerical target has been met for annual doses in a number of existing plants. Further reductions have been achieved in existing plants by improvements such as use of low-cobalt materials in replacement SG tubing and zinc injection. While it is now apparent from the routine dose uptake assessment that a significantly lower design target could have been met, there is little point in doing so at this stage: the value selected would simply be chosen to be just above the estimated routine collective dose. What is clear from the large margin by which the design target has been met is that the process of continuous improvement in the design has not been limited, even though the design target has been achieved. In addition, the application of ALARP philosophies ensure that radiological conditions within the plant are constantly challenged, and have helped to drive continuous improvement as the AP1000 design has progressed.

The doses to workers and the means by which they are kept ALARP are assessed in this chapter. The means for ensuring that doses to members of the public are ALARP are discussed in detail in Chapter 26.

Numerical targets are also specified for the frequency and consequences of accidents and for the overall risks from all accidents on the site, both for workers and for members of the public (Reference 24.1). These are reproduced in Table 24-2. The consequences and risks from accidents are assessed in detail in Chapters 8 to 14 in Volume 3.

In the event of a major accident, the regulations on emergency preparedness (Reference 24.4) allow the statutory dose limits to be exceeded for the purpose of intervention during a "radiation emergency". Provisional guidance on acceptable maximum doses for personnel during intervention has been issued (Reference 24.5) as shown in Table 24-3 subject to the overriding requirement to apply ALARP.

The AP1000 plant MCR has been designed to restrict doses to personnel for the duration of a limiting design basis accident to 50 mSv in compliance with general design criterion 19 (Reference 24.6), which is below the provisional guidance level for intervention (Reference 24.5).

24.3 Radiological Protection of Workers – Normal Operation External Radiation

Normal operation comprises power generation and refuelling shutdowns. The main sources of radiation hazard during operation and during refuelling and maintenance are described in Table 24-4. The radionuclides generated in the fuel by the fission process have been calculated using the industry standard computer code (References 24.7 and 24.8) with parameters specific to the AP1000 reactor. The concentrations of fission products from the fuel in the primary coolant and elsewhere in the reactor systems and generation and transport of activated corrosion products (crud) have been determined using computer codes developed by Westinghouse (References 24.9, 24.10, 24.11, and 24.12). Other codes have been used for determining N-16 and other primary circuit activities (Reference 24.15) and activity in the secondary circuit (References 24.16 and 24.17). The computer codes used to determine the source terms are described in Table 24-5. The basic source term information is collated in the radiation analysis design manual (Reference 24.26). A high-level look at the codes and process used to evaluate radiation source terms is shown in Figure 24-14.

The effects of design changes on source terms, for example measures to reduce crud, are assessed as part of the design change process. The specific source terms used in calculations are referenced and justified in the relevant calculation notes. Independent verification of each calculation ensures the validity of the source term evaluation. A detailed matrix shows how each assessment has been used.

In the design process, engineering measures such as source term reduction and shielding design were used to reduce doses to levels that are ALARP, and these measures were given precedence over administrative measures, such as dose sharing and procedural control. All aspects of the design have been considered to ensure that doses are ALARP, starting with source term reduction. The plant has been designed to reduce and simplify maintenance and refuelling, which account for a significant proportion of the dose. Shielding is provided to keep dose rates in occupied areas ALARP during operation and shutdown; remote techniques have been facilitated to reduce doses from essential operations in high dose rate areas.

Doses incurred during planned shutdown and normal refuelling operations are considered in this section. Special operations that may need to be undertaken at some time in the life of the plant, such as SG or RCP replacement, have been considered in the design of the plant to ensure that they can be undertaken if necessary, and the design provisions to reduce doses will ensure that dose rates are ALARP. However, the doses from these operations are not included in the normal operation dose assessment because there is no certainty that they will be necessary in the life of the plant. It will be the responsibility of the plant operators to prepare the relevant safety cases at the time.

24.3.1 Source Term Reduction

The design of the AP1000 plant incorporates a range of features to minimise the production and transport of radioactive corrosion products (crud), within the primary circuit that experience has shown to be responsible for doses to operators, increased discharges, and associated problems in decommissioning. The means by which radiation source terms have been minimised in the design of the AP1000 reactor include the following:

- Material selection
- Material quality control
- Piping design
- Reactor coolant chemistry control
- Primary coolant and SFP cleanup (chemical and volume control system (CVS) and spent fuel pool cooling system (SFS))
- Surface treatment (SG channel head)

24.3.1.1 Materials Selection

Controlling the choice of materials that come in contact with the primary coolant leads to a reduction in the production of corrosion products, including Co-58, Co-60, Fe-55, and Ni-63. In the AP1000 design, the following points are of particular note:

- Ferritic low-alloy and carbon steels used in principal pressure-retaining applications have corrosion-resistant cladding on surfaces exposed to the reactor coolant (Type 304 for roll bonding and Type 308/308L for overlay). The corrosion resistance of the cladding material is at least equivalent to the corrosion resistance of Types 304 and 316 austenitic stainless steel alloys or nickel-chromium-iron alloy, martensitic stainless steel, and precipitation-hardened stainless steel.

- Equipment specifications for components exposed to high-temperature reactor coolant limit the cobalt content of the base metal as given in Table 24-17. The use of hard-facing material with cobalt content such as stellite is limited to applications where its use is necessary for reliability considerations. Nickel-based alloys in the reactor coolant system (RCS) (Co-58 is produced from activation of Ni-58) are similarly used only where component reliability may be compromised by the use of other materials.

- The specification of low-cobalt tubing material (Inconel™ 690) for the AP1000 reactor SG design is an important feature of the design, not only in terms of reduced exposure relative to the SG, but to the total plant radiation source term. The cobalt content has been substantially reduced to 0.015 weight percent for the AP1000 reactor SG tubing, as shown in Table 24-17.

- Lead, antimony, cadmium, indium, mercury, and tin metals and their alloys are not allowed to come in contact with engineered safety features' component parts made of stainless steel or high-alloy metals during fabrication or operation. Bearing alloys containing greater than 1 percent of lead, antimony, cadmium, or indium are not used in contact with reactor coolant.

24.3.1.2 Piping Design

The piping in pipe chases has a 60-year design objective in relation to corrosion and operating environment. Pipe bends are used instead of elbows where reasonably practicable to reduce potential crud traps. .

24.3.1.2.1 Reactor Coolant Pipe Connections

Piping connections to the reactor coolant loops are located on or above the horizontal centreline of the pipe wherever reasonably practicable, particularly where there is no flow from the branch pipe under normal operations. The purpose of this is to minimise crud build up in branch lines resulting from gravitational separation.

24.3.1.3 Materials Quality Control

To ensure low corrosion rates in the AP1000 plant, quality assurance and quality control systems will be implemented during manufacture and construction. Austenitic stainless steel materials used in the fabrication, installation, and testing of nuclear steam supply components and systems are handled, protected, stored, and cleaned according to recognised, accepted methods designed to minimise contamination that could lead to stress corrosion cracking (SCC). The procedures covering these controls are stipulated in process specifications. Tools used in abrasive work operations on austenitic stainless steel, such as grinding or wire brushing, do not contain and are not contaminated with ferritic carbon steel or other materials that could contribute to intergranular cracking or SCC.

24.3.1.4 Reactor Coolant System Chemical Control

Chemical control of the reactor coolant is critical in ensuring reduction of corrosion and subsequent crud formation and transportation, thereby reducing the amount of radioactivity carried by the coolant, and reducing plant dose rates. The AP1000 design includes several features and provides for multiple measures to control reactor coolant chemistry. Examples include:

- The use of a chemical and volume control system
- Provisions for the duty holder to employ good or best practices in plant chemistry
- The application of zinc addition to the AP1000 plant

Many of these features and their impacts on plant chemistry are discussed in detail in Chapter 21 of this report.

24.3.1.5 Scoring of Options for Minimising Production of Radioactivity, Including Particulate

The AP1000 PWR design includes several features that are intended to minimize the production of radioactivity, including particulates. This section and subsequent portions of this chapter discuss these features as they relate to particulate radioactivity; however, many of the features mentioned are also expected to effect a decrease in the production of other forms of radioactivity.

As part of the overall options studies for identifying the BAT for reducing discharges to the environment, the techniques identified for reducing the production of particulates within the primary circuit were subjected to the same scoring system against a number of criteria as shown in Table 24-5. Each option was given a score of between -2 and 2, with 2 indicating beneficial, -2 indicating detrimental, and 0 indicating neither beneficial nor detrimental. All the options described above had an almost identical high positive score, indicating that they should all be adopted. Scores were assigned based upon operating experience from existing plants using one of the identified methods for reduction of particulate production as shown in Table 24-6.

No techniques were adopted where the benefits were not so clear. This is largely due to the need for only proven technology to be incorporated in the primary circuit design to avoid inadvertent challenges to the integrity of the circuit is maintained over the life of the plant. However, it is reasonable to assume that research is ongoing into other suitable techniques and that if any reach the stage where they can be backfitted to an existing plant (like zinc injection), then they will be adopted in operational AP1000 plants and incorporated into future ones. In addition, should the research result in beneficial techniques requiring

significant changes to the design of the primary circuit components, incorporating these changes at major outages will be considered.

The same process of evaluating options and assigning scores was applied to techniques for removing radionuclides from the primary coolant and reducing their activities in liquid and aerial discharges. In this case, a wider range of techniques could be evaluated because low-pressure and -temperature systems do not have the same safety-critical performance requirements. The detailed BAT studies are discussed in Reference 24.20. Techniques with a negative or zero net benefit were rejected.

24.3.1.6 Primary Coolant and Spent Fuel Pool Cleanup

Spent Fuel Pool, Refuelling Cavity, and Refuelling Water Storage Tank

The SFS maintains a controlled temperature in the SFP, by cooling the water to compensate for decay heat from stored spent fuel, reducing the evaporation rate from the SFP. The SFS also cleans up the water from the SFP, the refuelling cavity, and the in-containment refuelling water storage tank (IRWST) by filtration and ion exchange. The radionuclides involved will depend on the time since the spent fuel was in the reactor and the number of fuel defects.

In the absence of significant levels of failed fuel, the γ emitting nuclides of concern are primarily Co-58 and Co-60 from radioactive crud. Crud is defined as minute, solid, corrosion products that arise from within or travel into the reactor core and become radioactive. These corrosion products can then be transported to other portions of the RCS where they may deposit on surfaces such as piping. The AP1000 design allows the addition of zinc acetate to reduce ongoing corrosion rates for RCS materials and to reduce the corrosion products released to the coolant, which results in a reduction in crud deposits. Crud is transported to the SFP when fuel assemblies are offloaded from the core into the SFP during outages. A small amount of crud is resuspended in the water during the course of fuel handling. The SFS provides two water volume changes of the SFP in 24 hours. The SFS achieves a much better decontamination factor than in previous generations of PWRs, which reduces crud levels in the SFP. .

The tritium concentration within the SFP is monitored and reduced by dilution. The levels of tritium in the SFP water (as well as in the primary coolant, the water in the refuelling cavity, and IRWST) can only be reduced by dilution (i.e., bleed to the liquid radwaste system and feed with untritiated makeup). Airborne concentrations of tritium arise from evaporation from the SFP, which depends on the water temperature and the relative humidity of the ambient air. The ventilation extract maintains a safe airborne concentration by ventilating air above the spent fuel pit, allowing fresh makeup air to enter the area. The operator will be responsible for determining an acceptable level of airborne activity during refuelling operations against liquid effluent discharges. The acceptable levels of activity in the SFP water will be determined by the operator based on the background dose rates and the acceptable airborne activity concentration.

The passive HEPA filters are normally isolated and will not be contaminated or contribute to the background dose rates unless actuated for an event.

The SFS is discussed in further detail in Section 17.9 of this PCSR.

Chemical and Volume Control System

The CVS passes a proportion of the primary coolant through filters and ion exchange systems to reduce the levels of crud and ionic fission products. If necessary, fission gases can also be

removed using the liquid radwaste system (WLS) degasifier. This reduces the dose rates to workers from the primary circuit components. The CVS also controls the reactor coolant chemistry reducing the production of corrosion products.

The purification rate is based on minimising occupational radiation exposure (ORE) and providing access to the RCS equipment. The CVS provides a RCS purification rate of 22.7 m^3/h (Reference 24.21): this represents at least one RCS mass per 16 hours and has sufficient purification and degasification capability (in conjunction with the WLS) to allow the reactor vessel closure head (RVCH) to be removed in a timely manner during a refuelling shutdown. In addition, purification during shutdowns has a positive impact on the ORE to workers during the outage. Further details on the CVS system are discussed elsewhere; specifically in Section 21.5.8 of this document.

Spent Ion Exchange Resin

Changing the CVS resins involves the following actions:

- Confirm that the designated spent resin tank has sufficient volume for receipt of spent resins.
- Confirm that all remotely operated solid radwaste system (WSS) valves are correctly aligned.
- Close CVS purification valves.
- Close valves in Room 11209 in containment.
- Depressurise the resin sluice line and demineraliser by opening containment isolation valves in Room 12444 in containment.
- Backwash or “fluff” the demineraliser resin bed to prepare for transfer.
- Carry out the transfer.
- Close valves and flush the transfer line.
- Drain the vessel.
- Fill the empty vessel with fresh ion exchange resin.

Collective doses to operators during shutdown are predicted to be 240 person-μSv to sluice a single resin bed and 240 to 480 person-μSv to refill the demineraliser with fresh resin. The CVS is equipped with two mixed-bed resin beds, either of which is sized for operation over and entire fuel cycle. Changing CVS resin with the plant operating at power, while possible, is not anticipated to be necessary. If it is necessary to undertake the operation at power, the doses are expected to be up to double the doses during shutdown.

The spent resins are likely to be intermediate-level waste (ILW). While the selection of a suitable strategy for the treatment and disposal of spent resins will be the responsibility of the operator, flexibility is provided in the design for the treatment and disposal of spent resins. The plant design includes a shielded cell that can be used for storage of a high-integrity container, which is filled with spent resin and lifted remotely into a shielded flask for transfer to a central processing facility where it will be immobilised in a form suitable for the future

ILW repository. Alternatively, the method of choice described in the Environment Report (Reference 24.45), is for spent resin to be transferred directly from the spent resin tanks via pipework to a mobile encapsulation unit in the railcar bay for treatment.

In addition, smaller quantities of granulated carbon may be generated from the guard bed on the gaseous radwaste system (WGS), although this material does not deplete and is anticipated to last for the life of the plant. If change-out is required, the media is also likely to be ILW and for which a suitable treatment and disposal option will need to be selected by the operator. The Environment Report (Reference 24.45) includes a discussion of one means of treatment for this waste (encapsulation) using a mobile encapsulation unit in the auxiliary building.

Filter Changes

A shielded filter transfer flask is used to change the higher-activity filters of the CVS, SFS, WLS, and WSS. The filter vessel is drained, and the concrete floor plug is opened remotely. The filter vessel head is removed and the transfer flask, without its bottom shield cover, is lifted and positioned on the port directly over the cartridge in the filter vessel.

A grapple inside the transfer flask is remotely lowered and connected to the filter. The filter is lifted into the transfer flask, and the flask is transferred to the bottom shield cover. The transfer flask is lowered onto and connected to the bottom shield cover. The transfer flask is then moved to the auxiliary building rail car bay where the filter may be placed in a shielded temporary storage space, loaded directly into a waste container, or otherwise processed for treatment. If necessary, a sample of the filter media is obtained through a port in the transfer flask.

The primary filters are also expected to be ILW. Treatment and disposal of spent filters will be the responsibility of the operator; the flexibility to allow for this has been incorporated into the design. The transfer flask could be used to load the filters into a shielded container, which could then be transferred to a central processing facility. Alternatively, as described in the Environment Report (Reference 24.45), the filters could be taken to a mobile encapsulation unit in the auxiliary building for treatment without leaving the RCA.

Estimated doses from filter changes are discussed in Section 24.3.3.1.

24.3.2 Design Features

The AP1000 design incorporates features to reduce doses to operators SFAIRP during normal operations at power and from routine refuelling, shutdown operations, and maintenance. This is achieved by a combination of plant design, plant layout, shielding, and remote operations. Provisions are also made in the design to limit doses received following a major accident.

Systems, structures, or components (SSCs) are designed for reliability to reduce the need for breakdown maintenance, and maintainability to reduce the duration of maintenance operations. The ability of Westinghouse plants to achieve a high level of availability is demonstrated by the average availability of Westinghouse design reactors of over 91 percent between 2000 and 2008 (based on data taken from Reference 24.22 excluding any plant permanently shut down before 2008). A number of plants achieve an availability of 100 percent for years where there is no refuelling outage.

Wherever reasonably practicable, multiple electric lights are provided for rooms containing highly radioactive components: thus the burnout of a single lamp does not require entry and immediate replacement of the defective lamp since sufficient light is still available.

Incandescent lights or long life lamps with appropriate barriers and protection, or not containing restricted materials, are provided inside containment and in the fuel-handling area. The fluorescent lights used outside containment do not require frequent service due to the increased life of the tubes. High pressure sodium underwater lighting with appropriate barriers and protection to prevent contact with the water, or long life lighting not containing restricted materials, are used for underwater lighting in the fuel handling areas as they provide longer lamp life, less service intervals, and less personnel exposure.

Shielding is provided to separate equipment such as demineralisers and filters from nonradioactive equipment. This provides unrestricted maintenance on the nonradioactive equipment and between radiation sources and access and service areas.

SSCs are designed to reduce access, repair, and removal times. Where appropriate, labyrinth entrances are provided for radioactive pump, equipment, and valve rooms. Adequate space is provided in labyrinth entrances for easy access, a benefit that reduces the time spent in radiation fields during operation, maintenance, and inspection. The reduced exposure duration is demonstrated in the input data used in the job exposure model (JEM) calculations in Appendices 24B, 24C, and 24D.

The WGS guard and delay beds, which are passive components with minimal maintenance requirements and the potential to be highly radioactive, are located in completely enclosed compartments and are provided with access via a shielded hatch or removable blocks.

SSCs are designed to accommodate remote and semi-remote operation, maintenance, and inspection. This has the benefit of reducing the time spent in radiation fields.

24.3.2.1 Plant Design

The AP1000 plant is designed to reduce radiation doses received during refuelling operations and the associated maintenance. This is based on designing out the maintenance requirement, simplifying operations to reduce the duration of exposure, and reducing dose rates to operators. The first two design factors have the added advantage of reducing the amount of work required, thus reducing the shutdown duration and cost and improving plant availability.

Reactor Coolant Pumps

In the UK, the AP1000 plant will use hermetically sealed wet winding RCPs (Reference 24.23) rather than the canned pumps called for in the standard specification.

The pump/motor unit consists of a pump section, where a semi-axial impeller/diffuser combination is mounted in a one-piece pump casing. A short and rigid shaft, supported by a radial bearing, connects the impeller to the high inertia flywheel. This flywheel consists of a one-piece forged stainless steel cylinder, with several smaller heavy metal cylinders inside. The flywheel is located inside the thermal barrier, which forms part of the pressure boundary. A specific arrangement of cooling water circuits guarantees a homogeneous temperature distribution in and around the flywheel which minimises the friction losses of the flywheel and protects the motor from hot coolant. The driving torque is transmitted by the motor shaft, which itself is supported by two radial bearings. A three-phase, high-voltage squirrel-cage induction motor generates the driving torque. The cooling water is forced through the stator windings and the gap between rotor and stator by an auxiliary impeller. The **AP1000** plant RCPs are designed to not require maintenance over the 60 year life of the plant.

Reactor Vessel Insulation

Insulation in the area of the reactor vessel (RV) head is fabricated in sections with quick-release clasps to facilitate removal of the insulation. Each section of insulation has permanent identification markings to enable rapid reinstallation.

Reactor Vessel

The RV welds are designed to accommodate remote inspection with ultrasonic sensors from the interior or exterior. Nozzles are tapered along the reinforced areas to provide a smooth transition, and pipe branch locations are selected to avoid interference from one branch to the next. Weld-to-pipe interfaces require a smooth, high-quality finish.

Integrated Reactor Head Package

The integrated head package (IHP) combines several separate components in one assembly to simplify refuelling of the reactor. The purpose of the IHP is to reduce the outage time and personnel radiation exposure by combining operations associated with movement of the RVCH during the refuelling outage. In addition, the IHP concept reduces the setdown space required in the containment. With the IHP, disconnections from and connections to the control rod drive mechanisms (CRDMs) and the digital rod position indication system (DRPI) and other components within the cooling shroud assembly are not made at the individual component.

The IHP (see Figure 24-1) consists of the following main elements:

- Shroud assembly
- Lifting system
- CRDM seismic support structure
- Cable support structure
- IHP cables
- Quickloc bullet couplings
- CRDM cooling system
- Radial arm hoist
- Operating deck-mounted connector panel

Shroud Assembly

The shroud assembly is a carbon steel structure above the reactor head that includes a shielding shroud and an air baffle. During normal operation, it directs the flow of cooling air to the CRDM coil stacks. The DRPI are also cooled by this air flow. The ductwork and air baffle are integral to, and supported by, the shroud assembly. The air-cooling fans are attached to the IHP. Structurally, the shroud is integrated with the CRDM “seismic support structure”. The shroud also provides shielding at the vessel flange region. The shroud structure is bolted to attachment lugs on the RVCH. Cabling, conduit, and their supports and attachment hardware for the CRDMs, CRDM coil, and in-core instrumentation are routed around the cable support attached to the shroud.

Lifting System

The lifting system enables the RVCH and IHP to be lifted as a unit. The lift legs transfer the head load during a head lift from the head attachment lugs to the lift rig. The lifting system

consists of lift legs, sling block, clevises, and sling rods to interface with the polar crane hook.

Control Rod Drive Mechanism Seismic Support Structure

The CRDM seismic support structure provides seismic restraint for the CRDMs. It is located near the top of the CRDM rod travel housings. The DRPI connector plate attached to the rod travel housing interfaces with spacer plates, where required, to form a system of bumpers that interface with the mechanism seismic support structure. This support interfaces with the shroud assembly to transfer seismic loads from the mechanisms to the RVCH.

Cable Support Structure

The cable support structure is located at an elevation above the top of the rod travel housings. It provides permanent support and routing for the CRDM power cables and DRPI cables, which remain with the IHP and are normally not disturbed. These cables terminate at the connector panels, which constitute the interface with the mating cables. Cable disconnects are made at the connector panels.

Integrated Head Package Cables

The IHP cables include those portions of the CRDM power cables, in-core instrumentation, and DRPI instrumentation cables extending from the connector plates to the user devices. These cables remain with the IHP and are normally not disturbed. The individual cable length is sized to provide an orderly arrangement. For a refuelling or other operation requiring movement of the IHP, the cables that span the space over the cavity from the operating deck to the IHP are disconnected at the connector panels. The cables are then moved away from the IHP.

Quickloc Assemblies

The Quickloc assemblies provide the means by which the in-core instrument thimble assemblies (IITA) penetrate the pressure boundary of the reactor. The IITAs are monitored by equipment outside the pressure boundary. The Quickloc assemblies have an upper flange that is an integral part of the RVCH instrument nozzle. Referred to as the Quickloc instrument nozzle, it has an open-centre geometry that allows the Quickloc stalk, which is attached to the upper internals, to pass through the RVCH during installation and removal of the RVCH from the RV. The Quickloc stalk provides the top of the guide path through which the IITAs are installed.

The Quickloc assemblies reduce the disconnection and connection times compared to the use of Conoseal clamps. The in-core thermocouple instruments are now included with the in-core instrument connections in the eight Quickloc assemblies and the Conoseal clamps have been eliminated. When the cables attached to the IITA are disconnected and the Quickloc pressure boundary is taken apart, the bullet nose is installed over the top of the IITAs and attached to the top of the Quickloc stalk. The bullet nose protects the IITA electrical connectors as the RVCH is installed and removed. It also provides a watertight seal for the electrical connectors.

Control Rod Drive Mechanism Cooling System

The CRDM cooling system is located at the top of the upper shroud assembly, on the outside of the exterior work platform of the operating deck. The CRDM forced-air cooling system comprises the fans, fan supports, dampers, ducts, duct fittings, duct supports, baffles, shroud, instrumentation, and electric service components required to meet the CRDM magnetic jack coil assembly cooling requirements. The system consists of the following: four fans, fan power cables, fan motor heater, fan vibration monitoring, fan damper control, and CRDM cooling system inlet and outlet temperature monitoring.

Radial Arm Hoists

The radial arm hoists are located on the middle shroud. The radial arm hoist system includes the beams, rails, trolleys, hoists, and structure required to support RVCH stud-tensioning equipment handling and related lifting.

Operating Deck-Mounted Connector Panel

The operating deck-mounted connector panel is located at the top of the upper shroud. The connector panel is supported on the operating deck near the end of the cable bridge to allow for quick disconnect of the head assembly cables prior to refuelling. The connector panel is not attached to the IHP.

Other Refuelling Design Features

A number of other design features reduce the duration of exposure during refuelling and are discussed below:

Refuelling Machine (RM)

The RM is mounted on a gantry at the 110.74 m (135'-3.00") level in the containment (Figure 24-3). The fuel removal procedure is as follows:

1. The RM is positioned over a fuel assembly in the core.

2. The RM mast is lowered over a fuel assembly and engages it.

3. The RM withdraws a fuel assembly from the core and raises it to a predetermined height sufficient to clear the vessel flange and still leave sufficient water covering the fuel assembly.

4. The fuel transfer system car is moved into the refuelling cavity from the fuel storage area, and the fuel basket is pivoted to the vertical position by the lifting arm.

5. The RM is moved to line up the fuel assembly with the empty fuel basket.

6. The RM loads the fuel assembly into the empty fuel basket of the transfer car.

7. The RM then moves back over the core area, and is aligned over the next fuel assembly to be removed in the core offload sequence.

8. In parallel with item 7, the fuel basket is pivoted to the horizontal position and the fuel transfer system container is moved through the fuel transfer tube to the fuel-handling area by the transfer car and pivoted to the vertical position.

9. The fuel-handling machine unloads the fuel assembly from the fuel basket.

10. The fuel assembly is placed in the spent fuel storage rack.

11. The fuel basket is pivoted to the horizontal position, moved back into containment and pivoted to the vertical position.

12. This procedure is repeated until the core is unloaded.

Core reload is essentially the reverse of the unloading sequence described above.

The engagement of the gripper with the fuel assembly top nozzle is shown in Figure 24-4.

Quick-Opening Fuel Transfer Tube Closure System

The fuel transfer tube connects the fuel transfer canal in the auxiliary building to the refuelling cavity in the containment. During reactor operation, the fuel transfer tube is sealed at the containment end and acts as part of the containment pressure boundary. The AP1000 plant includes a quick-opening fuel transfer tube closure system rather than the conventional bolted cover. The cover is also hinged so that it does not have to be lifted from the area. These features significantly reduce the time required to open or close the Fuel Transfer Tube, which is important to exposure reduction since crud tends to accumulate in this area.

Permanent Reactor Cavity Seal Ring

The permanent reactor cavity seal ring eliminates installation and removal operation associated with bolted or inflatable types of cavity seals.

Permanent Guide Studs

Using permanent guide studs eliminates the operations to install and remove guide studs.

Shielded Storage Stand

The storage stand for the IHP located on the operating floor 110.744 m (135’-3.00”) includes shielding for the RVCH. The shielded storage stand reduces background dose rate from the RVCH on the operating floor.

Steam Generators

The SG incorporates many design features to facilitate maintenance and inspection in reduced radiation fields. The tube ends are designed to be flush with the tube sheet in the SG channel head to eliminate a potential crud trap. The SG manways (entrance to channel head) are sized for easy entrance and exit of workers with protective clothing, and to facilitate the installation and removal of tooling.

The SG design includes a sludge control system/mud drum designed to reduce the need for sludge lancing, and reduces tube and tube support degradation. The design of SG tube support plates and the full-depth tube sheet expansion of tubes reduce corrosion and occupational exposure.

24.3.2.2 Plant Layout

The layout of the AP1000 plant has built on many years of experience to ensure that exposures are ALARP in the UK sense of the term.

Within the auxiliary building, the non-radiologically-controlled areas are physically separated from the radiologicaly-controlled areas with separate access routes from the annex building.

Facility design considerations directed toward minimising radiation levels in plant access areas and near equipment requiring personnel attention generally include the following:

- Radiation sources are separated from occupied areas, where practicable (for example, pipes or ducts containing potentially highly radioactive fluids do not pass through occupied areas).

- In those systems where process equipment is a major radiation source, the pumps, valves, and instruments are separated from the process component to allow servicing and maintenance of these items in reduced-radiation zones.

- Redundant components requiring periodic maintenance that are a source of radiation are located in separate compartments to allow maintenance of one component while the other component is in operation.

- Control panels are located in low-radiation zones.

- Shielding is provided to separate equipment such as demineralisers and filters from nonradioactive equipment to provide unrestricted maintenance of the nonradioactive equipment. Labyrinth shields or shielding doors are generally provided for compartments from which radiation could stream or scatter to access areas and exceed the radiation zone dose limits for those areas.

- For potentially high radiation components (such as ion exchangers, filters, and spent resin tanks), shielded compartments with hatch openings or removable shield walls are used. Equipment in nonradioactive systems that requires lubrication is located in low-radiation zones.

- For radioactive systems, adequate space and ease of movement in a properly shielded inspection area are emphasised. Where longer times for routine inspection are required and permanent shielding is not feasible, space is provided for portable shielding.

- Wherever reasonably practicable, lubrication of equipment in high-radiation areas is achieved with the use of tube-type extensions to reduce exposure during maintenance.

- Shielding is provided between radiation sources and access and service areas.

For the plant layout to ensure that exposures to workers are ALARP, areas of the plant are classified according to the Westinghouse radiation and access zone scheme shown in Table 24-7. These represent the maximum dose rates expected to be present in each area using conservative source terms in shielding calculations. For comparison, the area designations likely to be required under the IRR99 (Reference 24.2), and the maximum occupancy times which are likely to be applied by an operator in order to ensure that doses received by workers are ALARP, are also shown in Table 24-7.

The plant layout is such that access to a given radiation zone does not generally require passing through a higher radiation zone.

24.3.2.3 Shielding

Shielding plays an important role in protecting workers and members of the public from radiation generated during power operation, residual radiation during refuelling outages, and major accidents when fission products are released into the containment. Bulk shielding walls form the structure of the building and both provide and challenge the ability of the structure to withstand a seismic event. Conservatively, calculations for concrete shielding are based on a density of 2200 kg/m^{-3} (140 lb/ft^3) (Reference 24.24). No account is taken of any rebar.

The level of shielding is a balance between the protection provided, the requirements for accessibility, structural implications, and cost. The purpose of the shielding assessment is to demonstrate that the shielding design of the AP1000 plant provides an adequate level of protection based on the use of conservative source terms and the required occupancy of each area. The dose rates from best-estimate source terms will be lower than those from the shielding studies. In most cases, it is expected that this approach is sufficient to ensure that doses received in operation will be ALARP; any further dose reduction by means of additional or temporary shielding will be assessed on a case-by-case basis as necessary during operations. (Note that temporary shielding was not credited in the AP1000 design shielding analyses.)

The shielding can be broken down into the following:

- Primary shielding
- Secondary shielding
- Fuel transfer shielding
- Auxiliary component shielding
- MCR shielding

Primary Shielding

During operation, very high levels of neutron and gamma radiation are generated within the RV. When the reactor is shut down, the fission products in the fuel and activation products in the reactor internals present significant sources of radiation.

The primary shielding includes:

- Water annuli around the core
- Carbon steel pressure vessel
- Massive reinforced concrete structure surrounding the RV

The primary shielding (or its parts) performs the following functions:

- Reduces, in conjunction with the secondary shield, the radiation level from reactor sources to a level that makes limited access inside the containment during power operation possible.
- Limits the radiation level after shutdown from sources within the RV and permits limited access to RCS equipment in areas that require access for inspection or maintenance.
- Reduces the neutron fluxes incident to the RV to prevent material property changes that might unduly restrict plant operation.
- Limits the gamma ray fluxes in the primary shield concrete to avoid large temperature gradients and dehydration of the concrete.
- Limits the neutron activation of components and structural materials in accessible areas outside the primary shield throughout the life of the plant to prevent those components from becoming significant radiation sources after shutdown.

Air cooling is provided to prevent overheating, dehydration, and degradation of the shielding and structural properties of the primary shield.

The reactor cavity has been designed so that the dose rates on the operating deck due to neutron streaming are less than 1 mSv/h.

Secondary Shielding

The secondary shielding consists of the shield walls surrounding the reactor coolant loops, the concrete operating floor, and the shield building surrounding the containment.

During plant operations, the major radiation source in the RCS is N-16, which is created by neutron activation of oxygen during passage of coolant through the core. The secondary shielding surrounds the primary shielding and the reactor coolant loops and attenuates the radiation originating in the reactor coolant and the reactor to a safe level.

The secondary shield is designed to permit limited access to certain areas within the reactor containment during full-power operation by reducing dose rates to <1 mSv/h and to reduce the full-power radiation levels outside the shield building to allow normal, continuous occupancy by reducing dose rates in occupied areas to ≤2.5 μSv/h. In addition, the secondary shielding serves to reduce the radiation intensity outside the shield building in the unlikely event of an accidental release of fission products into the containment.

Fuel Transfer Shielding

During refuelling operations, irradiated fuel is removed from the reactor through a canal to the auxiliary building, then on to a water-filled spent fuel pit located adjacent to the shield building. After sufficient decay, the spent fuel is transferred under water to fuel transport flasks in the cask loading pit. The lift height of the RM is limited to prevent exceeding dose limits to personnel on the bridge.

The fuel transfer shielding consists of the water in the refuelling cavity, the water over the spent fuel storage area and the walls of the refuelling cavity, transfer canal, and spent fuel pit. In addition, shielding is provided on the spent fuel transfer tube.

The fuel transfer tube is surrounded by concrete and no part of it is unshielded during any portion of the refuelling operation. The only potential radiation streaming path associated with the tube shielding configuration is the 50.8 mm (2 inch) seismic gap between the fuel transfer tube shielding and the steel containment wall. Shielding of this gap is provided by a water-filled bladder. This "expansion gap" radiation shield effectively reduces the radiation fields during fuel transfer and accommodates relative movement between the containment and the concrete transfer tube shielding with no loss in shield integrity. A removable hatch in the shield configuration provides access for inspection of the fuel transfer tube welds. The opening of this hatch is administratively controlled and is treated as an entrance to a very high-radiation area. This hatch is in place during the spent fuel transfer operation.

Spent fuel in the SFP is handled using a bridge crane on a bridge deck spanning the SFP. To compensate for reduced shielding from the mast and reduced distance from the surface of the SFP, the bridge floor is supplemented with additional steel.

The fuel transfer shielding protects plant personnel from fission product gamma radiation emitted from the spent fuel elements during core refuelling operations using the source terms described in the "Shielding Source Terms" section. The following design objectives have been applied:

- Shielding shall be provided for protection of personnel during all phases of spent fuel transfer and storage.

- Shielding shall be based on the access requirements and radiation zone designations of the areas above and around the refuelling cavity, spent fuel pit, and fuel transfer path.

- Minimum water depths allowed above the top of the fuel assemblies will be established to limit radiation dose rates at the surface of the water to levels that do not restrict accessibility when the fuel assemblies are being transferred.

- The concrete walls of the fuel transfer canal and SFP shall supplement the water shielding and will limit the maximum radiation dose rates in adjacent working areas inside the auxiliary building to levels consistent with access requirements.

Auxiliary Component Shielding

Auxiliary shielding consists of walls, floors, ceilings, and removable blocks used for shielding of the various sources of radiation associated with plant systems. These systems include, among others, the CVS, the waste disposal systems, SFS, and the primary sampling system (PSS). The following design criteria have been applied for auxiliary shielding:

- It shall be designed on the basis of RCS activity levels corresponding to the presence of fuel defects in fuel rods producing 0.25-percent of the power within the core.

- The design shall be sufficient to account for long-term buildup of radioactive corrosion and fission products on piping, fittings, valves, pumps and other equipment normally carrying radioactive liquid or gas, such as filters and demineralisers.

- The design shall be consistent with the anticipated access requirements and radiation zone designation of the area for all modes of operation.

The shielding calculations for the AP1000 plant design are based on a conservative choice of radiological source terms to ensure that the design of the shielding is applicable throughout

the plant lifetime. In addition, appropriate radiation transport calculation techniques were selected for each source/geometry situation.

Control Room Shielding Design

Limiting post-accident conditions dictate the shielding requirements for the MCR. Taking into account shielding provided by the shield building structure, shielding combined with other engineered safety features – including dedicated shielding of the VES filtration unit – is provided to permit access to and occupancy of the MCR following a postulated accident, so that individual radiation doses are limited to 50 mSv whole body from contributing modes of exposure for the duration of the accident.

Wall Penetrations

To minimise radiation streaming through wall penetrations, where practicable, offsets are incorporated between the radioactive source and the normally accessible areas. If offsets are not practicable, penetrations are located as far as practicable above the floor elevation to reduce radiation exposure to personnel. If these two methods are not used, alternate means, such as baffle shield walls, or sealing or grouting the penetration annulus, are used.

Shielding Source Terms

Sources used in the design of plant shielding must limit the radiation levels within the plant and at a site boundary to within acceptable limits. The shielding allows a plant to operate safely with fuel cladding defects and ensures that, in the event of an accident, the integrated offsite exposure due to the contained activity does not result in any harmful offsite radiation exposures.

The major radiation sources considered in shield design within the containment are core neutron and gamma fluxes and N-16 activity while at power, RCS piping and corrosion product sources, and spent fuel sources during refuelling operations. The major radiation sources considered in the auxiliary building shield design are the fission products associated with small cladding defects and crud sources. For the design basis source term, it is assumed that there is a significant fuel defect level well above that anticipated during normal operation. It is assumed that small cladding defects are present in fuel rods producing 0.25 percent of the core power output (also stated as 0.25-percent fuel defects). The defects are assumed to be uniformly distributed throughout the core. Details of the assumptions for the calculation of the reactor coolant fission product concentrations, including pertinent information concerning the fission product escape rate coefficients, coolant cleanup rate, and demineraliser effectiveness, are listed in Table 24-18.

The assumption regarding fuel leakage is a conservative one. For the AP1000 reactor core, this would correspond to around 110 leaking fuel rods. This is more than is observed during typical operations at most plants.

Sources for normal operations and accident conditions are listed in the radiation analysis design manual (Reference 24.26). For normal operations and shutdown, these include the following:

- Fast neutron flux and gamma ray energy flux at the inside surface of the primary shield
- N-16 concentration in the RCS at various locations in the primary circuit

- Reactor coolant fission and corrosion product-specific activity, based on 0.25-percent fuel defect level (which is the upper limit)
- Pressuriser liquid and steam phase source strength and pressuriser N-16 source strengths
- Core average inventory at various times after shutdown
- Core average fission product and actinide inventory at shutdown
- Core average and spent fuel neutron source strengths at various times after shutdown
- Spent fuel gamma ray source strengths at various times after shutdown
- Spent fuel fission product and actinide inventory at shutdown
- Isotopic composition and specific activity of typical out-of-core crud deposits for various full-power years of plant operation
- Mixed bed and cation bed ion exchange resin specific and total activities
- Specific activities and source strengths in various vessels

The radiation sources used in the shielding analyses are based on operation at a core power of 3400 MWt. Post-accident calculations assume core melt sources increased by 2 percent to account for uncertainty in determining thermal power. (Note that this is considered conservative, as more realistic analyses show that fuel-cladding failures are limited.) To account for variations in fuel management, both first and equilibrium core fuel management schemes are evaluated. A high-level perspective on the various codes used to develop radiation source terms is shown in Figure 24-14.

The release scenario consists of an initial release of activity from the gaps of a number of failed fuel rods 10 minutes into the accident. It is assumed that 3 percent of the core inventory of the volatile species (defined as noble gases, halogens, and alkali metals) is instantaneously released.

During the next 30 minutes following the instantaneous gap activity release, that is, from 10 to 40 minutes into the accident, an additional 2 percent of the core inventory is added to the inventory that exists based on the previous gap activity releases. At this point, 5 percent of the total core inventory of volatile species has been considered to be released.

Over the next 1.3 hours, releases associated with an early in-vessel release period are assumed to occur, that is, from 40 minutes to 1.97 hours into the accident. This source term is a time-varying release in which the release rate is assumed to be constant in the duration time, consistent with the assumptions in Reference 24.27. Additional releases during the early in-vessel release period include 95 percent of the noble gases; 35 percent of the halogens; and 25 percent of the alkali metals; as well as fractions of the tellurium group, barium and strontium, noble metals, lanthanides, and cerium groups.

Reference 24.26 gives instantaneous and integrated gamma and beta source strengths at various times following an accident.

In addition, Reference 24.26 provides normal operational source terms based on Reference 24.28 adjusted for plant-specific parameters. The numerical values given in this

standard are based on data from operating plants that use Zircaloy-clad uranium-dioxide fuel. These data are intended for use in environmental analyses and evaluations where operating conditions over the life of the plant are considered.

Shielding Analysis Methodology

The shielding calculations completed for the AP1000 plant design make use of a full suite of computer codes based on Monte Carlo, discrete ordinates, and point-kernel radiation transport techniques. The choice of a particular technique for individual shielding analyses is based primarily on the type of radiation and the complexity of the geometry under consideration. In general, the Monte Carlo and/or discrete ordinates methodologies are employed for neutron transport as well as for situations involving complex geometry or where there is the potential for radiation streaming. Point-kernel methodologies are suitable for calculating dose rates through bulk shielding from gamma sources with relatively simple geometries such as pipes and cylindrical vessels.

An example of a Monte Carlo application is the analysis of the reactor cavity area surrounding the pressure vessel where concerns for radiation streaming and component activation at locations both above and below the pressure vessel are paramount. Here these techniques are used in the design and analysis of streaming shields intended to reduce not only operating dose levels, but also dose levels in locations requiring access for inspection and maintenance during shutdown conditions.

Other examples of the application of these techniques include the evaluation of streaming through various wall penetrations in the containment and shield building, analysis of penetration and labyrinth design in the auxiliary and radwaste buildings, and the calculation of post-accident doses at some locations within and outside the shield building.

Point-kernel methods are generally used in the calculation of photon dose rates in geometric situations that are characterised primarily by penetration through bulk shielding materials without complex transport paths due to radiation streaming or material variations. Examples of the use of these analysis approaches include determining the attenuation of shield walls or calculating doses external to piping carrying radioactive sources.

These analysis methods and their application in specific areas of the plant are described in the various shielding calculation notes associated with the design of the AP1000 plant. For example, Reference 24.29 covers the annex building, Reference 24.24 covers the auxiliary building, Reference 24.25 covers the spent fuel route, and References 24.58 and 24.59 cover the containment interior.

Shielding Analysis Codes

The specific radiation transport codes used in the shielding analysis for the AP1000 plant comprise the following:

- Monte Carlo: MCNP5 – MCNP5 is a radiation/particle transport code used to calculate radiation-related quantities within nuclear systems. The code is based on established Monte Carlo statistical methodology (References 24.30 and 24.31).

- Discrete Ordinates: DOORS 3.2 – The DOORS 3.2 package is a system of codes (and associated pre- and postprocessors) used to perform neutron and photon transport calculations in 1-D, 2-D, and 3-D geometry using the discrete ordinates method (References 24.32 and 24.33).

- Point Kernel: SCAP-II – The SCAP-II code is a generalised geometry shielding code for photons based on the use of the point-kernel methodology. SCAP-II can be run in the conventional point-kernel mode with buildup applied to the calculated uncollided flux or in a single scatter mode that allows the calculation of an explicit first scatter with buildup applied on the scattered leg (References 24.34, 24.35, and 24.36).

- MicroShield 6.20 – MicroShield is used to analyse shielding and to estimate exposure from photon sources (References 24.37 and 24.38).

Results of Shielding Assessments

The shielding provided ensures that areas requiring routine access are shielded from significant sources of activity. The dose rates within the containment, the auxiliary building, the annex building, the radwaste building, and the turbine building have been calculated for the following:

- Normal operation and shutdown (Reference 24.61)
- Post-accident (Reference 24.62)

Access routes and requirements during normal operations and shutdown are shown in Reference 24.63; post-accident access requirements are included in Reference 24.62.

The areas are classified according to the scheme shown in Table 24-7. These represent the maximum dose rates expected to be present in each area. Average dose rates are expected to be lower. They have been used to confirm that dose rates will be acceptable for the levels of access required during normal operation and refuelling shutdowns.

The rooms and areas are identified in References 24.61, 24.62, and 24.63 and the access requirements are shown in Appendix 24A, Tables 24A-1, 24A-2, 24A-3, 24A-4, and 24A-5.

Outside Areas

The shield building completely surrounds the RCS components and additional shielding is around specific sources such as the reactor, SGs, and pressuriser. The concrete shield building wall and the RV and SG compartment shield walls reduce radiation levels outside the shield building to less than the 2.5 μSv/h Zone I dose rate criterion from sources inside the containment (e.g., RV and primary loop components) during power operations and refuelling outages.

Dose rates outside the auxiliary building have been calculated based on conservative source terms and locations 300 mm (11.81 inches) from the outer walls. In most locations, where there is no specific source identified inside the walls, dose rates of 0.1 μSv/h have been calculated (Reference 24.24). The adopted convention has been that these areas are designated as Zone I (up to 2.5 μSv/h) areas with no restriction on access. However, dose rates in most areas and farther away from the cell containing the spent resin tanks will be significantly lower than the maximum for Zone I.

All areas outside the buildings, with one minor exception, have been shown by calculation to have dose rates of less than 2.5 μSv/h under all normal operating and shutdown conditions. The exception is an area outside of Room 12471 (the WSS valve/piping area) above 7 m (22.97 feet), where the dose rate from a 75 mm (2.65 inches) spent resin line at a distance of 300 mm (11.81 inches) from the 0.6 m (1.97 feet) outer wall is 90 μSv/h during infrequent spent resin movement operations (Reference 24.24). Operational controls prohibiting

working at height in this area during resin transfers will eliminate the potential for exposure of workers. The dose rate calculations are based on spent resin activities in Reference 24.26.

Nonradioactive Areas

All nonradioactive areas within the auxiliary/annex buildings and other buildings outside the nuclear island have been shown by calculation to have dose rates of less than 2.5 μSv/h under all normal operating and shutdown conditions. The adopted convention has been that these areas are designated as Zone I areas with no restriction on access, although dose rates may be below the Zone 0 upper bound.

Radiation Areas

The RCA covers all areas of the reactor containment, auxiliary building, annex building, and radwaste building that could have dose rates greater than 2.5 μSv/h and/or where contamination may occur, as well as the RCA entry/exit area.

All areas within the RCA where dose rates have been calculated to be below 25 μSv/h, based on conservative assumptions on inventory and location, have been designated as Zone II.

The classification represents the maximum dose rate in the area based on the worst allowable operating conditions (fuel-cladding defects in the rods generating 0.25 percent of the core power). Detailed results in Reference 24.24 show that, in a number of locations, high dose rates are transitory, occurring only when resin sluicing is in process. Operational dose rates will normally be significantly below the maximum.

Restricted Occupancy Areas

Restrictions on occupancy apply to all areas designated Zone III or above, with the access restrictions increasing as the zone designation increases, as shown in Table 24-7. The classification represents the maximum dose rate in the area based on the worst allowable operating conditions (0.25-percent fuel defects, as described above) or other worst-case situations (e.g., crud bursts 4 hours after shutdown, resulting in high dose rates from the normal residual heat removal system (RNS) pump/valve room before the CVS removes the activity). Operational dose rates in many areas will, therefore, normally be significantly below the Zone maxima.

Detailed arrangements for access control will be the responsibility of the operator but typically, physical access restrictions (locked doors) will be implemented on all Zone V and above areas and warning signs will be provided for Zone III and IV areas.

For normal maintenance operations, pumps and tanks will be drained and flushed where appropriate to reduce dose rates. The relevant procedures will be the responsibility of the operator. It is likely to be compulsory for Zone V and above areas. For Zone III and IV areas, an ALARP judgement will be made depending on the duration of the operation and the likely operator dose balanced against additional waste generation, time, and cost.

Post-Accident Conditions

The gamma ray source term following an accident increases to a maximum after 1.97 hours and then decreases as a result of radioactive decay and other physical processes. The containment sources for various times are shown in Reference 24.26.

The maximum dose rate in the MCR following an accident has been calculated to be Zone IV (Appendix 24A, Table 24A-1), i.e., <1 mSv/h. The dose rate falls rapidly from this maximum as the short-lived fission products decay. Calculations have been carried out on MCR occupancy and ingress/egress and four other specific operations that are expected to be needed following a major accident (Reference 24.39):

- SFP makeup valve alignment (64 and 168 hours)
- Temporary water hookup to passive containment cooling system (PCS) (64 hours)
- Ventilation control for temporary heating, ventilation, and air conditioning (HVAC) to MCR and control and instrumentation (C&I) equipment room (64 hours)
- Starting diesel generators and entering electrical equipment rooms to provide temporary power to transformers (64 hours)

The timing, duration, integrated dose from the operation, dose from ingress/egress at yard area, and total integrated doses are shown in Table 24-8. The total dose resulting from 30 ingress and egress operations at 12-hour intervals is 30.5 mSv. This number does not allow for relief shifts. The highest dose from a post-accident vital area access operation (SFP makeup valve alignment after 64 hours after the accident) is 43.6 mSv. However, this falls to 25.7 mSv if delayed to 168 hours (1 week) after the accident.

All doses are below the recommended maximum doses in References 24.5 and 24.60. However, any such entries will be planned in advance, taking into account the need to ensure that all such exposures were ALARP, noting that the calculated dose rates and integrated doses are based on a worst-case situation.

Remote Operations

Remote/robotic techniques have been developed for repetitive operations that would result in high operator doses where the additional dose incurred during setting up and removing the equipment still results in a worthwhile net dose savings. The following robotic/remote systems have been accounted for in the routine dose uptake assessment:

- Eddy current inspections of SGs and tube, eliminating the requirement for worker entry into the SG head.
- Examination of the RVCH and penetration welds, eliminating the need for workers' access beneath the head when on its storage stand.

Operators may develop further remote techniques or may adopt different methodologies as part of their ALARP measures.

Temporary Shielding

Where it can provide significant dose reduction, the use of temporary shielding is considered a "best practice" in reducing radiation exposure ALARP. In most cases, the use of temporary shielding is a plant specific decision based on the actual operating dose rates and required maintenance and repair operations experienced at individual plants. Dose data obtained from these operating plants is reflected in AP1000 dose uptake assessments and, to the extent temporary shielding was used, the dose reduction was reflected in the AP1000 evaluations. That is, the exposure from operating plant experience included in the AP1000 dose assessments reflects the reduction afforded by temporary shielding.

In general, the shielding philosophy of the AP1000 has been to employ permanent shielding if a dose rate reduction was necessary (as opposed to providing means for temporary shielding). As a consequence, there are many applications of permanent shielding in the AP1000 plant. However, to facilitate various activities that may benefit from temporary shielding, the AP1000 design includes the following specific examples that allow for temporary shielding:

- Components (such as pumps) in the WLS are designed to allow for sufficient space around these components to facilitate the installation of temporary shielding.

- Unit coolers in the VAS that support cooling of CVS and (RNS) components are placed to enable temporary shielding to be installed during maintenance activities.

- To support maintenance in several areas of the auxiliary building, embedment plates are installed to allow for lugs with a capability well above the weight of the heaviest component in that area. This provides sufficient margin to allow the duty-holder/licensee to apply temporary shielding during maintenance activities if needed.

- Many components were designed to allow for sufficient "pull space" around these pieces to support maintenance. In some cases, this pull space can also be used to facilitate temporary shielding.

- Within the containment vessel, sufficient laydown space is provided to allow for maintenance activities. This could be used for temporary shielding during maintenance activities in these areas.

To store removable shielding, a utility has several options, depending upon the size and nature of the shielding. The radwaste building includes space within the radiologically controlled area that may be used to store some temporary shielding. Other pieces of temporary shielding may be stored in areas of the auxiliary building.

24.3.3 Predicted Doses to Workers

Radiological safety can be assessed in terms of several quantities; of most biological importance to people is the quantity of radiation dose (either absorbed dose, or dose equivalent). To ascertain the safety of the workers in an AP1000 plant, the potential doses to workers (both as a whole and also as individuals) are discussed below and compared against established limits and standards.

24.3.3.1 Collective Dose

The AP1000 design includes a variety of ways to reduce worker dose compared with existing Westinghouse and other PWR designs. The improvements fall into three main categories:

- Reducing source term by reducing crud production and deposition:

– Low cobalt tubing
    - Zinc injection

- Reducing component numbers:

    - Valves
    - Pumps and heat exchangers (HXs)

  - Demineralisers
  - Filters

- Figure 26-7 compares the number of valves, pumps, cables, piping, and amount of seismically qualified building volume in the AP1000 plant with those in previous PWRs to illustrate the achievements made in simplification and standardisation with the AP1000 PWR. The reduction in valves, piping, and other components is expected to result in a reduction in plant collective doses – with fewer valves, there are fewer required in-service inspections, fewer in-service tests, and a decreased potential for leaks. Specific design features relate to:

  - Refuelling operations
  - SG EC inspection and tube plugging
  - RCPs

To assess the likely doses from operation of the AP1000 design, a baseline case for the total annual collective dose to workers was developed from the collective dose calculation for the AP600 reactor design (Reference 24.40), which was based on dose data from a standard Westinghouse 2-loop reactor. The doses were divided into the following categories (Reference 24.41):

- Reactor operations and surveillance
- Routine maintenance
- In-service inspection (ISI)
- Special maintenance
- Waste processing
- Refuelling

The contributions to the collective dose from specific tasks within each category were established in Reference 24.42. This gave a total collective dose of 1.68 person-Sv, broken down as shown in Table 24-9.

The calculated total annual collective dose agreed well with the doses from Westinghouse-designed 2-loop reactors at Prairie Island and Kewaunee. (Prairie Island reactors averaged 1.67 person-Sv from startup in 1973/74 to 1990 (using data from Reference 24.22.)) However, from 1996 until 2003 (when the SGs in unit 1 were replaced), the average annual collective dose at Prairie Island was 0.89 person-Sv and has shown a steady reduction over the years, indicating improvements in dose control techniques.

On the assumption that current best practice will be employed in future operating plants, the average collective dose of 0.89 person-Sv for years in which outages took place at Prairie Island units 1 and 2 from 1996 to 2003 has been used in an assessment of expected doses from the AP1000 plant (Reference 24.40).

The method used to account for the reduction in crud production in the AP1000 plant and the reduction in the number of components used in Reference 24.40 is described in more detail in Appendix 24B.

The AP1000 design presented for generic design assessment (GDA) includes significant improvements to reduce doses to workers from refuelling operations over and above the improvements to reduce the dose rate from crud, such as the IHP. The collective and maximum individual doses from refuelling are calculated in Reference 24.42 and summarised in Appendix 24C.

In addition, JEM calculations for the following specific tasks (References 24.42 and 24.44) are described in detail in Appendix 24D:

- RCP inspection
- SG sludge lancing
- SG secondary side visual examination
- SG EC tube inspection and tube plugging
- SG ISI
- RCP ISI
- RVCH inspections
- RV inspections

The predicted AP1000 plant outage doses are shown in Table 24-9. These are slightly different from those in Reference 24.40 to take into account the revised refuelling dose calculation (Reference 24.42) and a different treatment of doses from operations that are not undertaken at every outage.

Additionally, Westinghouse has estimated collective doses incurred from several expected operations, including changeout of reactor coolant filters and CVS makeup filters. Based on these assessments, a collective dose of 1.17 person-mSv for a reactor coolant filter change is expected, while replacing a CVS makeup filter causes an estimated 0.037 person-mSv (Reference 24.57).

The total dose in a year in which an outage takes place is predicted to be 239 person-mSv, including the whole of the dose from the highest ISI (the RV, head, and SG ISIs each incur significant collective dose but are not all carried out during the same outage, therefore, only the highest contribution has been included). The dose from removal and inspection of an RCP has not been included because it is not a normally anticipated event, but would add another 4.2 person-mSv.

Potential dose from operations such as SG replacement has not been considered because a specific case will be made by the operators for these operations should they be required during the life of the plant.

The collective dose in years when there are no outages will be significantly lower. For example, the Prairie island unit 1 and 2 dose in 2007, when neither unit had a refuelling outage, was 63 person-mSv (Reference 24.22).

24.3.3.2 Doses to Groups and Individual Workers from Specific Operations

The assessments in Appendixes 24B, 24C, and 24D provide estimates of the total annual collective dose for a year including an outage. The average individual dose depends on the number of workers involved. The number of workers and the total annual collective dose will vary significantly between a year when a refuelling outage takes place and a year when there is no outage.

The number of personnel with measurable doses at Prairie Island varies from 130 in a year with no outage to around 500 during an outage year on a single unit (Reference 24.22). No detailed manning levels have been established for an operating AP1000 plant and the number per unit will depend on whether there is more than one unit, as some resources will be shared. The number required should be less than on the Prairie Island units because the number of components requiring maintenance has been reduced. However, it would be unreasonable to assume that an AP1000 plant outage could be achieved with fewer than

300 workers, resulting in an average individual dose from the overall outage dose of 239 person-mSv of below 1 mSv.

The details in Appendixes 24B, 24C, and 24D indicate the average and maximum individual dose within each work category.

Reactor Operations and Surveillance

The annual collective dose from reactor operations and surveillance is estimated to be 39.3 person-mSv (Appendix 24A, Table 24A-5). This includes a contribution from chemistry sampling. The subtotal for Health Physics personnel is 16.7 person-mSv.

A significant proportion of the dose in this category is expected to arise during operations at power with more than 50 percent of the total arising from patrols and inspections. The dose will be shared evenly amongst a team of workers and is likely to be on the order of 0.5 mSv (i.e., shared amongst 80 workers).

Routine Maintenance

The majority of the routine maintenance dose is expected to be incurred during outages. The highest contribution is from SG sludge lancing (12.8 person-mSv). However, as shown in Appendix 24D, Table 24D-2, the sludge lancing operation has a total duration of 23.5 hours (three shifts). Therefore, the individual dose can be controlled by the operator.

In-Service Inspection

The ISI collective dose is the highest contributor to the total collective dose. Even with the large reduction in components and crud, the dose is dominated by inspection of valve bodies and bolting. A number of periodic examinations are not carried out at every outage. Remotely operated equipment is used where practicable.

The RVCH inspection and, in particular, the J-weld examinations, make the highest contribution of 10 person-mSv even though remotely operated equipment is used. The original assessment of the dose from this operation was carried out (2005) when it was a relatively new procedure and included a high individual dose from man access beneath the RVCH on its stand. However, the procedure has been revised so that the instruments are set up before the head is placed on the stand and removed only after the head has been lifted from it. The revised procedure ensures that no operation results in more than a 0.5-mSv individual dose.

The reduction in the number of components and the elimination of many items ensure that routine doses from ISI are ALARP. Future developments in remote techniques will be incorporated where reasonably practicable.

Special Maintenance

The issue of special maintenance arises either as a result of faults identified during ISI or because of significant replacements or upgrades. The latter cannot be predicted in advance. Specific cases will be made for both major repairs and upgrades by the operator at the time and includes making a sound ALARP justification.

The special maintenance of other components represents a typical value as some outages may find more faults than others. However, the reduction in the number of components and the elimination of many items ensure that routine doses from ISI are ALARP.

Waste Processing

The AP1000 plant radwaste system designs incorporate an uncomplicated approach to waste processing. The AP1000 design does not include waste or boron recycle evaporators and it does not include a catalytic hydrogen recombiner in the gaseous radwaste system. Elimination of high-maintenance components contributes significantly to lower anticipated doses due to waste processing activities.

Section 24.8 contains a detailed description of the proposed waste processing arrangements and an estimate of collective dose. Additional descriptions of wastes, waste types, and proposed treatment options are included in Chapter 26 of this document. As a summary, the routine waste arisings will consist of the following:

- Low-level waste (LLW)
    - HVAC filters
    - Protective clothing
    - Contaminated equipment
- Intermediate Level Waste (ILW)
    - Activated Carbon
    - Spent filter cartridges
    - Spent ion exchange resins
- High-level waste (HLW) – Spent fuel

Spent fuel is excluded from waste processing considerations because it will remain in the pond until a suitable dry storage facility is available.

The quantities of LLW and ILW arisings are given in the Environment Report (Reference 24.45) as the following totals:

- 19 x 3 m^3 (100 ft^3) drums or boxes for ILW
- 305 x 200 litre (55 gal) drums or eight half-height ISO (HHISO) containers for LLW

ILW processing equipment will need to be provided with suitable shielding (this would apply to the mobile encapsulation unit discussed elsewhere); there is no reason to expect exposures to significant dose rates.

It is concluded that the contribution to collective dose from waste processing included in Table 24-9 provides a suitable margin above that discussed in Section 24.8 and is therefore considered to be appropriate.

Refuelling

Refuelling is the most readily assessable category as it has clearly defined operations and start and end points.

The collective dose assessed in Appendix 24B (Table 24B-9) of 41.3 person-mSv is dominated by reactor disassembly and assembly, which in turn are dominated by disconnection and connection of the in-core instrumentation system (IIS), each of which results in an individual dose of 2.02 mSv. The refuelling team consists of a shift team of 32 plus a supervisor, and it is reasonable to expect that, apart from the maximum individual

doses, the dose will be evenly distributed, giving an average dose, excluding the supervisor, of 1.3 mSv.

The AP1000 design uses Quickloc couplings for the IIS connections, which are considered to be an improvement over, for example, the Conoseal connections used at existing PWRs.

It is clear that the IHP (and specifically the IIS) represents a significant improvement over previous designs where the flux thimbles were inserted through additional penetrations in the bottom of the RV (which the US Regulatory Guide on Control of Access to High and Very High Radiation Areas in Nuclear Power Plants (Reference 24.46) specifically identifies as creating a potentially hazardous situation because of the potential for workers to enter areas with very high radiation dose rates).

Therefore, although the maximum dose to a worker is estimated to be 2.02 mSv from disconnection and connection of the IIS, the design adopted represents the BAT.

Internal Doses

Westinghouse has performed an evaluation of the potential for internal dose uptakes in the AP1000 considering operating experience from existing plants of broadly similar design, and AP1000 design features. The evaluation concluded that internal exposures at existing nuclear power plants typically involve a small number of individuals and typically result in small committed effective dose equivalents (CEDEs) per individual. While the US and European Union use different International Commission on Radiological Protection (ICRP) standards for internal doses, the ICRP 30 standard used in the US is conservative for a majority of the nuclides that are typically ingested or inhaled at nuclear power facilities. For the radionuclides where the dose conversion factor (DCF) increases with the use of ICRP 68, only a relatively small increase in DCF (less than an order of magnitude) over those from ICRP 30 is seen.

Many of the recorded internal exposure events at existing plants are a result of human performance errors, and so it is important for the licensee to have an adequate radiological protection programme in place. Examples of actions within the responsibility of a licensee's radiation protection programme that could reduce or preclude internal doses are (note that these are the responsibility of the licensee/duty holder):

- Suitable procedures to control airborne activity and surface contamination to within acceptable levels

- Continuous review of airborne activity levels in areas such as the fuel handling area and containment and,

- Installation of additional 'frisking' probes at locations where contamination may arise, for example, the primary chemistry laboratory and the hot machine shop,

- Preplanning for any maintenance operations involving a breach of radiological containment such as pump or valve replacement

    - Setting up tenting or other ventilated enclosure,
    - Location of additional change barriers close to working area,
    - Specification of suitable PPE,
    - Use of portable activity in air monitors,
    - Mocking up the work in a non-radiological space before the task takes place

- Rigorous enforcement of access control and posting requirements during routine and maintenance operations,
- Rapidly responding to any incident with the potential for release of radioactive material (to identify contamination and minimise its spread), and
- A robust monitoring programme to identify trends and incidents in airborne radioactivity and surface contamination.

The AP1000 design has also further reduced the likelihood or magnitude of internal exposures through several design features including:

- Fewer valves and pumps requiring maintenance and potential replacement,
- Improved SFS decontamination flow (maximising cleanup of particulate in the Spent Fuel Pool) and cooling (minimising evaporative losses of the spent fuel pool),
- Physical boundaries between radiologically controlled areas and non-radiologically controlled areas,
- A comprehensive Radiation Monitoring System (RMS) design,
- The inclusion of an ALARA briefing room in the plant layout, and
- Comprehensive ventilation of plant areas.

Based on these considerations, internal doses should not be a major concern during the operation and maintenance of the AP1000 reactor when a rigorous radiation protection programme is employed.

24.3.4 Comparison of Doses against Numerical Targets

Target 1 – Normal Operation, Any Person on the Site

Employees working with ionising radiation:

- BSL(LL): 20 mSv
- BSO: 1 mSv

The highest individual dose from a single operation is estimated in Appendix 24B (Table 24B-9) to be 2.02 mSv from disconnection and connection operations on the IIS at the RVCH. This dose is above the BSO and is received in a short time (1.6 hours). It is possible for two workers to undertake this task so that the individual dose is 1 mSv (it is unlikely that more than two workers could be involved). However, as it is likely that some workers will receive exposures from other operations during refuelling, individual doses will exceed the BSO.

Some other operations involve either short exposures to relatively high dose rates (e.g., RVCH inspection has a 1-hour exposure up to 0.5 mSv/h) or longer exposures to moderate to high dose rates (e.g., SG sludge lancing has 12 hours exposure to 150 μSv/h). However, the maximum individual doses from these operations could, legitimately, be reduced by dose sharing among members of the team or between shifts. In addition, the number of such operations has been reduced SFAIRP.

As discussed above, BAT has been adopted to reduce the sources of radiation (especially crud) and the principle of keeping doses ALARP has been considered throughout the design of the AP1000 plant by minimising maintenance requirements, using remote techniques, and reducing exposure durations. For example:

- The number of pumps, valves, vessels, and other components and the length of primary circuit piping have been significantly reduced compared with previous generations of PWRs.

- The seal-less RCPs are designed to eliminate required maintenance and the potential for RCS seal leakage.

- The IHP design represents best current industry practice and the use of Quickloc couplings in place of Conoseal couplings has been part of the continuous improvement process by Westinghouse.

- The design facilitates remote SG inspection and tube plugging, and remote RVCH inspection.

In the operational phase, to ensure that individual doses are ALARP, administrative controls will be implemented. Operators will be expected to set dose constraints based on industry best practice. During outages and any other operations involving short duration exposure to high dose rates, entries will be carefully planned, taking account of previous experience, and, where appropriate, will be practiced on inactive mockups to minimise the duration of exposures. Worker doses will be monitored using personal alarming dosimeters (PADs) as well as statutory dosimeters and extremity dosimeters where necessary.

The overall collective dose is predicted to be significantly lower than any similar nuclear power plant. However, there remain some tasks that involve exposure to relatively high levels of external radiation, and no further viable improvements have been identified, at this time, that could reduce doses further. Therefore, it is concluded that individual doses in excess of the BSO, but still significantly below the BSL, are ALARP.

Target 1 – Normal Operation, Any Person on the Site

Other employees on the site:

- BSL: 2 mSv
- BSO: 0.1 mSv

The convention has been adopted that all non-radiation areas within buildings have been designated as Zone I areas (up to 2.5 μSv/h). Areas up to the limit of the Zone I designation could, in theory, result in radiation exposure up to 5 mSv for an annual occupancy of 2000 hours. However, the calculated dose rates represent an upper limit based on pessimistic assumptions. Non-radiation areas of the auxiliary building, particularly those adjacent to the shield building, could have detectable levels of radiation during full power operations, but these are low occupancy areas and no specific controls are considered necessary. There is no reason to expect the dose rates in normally occupied areas, such as the office areas of the annex building, to be detectable above ambient background conditions.

Dose rates outside the west of the spent resin storage tank room at an elevation of over 7 m have been calculated to be as high as Zone III (25 to 150 μSv/h) during spent resin transfers.

However, as permits will be required for working at height, the operator will be able to ensure that no additional exposures are caused.

There is no reason to believe that radiation from AP1000 plant operations will result in any employee in a non-radiation area receiving additional radiation exposure above background radiation levels above the BSO.

Target 2 – Normal Operation Any Group on Site

- BSL: 10 mSv
- BSO: 0.5 mSv

The average dose to all radiation workers on site depends on the total number of workers but is expected to be less than 1 mSv.

The doses to specific groups of workers also depend on the number in each group and the dose assigned to the group.

The only readily identifiable group, and probably the group with the highest average exposure, is the group of 32 workers undertaking the refuelling operation. The average dose to this group is estimated in Appendix 24B (Table 24B-9) to be 1.3 mSv.

As discussed in Appendix 24C, all aspects of the refuelling operation have been reviewed to identify best practices. Where improvements have been identified, these have been incorporated into the design. No further viable improvements have currently been identified that could reduce doses further. However, in line with continuing the improvement policy and learning from experience, any refinement of the procedures or new equipment that has been shown to reduce doses in other plants will be introduced in the AP1000 design where relevant.

Therefore, although the predicted maximum group doses are above the BSO, they are ALARP.

24.4 Radiological Protection, Members of the Public

24.4.1 Normal Operations

Doses to the public from normal operations are the sum of doses from external radiation, airborne discharges, and liquid discharges. Typically the contribution from direct external radiation from containment is insignificant, because dose rates are low and there is limited occupancy at the site boundary. External radiation is more likely to result from exposure to sediments containing radionuclides discharged as liquids.

24.4.1.1 External Radiation

The primary shielding provided by the reactor and the concrete primary shield; the secondary shielding around the SGs, pressuriser, and other primary circuit components; and the shield building around the containment ensure that dose rates outside during operation are less than 2.5 μSv/h based on conservative estimates of the source term. Calculations of dose rates between 30 m (98.43 ft) and 500 m (1640.42 ft) from the shield building (Reference 24.47) show the dose at 30 m (98.43 ft) is 0.0056 μSv/h, 0.0047 μSv/h at 70 m (229.66 ft) and 0.0015 μSv/h at 150 m (492.13). The dose rate profile has a maximum of 0.0061μSv/h at 50 m (164.04 ft) as a result of scattered radiation through the passive containment cooling

system air vents in the shield building. A comparison with existing UK PWR confirms that direct external radiation does not present a significant exposure pathway.

24.4.1.2 Routine Discharges

BAT is employed to reduce arisings and discharges SFAIRP so that doses to members of the public are ALARP. Techniques to minimise arisings and discharges include the following:

- C-14 minimisation
    - Oxygen scavenging
    - Control of nitrogen impurities in fuel
    - pH control by lithium hydroxide
- Cs-137
    - Minimisation of fuel defects in operation
    - Control of uranium contamination in fuel manufacture
    - Demineraliser
- I-131
    - Minimisation of fuel defects in operation
    - Control of uranium contamination in fuel manufacture
    - Mixed bed demineralisers
    - Deposition
    - Carbon delay beds
- N-16
    - Hydrazine addition
    - Oxygen elimination
    - Delay for Decay techniques
- Noble gases
    - Minimisation of fuel defects in operation
    - Carbon delay beds
- Activation products (see Section 24.3)
    - Minimisation of plant shutdowns
    - Carbon delay beds
    - HEPA filters
    - Liquid filtration and demineralisers

- Pu-241
    - Control of uranium contamination in fuel manufacture
    - Minimisation of plant shutdowns
    - Liquid filtration and demineralisers
    - HEPA filters
    - SFP clean-up system
- Sr-90
    - Minimisation of fuel defects in operation
    - Control of uranium contamination in fuel manufacture
    - Liquid filtration and demineralisers
    - HEPA filters
- Tritium
    - Li-7 tailored lithium hydroxide
    - Zirconium cladding
    - Grey rods
    - Minimisation of plant shutdowns
    - Minimisation of primary coolant leaks
    - Condenser

The plant design also facilitates the application of additional BATs by the duty holder to minimise radioactivity arising from routine discharges SFAIRP. Such additional BATs include the application of good chemistry and the potential use of ultrasonic fuel cleaning.

The predicted doses from routine airborne discharges are calculated in the Environment Report (Reference 24.45) to be 7.6 μSv from representative annual discharges and 12 μSv from the calculated annual discharge limits. The doses from liquid effluent discharges have been calculated to be 2.3 μSv for representative discharges and 3.8 μSv for calculated annual discharge limits.

The total annual predicted doses from discharges are therefore 9.9 μSv from representative discharges and 15.8 μSv for airborne and liquid discharges at the calculated limits.

24.4.1.3 Total Dose

The total annual predicted doses from all sources are therefore 14 μSv from representative discharges and estimated external radiation and 20 μSv for airborne and liquid discharges at the calculated limits. These are at or below the BSO for any person off the site (Reference 24.1).

Target 3 – Normal Operation, Any Person Off the Site

- BSL(LL): 1 mSv
- BSO: 0.02 mSv

The maximum dose requirements in EPR2010 (Reference 24.3) have also been met.

Maximum Doses to Individuals from a Defined Source (EPR2010)

- 0.3 mSv per year from any source from which radioactive discharges were first made on or after 13th May 2000, or

- 0.5 mSv per year from the discharges from any single site.

Westinghouse notes that an objective of 150 microSv per year has been established for future construction. The actual critical group dose will be dependent on habit survey data. However, it is reasonable to conclude that the systems employed to reduce activity in airborne and liquid discharges and to restrict direct radiation doses will ensure that doses are ALARP.

24.5 Control of Surface and Airborne Contamination

The RCA specified as Zone II or above in Appendix 24A also forms the boundary of the areas with potential for contamination. Within the RCA, some areas will have higher potential for surface and airborne contamination particularly during refuelling and maintenance. Access control and traffic patterns are considered in the plant layout to reduce the spread of contamination.

24.5.1 Personnel Access to the Radiologically Controlled Area

All personnel access to the RCA of the annex building, the auxiliary building, the shield building, the containment, and the radwaste building is via a single entry/exit area in the annex building, during normal operations and outages.

The facilities have been designed according to Reference 24.48, which has been developed in agreement with utility operators. Personnel will change from personal clothing into work clothing in the change rooms (Figure 24-5). It is normal for clothing to be worn in the RCA to be differentiated from work clothing that may be worn in nonactive areas to minimise the potential for spread of contamination but the plant operator will make such arrangements. The change rooms have been sized for 30 male and 12 female personnel at any time (male change room is 15.25 m (50 ft) x 16.15 m (53 ft), female change room is 6.7 m (22 ft) x 16.15 m (53 ft)). During outages there may be up to 200 personnel in the RCA at any one time but entry and exit will be staggered to avoid overloading the change rooms.

When in work clothing, personnel will go to the RCA entry area. Work permits, dosimetry including PADs, respirators, and keys for access to restricted areas will also be issued on entry to the RCA at the Health Physics Booth (Figure 24-6). The human factors aspects of this portion of the plant have been reviewed as part of several design reviews and iterations between Westinghouse, design partners, and Westinghouse AP1000 customers. The current layout is the result of several iterations and changes, which were enacted to address such concerns as ergonomics. Thus, although there is not a formal human factors assessment of this portion of the plant, these considerations have been included in the design. Additional PPE will be obtained from the PC Pickup and Suitup Room which includes provision for benches and shelving (Figure 24-7).

Although the radiation zoning for these areas is shown as Zone II in Table 24A-3, no sources of radiation are present or would need to be brought into the area and dose rates will be at or near indoor background levels.

Following a design basis accident, entry arrangements will be determined according to conditions at the time. Suitable forward control points are likely to be established at low dose rate locations.

Access into the RCA, the non-active areas of the auxiliary building, and the turbine building is limited to authorised personnel via turnstiles. Entries are recorded, enabling rapid roll calls in emergencies (Figure 24-8).

Additional PPE will be removed prior to exit from the RCA. Workers in work clothing will pass through installed personal monitors that will not allow egress on alarm except in emergencies. Washbasins and showers are located on the active side of the barrier for personal decontamination (Figure 24-10). First aid equipment is located within the area. Showers are also provided in the change rooms. As workers will have been monitored on exit, these showers do not need to be connected to the active liquid waste system although the waste water will be monitored as a precaution before discharge to the normal sewage system.

All personal equipment and portable tools taken into the RCA must be monitored at the Health Physics Booth before removal from the RCA and decontaminated, retained in the area, or disposed of as active waste. Decontamination of tools can be undertaken in the hot machine shop. Only essential items will be permitted to be taken into the active area to minimise the monitoring, decontamination, and waste generation.

Any equipment used in the active area could be stored in the RCA for reuse; for example, equipment that may be contaminated could be kept in the hot tool crib in the hot machine shop. Larger items which are not significantly contaminated could be kept in the staging and storage area on the first floor of the annex building. This could apply to dedicated equipment such as the remote control SG examination and tube plugging equipment and the RVCH remote inspection equipment; however, it may be cost effective to share such equipment among a number of reactors.

24.5.1.1 Hot Machine Shop

The hot machine shop (Figure 24-11) provides facilities for decontamination of tools and other items either to allow tools to be taken off site or to reduce the dose rates associated with the tools. If a tool cannot be decontaminated sufficiently for free release then a judgment would be made by the plant operator based on the residual contamination and the value of the item. The tool would either be scrapped as LLW or, if it was to be reused, it could be stored in the "hot tool crib". The plant operator would make the decision based on an ALARP assessment.

The hot machine shop also houses machine tools and an enclosure for undertaking work on pump seals. The amount of work which will be undertaken will be determined by the plant operator. It is likely that a lot of the work undertaken will be on components which are not significantly contaminated but which would be difficult to monitor sufficiently to clear them from the RCA. Dose rates in the hot machine shop will depend on the operations being undertaken. The shielding provided has been assessed for a 555 MBq Cs-137 source and a 148 MBq Co-60 source based on a dose rate of 150 μSv/h at 300 mm (11.81 ft) which is considered to be the limit for this area (Reference 24.29). However, this is purely used as a bounding case. In practice, the plant operator would make an ALARP justification for undertaking work on high dose rate components rather than disposing of them as waste. High dose rate components would remain in the hot machine shop for as short a period as possible and only essential workers would enter the workshop while such components were present.

Decontamination and local shielding would also be use as appropriate to ensure that doses were ALARP.

24.5.2 Equipment/Materials Access to the Radiologically Controlled Area

The number of access routes from the RCA to the environment is limited to the following:

- The containment access corridor in the annex building leading to the ground floor staging area in the auxiliary building
- The truck staging area in the radwaste building leading to the rail car bay in the auxiliary building
- The mobile systems facilities bays in the radwaste building

Drains, floors, and exterior concrete sloping are used at access points to prevent (potentially radioactive) fluids from the interior of the buildings escaping from the buildings, and also to prevent exterior surface water from entering the buildings.

The containment access corridor and the truck staging area provide for final contamination monitoring prior to dispatch.

24.5.3 Access Routes within the Auxiliary Building

Access requirements and the potential for the spread of contamination vary between power operation and refuelling outages.

During power operations, access requirements will be relatively low. Regular access will be required to the primary sampling room during both power operations and refuelling outages. Air and liquid filters may need to be replaced and some patrols, inspections, and calibrations will be carried out. In addition, fresh fuel will be brought into the plant in preparation for refuelling.

Air filters will be of the safe change type and therefore only precautionary contamination control arrangements will be required. Changing of CVS filters uses a bottom-opening transport flask, and only local contamination control arrangements will be required. Similarly, local contamination control arrangements will be set up for any breakdown maintenance where there is the potential for a spread of contamination.

During refuelling outages the RVCH IHP is removed and moved to a storage stand on the operating deck (110.744 m (135’-3”) level). The upper and lower refuelling cavities and fuel transfer canal are flooded, and the upper internals are lifted into their storage racks in the refuelling pool. Fuel is lifted out of the reactor, rotated to the horizontal position for transfer out of the containment, returned to the vertical by the up-ender, and placed in the spent fuel storage racks. New and reload fuel will be taken into the containment in a similar manner. In addition, the SGs will be opened and inspected during the refuelling outage and other maintenance operations on pumps will be undertaken. In addition to contamination controls at the RCA boundary, local contamination control areas are likely to be established within the containment and auxiliary buildings to limit the spread of contamination to the general operating areas.

Later in the life of the plant, after the refuelling shutdown is complete and the reactor is at power, decayed spent fuel will be loaded into fuel flasks to be taken out of the auxiliary building. The fuel transfer flask is loaded underwater in the loading pit connected to the SFP.

After loading, the flasks are transferred to the cask washdown pit for decontamination and initial monitoring before transfer to the transport vehicle in the rail car bay. Similarly, spent resin containers and filters from the CVS will be packaged in some suitable form for export to long-term storage or the ILW repository (Section 24.8). Fuel flasks and waste containers are transferred into and out of the rail car bay via the truck staging area of the radwaste building, which provides a buffer area where final clearance monitoring can be undertaken prior to leaving the RCA.

LLW arising in the containment or auxiliary building can be transferred to the radwaste building via the rail bay and truck staging area; LLW from the annex building, including the hot machine shop, can be transferred to the radwaste building via the access corridor and the truck staging area.

24.5.3.1 Access to the Containment

Access into the containment is via shielded personnel airlocks on the 100 m (100') and 110.744 m (135'-3") operating deck level and via equipment shield doors on the same levels.

Large items transferred into or out of the containment can be transferred through the auxiliary building and temporarily housed in a staging area in the annex building. Otherwise, large items from within containment can be removed from the nuclear island via the containment access corridor in the auxiliary building, which provides a buffer area where final clearance monitoring can be undertaken.

24.5.3.2 Local Access Controls

Local access controls will be implemented close to areas under maintenance with temporary barriers for additional PPE and monitoring as necessary. Different arrangements may be adopted to handle the larger numbers present during refuelling. However, the aim remains to isolate contamination to the area where it is generated and to decontaminate the area as soon as possible after the work has finished.

24.5.4 Surface Contamination Control

The AP1000 plant is designed to contain radioactive liquids and gases within vessels, pipes, and pumps. Potential sources of contamination, with the exception of the SFP, are isolated from normally occupied areas.

Liquid sampling systems are designed to maintain containment and, where necessary, shielding.

Surface contamination will be limited to areas where breach of containment is necessary for maintenance. Equipment is designed to minimise the generation and spread of contamination.

24.5.4.1 Drains from Vessels

Equipment vents and drains from highly radioactive systems are piped directly to the collection system to minimise airborne and floor contamination. Welded piping systems are employed on radioactive systems to the maximum extent practicable to reduce system leakage and crud buildup at joints.

24.5.4.2 Surface Treatment

Decontamination of potentially contaminated areas and equipment within the plant is facilitated by the application of epoxy paints and suitable smooth-surface coatings to the concrete floors and walls. Sloping floors with floor drains are provided in potentially contaminated areas of the plant, where practicable. In addition, radioactive and potentially radioactive drains are separated from nonradioactive drains.

24.5.5 Airborne Contamination

The containment and ventilation systems are described in detail in Chapter 23. There are a number of different systems serving active and inactive areas:

- Nuclear island nonradioactive ventilation system (VBS)
- Annex/auxiliary building nonradioactive ventilation system (VXS)
- Diesel generator building heating and ventilation system (VZS)
- Containment recirculation cooling system (VCS)
- Containment ventilation system (VFS)
- Health physics and hot machine shop HVAC system (VHS)
- Radwaste building HVAC system (VRS)
- Turbine building ventilation system (VTS)
- RCA ventilation system (VAS)
- MCR habitability system (VES)

The extracts from areas with the potential for radioactive discharges are individually continuously monitored and alarmed. Additionally, the plant vent combined discharge is monitored and alarmed. HEPA filtration is also provided for some of the areas with a higher potential for contamination, as discussed below.

The ventilation systems have been designed to maintain areas that have the potential for contamination at a negative pressure differential with respect to the outside atmosphere and to adjacent areas with lower potential for airborne activity.

The detailed classification of areas with respect to the potential for surface and airborne contamination will be the responsibility of the site operator. However, the classification used in Reference 24.49 and shown in Table 24-9 has been adopted here to justify the ventilation arrangements for the various areas.

24.5.6 Nuclear Island Nonradioactive Ventilation System

The VBS serves the MCR, control support area (CSA), Class 1 electrical spaces, and PCS valve room. These areas do not have sources of activity present during normal operation or during fault conditions. The VBS is described in more detail in Section 23.11.

HEPA filters and charcoal absorbers are provided in the MCR/CSA HVAC subsystem.

24.5.7 Annex/Auxiliary Building Nonradioactive Ventilation System

The VXS serves the office areas, switchgear rooms, locker rooms, battery rooms, computer rooms, toilets, and other similar spaces. These areas do not typically have sources of radioactive contamination present during normal operation. The VXS is described in more detail in Section 23.12.

A drain line from the steam generator blowdown system (BDS) to the WLS passes through some of the areas served by the VXS. The drain line can be contaminated by the BDS if there is a fuel leak and SG leakage, or an isolation valve failure. Since the drain system has no valves or connections within the area served by the VXS, and it is gravity drained, the chance of leakage into the VXS area is negligible.

It is not reasonably foreseeable for activity to be present in the areas served by the VXS. The area is classified as a white area for both normal and fault conditions. There is no requirement for HEPA filtration.

24.5.8 Diesel Generator Building Heating and Ventilation System

The VZS supplies air to and exhausts from the diesel generator building. The diesel generator building is a physically separate building. The VZS is described in more detail in Section 23.14

There is no credible source or fault that will result in a radioactive release from the diesel generator building, and thus there is no normal or fault condition. The area served by the VZS is classified as a white area for both normal and fault conditions. There is no requirement for HEPA filtration for radiological protection.

24.5.9 Containment Recirculation Cooling System

The VCS recirculates and cools air within the containment during power operations and shutdown. This results in an energy saving and a reduction in waste generated in the form of used filters when compared with that which will arise from the level of a once-through HVAC system. The air recirculated by the VCS is expected to contain some activity (mostly noble gases and some iodine), although it does not penetrate the containment boundary and therefore does not give rise to any discharges to atmosphere. The VCS is described in more detail in Section 23.4.

During shutdown operations in the containment, local, filtered extract systems will be used for particular operations where airborne activity may be generated. This reduces the potential for airborne activity to be released into the general containment atmosphere, which the recirculation system could spread to other parts of the containment.

The extracted air is continuously monitored for airborne activity that will give an early warning to workers in the containment.

There is no path to discharge the VCS to the environment, hence HEPA filtration is not provided.

24.5.10 Containment Ventilation System

The VFS purges the containment intermittently by providing fresh air from outside and exhausting air to the plant vent stack. The air exhausted by the VFS is filtered with high-efficiency filters, HEPA filters, charcoal filters, and high-efficiency post filters. The VFS also exhausts from areas served by the VAS and VHS after receipt of a high radiation signal in the VAS or VHS exhaust. The VFS is diesel backed to improve its reliability.

A radiation monitor located in the common ductwork downstream of the filtration units is provided to detect deterioration in performance of either ventilation train. These provisions represent good industry practice for ensuring that discharges to the atmosphere and doses to members of the public are ALARP. The VFS is described in more detail in Section 23.3.

The containment is an amber area with a potential for occasional releases. It is, therefore, provided with full-time HEPA filtration on the exhaust.

24.5.11 Health Physics and Hot Machine Shop Heating, Ventilation, Air-Conditioning System

The VHS consists of two 100 percent capacity exhaust fans (duty and standby) with supplies from duty and standby air-handling units sized to allow the system to maintain a negative air pressure differential with respect to adjacent areas.

The hot machine shop provides a location within the controlled area for repair and refurbishment of items of equipment from within the controlled area. This equipment may not actually be contaminated or activated, but it is easier to have a dedicated workshop rather than undertake clearance monitoring, which may not be possible. Operations in the hot machine shop are conventional hands-on work; i.e., there is no provision for remote handling. The routine arisings of airborne contamination from machining operations are not expected to be significant because equipment that can be repaired will be decontaminated beforehand. Equipment that is too active to handle manually and cannot be decontaminated will be packaged and disposed of as radioactive waste.

Airborne contamination from the remaining space extract from the hot machine shop and other areas served by this system is not expected to be significant during normal operations or fault conditions.

The facility has a dedicated decontamination facility with HEPA filtration and a glovebox with HEPA filtration.

Individual machine tools may have local exhaust ventilation arrangements that include HEPA filters. The VHS fans also shut down on a high radiation signal and the exhaust is then directed through the VFS, thus reducing the airflow from the served spaces but allowing for the exhaust to be filtered.

The VHS is described in more detail in Section 23.10.

24.5.12 Radwaste Building Heating, Ventilation, and Air-Conditioning System

The VRS supplies and exhausts air from the radwaste building.

The radwaste building has the following three potential sources of radioactive contamination:

- Tanks for low-level liquid effluent for monitoring and sentencing. The monitor tanks contain water that has the potential of having radiological contamination. The water in the monitoring tanks is not expected to contain significant contamination and will typically be below environmental discharge limits.

- An area for loading packaged solid LLW into containers for dispatch to the low-level waste repository (LLWR). Packaged solid radwaste is stored in the radwaste building. This material is bagged or loaded into storage containers at the point where it is generated/processed, so the chance of a significant release is low. LLW will be sorted, compacted, decontaminated, and size reduced in the radwaste building within ventilated

enclosures. Condensate polishing resins might be LLW in the event of SG tube failures and are encapsulated at the spent resin tank. Other LLW is not encapsulated. LLW processing equipment is currently expected to be permanently installed. ILW processing equipment is mobile. The equipment may be permanently located at each site or may be transportable to undertake campaigns at more than one site.

- The AP1000 design has provisions for portable ILW processing equipment. This equipment will connect to the railcar bay auxiliary building HVAC system (VAS). Therefore, risk of contamination from equipment and processing equipment is small. In addition all potential sources are filtered at the component level.

The VRS is described in more detail in Section 23.9.

The VRS general extract may contain significant airborne activity either during normal operation or fault conditions if the portable radwaste equipment is not properly operated.

The radwaste building is classified as an amber area with potential for significant airborne activity release. Therefore, the VRS extract is equipped with HEPA-filtration as discussed in Section 23.9 of this PCSR.

24.5.13 Turbine Building Heating, Ventilation, and Air-Conditioning System

The VTS serves all areas of the turbine building. The HVAC systems serving the switchgear rooms, rectifier room, security rooms, and plant control system cabinet rooms do not have a credible source of radioactive contamination. The general area of the turbine building is ventilated through roof ventilators. This part of the AP1000 plant does not have a likely source of radioactive contamination. These areas do not have HEPA filtration because it does not offer a significant protection benefit.

The Bay 1 area of the turbine building contains the RCP variable speed drives, component cooling water system (CCS) equipment (a nonradioactive system), and the BDS. The BDS may be contaminated in the unlikely event of concurrent fuel defects, SG leakage, radiation monitor or BDS isolation failure, or a BDS leak. The VTS includes dampers that can be closed if the BDS becomes radioactive (as detected by radiation monitors). This minimises the possible spread of contamination from the BDS room. An exhaust path from the BDS room to the turbine building vent can be actuated to reduce the airborne radioactivity in the BDS room to minimise the contamination level for personnel entry for inspection and maintenance. The VTS is described in further detail in Section 23.13.

The turbine building, except for the Bay 1 area, is a white area. The Bay 1 area is a green area with a very limited potential for airborne release. Therefore, HEPA filtration is not required.

24.5.14 Radiologically Controlled Area Ventilation System

The VAS serves the RCA of the auxiliary/annex buildings. The VAS consists of two separate air supply subsystems, the fuel-handling area ventilation subsystem, and the auxiliary/annex building ventilation subsystem. Both of these subsystems are once-through type ventilation systems.

During normal operation the supply air-handling units and the exhaust fans on each of the ventilation subsystems operate continuously to ventilate the areas served on a once-through basis. The supply airflow rate is modulated to maintain the areas served at a slightly negative pressure differential with respect to the outside environment. The unfiltered exhaust air is directed to the plant vent stack where the radioactive airborne discharges are monitored.

The exhaust air radioactivity is also monitored in the VAS ductwork prior to the monitoring at the plant vent stack. Detection of radiation in the exhaust ductwork will result in the supply and exhaust fans being shut down and initiation of the VFS.

24.5.14.1 Fuel-Handling Area

The fuel-handling area ventilation subsystem supply and exhaust ductwork is arranged to exhaust the SFP area separately from the auxiliary building. It provides directional airflow from the waste disposal container area into the spent resin equipment rooms.

All spent fuel-handling operations are performed under borated water to provide radiation protection. Activity levels in the SFP are controlled by technical specification (Tech Spec). The activity level in the SFP is reduced, if necessary, by transferring a portion of the SFP water to the WLS for discharge and replacing it with clean water. The SFP water is constantly filtered and purified by the SFS.

Routine releases for the fuel-handling area are expected to be low and the potential accidental release is low. However, the fuel-handling area is classified amber, and there is the potential for contamination to be present in the SFP water, which may become airborne if the spent fuel pool were to boil. In addition, the fuel-handling area extract on Sizewell B is filtered. Therefore, HEPA filtration of the fuel-handling area extract is provided as discussed in Section 23A.1.9.1 of this PCSR.

24.5.14.2 Auxiliary/Annex Buildings

The remainder of the radiologically controlled part of the auxiliary/annex buildings exhaust air ductwork is routed to minimise the spread of airborne contamination by directing the supply airflow from the low radiation access areas into the radioactive equipment and piping rooms with a greater potential for airborne radioactivity. Additionally, the exhaust air ductwork is connected to the radwaste effluent holdup tanks to prevent the potential buildup of gaseous radioactivity or hydrogen gas within these tanks. The exhaust fans discharge the exhaust air into the plant vent stack where the radioactive airborne discharges are monitored. The exhaust air radioactivity is also monitored in the VAS ductwork prior to the monitoring at the plant vent stack.

The supply and exhaust ducts are configured so that two building zones may be independently isolated. The annex building staging and storage area, containment air filtration exhaust rooms, containment access corridor, and adjacent auxiliary building staging, equipment areas, middle annulus, middle annulus access room, and security rooms are aligned to one zone. The other zone includes the remaining rooms and corridors, including but not limited to the radiation chemistry laboratory, primary sample room, SFP cooling water pump and HX rooms, RNS pump and HX rooms, CVS makeup pump room, lower annulus, and various radwaste equipment rooms, pipe chases, and access corridors. Radiation monitors are located in the exhaust air ducts of each zone.

All active liquids and resins are contained within system piping and equipment. Routine discharges are low; no single fault will result in higher discharge levels. However, if the radiation monitors detect a high level of radiation, the relevant extract is diverted to the VFS, which contains HEPA filters. The extract can also be diverted manually if particular operations are being undertaken that could result in the release of activity.

The radiologically controlled part of the auxiliary/annex buildings served by the VAS is classified amber with low risk for activity release. Therefore, the extract is not normally filtered, but the VFS is used when needed.

Section 23A.1.11 describes how area radiation monitors (in addition to duct monitors) can actuate the VFS extract filtration.

Where major breaches of containment that could result in airborne contamination are necessary for repairs, suitable local containment and filtered extract ventilation systems are used to control the spread of contamination and reduce discharges.

24.5.15 Main Control Room Emergency Habitability System

The AP1000 design includes an emergency habitability system for the MCR, which consists of a supply from banks of compressed air storage tanks that are available to maintain the MCR environment for up to 11 personnel over a period of up to 72 hours. The VES is initiated by "High-2" particulate or iodine radioactivity in the MCR supply air duct, or the loss of ac power for more than 10 minutes. More details can be found in Sections 6.9 and 23.7 of this PCSR.

24.6 Radiation Monitoring

The RMS provides plant effluent monitoring, process fluid monitoring, airborne monitoring, and continuous indication of the radiation environment in plant areas where such information is needed. Radiation monitors that have a safety-related function are qualified environmentally, seismically, or both. A description of the RMS is presented in Section 6.8.10.

The RMS provides radiation monitoring in operating areas, post-accident monitoring, duct monitoring, effluent monitoring, and process and fluid monitoring.

In addition, personal monitoring of exposure of all workers in the RCA will be undertaken by the plant operator in compliance with the IRR99. PADs will be used for short-term dose control in particular during refuelling and maintenance activities as part of the arrangements for ensuring that doses are ALARP. The operator may require the universal use of PADs for all work within the RCA and sufficient capacity has been provided in the conceptual design for their storage. Dose budgets will be prepared for specific operations (similar to the JEM calculations in Appendix 24B) and dose received will be compared against the initial estimates to provide assurance that best work practices are being followed and to determine where improvements can be made.

Data obtained during refuelling and maintenance operations will be used to identify tasks where dose reduction efforts should be concentrated.

24.6.1 Area Gamma Monitors

Area radiation monitors are installed in locations listed in Table 24-11. The CSA monitor is in the annex building outside the RCA and is provided for post-accident monitoring.

The permanent area monitors in the fuel-handling area are physically separated by a large distance and have overlapping fields of view to enable them to monitor for increasing radioactivity that could be an indication of fuel reaching criticality. Each monitor can detect radiation from a fuel criticality accident in the areas occupied by personnel where fuel is stored and handled. Indication and alarms are also provided in the MCR.

Additionally, area monitors provide signals to the C&I systems that are used for control of various ventilation systems, as described in Section 23A.1.11 of this PCSR. This allows for filtration of airflow upon detection of a high radiation signal.

24.6.2 Post-Accident Area Monitors

Post-accident area monitors include the following:

- **Containment high-range radiation monitors** – These four monitors measure the radiation from the radioactive gases in the containment atmosphere. The data are displayed in the MCR. Alarms are provided in the MCR and signals to the protection and safety monitoring system for containment air filtration isolation (High-1) and RNS valve closure (High-2) and containment isolation. The monitors have a nominal range of 10 mSv/h to 105 Sv/h.

- **Primary sampling room area monitor** – The primary sampling station is the location where samples are collected after a postulated accident. The monitor provides local readout, and audible and visual alarms are visible upon entry into the sampling room. Indication and alarm are also provided in the MCR.

- **CSA monitor** – The CSA is the location from which engineering support will be provided to the operators following a postulated accident. A local readout, and audible and visual alarms are visible upon entry into the CSA. Indication and alarm are also provided in the MCR.

- **Fuel-handling area criticality monitors** – Two radiation monitors perform general area monitoring of the fuel-handling and storage areas. Any increase in this could be an indication of fuel reaching criticality. The area radiation monitoring is augmented during fuel-handling operations by a portable radiation monitor on the fuel-handling machine. A criticality excursion will produce an audible local alarm and an alarm in the MCR.

24.6.3 Discharge Duct Monitors

Radiation monitors set up to detect the principal noble gases present (Kr-85 and Xe-133) are located in the extract ducts from the fuel-handling area, auxiliary/annex building (VAS), and containment purge extract (VFS). The ducts from the VRS and the VHS are monitored for Sr-90 and Cs-137.

Releases from fuel or primary coolant will include releases of noble gas. The VAS and VHS monitors will stop the associated supply and exhaust systems, and start the VFS extract to filter all extract from the impacted area. The VFS maintains the affected area at a negative pressure with respect to atmosphere, so that there is no unfiltered release to atmosphere during or after an abnormal release into the areas served by the VAS.

The VFS and VRS duct monitors alarm on a high signal, but do not stop the associated fans. The high signal alarms from VFS and VRS are displayed in the MCR to allow operators to determine the appropriate manual actions.

24.6.4 Main Control Room Supply Air Duct Monitors.

Radiation monitors (for I-131, Kr-85, Xe-133, Sr-90, and Cs-137) measure the concentration of radioactive materials in the air that is supplied to the MCR. The monitors initiate the supplemental air filtration system on High-1 gaseous, particulate, or iodine activity concentrations, isolate the air intake and exhaust ducts, and activate the VES on either High-2 particulate or High-2 iodine concentrations. Alarms are provided in the MCR.

24.6.5 Process Fluid Monitors

Fluid process, airborne, liquid, and gaseous radiation monitors include the following:

- **BDS radiation monitors** – The presence of radioactive material in the BDS indicates a leak between the primary and secondary side of the SG. The monitor initiates an alarm in the MCR, initiates closure of the SG blowdown containment isolation and flow control valves, and diverts flow to the WLS.

- **CCS radiation monitor** – Radioactive material in the CCS indicates leakage. The monitor initiates an alarm in the MCR for operator action.

- **Main steam line radiation monitors** – Radioactive material in the main steam line provides early indication of leakage in the form of an SG tube leak. The monitor initiates an alarm in the MCR for operator action.

- **Service water blowdown radiation monitor** – The monitor measures the concentration of radioactive materials in the blowdown flow from the service water system. The monitor initiates an alarm in the MCR for operator action.

- **PSS liquid sample radiation monitor** – The monitor's principal function is to indicate elevated reactor coolant sample radiation levels following a design basis event or severe accident. It may also be used to provide early indication of a possible fuel-cladding breach. The monitor isolates the sample flow and initiates an alarm in the MCR for operator action and locally.

- **PSS gaseous sample radiation monitor** – The monitor provides indication of significant radioactivity in a gaseous sample taken from the containment atmosphere. The monitor initiates an alarm locally and in the MCR for operator action.

- **Gaseous radwaste discharge radiation monitor** – The monitor provides an alarm in the MCR and terminates the release of radioactive gas to the plant vent by closing the discharge isolation valve when a predetermined setpoint is exceeded.

- **Containment atmosphere radiation monitor** – The containment atmosphere radiation monitor is part of the reactor coolant pressure boundary leak detection system described in Chapter 21.

- **Turbine island vent discharge radiation monitor** – This monitor measures the concentration of radioactive gases in the steam and non-condensable gases that are discharged by the condenser vacuum pumps and the gland steam condenser. This measurement provides early indication of leakage between the primary and secondary sides of the SGs. The monitor provides an alarm in the MCR for operator action.

- **Liquid radwaste discharge radiation monitor** – The liquid discharge monitor provides signals to isolate the discharge of liquid radwaste, stop the discharge pumps, and provide an alarm to the MCR if concentration exceeds a predetermined setpoint.

- **Waste water discharge radiation monitor** – Upon detection of radioactivity concentrations above a predetermined setpoint, an alarm in the MCR will be initiated. The C&I control system will isolate the discharge line, and the turbine drain tank pumps will be automatically tripped to stop further discharge. Following the alarm, the operator can manually realign the discharge to the Liquid Radwaste System for processing.

24.7 Operational Health Physics

The operational health physics organisation is the responsibility of the plant operator. Radiation Protection Advisers (RPAs) will be appointed to advise the operator on compliance with the IRR99. These RPAs may be separate from the executive control of health physics surveyors but will be required to advise on radiological protection requirements for permits to work, suitable PPE including respiratory protective equipment, and precautions on entry into areas with high radiation or contamination. The RPA will advise on the preparation of local rules for working in the RCA.

The plant operator will also be required to appoint Radiation Protection Supervisors (RPSs) according to the IRR99 to ensure compliance with local rules and permit-to-work conditions. The plant operator will also decide on the organisational structure of operational health physics (for example, consideration may be given to self monitoring at workplaces to reduce doses to health physics surveyors).

Provisions have been made for health physics operations in the AP1000 design although flexibility remains within the annex building for detailed arrangements, and there are no restrictions on additional facilities outside the power block.

24.7.1 Issue, Storage, and Maintenance of Dosimeters

Personal dosimetry will consist of the following:

- Statutory "whole body" dosimeters, e.g., thermoluminescent dosimeter (TLD) for monitoring of external dose as required under the IRR99
- Extremity monitoring (e.g., finger and head TLDs) for monitoring extremity dose for compliance with the IRR99
- PADs for monitoring external dose on a daily or task basis
- Personal air samplers where airborne activity is of concern

PADs can be issued from the Health Physics Booth (Figure 24-6), which is located in a suitable low-background area in the annex. The type of dosimetry and alarm settings will be dictated by the permit-to-work requirements, which can also be issued from the Health Physics Booth.

Statutory "whole body" monitors may be issued separately from an administrative area depending on the approved dosimetry service arrangements made by the operator for processing and recording doses. However, it is likely that the plant operator will need to operate as an approved dosimetry service at least for extremity dosimeters.

Urine samples may also be required for bioassay. Urine sampling to assess tritium exposure is likely to be required but faecal sampling will probably not be necessary. Because it is important to avoid cross contamination, part of the change rooms could be designated for urine samples or facilities could be provided outside the power block.

24.7.2 Portable Survey Equipment

Portable radiation survey instrumentation is stored at the Health Physics Booth and at in-plant control points. This instrumentation allows plant personnel to perform radiation, contamination, and neutron surveys, as needed, as well as collect samples of airborne activity for analysis. Transportable activity in air monitors may be used for operations where airborne contamination may be generated and where local control measures such as tenting are implemented.

The specification of the type and number of portable instruments will be the responsibility of the plant operator.

24.7.3 Calibration and Maintenance of Radiological Protection Instrumentation

There is no specific provision for calibration and maintenance of radiological protection instrumentation (RPI) within the existing AP1000 design. Functional testing will be carried out in situ. It will be the responsibility of the plant operator to make arrangements for annual examination and testing of all RPI (including PADs) in accordance with the IRR99. These arrangements may be outside the power block, at a central location offsite, or with a third party.

24.7.4 Collection of Liquid and Gaseous Samples for Radioactive Analysis

A summary of the samples likely to be taken on AP1000 design is given in Table 24-1. In addition, representative air samples will be taken from the main discharges stack and may be taken from workplaces using static air samplers.

The analysis of the samples will depend on their purpose and the level of activity present. Some samples will be prepared and analysed within the RCA. To avoid cross contamination, operational restrictions ensure that environmental samples may not be brought into the RCA for analysis. The plant operator may carry out analysis elsewhere onsite or at a central facility, or have the analysis undertaken by a third party.

24.7.4.1 Radiochemistry Laboratory

The radiochemistry laboratory (Room 12252) on the 94.666 m (82’-6”) level is equipped to prepare and analyse primary coolant samples.

24.7.4.2 Secondary Sampling Laboratory

The laboratory for analysing samples from the secondary circuit is located at the far end of the turbine building from the reactor (Figure 24-13). Dose rates from these samples, under normal operating conditions will be very low. The secondary sampling laboratory is not part of the RCA.

24.7.4.3 Counting Room

A room is provided in the health physics area of the annex building for analysis of swabs, filters, and other items using α, β, and γ counting equipment and γ spectrometry. Fly ash must not be used, or must be assayed and found to be below applicable limits before being used in the construction of these rooms to support a low background.

24.7.5 Job Planning Facilities

Areas, such as the ALARA briefing and operational support room in the annex building, are provided for familiarising personnel with plant procedures for both routine and nonroutine inspection and maintenance operations. Access will be provided to detailed plans, drawings, photographs, videotapes, previous inspection reports, previous radiation and contamination surveys, or previous work plans appropriate to the particular job prior to entry into radiation areas.

Procedures for routine inspection and maintenance operations will be reviewed before an outage to ensure that any lessons learned from previous outages have been incorporated.

24.8 Handling of Radioactive Waste

The following facilities form the AP1000 plant solid radioactive waste management system:

- Radwaste building
- Mobile encapsulation unit (MEU)
- ILW store
- Spent fuel store

These facilities were identified from the BAT assessment (Reference 24.20) as the preferred technique for dealing with the expected radioactive wastes. Throughout the design development (including the BAT assessment), efforts were made to gather information from other similar designs, processes, and facilities along with the experience of station operators. The Learning From Experience process (also called Lessons Learned) is an important feature of BAT. The information and data were ascertained in several ways:

- Literature research, e.g., Nirex documents, research papers
- Reference to previous designs, e.g., Sizewell B
- Liaison with equipment manufacturers, e.g., self-propelled transporters
- Liaison with utility companies and station operators to ascertain current waste-handling practices in the UK and abroad and some of the difficulties encountered, e.g., RWE, Engie (Tractebel), Iberdrola, Endessa, Vattenfall, British Energy (Sizewell B)

The radwaste building footprint and layout may change during site-specific detail design, when an exact radwaste-handling regime has been agreed. The owning utility may choose to increase the building size, build a separate radwaste treatment building, embrace a contractual radwaste management system, or use a combination of these options.

Cementitious encapsulation was derived from the BAT assessment as the current favoured technique for processing ILW. During site-specific detail design, utility companies can reassess this and may choose to adopt different systems. Overall, it is important to note that other techniques are available and these should be reconsidered at appropriate intervals to determine the suitability and maturity of new technologies and methods.

The LLW and ILW streams arising from the operation and maintenance of the AP1000 plant are shown in Table 24-13. The ion exchange resins, activated carbon, and filter cartridges have been identified as the only ILW arising from the AP1000 plant. These will be encapsulated in the auxiliary building rail car bay by the MEU. Therefore, all wastes entering the radwaste building will be classified as LLW or lower, negating the need for ILW-handling facilities within the LLW area.

24.8.1 Receipt of Solid Low-Level Waste

Solid LLW from the auxiliary building and containment can either be taken into the rail bay and then through the truck staging area into the radwaste building or via the annex building containment access corridor and radwaste building access corridor into the truck staging area. The solid LLW will be received at the radwaste building buffer/marshalling area (temporary container storage bay). The buffer/marshalling area (temporary container storage bay) is located in the northeast corner of the LLW processing area (Waste Accumulation Room 50351). LLW arising from the AP1000 plant will be collected and placed into specific bags/containers that are distinguished from nonactive waste bags/containers; for example, through colour. In general, wastes collected from radiation/contamination-controlled areas will be assumed to be LLW and treated as such until assessed and categorised.

As described in Reference 24.51, when collected, LLW will be transferred from the AP1000 plant areas to a temporary storage bay (buffer/marshalling area) located within the radwaste building until required for sorting. This is a tried and tested method currently implemented on existing nuclear sites across the UK.

24.8.2 Sorting and Packaging of Solid Low-Level Waste into Drums

Solid LLW will be sorted and packaged into drums in the LLW processing area of the radwaste building using a sealed and vented glovebox. When called for, an LLW container/bag will be transferred from the storage bay to the sorting glovebox, delidded/opened, and the LLW tipped onto a sorting table. The LLW will be sorted and graded by waste type and/or activity level and placed in drums ready for compaction/ISO loading, clearance monitoring, or offsite treatment (Reference 24.51, Section 3.4.5.4). This is a tried and tested method currently implemented on existing nuclear sites across the UK.

Solid wastes will, as far as practicable, be segregated and sorted at the source to minimise primary and secondary wastes (including labelling to identify the source, if required).

24.8.3 Characterisation of Solid Low-Level Waste

Solid LLW will be characterised and assayed in the radwaste building by a low-resolution gamma spectrometer (LRGS). The LRGS will be located in an area of low background activity, or will have additional shielding installed to ensure that measured count rates are attributable to emissions from the waste drum. The LRGS will be integrated with the package tracking system (Reference 24.51, Section 3.7.15.2).

The radwaste building layout shows the position of the LRGS in the Mobile Systems Facility Room 50350 directly adjacent to the door leading into the LLW processing area (Waste Accumulation Room 50351). During site-specific detail design this position could change, or local shielding may be added if the area's background radiation impedes the functionality of the LRGS.

24.8.4 Size Reduction and Decontamination of Solid Radioactive Waste

The only radioactive waste that will be subjected to size reduction and decontamination is LLW, and this will be performed using (enclosed and vented) workstations and in-drum compactor within the LLW processing area of the radwaste building.

During sorting, some of the waste may be removed from the sorting glovebox via temporary containers for reduction in size and/or decontamination at the enclosed workstations. The size reduction workstation will contain simple dismantling and cutting tools (i.e., spanners, cutting shears). The decontamination enclosure could include a small wet area for washing/wiping/scrubbing with decontamination solutions, as well as manual cleaning cloths/swabs. The selection of decontamination and size-reduction techniques will be part of the detail design stage (based on site preference and experience), but will emphasise avoiding increased generation of secondary wastes. On completion of the size reduction/decontamination, the waste is transferred back to the sorting glovebox via temporary containers for further sorting (Reference 24.51, Section 3.4.5.4).

As drums within the sorting glovebox are filled, a spring-back disc is placed on top of the compactable waste, the drum moved to the compactor unit, and the waste compacted. Following compaction, if the drum still has space for additional waste, it is returned to the filling position to allow additional waste to be added. This process of filling and compacting is repeated until the drum is full. Thereafter, the drum is lidded and sealed (Reference 24.51, Section 3.4.5.4).

24.8.5 Storage of Drummed, Solid Low-Level Waste

Drummed solid LLW will be placed into an HHISO container within the radwaste building prior to transit offsite to the LLW repository. Sealed, fully compacted drums are assayed using an LRGS. The information obtained during this assay is used as the basis for the final categorisation and sentencing arrangements for the drum (Reference 24.51, Section 3.4.5.4).

The HHISO loading area (and/or northern loading bay) of the radwaste building can be reconfigured if required to package waste in accordance with the conditions for acceptance of other offsite treatment facilities.

24.8.6 Storage of Large Low-Level Waste Items

Large items of LLW that cannot be size reduced and cannot be placed into drums are wrapped and placed directly into an HHISO container. This activity is conducted within the radwaste building.

Large LLW items will be transported to the radwaste building by suitable means (e.g., manual trolley, forklift truck, flatback lorry) and placed into the buffer/marshalling area. Where such items are too large to be moved within the building they would be wrapped and monitored for contamination in the containment access corridor and then be transported to the mobile systems facility area of the radwaste building outside the building.

Any waste that is too large to be packaged into a drum and cannot be reduced in size is wrapped before being passed through QA and placed directly into an HHISO container (Reference 24.51, Section 3.4.5.4).

Although not expected, the only large solid radwaste item that could be generated during the operation period of the AP1000 plant is the SGs. It is expected that the SGs will be radioactive but with an activity level that will fall into the LLW category. It is intended that these items are handled as they arise, are size reduced, and are decontaminated to the extent practicable. To facilitate this disposal route, a temporary facility could be erected; for example, a tent with mobile HVAC equipment and connections to AP1000 plant power, water, and air systems, as necessary (Reference 24.51, Section 3.5.7.1).

24.8.7 Loading Solid Low-Level Waste into Transport Packages

When LLW has been processed (decontaminated, size reduced, packaged, and assayed), it will be loaded by the radwaste building crane (using safe slinging/lifting methods for large loads) or a forklift truck into an HHISO container ready for dispatch offsite to the LLW repository.

After drums have completed QA, they are placed in an HHISO container positioned within the radwaste building (Reference 24.51, Section 3.4.5.4).

24.8.7.1 Storage of Filled Low-Level Waste Transport Packages Prior to Dispatch Offsite

Full HHISO containers (transport packages) can be stored in the LLW buffer store or remain in the loading bay of the radwaste building if the LLWR is not immediately available.

The LLW buffer store is a covered area comprising a concrete hard-standing area with a steel-framed overcanopy. The buffer store is designed for HHISO containers that have been filled in the radwaste building. Standard handling machinery (forklift truck) will be used to move the containers from the radwaste building to the buffer store. The combined capacity for HHISO containers within the buffer store and the radwaste building provides for up to 2 years waste arisings if the disposal route to the national LLW repository is temporarily unavailable (Reference 24.51, Section 3.2.1.3).

24.8.8 Conditioning of Intermediate-Level Waste

ILW will be encapsulated/conditioned using the MEU deployed within the auxiliary building rail car bay. The waste encapsulation will be carried out on a campaign basis. When not in use, the MEU will be stored in the radwaste building and moved to the AP1000 plant auxiliary building rail car bay for the campaign (Reference 24.51, Section 3.4.2.1). The MEU may be shared with other plants onsite or offsite.

24.8.9 Packaging of Intermediate-Level Waste

The MEU will be used to process ILW in the form of ion exchange resins, carbon guard bed media, and primary circuit filters. The MEU will encapsulate/immobilise the ILW in a cement matrix within a 3-m^3 (106 ft^3) Radioactive Waste Management Directorate (RWMD)-compliant container.

Dry ILW (primary circuit filters) is loaded into a 3-m^3 (106 ft^3) box that is positioned in the Waste Disposal Container Area, Room 12374. When the box is full or at a time to suit encapsulation campaigns, the boxes will be transferred to the MEU using the rail car bay crane.

During this transfer the rail car bay will be vacated and access prohibited to ensure that operator dose uptake is ALARP (Reference 24.51, Section 3.4.3.4).

Wet ILW (spent resin) will be pumped via shielded pipe work from a position local to the MEU directly into a 3-m^3 (106 ft^3) RWMD-compliant drum ready for encapsulation.

24.8.10 Characterisation of Intermediate-Level Waste

The packages will then be loaded into a shielded transport overpack for transfer to the ILW buffer store.

ILW packages will be assayed (characterised) in the ILW store import bay using a high-resolution gamma spectrometer (HRGS). The HRGS will be located in an area of low background activity or will have additional shielding installed to ensure that measured count rates are attributable to emissions from the waste drum. The HRGS will be integrated with the package tracking system (Reference 24.51, Section 3.7.16.1).

24.8.11 Buffer Storage of Intermediate-Level Waste Packages

The transporter bringing the packaged ILW from the rail car bay in a shielded overpack will enter via a shielded door and park in the package import bay of the ILW store. The waste packages will be transferred out of the overpack and into the shielded import bay. The import bay will be equipped with an HRGS and closed-circuit television cameras to assay and visually check the package. Other checks that may be necessary are dependent on visual inspection of the package (Reference 24.51, Section 3.4.7.1).

It is envisaged that, after immobilisation, the ILW packages will be immediately transferred to the ILW store. However, if the transport vehicle and overpack are not available, the encapsulated packages could be held temporarily within the MEU.

24.8.12 Personnel Access to Radwaste Building

Personnel involved in radioactive waste management will enter the RCA through the main entry area in the annex building, which limits access to authorised personnel. Additional PPE will be obtained at the subchange area within the annex building access corridor into the radwaste building work areas.

Egress from the radwaste building is via the subchange area, in which the protective clothing will be removed and placed in contaminated clothing containers (Reference 24.51, Section 3.4.6.1). Hand and foot contamination monitors and frisking probes will be provided at the subchange area for monitoring prior to return to the main RCA entry area.

The Monitor Tanks Room 50355 and Waste Accumulation Room 50351 within the radwaste building are classified as C2 areas and can only be accessed through a secondary subchange located in the northwest corner of the Waste Accumulation Room 50351.

24.8.13 Storage and Monitoring of Nonactive Wastes from the Radiologically Controlled Area

Very LLW/nonactive wastes can be generated through maintenance activities within the RCA and during decontamination/size reduction of LLW. These nonactive wastes will be monitored using the existing LLW monitoring equipment within the radwaste building, placed into bags/drums, and then transferred to the clearance and exemption area. The clearance and exemption area is located to the southeast of the Waste Accumulation Room 50351 within the Mobile Systems Facility Room 50350.

This area will be used for clearance monitoring of the waste to ensure it meets the required limits for disposal. Within the clearance and exemption area there is a working table and non-active waste clearance monitoring equipment. The exact equipment will be chosen at the detail design stage, depending on utility preference and experience.

Once the waste has been monitored and cleared it will be loaded into a dedicated HHISO container positioned to the west of the LLW HHISO loading area.

24.8.14 Radwaste Processing Dose Assessment

Radwaste processing involves the following facilities:

- Radwaste building
- Auxiliary building WLS, WGS, and WSS facilities
- Auxiliary building rail car bay (MEU)
- ILW store

24.8.14.1 Radwaste Building Occupancy

The total occupancy of the radwaste building is presumed to be 1280 man-hours per year: this is based on 4 workers, 8 hours per day, 5 days per campaign, 8 campaigns per year (i.e., 320 hours per year).

This figure is an estimate, taking into account the annual LLW arisings to be 8 HHISO containers (Reference 24.52) and each container taking 5 days to fill (8 campaigns of 5 days). During each campaign it is estimated that 4 workers will be required to operate the following radwaste equipment:

- Sorting glovebox
- Work stations (decontamination and size reduction)
- LRGS
- In-drum compactor
- Forklift
- Building crane
- Remote operation of the MEU (during ILW encapsulation campaigns)

24.8.14.2 Auxiliary Building Rail Car Bay (Mobile Encapsulation Unit) Occupancy

A conservative occupancy of 2000 hours per year (50 weeks per year, 5 days per week, 8 hours per day) has been used as the criterion for the surface dose rate limit on the MEU. This was taken as the worst-case scenario, in that other workers will be in the rail car bay performing unrelated tasks during the MEU operation. This is a very conservative value as the MEU is expected to be in operation for only 3 months of the year and the rail car bay will be used for other purposes, including import of new fuel and, in time, export of spent fuel; therefore reducing the maximum occupancy with the MEU present down to 480 hours (12 weeks per year, 5 days per week, 8 hours per day). The occupancy directly resulting from operation of the MEU is assumed to be 180 hours (3 hours per day, 5 days per week, 12 weeks per year), which is based on a 3-month ILW encapsulation campaign every 12 to 18 months, depending on the chosen refuelling cycle. Due to the remote operation design of the MEU, 3 hours per day is judged to be required for manual observation and recovery of the MEU. If it is assumed that 2 workers are involved, then the total time will be 360 man-hours. This is still a very conservative estimate, as under normal conditions manual intervention will only be required during setup and dismantling.

24.8.14.3 Intermediate-Level Waste Store Occupancy

A conservative occupancy of 2000 hours per year (50 weeks per year, 5 days per week, 8 hours per day) has been used as the criterion for the surface dose rate of the ILW store external wall. This was taken as the worst-case scenario on the grounds that other workers could be in the vicinity of the ILW store performing unrelated tasks.

It is envisaged that the ILW store will only require operators during the import and random inspection of packages. During the import of a package to the store it is assumed that the following workers will be required:

- One worker is required to operate the transporter within the import/export area.
- One or two workers are required in the ILW store control room.

The AP1000 plant will produce 19 ILW packages per year (Reference 24.51, Table 5) for storage within the onsite ILW store. Assuming the import of a package takes 1 day, the resulting occupancy will be 152 hours per year occupancy per worker.

During the inspection of a package it is assumed that one or two workers will be required in the control room for up to 40 hours per package.

Waste packages will be placed in vaults in the ILW store but these will remain open to allow packages to be retrieved for inspection. The packages could be retrieved using the existing emplacement equipment in reverse. The aim is to have the capacity to retrieve any targeted package within one week (Reference 24.53).

Currently, an ILW stored package monitoring strategy (Reference 24.49) does not exist. This will be developed during the site-specific design stage. Inspection and monitoring of ILW packages is discussed in PCSR Chapter 26, Radioactive Waste Management (Section 26.8.5.2). The total hours of occupancy related to monitoring is 1116 x 40/60 = 744 hours per worker, per year, giving a total occupancy of 1944 hours per year ((152 x 3) + (744 x 2)), with a maximum per worker of 896 hours per year (152 + 744).

24.8.14.4 Anticipated Dose Rate Profile of the Facility

The dose target for individual annual dose from radwaste operations is taken as the BSO (Table 24-1), i.e., 2 mSv.

The provisional radiological areas classifications for the radwaste building, the rail car bay during an encapsulation campaign, and the ILW store presented below will require further evaluation, by an agreed methodology, during the detailed design work associated with a specific site (Reference 24.51, Section 3.8.3).

Radwaste Building

A radiological classification of the radwaste building (Table 24-14) has been developed by the design team but will require review and endorsement by a RPA during detailed design. Radiation and contamination zone drawings have been developed supporting the classification assessment.

Ultimately, the area classification zoning is produced and implemented by the licensee during the specific site licensing stage (in line with site licence condition 18 (Reference 24.55)).

For the purpose of the GDA an existing Sellafield/British Nuclear Fuels Limited (BNFL) guidance (Tables 24-15 and 24-16) has been adopted (Reference 24.56, Pages 31 and 33).

The following radwaste building areas have been zoned R2:

- Mobile Systems Facility Room 50350
- HVAC Equipment Room 50353
- Truck Staging Area 50354
- Monitor Tanks Room 50355
- East-west radwaste corridor

This is very conservative, in that only during abnormal operations or when a HHISO is fully loaded could the dose enter this range. In these conditions the dose will be local to the source (i.e. HHISO) and could be managed and access limited through the erection of temporary barriers as required. During normal operation this dose would be much less, in line with an R1 classification (2.5 to 7.5μSv/h).

From the classification assessment the dose rate for the personnel access area of the radwaste building can be substantiated as 2.5 to 7.5μSv/h for the main area, and 7.5 to 25μSv/h for the LLW processing area. For this dose estimate it is assumed that the occupancy is evenly divided between these two areas.

Based on an individual occupancy of 320 hours per year and a collective occupancy of 1280 man-hours per year, the individual annual dose will be between 1.6 and 5.2 mSv, and the collective dose will be between 6.4 and 20.8 person-mSv. Realistically, most of the area will be at the lower limit and, therefore, a collective dose from an average dose rate of 6.5 μSv/h is reasonable, giving a collective dose of 8 person-mSv.

This results in an annual operator dose uptake at the target limit of 2 mSv. This is only an estimate, and the information supporting it is very conservative. If, during site-specific detail design, these values are substantiated, the site licensee could control the dose uptake through developed operating procedures.

Rail Car Bay (Mobile Encapsulation Unit)

The contact dose rate design specification for the MEU is designed to be 1μSv/h. The MEU will be deployed in the AP1000 plant auxiliary building rail car bay, and it has been assumed that there is an increased potential for operational staff to be in the area. Therefore, because of the increased occupancy, a lower dose limit is appropriate. The dose rate limit is determined by assuming a conservative occupancy of 2000 hours per year (50 weeks per year, 5 days per week, 8 hours per day) and a target annual dose of 2 mSv/y. This leads to a surface dose rate limit for the MEU of 1μSv /h (Reference 24.51, Section 3.9.2.3).

It was also assumed that the contact dose rates applicable to the overpack will be 50 μSv/hr. These dose rates can be reassessed during the detailed design phase associated with the specific site (Reference 24.51, Section 3.9.2.3).

The contact dose rate is used as a worst case; actual dose rates could be much less due to the distance from the source within the MEU. The contact dose rate specification of 1μSv/h is based on an occupancy value of 2000 hours per year (worst case, other personnel working in the area) and a dose target of 2 mSv per year.

As stated in Section 24.8.14.2, the actual occupancy directly resulting from operation of the MEU is estimated as 180 hours (substantially less than the assumed 2000 hours), giving a yearly dose uptake of 0.18 mSv using the current dose rate of 1μSv/h and a collective dose of 0.36 person-mSv per year.

The main operation of the MEU will be done remotely from within the radwaste building. The occupancy resulting from the operation of the MEU remotely is 480 hours per year (8 hours per day, 5 days per week, 12 weeks per year), which is based on a 3-month ILW encapsulation campaign.

There will be some additional dose from handling the shielded transport overpacks and transporting them to the ILW store. Assuming 2 workers are exposed for 1 hour per package at the contact dose rate of 50 μSv/h, the individual dose is 0.95 mSv and the collective dose is 1.9 person-mSv. The actual doses will be significantly lower, as the dose rate will fall with distance from the overpack and only a fraction of the operation will be close to the overpack. A reduction by 50 percent is reasonable to account for distance, giving a collective dose of 0.95 person-mSv.

Intermediate-Level Waste Store

The contact dose rate of the ILW store external wall is designed to be 0.5 μSv/h based on a target dose for others onsite of 1 mSv/y and a pessimistic occupancy of 2000 hours per year. In addition, the design will take account of the external dose rate at the site boundary and at the nearest habitation and workplace.

The actual occupancy directly resulting from operation of the ILW store is estimated as 896 hours (substantially less than the assumed 2000 hours), giving a yearly dose uptake of 0.448 mSv using the current dose rate of 0.5 μSv/h. Assuming 2 workers are present, the collective dose will be 0.896 person-mSv.

There will be some additional dose from handling the shielded transport containers at the ILW store. It can be assumed that the doses from unloading and emplacing packages will be the same as for loading the package onto the transport vehicle.

Total Dose from Radwaste Operations

The total collective dose from radwaste operations assessed above is 11.2 person-mSv. The overall collective dose in an outage year (based on 11 operators) includes a contribution of 22 person-mSv for waste processing. Therefore, the overall collective dose estimate includes a reasonable margin.

24.8.15 Design Features for Control of Surface and Airborne Contamination

Surfaces that may experience contamination will be finished with a decontaminable coating in preparation for decommissioning. In radioactive areas the materials for surface finishes must also be radiation tolerant (Reference 24.51, Section 3.5.14).

24.8.15.1 Radwaste Building

In addition to the overall radwaste building HVAC system, there is a requirement for a local dedicated air extraction system for the removal of any airborne waste particles within the following working enclosures:

- Sorting glovebox
- In-drum compactor enclosure
- Size reduction enclosure
- Decontamination enclosure

The air extraction system design will be based on established HVAC principles used within the nuclear industry and will incorporate flexible/adjustable overhead extraction hoods for large item size reduction. The LLW sorting, size reduction, and decontamination areas will be fully contained within a glovebox to mitigate the possible spread of contamination. Also the compaction of LLW is performed within the drum by an in-drum compactor to limit the spread of contamination. The spread of contamination is controlled through good housekeeping and dedicated HVAC hoods.

Waste will enter and exit the LLW processing area (Waste Accumulation Room 50351) via the west door. The threshold will act as a radiological control boundary. Package movements within the radwaste building but external to the Waste Accumulation Room 50351 will be achieved using the building crane or forklift. Package movements within the Waste Accumulation Room 50351 will be achieved using a dedicated pallet truck. Any waste packages leaving the LLW processing area will be fully swabbed and cleaned prior to crossing the threshold.

24.8.15.2 Rail Car Bay (Mobile Encapsulation Unit)

The MEU requires connections to the auxiliary building HVAC system to do the following (Reference 24.51, Section 3.4.4.3):

- Maintain containment by ensuring that air always flows towards areas with a relatively higher degree of contamination potential
- Provide a safe working environment for operating personnel
- Provide a satisfactory working environment for equipment
- Remove any airborne particulates from the discharge air to ensure that emissions are within the agreed limits for the module
- Provide sufficient ventilation to prevent any heat buildup and to maintain the temperature within the agreed limits for the module
- Maintain an air depression relative to ambient during operation of the encapsulation plant module to minimise the risk of an unmonitored release to the environment outside of the module

Additional details of the auxiliary building rail car bay HVAC systems are presented in Chapter 23.

The MEU is a fully shielded unit and sealed container used to mitigate the spread of contamination. The internals of the unit are capable of being washed down with demineralised water in the event of contamination through spillage. The washdown water is recycled through the process and used for further encapsulation. Packages leaving the MEU will be subject to QA testing and, where necessary, decontaminated through swabbing.

24.8.15.3 Intermediate-Level Waste Store

The ILW store will have its own independent ventilation plant (Reference 24.51, Section 3.6). Environmental conditions such as flow, temperature, moisture, and chloride content will be controlled by ventilation supplied at a low level via a plenum and by extract at a high level from the opposite end of the vault. The store will have inlet and outlet HEPA filters (Reference 24.51, Section 3.4.7.10). The condition of the stored packages will be routinely checked and where necessary remedial work will be conducted. ILW package import/export area of the ILW store. The ventilation system in this area will ensure a suitable cascade is provided to prevent migration of any contamination to the external environment (Reference 24.51, Section 3.4.7.1).

24.9 References

24.1 "Safety Assessment Principles for Nuclear Facilities," Revision 0, Office for Nuclear Regulation, 2014.

24.2 UK Statutory Instrument No. 3232, "The Ionising Radiations Regulations," 1999.

24.3 UK Statutory Instrument No. 675, "The Environmental Permitting (England and Wales) Regulations," 2010.

24.4 UK Statutory Instrument No. 2975, "The Radiation (Emergency Preparedness and Public Information) Regulations," 2001.

24.5 UK Statutory Instrument No. 2975, "REPPIR Regulations 14(2), (3) & (4), Provisional HSE Internal Guidance on Dose Levels for Emergencies," 2001.

24.6 NRC 10 CFR Part 50 Appendix A, "General Design Criteria for Nuclear Power Plants," U.S. Nuclear Regulatory Commission.

24.7 NUREG/CSD-2/V2/R7, Section F7, Rev. 0, "ORIGEN-S: Scale System Module to Calculate Fuel Depletion, Actinide Transmutation, Fission Product Buildup and Decay, and Associated Radiation Source Terms," 2004.

24.8 Westinghouse Document CN-REA-06-20, Rev. 0, "ORIGEN-S, Version 2.0 Software Change Specification and Validation Package," 2006.

24.9 Westinghouse Letter LTR-REA-04-46, Part 1, Rev. 0, "FIPCO User's Manual," April 2004.

24.10 Westinghouse Document CN-REA-08-6, Rev. 0, "Implementation and Validation of a Fully Implicit Solver for the FIPCO Computer Code," 2008.

24.11 Westinghouse Letter LTR-REA-03-45, Rev. 0, "Software Release Letter for CORA Version 2.0," April 2003.

24.12 Westinghouse Document CN-REA-09-92, Rev. 0, "Software Change Specifications and Validation for CORA Version 3.0," 2010.

24.13 Not used.

24.14 Not used.

24.15 Westinghouse Document CN-REA-02-18, Rev. 0, "Software Change Specification and Software Validation Package for SSP Version 3.5," May 2002.

24.16 Westinghouse Letter LTR-REA-01-141, Rev. 0, "Release of SECONS Version 1.4," December 2001.

24.17 Westinghouse Document CN-REA-01-56, Rev. 0, "Software Change and Validation Package for SECONS Version 1.4," November 2001.

24.18 Not Used.

24.19 Not Used.

24.20 Westinghouse Report UKP-GW-GL-026, Rev. 2, "AP1000 Nuclear Power Plant BAT Assessment," March 2011.

24.21 Westinghouse Report APP-CVS-M3-001, Rev. 7, "AP1000 Chemical and Volume Control System (CVS) System Specification Document," October 2015.

24.22 NUREG-0713, Vol. 30, "Occupational Radiation Exposure at Commercial Nuclear Power Reactors and Other Facilities 2008 Forty-First Annual Report," U.S. Nuclear Regulatory Commission, January 2010.

24.23 Sven Baumgarten, et al., "Reactor Coolant Pump Type RUV for Westinghouse Reactor AP1000," 15 December 2009.

24.24 Westinghouse Report APP-1200-N2C-001, Rev. 3, "AP1000 Auxiliary Building Shielding Calculation," December 2015.

24.25 Westinghouse Report APP-GW-N2C-006, Rev. 3, "AP1000 Spent Fuel Shielding Evaluation," January 2015.

24.26 Westinghouse Report APP-GW-N1-021, Rev. 2, "AP1000 Radiation Analysis Design Manual," July 2015.

24.27 NUREG-1465, "Accident Source Terms for Light-Water Nuclear Power Plants – Final Report," U.S. Nuclear Regulatory Commission, 1995.

24.28 ANSI/ANS-18.1, "Radioactive Source Term for Normal Operation of Light Water Reactors," American National Standards Institute/American Nuclear Society, 1984.

24.29 Westinghouse Report APP-4000-N2C-001, Rev. 1, "AP1000 Annex Building Shielding Calculation," October 2015.

24.30 Westinghouse Letter LTR-REA-09-63, Rev. 0, "Software Release Letter for MCNP5.mpi Version 1.40," July 2009.

24.31 ORNL RSICC CCC-710 MCNP5, Overview and Theory. In *MCNP – A General Monte Carlo N-Particle Transport Code, Version 5, Volume I: Overview and Theory*, X-5 Monte Carlo Team, Los Alamos National Laboratory, December 2005.

24.32 Westinghouse Letter LTR-REA-05-48, Rev. 0, "Software Release Letter for DOORS 3.2 Code Package," March 2005.

24.33 RSICC Computer Code Collection CCC-650, *DOORS 3.2 One-, Two-, and Three-Dimensional Discrete Ordinates Neutron/Photon Transport Code System*, Radiation Safety Information Computational Center, Oak Ridge National Laboratory, April 1998.

24.34 Westinghouse Letter LTR-REA-03-6, Rev. 0, "Installation Testing of SCAP-II 1.0 on Solaris 2.8," January 2003.

24.35 Westinghouse Report SAE-REA-99-442, "SCAP-II User's Manual Sun Version," July 1999.

24.36 Westinghouse Letter SE/REA-113/94, "SCAP-II Version 1," September 1994.

24.37 Westinghouse Document CN-REA-08-55, Rev. 0, "Validation of MicroShield Version 6.20 on Windows XP Service Pack 2 Platforms," October 2008.

24.38 Westinghouse Letter LTR-REA-08-126, Rev. 0, "Release of MicroShield Version 6.2 on Windows PC Platform," November 2008.

24.39 Westinghouse Report APP-SSAR-GSC-723, Rev. 1, "AP1000 – Dose Evaluation for Vital Area Access Outside Containment in Post-Accident Conditions," December 2014.

24.40 Westinghouse Report APP-SSAR-GSC-565, Rev. 1, "AP1000 Annual Occupational Dose Assessment," July 2006

24.41 NUREG-0713 Vol. 19, "Occupational Radiation Exposure at Commercial Nuclear Power Reactors and Other Facilities, Thirtieth Annual Report," U.S. Nuclear Regulatory Commission, 1997.

24.42 Westinghouse Report APP-SSAR-G3C-001, Rev. 0, "AP1000 Occupational Radiation Exposure Estimate for Refueling," July 2009.

24.43 Not Used.

24.44 Westinghouse Document CN-REA-05-58, Rev. 0, "AP1000 ORE Estimates for Refueling and Rx Head Inspection," October 2005.

24.45 Westinghouse Report UKP-GW-GL-790, Rev. 6, "UK AP1000 Environment Report," January 2017.

24.46 NRC Regulatory Guide 8.38, "Control of Access to High and Very High Radiation Areas in Nuclear Power Plants," U.S. Nuclear Regulatory Commission, June 1983.

24.47 Westinghouse Report APP-0000-N5C-001, Rev. 4, "AP1000 Dose Rate Outside the Shield Building at grade level during normal operation at full Power," July 2015.

24.48 Westinghouse Report APP-4000-G1-001, Rev. 0, "Functional Requirements for Annex Building," February 2009.

24.49 NVF/DG001, Issue 1, "An Aid to the Design of Ventilation of Radioactive Areas," Nuclear Industry Safety Directors Forum, January 2009.

24.50 Not Used.

24.51 Westinghouse Report UKP-GW-GL-027, Rev. 2, "Radioactive Waste Arisings, Management and Disposal," March 2011.

24.52 Westinghouse Report UKP-GW-GL-004, Rev. 1, "Process Mass Balance for AP1000 Solid Waste," March 2011.

24.53 Issues associated with the co-disposal of ILW/LLW and HLW/SF in the United Kingdom, WM 2002 Conference, February 24-28, 2002, Tucson, AZ.

24.54 Not Used.

24.55 "Nuclear Site Licence Conditions, 18, Radiological Protection," Office for Nuclear Regulation, January 2016.

24.56 "Health Physics Monitor's Handbook," Issue 3, Sellafield Ltd, July 2007.

24.57 Westinghouse Report APP-CVS-N0C-002, Rev. A, "AP1000 Occupational Radiation Exposure Estimate for the Chemical and Volume Control System (CVS)," October 2010.

24.58 Westinghouse Report APP-1100-N5C-005, Rev. 2, "AP1000 – In Containment Radiation Zoning During Normal Operation," June 2015.

24.59 Westinghouse Report APP-1100-N5C-004, Rev. 2, "AP1000 – In containment radiation zoning 24 hours after shutdown," November 2015.

24.60 Provisional HSE Internal Guidance on Dose Levels for Emergencies. HSE. 2008.

24.61 Radiation Zones Normal Operation / Shutdown

A. Westinghouse Document APP-0000-N5-001, Rev. 0, "SITE RADIATION ZONES NORMAL OPERATION / SHUT DOWN," November 2015.

B. Westinghouse Document APP-1010-N5-001, Rev. 2, "Radiation Zones Normal Operation / Shutdown Nuclear Island EL. 66'-6"," January 2008.

C. Westinghouse Document APP-1020-N5-001, Rev. 3, "Radiation Zones Normal Operation / Shutdown Nuclear Island EL. 82'-6"," January 2008.

D. Westinghouse Document APP-1020-N5-002, Rev. 3, "Radiation Zones Normal Operation / Shutdown Nuclear Island EL. 96'-6"," January 2008.

E. Westinghouse Document APP-1030-N5-001, Rev. 3, "Radiation Zones Normal Operation / Shutdown Plan at EL. 100'-0" and 107'-2"," December 2007.

F. Westinghouse Document APP-1040-N5-001, Rev. 3, "Radiation Zones Normal Operation / Shutdown Nuclear Island EL. 117'-6"," December 2007.

G. Westinghouse Document APP-1050-N5-001, Rev. 3, "Radiation Zones Normal Operation / Shutdown Nuclear Island EL. 135'-3"," December 2007.

H. Westinghouse Document APP-1060-N5-001, Rev. 1, "Radiation Zones Normal Operation / Shutdown Nuclear Island EL. 153'-0" and 160'-6"," December 2007.

I. Westinghouse Document APP-1070-N5-001, Rev. 1, "RADIATION ZONES NORMAL OPERATION / SHUTDOWN NUCLEAR ISLAND EL. 160'-6" & 180'-0"," September 2015.

J. Westinghouse Document APP-2030-N5-001, Rev. 3, "Radiation Zones Normal Operation/Shutdown Turbine Building EL 100'-0"," June 2015.

K. Westinghouse Document APP-2040-N5-001, Rev. 2, "Radiation Zones Normal Operation/Shutdown Turbine Building EL 117'-6" & 120' - 6"," June 2015.

L. Westinghouse Document APP-4030-N5-001, Rev. 4, "Radiation Zones Normal Operation/Shutdown Annex BLDG EL 100' - 0" & 107' - 2"," August 2014.

M. Westinghouse Document APP-4040-N5-001, Rev. 2, "RADIATION ZONES, NORMAL OPERATION/SHUTDOWN ANNEX BUILDING ANNEX BLDG EL 117'-6" & 126'-3"," August 2014.

N. Westinghouse Document APP-4050-N5-001, Rev. 2, "Radiation Zones, Normal Operation/Shutdown Annex Building EL 135'-3", 150'-3" & 158'-0"," August 2014.

O. Westinghouse Document APP-5030-N5-001, Rev. 2, "Radwaste Building Radiation Zones, Normal Operation/Shutdown EL 100' - 0"," December 2015.

24.62 Radiation Zones Post-Accident

A. Westinghouse Document APP-1010-N5-101, Rev. 1, "RADIATION ZONES POST-ACCIDENT NUCLEAR ISLAND EL. 66'-6"," September 2015.

B. Westinghouse Document APP-1020-N5-101, Rev. 3, "RADIATION ZONES POST-ACCIDENT NUCLEAR ISLAND EL. 82'-6"," November 2015.

C. Westinghouse Document APP-1030-N5-101, Rev. 3, "RADIATION ZONES POST-ACCIDENT PLAN AT 100'-0" & 107'-2"," November 2015.

D. Westinghouse Document APP-1040-N5-101, Rev. 2, "Radiation Zones Post-Accident Nuclear Island EL. 117'-6"," December 2003.

E. Westinghouse Document APP-1050-N5-102, Rev. 1, "RADIATION ZONES POST-ACCIDENT NUCLEAR ISLAND EL. 153-0"," October 2015.

F. Westinghouse Document APP-1060-N5-101, Rev. 2, "RADIATION ZONES POST-ACCIDENT NUCLEAR ISLAND EL. 153-0" & 160'-6"," October 2015.

G. Westinghouse Document APP-1070-N5-101, Rev. 2, "RADIATION ZONES POST-ACCIDENT NUCLEAR ISLAND EL. 160'-6" & 180'-0"," September 2015.

H. Westinghouse Document APP-2030-N5-101, Rev. 3, "Radiation Zones Post-Accident Turbine Building EL 100'-0"," June 2015.

I. Westinghouse Document APP-4030-N5-002, Rev. 2, "Radiation Zones, Post-Accident Annex Building EL. 100'-0" and 107'-2"," August 2009.

J. Westinghouse Document APP-4040-N5-002, Rev. 2, "Radiation Zones, Post-Accident Annex Building EL. 117'-6" and 126'-3"," August 2009.

K. Westinghouse Document APP-4050-N5-002, Rev. 2, "Radiation Zones, Post-Accident Annex Building EL. 135'-3" 146'-3" 156'-0" and 158'-0"," August 2009.

L. Westinghouse Document APP-5030-N5-101, Rev. 2, "Radwaste Building Radiation Zones, Post-Accident EL 100' - 0"," December 2015.

24.63 Radiological Access Controls Normal Operation / Shutdown

A. Westinghouse Document APP-0000-N5-201, Rev. 0, "RADIOLOGICAL ACCESS CONTROLS NORMAL OPERATION/SHUTDOWN," November 2015.

B. Westinghouse Document APP-1010-N5-201, Rev. 1, "Radiological Access Controls Normal Operation/Shutdown Nuclear Island EL. 66'-6"," January 2008.

C. Westinghouse Document APP-1020-N5-201, Rev. 3, "RADIOLOGICAL ACCESS CONTROLS NORMAL OPERATION / SHUTDOWN NUCLEAR ISLAND EL. 82'-6"," November 2015.

D. Westinghouse Document APP-1020-N5-202, Rev. 3, "RADIOLOGICAL ACCESS CONTROLS NORMAL OPERATION / SHUTDOWN NUCLEAR ISLAND EL. 96'-6"," October 2015.

E. Westinghouse Document APP-1030-N5-201, Rev. 3, "Radiological Access Control Normal Operation/Shutdown Plan at EL. 100'-0" & 107'-2"," December 2007.

F. Westinghouse Document APP-1040-N5-201, Rev. 1, "Radiological Access Control Normal Operation/Shutdown Nuclear Island El. 117'-6"," December 2007.

G. Westinghouse Document APP-1050-N5-201, Rev. 1, "Radiological Access Control Normal Operation/Shutdown Nuclear Island EL. 135'-3"," December 2007.

H. Westinghouse Document APP-1050-N5-202, Rev. 0, "AP1000 Radiological Access Controls Normal Operation Shutdown Nuclear Island EL 153'-0"," January 2003.

I. Westinghouse Document APP-1060-N5-201, Rev. 1, "Radiological Access Control Normal Operation/Shutdown Nuclear Island EL. 153'-0" & 160'-6"," December 2007.

J. Westinghouse Document APP-1070-N5-201, Rev. 1, "RADIOLOGICAL ACCESS CONTROLS NORMAL OPERATION / SHUTDOWN NUCLEAR ISLAND EL. 160'-6" & 180'-0"," September 2015.

K. Westinghouse Document APP-2030-N5-201, Rev. 2, "Radiological Access Controls Normal Operation/Shutdown Turbine Building EL 100'-0"," June 2015.

L. Westinghouse Document APP-2040-N5-201, Rev. 2, "Radiological Access Control Normal Operation/Shutdown Turbine Building EL 117'-6" & 120' -6"," June 2015.

M. Westinghouse Document APP-4030-N5-201, Rev. 4, "Radiological Access Controls Normal Operation/Shutdown Annex BLDG EL 100'-0" & 107'-2"," August 2014.

N. Westinghouse Document APP-4040-N5-201, Rev. 2, "RADIOLOGICAL ACCESS CONTROLS NORMAL OPERATION/SHUTDOWN ANNEX BLDG EL 117'-6" & 126'-3"," August 2014.

O. Westinghouse Document APP-4050-N5-201, Rev. 2, "Radiological Access Controls Normal Operation/Shutdown Annex Building EL 135'-3", 150'-3" & 158'-0"," August 2014.

P. Westinghouse Document APP-5030-N5-201, Rev. 2, "Radwaste Building Radiological Access Controls Normal Operation/Shutdown EL 100' -0"," December 2015.

Table 24-1. Numerical Dose Targets and Legal Limits for Normal Operation (Reference 24.1)

Normal Operation – Any Person on the Site	**Target 1**
The targets and a legal limit for effective dose in a calendar year for any person on the site from sources of ionising radiation are:	
Employees working with ionising radiation:	
BSL(LL):	20 mSv
BSO:	1 mSv
Other employees on site:	
BSL:	2 mSv
BSO:	0.1 mSv
Note that there are other legal limits on doses for specific groups of people, tissues and parts of the body (IRR99).	
Normal Operation – Any Group on the Site	**Target 2**
The targets for average effective dose in a calendar year to defined groups of employees working with ionising radiation are:	
BSL:	10 mSv
BSO:	0.5 mSv
Normal Operation – Any Person off the Site	**Target 3**
The targets and a legal limit for effective dose in a calendar year for any person off the site from sources of ionising radiation originating on the site are:	
BSL(LL):	1 mSv
BSO:	0.02 mSv
Note that there are other legal limits to tissues and parts of the body (IRR99).	
Maximum Doses to Individuals from a Defined Source (EPR2010 (Reference 24.3))	
0.3 mSv(1) per year from any source from which radioactive discharges are first made on or after 13th May 2000 or	
0.5 mSv per year from the discharges from any single site.	

Note:

1. Recent guidance indicates that new power plants should target a dose below 150 microSv for this category.

Table 24-2. Numerical Accident Consequence Dose and Risk Targets (Reference 24.1)

Individual Risk of Death from Onsite Accidents – Any Person on the Site	**Target 5**
The targets for the individual risk of death to a person on the site, from on-site accidents that result in exposure to ionising radiation, are: BSL: 1×10^{-4} pa(1) BSO: 1×10^{-6} pa	

Frequency Dose Targets for Any Single Accident – Any Person on the Site	**Target 6**
The targets for the total predicted frequencies of accidents on an individual facility, which could give doses to a person on the site, are:	

Effective Dose, mSv	**Total Predicted Frequency per Annum**	
	BSL	BSO
2-20	1×10^{-1}	1×10^{-3}
20-200	1×10^{-2}	1×10^{-4}
200-2000	1×10^{-3}	1×10^{-5}
>2000	1×10^{-4}	1×10^{-6}

Individual Risk to People Off the Site from Accidents	**Target 7**
The targets for the individual risk of death to a person off the site, from on-site accidents that result in exposure to ionising radiation, are: BSL: 1×10^{-4} pa BSO: 1×10^{-6} pa	

Frequency Dose Targets for Any Single Accident – Any Person Off the Site	**Target 8**
The targets for the total predicted frequencies of accidents on an individual facility, which could give doses to a person off the site, are:	

Effective Dose, mSv	**Total Predicted Frequency per Annum**	
	BSL	BSO
0.1-1	1	1×10^{-2}
1-10	1×10^{-1}	1×10^{-3}
10-100	1×10^{-2}	1×10^{-4}
100-1000	1×10^{-3}	1×10^{-5}
>1000	1×10^{-4}	1×10^{-6}

Note:

1. "pa" stands for "per annum"

Table 24-3. Provisional HSE Internal Guidance on Dose Levels in Emergencies (References 24.5 and 24.60)

Emergency dose levels up to those listed below should normally be regarded as acceptable to HSE (subject to ALARP)	
Effective Dose	100 mSv
Equivalent Dose to Skin	1000 mSv
Equivalent Dose to Eye Lens	300 mSv
For life saving, it is desirable that for planning purposes the objective should normally be to apply the following levels:	
Whole Body Dose	500 mGy
Dose to Skin	5000 mGy

Table 24-4. Sources of Radiation

Source	Source Term/ Radionuclide	Hazard	Exposed Group	Protection Measures
Radiation Sources (Power Operation and Shutdown)				
Direct core radiation	Gamma and neutron flux	External radiation during operation	Workers	The reactor internals, RV, in-containment primary and secondary interior shield systems, and shield building attenuate the radiation, reducing the predicted dose exposure to workers in normal power operation to low levels. Strict control of access to the containment during operation is necessary to minimise dose uptake.
			Public	The plant geometry and shielding design ensure that exposure of members of the public to external radiation is negligible.
		External radiation during shutdown	Workers	The gamma and neutron flux is significantly reduced when the reactor is shut down and is shielded by the reactor internals, reactor pressure vessel, and in-containment primary and secondary interior shield systems. Water in the refuelling cavity reduces doses further during refuelling operations as described below.
			Public	The plant geometry and shielding design ensure that exposure of members of the public to external radiation is negligible.
Fission product	Fission products	Fission products in the reactor coolant and deposited on primary circuit surfaces present a direct and potential internal radiation hazard to maintenance workers	Workers	Fission products are normally retained within the fuel. Pinhole defects in the fuel rod cladding may lead to fission product release to the reactor primary coolant. The design basis for fission product leakage is operation with cladding defects in fuel rods producing 0.25% of the core thermal power. The secondary shield surrounding the RCS equipment (including piping, pumps, and SGs) protects personnel from the direct gamma radiation emanating from the fission products carried away from the core by the primary coolant in power operation.
			Public	The plant geometry and shielding design ensure that exposure of members of the public to external radiation is negligible.

Table 24-4. Sources of Radiation (cont.)

Source	Source Term/ Radionuclide	Hazard	Exposed Group	Protection Measures
Fission product (cont.)	Fission products	Fission products will be released in the unlikely event of a severe accident that damages the fuel clad. In this case, fission products present a risk to the workers and others.	Workers	Shielding is provided for the MCR and certain access routes based on the design basis loss-of-coolant accident (LOCA). Air is supplied to the MCR from pressurised cylinders to eliminate reliance on active ventilation systems in an emergency.
			Public	The containment and passive cooling systems mitigate the effect of such releases. The containment isolation can withstand an overpressure of 0.6 MPa (87.023 psi) gauge.
Coolant activation processes	N-16	The activation of oxygen in the primary coolant results in the formation of N-16, which is a strong gamma emitter. Due to its short half-life of 7.1 seconds, N-16 is not a concern outside containment. N-16 is the predominant contributor to the activity in the RCPs, SGs, and reactor piping during operation. The activity in each component depends on the transit time to the component and the residence time.	Workers	The secondary shield surrounding the RCS equipment (including piping, pumps, and SGs) protects personnel in power operation. The source is terminated when the reactor is shut down.
			Public	Due to its short half-life of 7.1 seconds, N-16 is not a concern outside containment. The source is terminated when the reactor is shut down.

Table 24-4. Sources of Radiation (cont.)

Source	Source Term/ Radionuclide	Hazard	Exposed Group	Protection Measures
Coolant activation processes	Ar-41	The activation of residual argon in the primary coolant results in the formation of Ar-41, a short-lived isotope source (half-life 1.827 hr).	Workers	The secondary shield surrounding the RCS equipment (including piping, pumps, and SGs) protects personnel in power operation. The source is terminated when the reactor is shut down.
			Public	The shielding ensures that exposure of members of the public to external radiation is negligible. The source is terminated when the reactor is shut down and decays quickly away.
Coolant activation processes (cont.)	Tritium	A number of processes add tritium to the reactor coolant. Tritium is created as a result of ternary fission, where the uranium nucleus splits into three, and can then diffuse through the fuel clad or leak through fuel clad defects. Tritium is also produced as a result of neutron reactions with soluble boron, soluble lithium, and deuterium in the reactor coolant. Tritium emits beta radiation and presents limited public health implications. Tritium exists in the reactor coolant primarily combined with hydrogen (that is, a tritium atom replaces a hydrogen atom in a water molecule) and thus cannot be readily separated from the coolant by normal processing methods.	Workers	Presents no significant hazard during power operations.
			Public	Tritium discharges are assessed in the Environment Report (Reference 24.45) and will be monitored to ensure that doses to the public are low.

Table 24-4. Sources of Radiation (cont.)

Source	Source Term/ Radionuclide	Hazard	Exposed Group	Protection Measures
Coolant activation processes (cont.)	C-14	C-14 may be produced by neutron activation of O-17 (n,α reaction) and N-14 (n,p reaction). It is also present in activated corrosion products (see below). C-14 emits low-energy beta radiation and presents no hazard during power operation. C-14 is present in all coolant liquor released during maintenance activities and is an important isotope in radioactive waste management but presents only a limited hazard to workers.	Workers	Presents no significant hazard during power operations.
			Public	C-14 discharges are assessed in the Environment Report (Reference 24.45) and will be monitored to confirm that doses to the public are low.

Table 24-4. Sources of Radiation (cont.)

Source	Source Term/ Radionuclide	Hazard	Exposed Group	Protection Measures
Activation of corrosion products (crud)	Co-58, Co-60, Fe-55, Fe-59, Mn-56, Mn-54, Cr-51	The activation of primary circuit component corrosion and wear products results in dissolved activation products within the primary coolant. These may be deposited as a contamination film on primary circuit components (termed crud). The dominant gamma-emitting isotope in crud is Co-60 (half-life 5.27 yr). Activated corrosion products in reactor coolant and deposited on primary circuit surfaces (crud) present a direct and potential internal radiation hazard to maintenance workers.	Workers	BAT has been incorporated in the design and operating regime (including material selection and zinc injection) for the AP1000 design to keep the formation and deposition of crud ALARP. Shielding is provided for reactor components where crud is likely to be present, and for vessels and pipes used to remove crud and fission products from the primary coolant. The secondary shield surrounding the RCS equipment protects personnel in power operation. Access to high dose rate areas is physically restricted, and any entries into such areas will be strictly controlled. Although BAT is used to reduce crud SFAIRP, it is not possible to eliminate it completely; therefore, design features have been incorporated to reduce the maintenance operations required and the preparation time for inspection and maintenance. In addition, remote inspection systems have been developed to reduce the need for workers to remain in high dose rate areas such as the SGs and RVCH.
			Public	In addition to techniques to limit the production of these nuclides, BAT is incorporated in the plant to reduce the concentration of these nuclides from liquid waste before discharge, and HEPA filtration will reduce routine atmospheric discharges SFAIRP.
Containment atmosphere	Ar-41	The main source of airborne activity in containment is activation of naturally occurring argon in the atmosphere.	Workers	Ar-41 has a short half-life (1.827 hr) and does not present a hazard to workers so long as it does not build up in the containment. Periodic purging prevents excessive activity buildup.
			Public	Ar-41 is discharged from the ventilation stack so that the dose to the public is ALARP.

Table 24-4. Sources of Radiation (cont.)

Source	Source Term/ Radionuclide	Hazard	Exposed Group	Protection Measures
Radiation Sources (Refuelling)				
Spent reactor fuel	Gamma and neutron (fission products and actinides)	Spent fuel is the primary source of radiation during refuelling.	Workers	Extensive shielding is provided for areas surrounding the refuelling cavity and fuel transfer canal to limit radiation levels to refuelling personnel. Water provides shielding over the spent fuel assemblies during fuel handling.
			Public	Protection of workers ensures protection of the public from high radiation levels. Additionally, physical security and the use of dry storage casks when the spent fuel is removed from the SFP protect the public from radiation exposure due to spent fuel.
Irradiated control and grey rods	Gamma	Irradiated control rods and grey rods present a hazard from external gamma radiation. The gamma ray source strengths of the irradiated control rods and grey rods are used in establishing radiation shielding requirement during refuelling operations and during shipping of irradiated rods.	Workers	Extensive shielding is provided for areas surrounding the refuelling cavity and fuel transfer canal to limit radiation levels to refuelling personnel. Water provides shielding over the spent fuel assemblies during fuel handling.
			Public	Protection of workers ensures protection of the public from high radiation levels. Protection measures mentioned above for spent fuel are also applicable.
Secondary source rods	Gamma and neutron	The photoneutron source material used in the secondary source rods is an equal volume mixture of antimony and beryllium (Sb-Be).	Workers	Extensive shielding is provided for areas surrounding the refuelling cavity and fuel transfer canal to limit radiation levels to refuelling personnel. Water provides shielding over the spent fuel assemblies during fuel handling.
			Public	Protection of workers ensures protection of the public from high radiation levels. Protection measures mentioned above for spent fuel are also applicable.

Table 24-4. Sources of Radiation (cont.)

Source	Source Term/ Radionuclide	Hazard	Exposed Group	Protection Measures
Radiation Sources (Refuelling) (cont.)				
In-core Thimbles	Gamma	High dose rates to workers during refuelling. (Early designs had thimbles inserted from beneath the RV, resulting in high doses during RV inspection).	Workers	Thimbles remain in the upper internals and are stored under water during refuelling.
			Public	Localised high dose rates only. Shield building eliminates hazard to public.
Activated RV, primary shield concrete	Gamma: Na-24, Co-60	High dose rates to workers during RV inspections and who maintain the digital metal impact monitoring system.	Workers	Neutron shield collar to minimise activation of the lower vessel cavity. Robotic inspection of undervessel components under development.
			Public	Primary shielding and shield building eliminates hazard to public.
Coolant Activation Processes	Tritium	Tritium is present in all coolant liquor released during maintenance activities and can, therefore, present a potential internal radiation hazard to maintenance workers.	Workers	Ventilation extract systems limit the airborne concentration of tritium. Normal protective clothing, particularly the use of gloves, and controlled area procedures prevent uptake via skin absorption and ingestion. During refuelling the level of tritium in the primary coolant will be diluted by the water from the IRWST.
			Public	Tritium discharges are assessed in the Environment Report (Reference 24.45) and will be monitored to demonstrate that doses to the public are low.

Table 24-5. Source Term Derivation

Computer Code	Output	Purpose
ORIGEN (Oak Ridge National Laboratory) (References 24.7 and 24.8)	Determination of core activities at various irradiation and decay times: • Fuel nuclides and their heavy metal reaction and decay products • Fission products and decay products • Light elements and other activation products in reactor coolant, cladding and fuel assembly materials and reactor components	Core inventories for: • Primary circuit activity concentration assessment • Accident analyses • Spent fuel handling/storage shielding • SFP decay heat • Waste handling and decommissioning
FIPCO (Westinghouse) (References 24.9 and 24.10)	Design basis fission product activity levels in: • Primary coolant • Pressuriser • CVS demineraliser	• Accident analyses • Shielding assessments • ILW arisings
CORA (Westinghouse) (References 24.11 and 24.12)	Generation and transport of corrosion products in the RCS of a PWR giving activity concentrations in: • Primary coolant • Pressuriser • CVS demineraliser • crud	• Shielding assessments • Routine dose assessment • ALARP assessments
SSP (Westinghouse) (Reference 24.15)	N-16 sources, auxiliary system sources and expected source terms in primary and secondary systems	• Shielding assessments • Environmental discharges
SECONS (Westinghouse) (References 24.16 and 24.17)	Activity concentrations and source strengths in: • Secondary water • Secondary steam • BDS • AP1000 electrodeionisation units	• Shielding assessments • Ion exchange resin arisings • Environmental discharges

Table 24-6. Techniques for Minimising Production of Particulate

Criteria	Material Selection and QA/QC	Chemical Treatment (RCS and CVS)				Piping Design
		Constant Elevated pH	Hydrazine Addition	Oxygen Elimination	Zinc Injection	
Proven Technology	2[(1)]	2[(1)]	2[(1)]	2[(1)]	2[(1)]	2[(1)]
Available Technology	2[(1)]	2[(1)]	2[(1)]	2[(1)]	2[(1)]	2[(1)]
Effective Technology	2[(1)]	2[(1)]	2[(1)]	2[(1)]	2[(1)]	2[(1)]
Ease of Use	2[(1)]	1[(1)]	1[(1)]	1[(1)]	1[(1)]	2[(1)]
Cost	-2[(1)]	-1[(1)]	-1[(1)]	-1[(1)]	-1[(1)]	-1[(1)]
Impact (Public Dose)	2[(1)]	2[(1)]	2[(1)]	2[(1)]	2[(1)]	2[(1)]
Impact (Operator Dose)	2[(1)]	2[(1)]	2[(1)]	2[(1)]	2[(1)]	2[(1)]
Impact (Environmental)	2[(1)]	2[(1)]	2[(1)]	2[(1)]	2[(1)]	2[(1)]
Generates Suitable Waste Form	2[(1)]	2[(1)]	2[(1)]	2[(1)]	2[(1)]	2[(1)]
Secondary & Decommissioning Waste	2[(1)]	2[(1)]	2[(1)]	2[(1)]	2[(1)]	2[(1)]
Totals	16	16	16	16	16	17

Note:

1. Scoring from -2 to 2:
   2 = Good
   -2 = Bad
   0 = Neither a benefit nor a disadvantage

Table 24-7. Plant Radiation Zones

Designation	Maximum Design Dose Rate	Westinghouse Radiation Zone Designation		Typical UK Area Designation Arrangements Details to be Specified by Operator[1]
		Description	Access	
0	≤0.5 μSv/h	No radiation sources	Unlimited general occupancy	Undesignated area
I	≤2.5 μSv/h	Very low or no radiation sources	No restriction on access	Supervised area
Restricted Area Zones				**Controlled Area**
II	≤25 μSv/h	Low radiation sources	Occupational access	Further subdivision for normal operations Areas >2.5 μSv/h subject to limits on occupancy
III	≤150 μSv/h	Low to moderate radiation sources	Periodic access	Access restricted to 1 to 10 hours per week
IV	≤1 mSv/h	Moderate radiation sources	Limited access	Access restricted to <1 hour per week
V	≤10 mSv/h	High radiation sources	Controlled access	Access restricted to a few hours per year at most
VI	≤100 mSv/h	High radiation sources	Normally restricted Post-accident: limited	No access during normal operations[2] Limited post-accident access
VII	≤1 Sv/h	High radiation sources	Normally severely restricted Post-accident: restricted	No access during normal operations Very limited post-accident access
VIII	≤5 Gy/h	High radiation sources	Normally inaccessible Post-accident: severely restricted	No access during normal operations Extremely limited post-accident access

Table 24-7. Plant Radiation Zones (cont.)

Designation	Maximum Design Dose Rate	Westinghouse Radiation Zone Designation		Typical UK Area Designation Arrangements Details to be Specified by Operator[1]
		Description	Access	
Restricted Area Zones				**Controlled Area**
IX	> 5 Gy/h	Very high radiation sources		No access

Notes:

1. These are typical arrangements based on an existing UK operator. It is the responsibility of an operator to make appropriate arrangements to ensure that doses are ALARP.
2. There is a potential conflict in some areas identified in Appendix 24A where rooms are identified as Zone VI during shutdown and requiring access during shutdown (e.g., the RV cavity), which, with the example UK designation, will prohibit entry. However, the zones are based on conservative source terms including 0.25 percent fuel defects. In operation, dose rates in such areas are expected to be lower than calculated. In other areas, dose rates are nonuniform and entries will be possible with care.

Table 24-8. Summary of Integrated Doses and Durations of Defined Post-Accident Operations

Post-Accident Action	Timing (After Accident) (hr)	Duration (min)	Inhalation Dose (mSv)	Direct Dose (mSv)	Total Integrated Dose (mSv)
MCR Occupancy	Various	30 days	37.1	6.2	43.3
MCR Ingress and egress(1)	Various	55.25	0.45	29.5(2)	30.5
SFP Makeup Valve Alignment	64	44.5	1.1	42.5	43.6
	168	44.5	0.06	25.6	25.7
Temporary Water Hookup to PCS	64	75.6	0.07	12.8	12.9
Ventilation Control for Temporary HVAC to MCR and C&I Equipment Room	64	103.1	9.97	0.06	10.0
Electrical Equipment Rooms – Start Diesel Generators and Provide Temporary Power to Transformers	64	82.7	10.0	1.1	11.1

Notes:

1. It is assumed that a 12-hour shift begins at the time of the accident. A shift change occurs every 12 hours afterwards for 30 days.
2. The dose considers ingress/egress for one crew on 12-hour shifts for 30 days only. MCR occupancy doses are evaluated in a separate calculation.

Table 24-9. Breakdown of Collective Dose

Overall Categories	Original Dose in Outage Year from (Reference 24.42) (person-mSv)	Average % of Dose per Category	Prairie Island Average Outage Year Dose 1996-2003 (person-mSv)	Adjusted AP1000 Outage Year Dose (person-mSv)	% of Dose per Category
Reactor Operations and Surveillance	263.0	9.27	82.9	39.3	16.49
Routine Maintenance	245.7	16.14	144.3	44.9	18.82
ISI	297.0	27.26	243.7	60.2	25.26
Special Maintenance	629.2	25.28	226.0	30.1	12.64
Waste Processing	72.0	2.60	23.2	23.2	9.46
Refuelling	170.0	19.46	174.0	41.3	17.32
Total	**1676.9**	**100.00**	**894.1**	**239.0**	**100.00**

Table 24-10. Containment Area Classification (Reference 24.49)

Area Classification	Description
White	Clean area free from radioactive contamination, whether surface or airborne.
Green	An area which is substantially clean. Only in exceptional circumstances is airborne contamination such that provisions must be made for its control.
Amber	An area in which some surface contamination is expected. In some cases there will be a potential for airborne contamination such that provision must be made for its control.
Red	An area in which contamination levels are so high that there is normally no access without appropriate respiratory protection.

Area Classification	Surface Contamination $Bq.cm^{-2}$ $\beta\gamma$	Airborne Activity DAC	Typical Area
White	<4	<0.01	Nonactive areas
Green	Usually <4	<0.03	Most of the RCA during normal operations
Amber	Possibly >4	<0.1	Some parts of containment during shutdown e.g., around SGs and RVCH stand
Red	>4 expected	>0.1	Flask pit before and during decontamination Vessel and pump rooms during breach of containment

Note:
Detailed surface contamination limits and maximum airborne activity concentration allowed in each area will be specified by the operator. A possible area classification scheme and limits are shown below. Only $\beta\gamma$ contamination is likely to be present; if present, levels for α surface contamination would be 10 percent of the $\beta\gamma$ limits.

Table 24-11. Area Radiation Monitor Locations

Area
Primary Sampling Room
Containment Area Personnel Hatch – Operating Deck – 135'-3" (110.74 m) Elevation(1)
MCR
Chemistry Laboratory Area
Rail Car Bay/Filter Storage Area(2)
Liquid and Gaseous Radwaste Area
CSA
Radwaste Building, Mobile Systems Facility(2)
Hot Machine Shop
Annex Staging and Storage
Fuel-Handling Area(3)
Containment Area Personnel Hatch – Maintenance Level – 100'-0" (100 m) Elevation

Notes:

1. Radiation levels are monitored by the permanent containment area radiation monitor and by a portable bridge monitor during refuelling operations. The containment area radiation monitor is located to best measure the increase in exposure rates for this area and to provide an alarm locally and in the MCR.
2. Monitors areas used for storage of wet wastes (including processed and packaged spent resins) and dry wastes.
3. Radiation levels are monitored by the permanent fuel-handling area radiation monitors and by a portable bridge monitor during fuel-handling operations. The fuel-handling area radiation monitors are located to best measure the increase in exposure rates for this area and to provide an alarm locally and in the MCR.

Table 24-12. Summary of Liquid and Gaseous Samples for Radioactive Analysis

General Radiological Sample Purpose	Example Sample Collection Point(s)	Description
Primary system samples	Primary sampling room in the auxiliary building, on or near elevation 89.789 m (66’-5”)	Samples of the RCS and other primary fluids to satisfy requirements, monitor plant conditions, or support operations
SFP samples	SFP in the auxiliary building, on or near elevation 110.744 m (135’-3”)	Samples taken to monitor plant conditions or satisfy Tech Specs
Secondary and blowdown samples	Secondary sampling system in the turbine building, on or near elevation 106.248 m (100’-6”)	Satisfy Tech Specs, and monitor plant conditions (primary to secondary leakage)
Waste samples	Samples from WSS, WLS, WGS, radwaste building, or other locations as needed	Samples taken to characterise or quantify waste parameters
Environmental samples	Waste monitor tanks, building sumps (turbine building or annex building, for example), retention basin, waste water system WWS, groundwater monitoring wells, and other exterior locations	Samples taken to satisfy environmental requirements or to document/quantify the activity released to the environment
Operational samples	Various	Taken as needed to support outages/local procedures

Table 24-13. Radioactive Low and Intermediate Waste Streams

Item	Type	Category	Description
1	Wet Solid	ILW	Ion exchange resins (polymeric types, WLS)
2	Wet Solid	ILW	Ion exchange resins (mineralic types, WLS), could contain charcoal from filter guard bed
3	Dry Solid	ILW	Filter cartridges (from WLS)
4	Dry Solid	LLW	HVAC HEPA filters, disposable PPE, general LLW
5	Liquid	VLLW	WLS dischargeable liquid effluent
6	Gaseous	VLLW	WGS dischargeable gaseous effluent

Table 24-14. Radwaste Building Area Classification

Area	Location	Notes	Radiological Classification	Contamination Classification
50353	HVAC Equipment Room	Safechange HEPA Filters	R2	C1
50355	Monitor Tanks Room	Tank internals will be C3	R2	C2
50351	Waste Accumulation Room	General personnel areas	R2	C2
50351	Sorting Enclosure	Local C3 (internal) with appropriate contamination controls	R2	C3
50351	In-Drum Compactor	Local C3 (internal) with appropriate contamination controls	R2	C3
50351	Size Reduction Enclosure	Local C3 (internal) with appropriate contamination controls	R2	C3
50351	Decontamination Enclosure	Local C3 (internal) with appropriate contamination controls	R2	C3
50350	Mobile Systems Facility	General personnel areas	R2	C1
50354	Truck Staging Area	General personnel areas	R2	C1

Table 24-15. BNFL Classification of Areas – Radiation

Area Classification	Action Level (µSv/h Gamma)	Target Level
R0	<2.5	ALARP
R1	2.5 – 7.5	ALARP
R2	7.5 – 25	ALARP
R3	25 – 100	ALARP
R4	100 – 500	ALARP
R5	>500	ALARP

Note:
1. Intermittent local areas of elevated dose rate may be present.

Table 24-16. BNFL Classification of Areas – Contamination

Area Classification	Surface Contamination		Airborne Contamination Level
	Bq/cm² α	Bq/cm² β	DAC
C0	<0.4	<4	<0.01
C1	RPA advice on Local Practice		
C2	>0.4	>4	<0.05
C3	>4	>40	<1
C4	>40	>400	<10
C5	>400	>4000	>10

Note:
1. Actual contamination levels will generally be much lower in practice.

Table 24-17. Equipment Specification Limits[1] for Cobalt Impurity Levels

Region, Component or Application (Specific Inclusions and Examples are noted parenthetically)			Maximum Weight Percent of Cobalt
Primary Components	Steam Generator Tubing	(Inconel tubing)	0.015
	Primary Component Other than the Steam Generators	(Primary weld cladding surfaces, core shroud, lower and upper core plates, lower core barrel, and neutron panels or thermal shields)	0.05
Fuel Assembly Components		(Inconel and stainless steel components in the Fuel Assembly)	
Auxiliary Heat Exchangers			
Other Components in Regions of High Neutron Flux[4]			
Steam Generator Surfaces other than tubing			0.10
Small Components	In regions of high neutron flux[4]		0.20
Bolting Materials or Fasteners			
	Outside of regions of high neutron flux[4]	(Bolting materials in primary and auxiliary components)	Not limited
Weld Material, other than cladding[2]			
Bearing and Hardfacing Materials[3]			
Other Auxiliary Components[2]		(Valves, piping, instrumentation, and tanks)	

Table 24-17. Equipment Specification Limits[(1)] for Cobalt Impurity Levels (cont.)

Notes:

1. Should a part be fabricated with cobalt above these limits, the responsible engineer must evaluate that cobalt input, considering the wetted surface of a particular component and determine whether using the part as-is or refabricating the part better controls cobalt SFAIRP. This demonstration shall be in accordance with ALARP design principles.
2. Stainless steels manufactured without cobalt limitations generally contain 0.15-0.20 weight percent cobalt. This is based upon historical evaluations of the cobalt content of stainless steels documented in Reference 300.
3. Low- or no-cobalt materials will be used, as available.
4. The following components are to be considered to be in a "high flux" region:
   - in the radial direction – all reactor internals components to a height of at least 0.607 m (2 feet) above and 0.607 m (2 feet) below the active core region. In addition, the weld layer on the inside of the reactor vessel opposite the core and 0.607 m (2 feet) above and 0.607 m (2 feet) below the active core elevations should be considered to be in the "high flux" region.
   - above the core – all components up to and including the upper core plate
   - below the core – all components down to the lower support plate
5. The cobalt content of vent and drain lines is not restricted as these lines are not expected to produce significant cobalt input as a result of corrosion and wear.
6. Temporary equipment that is installed and removed prior to fuel load is not subject to the limitations provided in this table. The limitations in this table apply to surface exposed to reactor coolant that may produce corrosion, activation, or wear products. Equipment that is removed from the primary circuit prior to fuel load is exempt from these limitations as any wear or corrosion products from this temporary equipment is expected to be minimal, can be cleaned up by the CVS filtration train, and has no mechanism to directly deposit or dwell in regions of high neutron flux.
7. Parts that are not exposed to reactor coolant are not subjected to the limitations on cobalt shown in the table above.
8. These limits apply only to components subjected to normal operating fluid temperatures of 93.33°C (200°F) or more.

Table 24-18. Parameters Used in the Calculation of Design Basis Fission Product Activities

Core thermal power (MWt)	3,400
Reactor coolant liquid volume (ft^3)[(a)]	9,575 (271.134 m^3)
Reactor coolant full-power average temperature (°F)	578.1 (303.39°C)
Purification flow rate (gal/min)	
Maximum	100 (22.71 m^3/hr)
Normal	91.3 (20.74 m^3/hr)
Effective cation demineralizer flow, annual average (gal/min)[(b)]	9.1 (2.07 m^3/hr)
Nuclide release coefficients (the product of the failed fuel fraction and the fission product escape rate coefficient)	
Equivalent fraction of core power produced by fuel rods containing small cladding defects (failed fuel fraction)	0.0025
Fission product escape rate coefficients during full-power operation (s^{-1}):	
Kr and Xe isotopes Br, Rb, I, and Cs isotopes Mo, Tc, and Ag isotopes Te isotopes Sr and Ba isotopes Y, Zr, Nb, Ru, Rh, La, Ce, and Pr isotopes	6 x 5 10^{-9} 1.3 x 10^{-8} 2.0 x 10^{-9} 1.0 x 10^{-9} 1.0 x 10^{-11} 1.6 x 10^{-12}
Chemical and volume control system mixed bed demineralizers	
Resin volume (ft^3)	50 (1.416 m^3)
Demineralizer isotopic decontamination factors:	
Kr and Xe isotopes Br and I isotopes Sr and Ba isotopes Other isotopes	1 10 10 1

Table 24-18. Parameters Used in the Calculation of Design Basis Fission Product Activities (cont.)

Chemical and volume control system cation bed demineralizer	
Resin volume (ft^3)	50 (1.416 m^3)
Demineralizer isotopic decontamination factors:	
Kr and Xe isotopes Sr and Ba isotopes Rb-86, Cs-134, and Cs-137 Rb-88, Rb-89, Cs-136, and Cs-138 Other isotopes	1 1 10 1 1
Other isotopic removal mechanisms	See Note c.
Initial boron concentration (ppm)	1,400
Operation time (effective full-power hours)	12,492

Notes:

a. Reactor coolant mass used in defining fission product activities is based on above stated conditions before thermal expansion (conservative).

b. Flow calculated at 15.513 MPa abs (2250 psia) and 121.11°C (250°F).

c. For all isotopes, except the isotopes of Kr, Xe, Br, I, Rb, Cs, Sr, and Ba, a removal decontamination factor of 10 is assumed to account for removal mechanisms other than ion exchange, such as plateout or filtration. This decontamination factor is applied to the normal purification letdown flow.

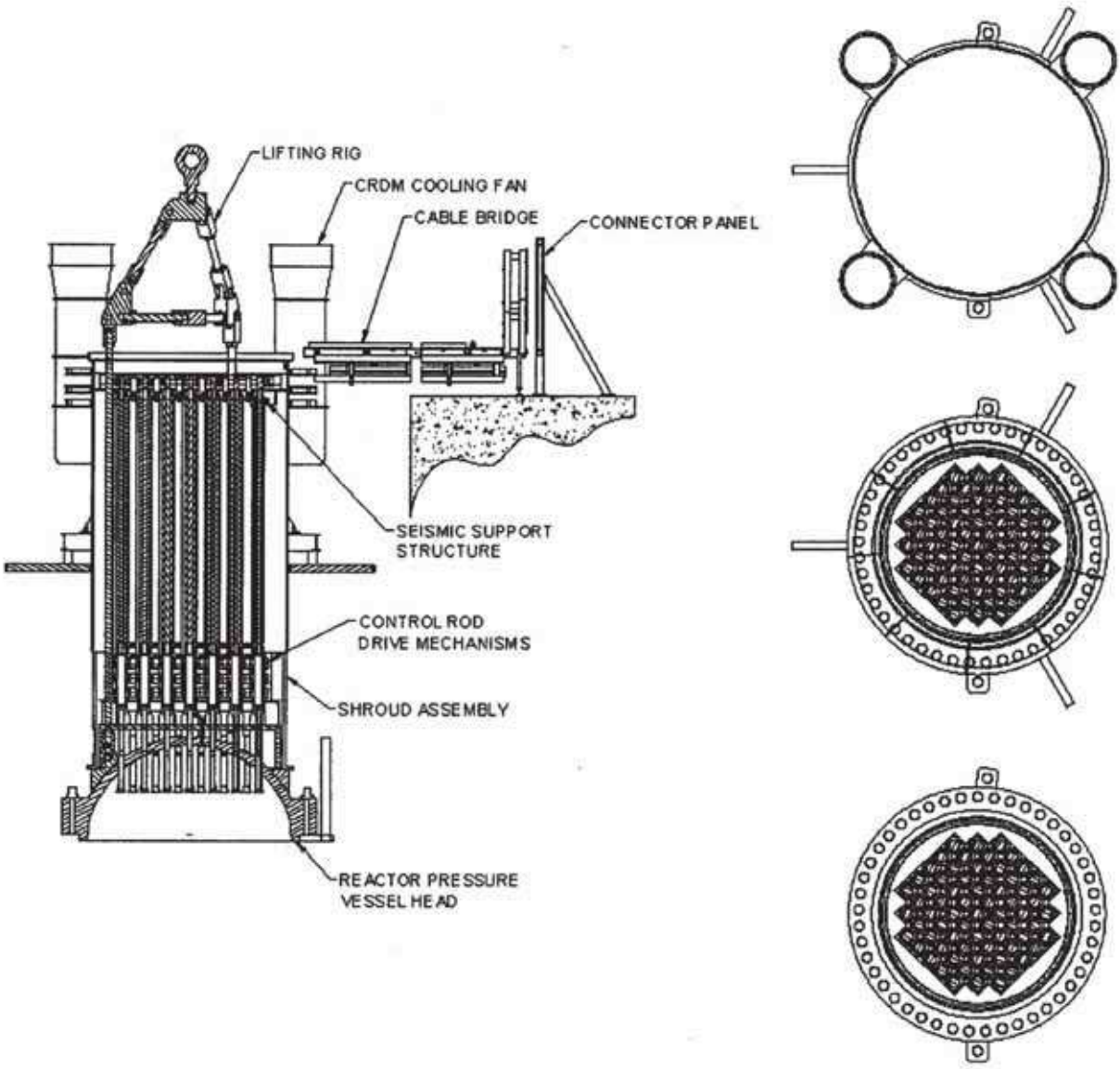


Figure 24-1. Integrated Head Package

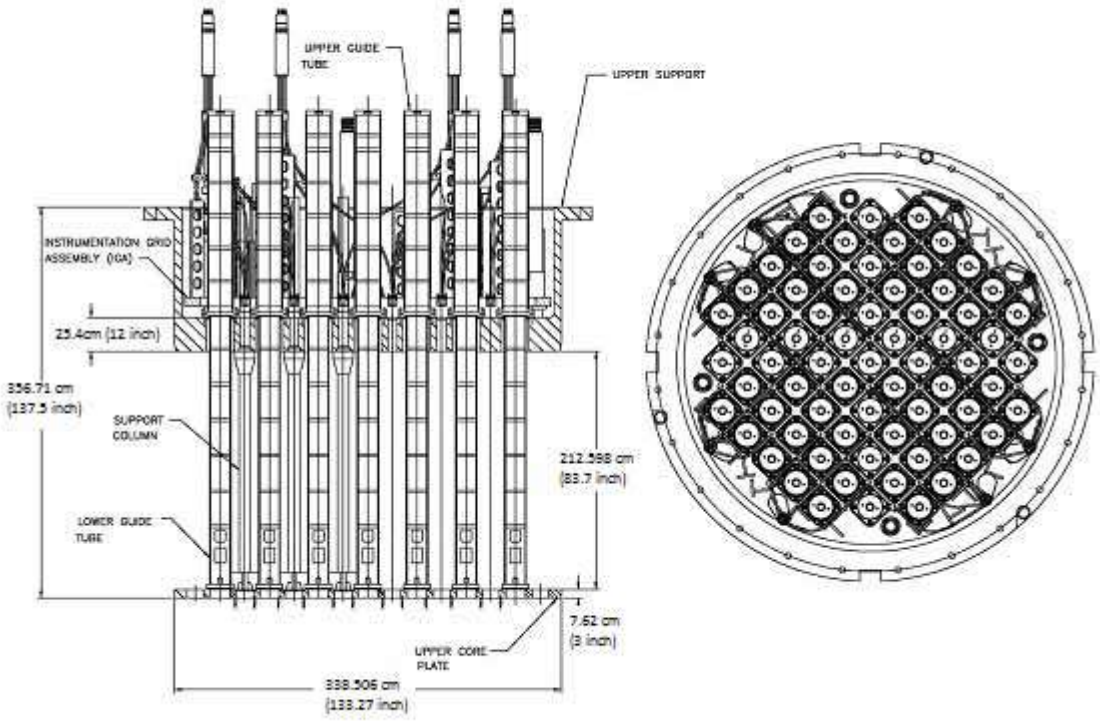


Figure 24-2. Instrument Grid Assembly and Upper Core Support Structure

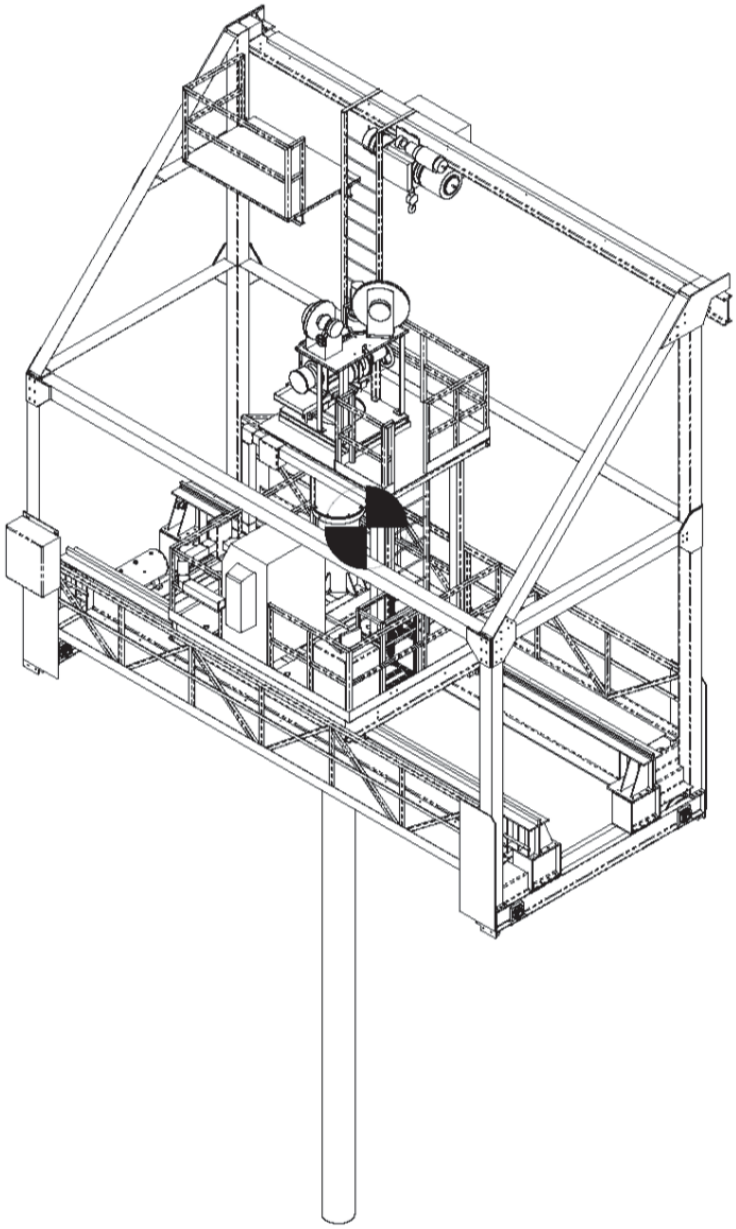


Figure 24-3. Refuelling Machine

Figure 24-4. Refuelling Machine Gripper Engagement with Fuel Assembly Top Nozzle

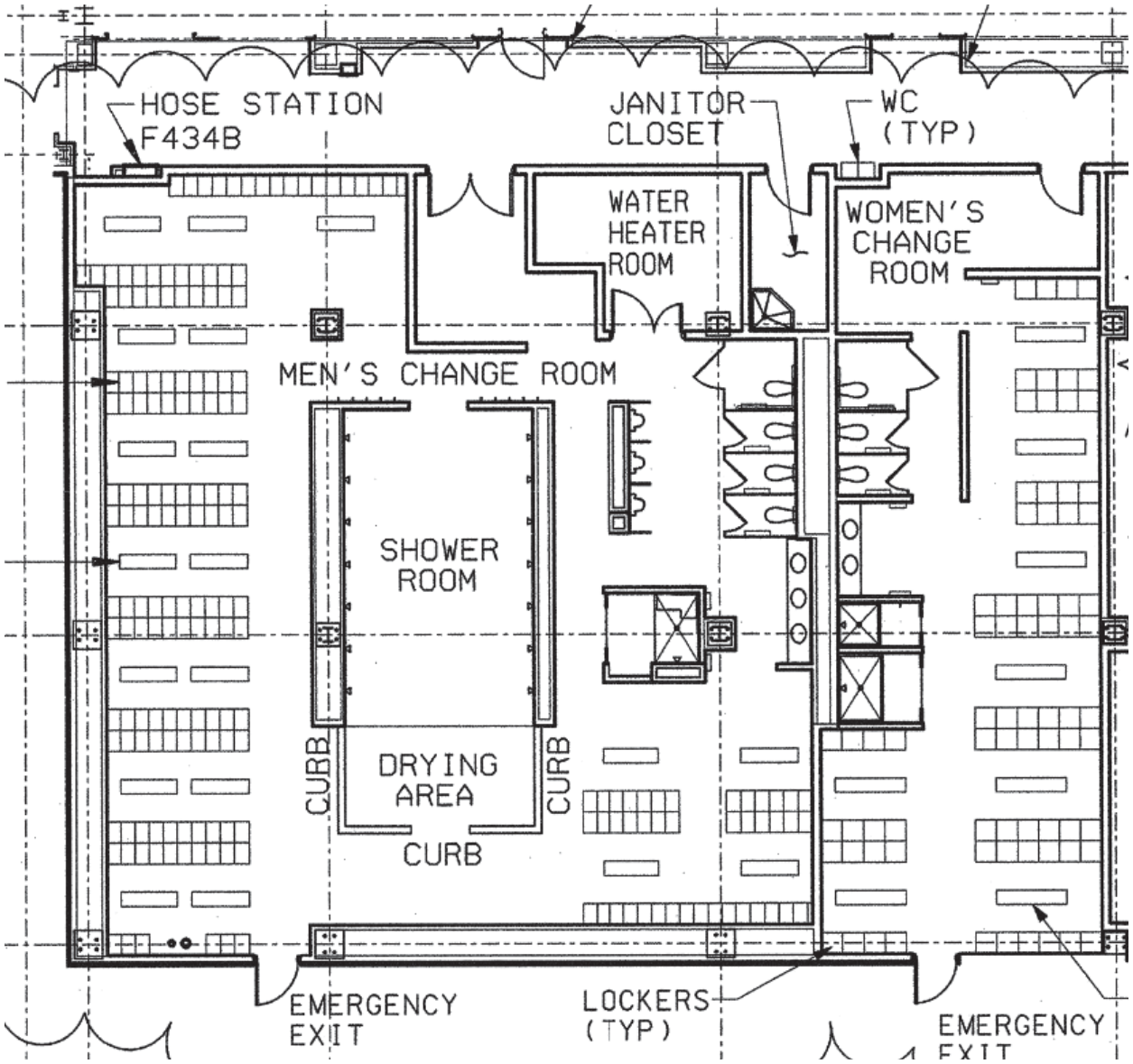


Figure 24-5. Layout of Male and Female Change Rooms

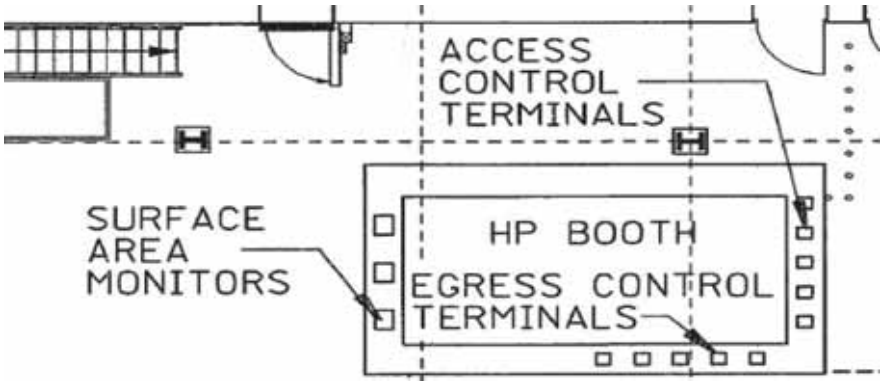


Figure 24-6. Health Physics Booth

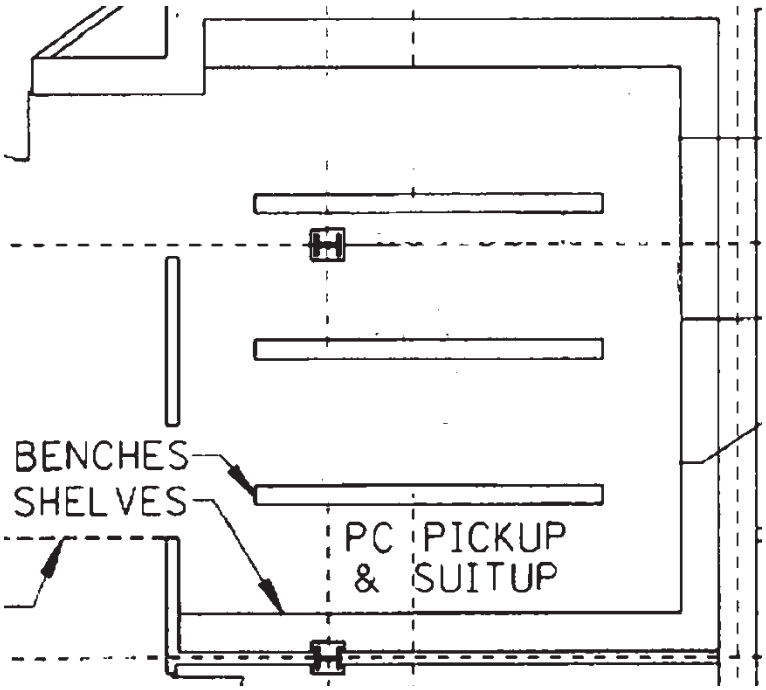


Figure 24-7. PC Pickup and Suitup Room

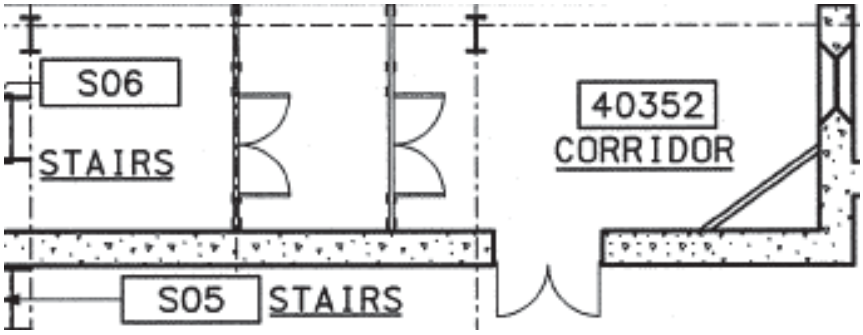


Figure 24-8. Entry to Radiologically Controlled Area

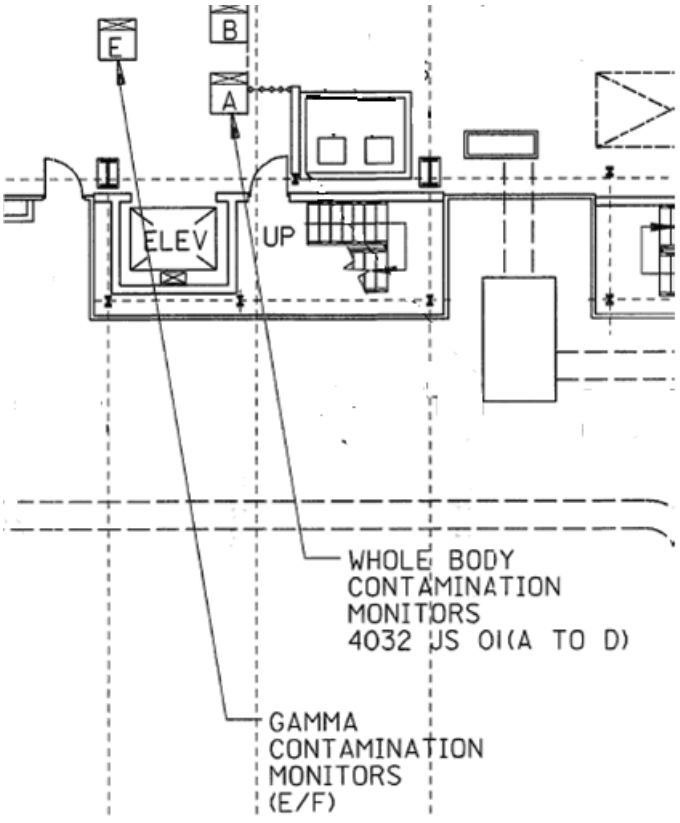


Figure 24-9. Personnel Contamination Monitors at RCA Exit

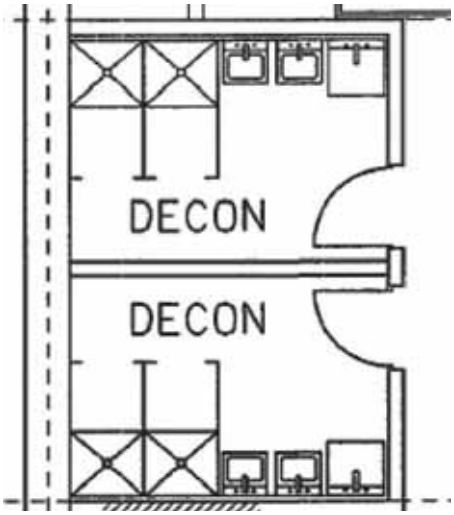


Figure 24-10. Personal Decontamination Area

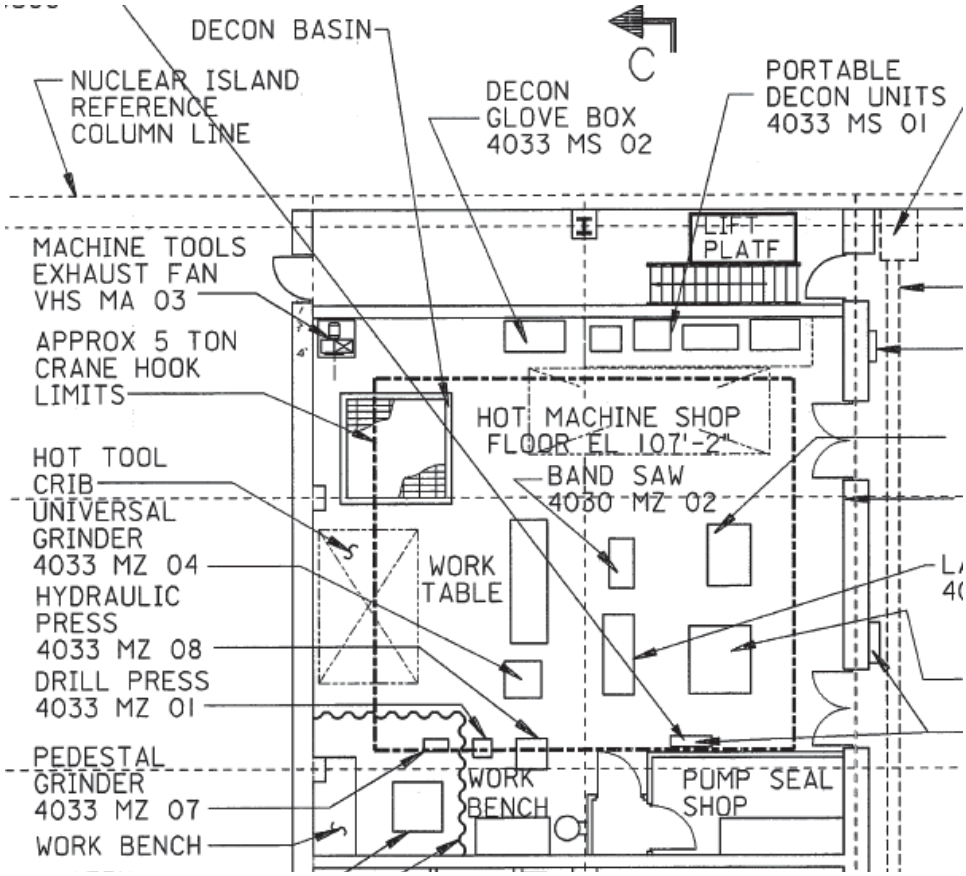


Figure 24-11. Hot Machine Shop Layout

Figure 24-12. Not Used

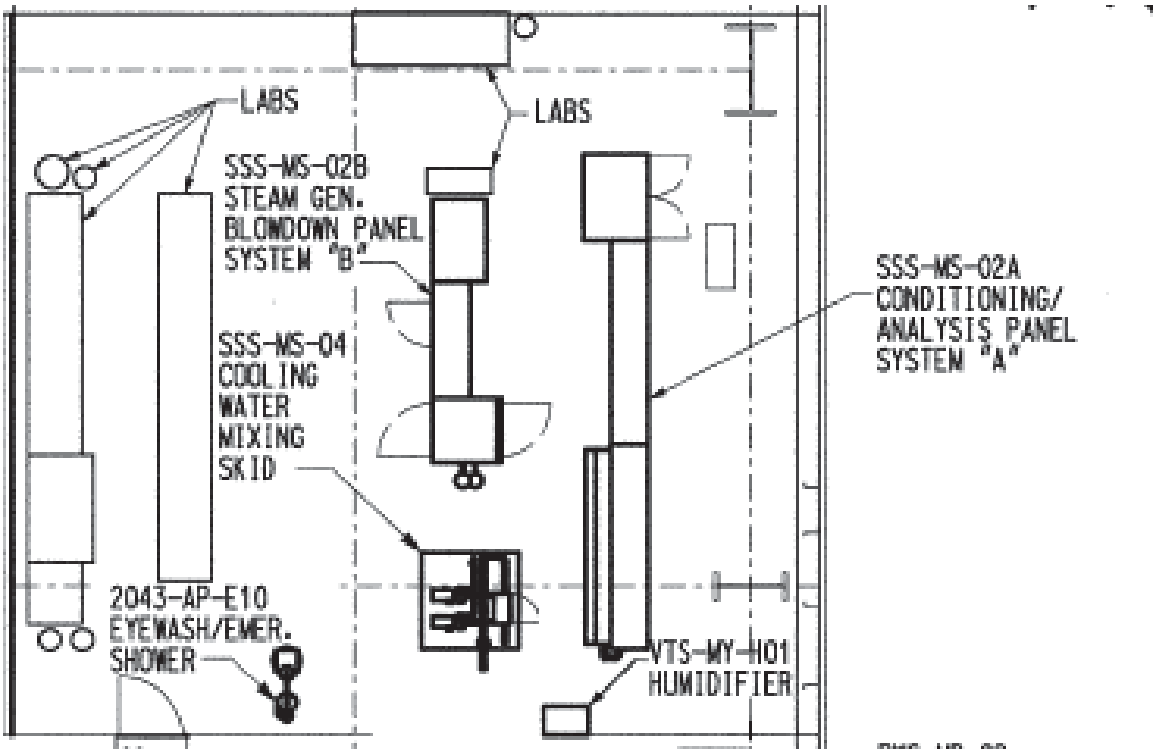


Figure 24-13. Secondary Sampling Laboratory

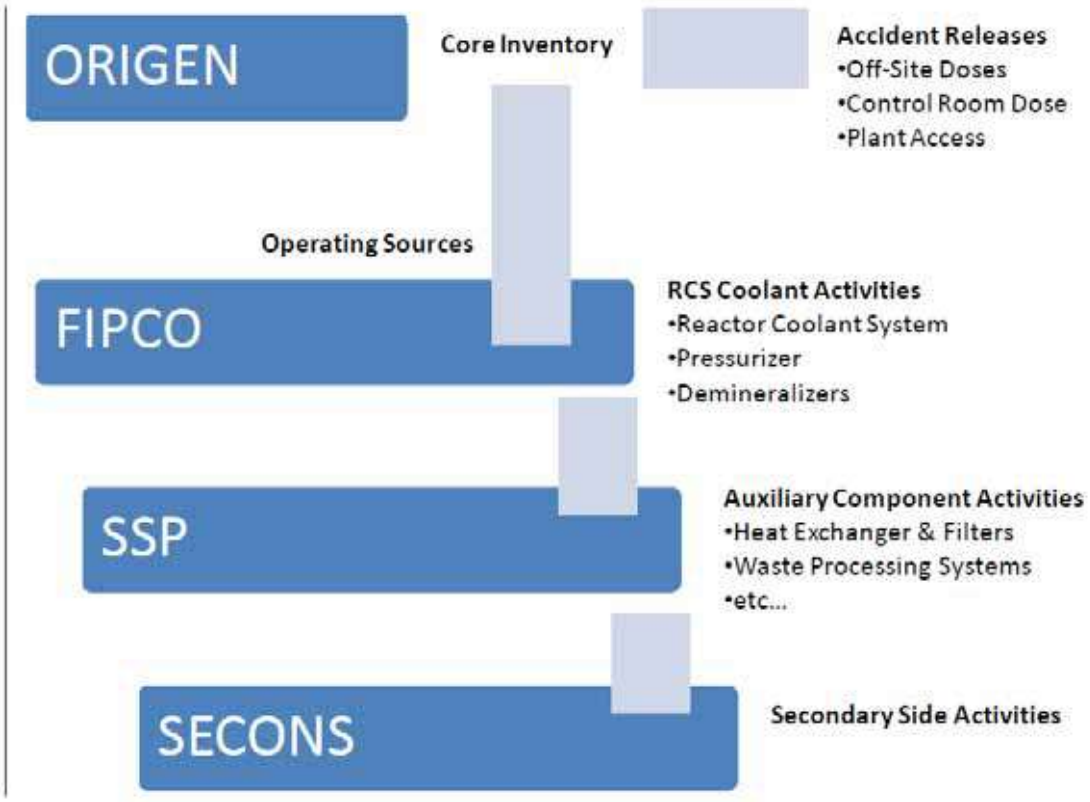


Figure 24-14. High Level Approach to Modelling Radiation Source Term Generation

APPENDIX 24A
RADIOLOGICAL CLASSIFICATION OF AREAS AND ACCESS REQUIREMENTS

Table 24A-1. Containment Areas Radiation Zones

Number	Name	Elevation	Zone Operation	Zone Shutdown	Zone Accident	Access Requirements
11104	Reactor coolant drain tank room	89.789 m (66’-6”)	VI	V	IX	Shutdown
11105	RV cavity	89.789 m (66’-6”)	IX	VI	IX	Shutdown only
11105	RV cavity	94.666 m (82’-6”)	IX	VI	IX	Shutdown only
11105	RV cavity	98.932 m (96’-6”)	IX	V	IX	Shutdown only
11201	SG compartment 1	94.666 m (82’-6”)	VI	V	IX	Shutdown only
11201	SG compartment 1	98.932 m (96’-6”)	VII	V	IX	Shutdown only
11202	SG compartment 2	94.666 m (82’-6”)	VI	V	IX	Shutdown only
11202	SG compartment 2	98.932 m (96’-6”)	VII	V	IX	Shutdown only
11204	Vertical access	94.666 m (82’-6”)	VI	V	IX	
11205	Nozzle Gallery	98.932 m (96’-6”)	IX	VI	IX	
11206	Passive core cooling system (PXS) valve/accumulator room A	94.666 m (82’-6”)	V	IV	IX	
11206	PXS valve/accumulator room A	98.932 m (96’-6”)	VI	VI	IX	
11207	PXS valve/accumulator room B	94.666 m (82’-6”)	V	IV	IX	
11207	PXS valve/accumulator room B	98.932 m (96’-6”)	V	VI	IX	
11208	RNS Valve room	98.932 m (96’-6”)	V	IV	IX	
11209	CVS room, Inner	94.666 m (82’-6”)	VIII	VIII	IX	

Table 24A-1. Containment Areas Radiation Zones (cont.)

Number	Name	Elevation	Zone Operation	Zone Shutdown	Zone Accident	Access Requirements
11209	CVS room, middle	94.666 m (82’-6”)	VII	VI	IX	
11209	CVS room, outer	94.666 m (82’-6”)	V	IV(1)	IX	
11300	Maintenance floor, east	100.0 m & 102.184 m (100’ & 107’-2”)	III(2)	II	IX	
11300	Maintenance floor, north and south	100.0 m & 102.184 m (100’ & 107’-2”)	IV(2)	II	IX	
11300	Maintenance floor, northwest (residual heat removal piping)	100.0 m & 102.184 m (100’ & 107’-2”)	V(23)	IV (V)	IX	
11301	SG 1 lower manway area	100.0 m & 102.184 m (100’ & 107’-2”)	VII(2)	V	IX	
11302	SG 2 lower manway area	100.0 m & 102.184 m (100’ & 107’-2”)	VII(2)	V	IX	
11303	Lower pressuriser compartment	100.0 m & 102.184 m (100’ & 107’-2”)	VI(2)	V	IX	
11303	Lower pressuriser compartment	105.334 m (117’-6”)	VI	V	IX	
11304	SG 1 access room	100.0 m & 102.184 m (100’ & 107’-2”)	V(2)	III	IX	
11305	Refuelling water storage tank	100.0 m & 102.184 m (100’ & 107’-2”)	IV(2)	VI	IX	
11305	Refuelling water storage tank	105.334 m (117’-6”)	IV	VI	IX	

Table 24A-1. Containment Areas Radiation Zones (cont.)

Number	Name	Elevation	Zone Operation	Zone Shutdown	Zone Accident	Access Requirements
11306	Divisions B&D penetration room	100.0 m & 102.184 m (100’ & 107’-2”)	IV(2)	IV	IX	
11400	Maintenance floor mezzanine	105.334 m (117’-6”)	IV/V	II	IX	Occasional operation/regular shutdown
11401	SG 1 tube sheet area	105.334 m (117’-6”)	VII	V	IX	
11402	SG 2 tube sheet area	105.334 m (117’-6”)	VII	V	IX	
11403	PRZ spray valve room	105.334 m (117’-6”)	VII	V	IX	
11500	Operating deck	110.744 m (135’-3”)	IV	II	IX	Occasional operation/regular shutdown
11500	Operating deck reactor head stand	110.744 m (135’-3”)	IV	V	IX	
11501	SG 1 operating deck	110.744 m (135’-3”)	VII	V	IX	
11502	SG 2 operating deck	110.744 m (135’-3”)	VII	V	IX	
11503	Upper pressuriser compartment	110.744 m (135’-3”)	V	V	IX	
11504	Refuelling cavity	98.932 m (96’-6”)	VI	V (IX)	IX	
11504	Refuelling cavity	100.0 m & 102.184 m (100’ & 107’-2”)	VI	V (IX)	IX	
11504	Refuelling cavity	105.334 m (117’-6”)	VI	V (IX)	IX	
11504	Refuelling cavity above water	110.744 m (135’-3”)	V	II	IX	Occasional operation/regular shutdown
11603	Automatic depressurisation system valve area	116.154 m & 118.440 m (153’ & 160’-6”)	V	V	IX	Shutdown only

Table 24A-1. Containment Areas Radiation Zones (cont.)

Number	Name	Elevation	Zone Operation	Zone Shutdown	Zone Accident	Access Requirements
11701	SG 1 upper manway level	116.154 m & 118.440 m (153’ & 160’-6”)	V	V	IX	Occasional operation/regular shutdown
11702	SG 2 upper manway level	116.154 m & 118.440 m (153’ & 160’-6”)	V	III	IX	Occasional operation/regular shutdown

Notes:

1. Room 11209: Dose rates may reach zone VI levels during resin transfer operations.

2. Rooms 11300, 11303, 11304, 11305, 11306: During power increases, an influx of reactor coolant into the pressurizer surge line can cause a short term increase in radiation levels temporarily exceeding the listed radiation zone.

Table 24A-2. Auxiliary Building Radiation Zones

Number	Name	Elevation	Zone Operations	Zone Shutdown	Zone Accident	Access Requirements
12101	Division A battery room	89.789 m (66’-6”)	I	I	III	No restrictions on access
12102	Division C battery room	89.789 m (66’-6”)	I	I	II	No restrictions on access
12103	Spare battery room	89.789 m (66’-6”)	I	I	II	No restrictions on access
12104	Division B battery room	89.789 m (66’-6”)	I	I	II	No restrictions on access
12105	Division D battery room	89.789 m (66’-6”)	I	I	II	No restrictions on access
12111	Corridor south section	89.789 m (66’-6”)	I	I	IV	No restrictions on access
12111	Corridor main east-west section	89.789 m (66’-6”)	I	I	IV	No restrictions on access
12111	Corridor northwest section	89.789 m (66’-6”)	I	I	III	No restrictions on access
12112	Spare room	89.789 m (66’-6”)	I	I	II	No restrictions on access
12113	Spare battery charger room	89.789 m (66’-6”)	I	I	II	No restrictions on access
12151	Demineraliser/filter room, corridor	89.789 m (66’-6”)	V	V	VII	**Occasional access required**
12151	Demineraliser/filter room, inside wall	89.789 m (66’-6”)	IX	IX	VII	No routine access required
12151	Demineraliser/filter room, outside wall	89.789 m (66’-6”)	VI	V	VII	No routine access required
12152	Primary sampling room	89.789 m (66’-6”)	II(1)	II	IX	Regular access required
12153	Delay beds compartment	89.789 m (66’-6”)	VII	IX	VII	No routine access required
12154	Auxiliary building, sump room dose over sump	89.789 m (66’-6”)	IV	VI	IX	**Occasional access required**

Table 24A-2. Auxiliary Building Radiation Zones (cont.)

Number	Name	Elevation	Zone Operations	Zone Shutdown	Zone Accident	Access Requirements
12155	WGS equipment room, alcove section	89.789 m (66’-6”)	IV	V-VI	VII	No routine access required
12155	WGS equipment room, corridor section	89.789 m (66’-6”)	V	VI	VII	**Occasional access required**
12156	WLS equipment room	89.789 m (66’-6”)	VI	VI	VII	**Occasional access required**
12158	Degasifier discharge pump room	89.789 m (66’-6”)	VI	VI	VII	No routine access required
12161	Corridor	89.789 m (66’-6”)	II(2)	II(2)	VII	Regular access required
12162	RNS pump room A	89.789 m (66’-6”)	V	VI	VII	**Occasional access required**
12163	RNS pump room B	89.789 m (66’-6”)	V	VI	VII	**Occasional access required**
12166	Waste holdup tank room A	89.789 m & 94.666 m (66’-6” & 82’-6”)	VI	VI	VII	**Occasional access required**
12167	Waste holdup tank room B	89.789 m & 94.666 m (66’-6” & 82’-6”)	VI	VI	VII	**Occasional access required**
12168	Vestibule	89.789 m (66’-6”)	V(2)	V	VII	**Occasional access required**
12169	Corridor	89.789 m (66’-6”)	V	V	VII	**Occasional access required**
12171	Effluent holdup tank room A	89.789 m (66’-6”)	VI(3)	VI	VII	**Occasional access required**
12172	Effluent holdup tank room B	89.789 m (66’-6”)	VI(3)	VI	VII	**Occasional access required**
12201	Division A DC equipment room	94.666 m (82’-6”)	I	I	III	No restrictions on access
12202	Division C battery room 2	94.666 m (82’-6”)	I	I	III	No restrictions on access
12203	Division C DC equipment room	94.666 m (82’-6”)	I	I	IV	No restrictions on access
12204	Division B battery room 2	94.666 m (82’-6”)	I	I	IV	No restrictions on access

Table 24A-2. Auxiliary Building Radiation Zones (cont.)

Number	Name	Elevation	Zone Operations	Zone Shutdown	Zone Accident	Access Requirements
12205	Division D DC equipment room	94.666 m (82’-6”)	I	I	IV	No restrictions on access
12207	Division B DC equipment room	94.666 m (82’-6”)	I	I	IV	No restrictions on access
12211	Corridor, west	94.666 m (82’-6”)	I	I	III	No restrictions on access **Access required in accident**
12211	Corridor, middle	94.666 m (82’-6”)	I	I	III-V	No restrictions on access **Access required in accident**
12211	Corridor, east	94.666 m (82’-6”)	I	I	III	No restrictions on access **Access required in accident**
12212	Division B RCP trip switchgear room	94.666 m (82’-6”)	I	I	III	No restrictions on access
12213	Spare room	94.666 m (82’-6”)	I	I	IV	No restrictions on access
12241	Lower annulus, east	94.666 m (82’-6”)	II	II	VII	**Occasional access required**
12241	Lower annulus, northeast	94.666 m (82’-6”)	VII	VII	VII	**Occasional access required**
12242	Lower annulus, southeast	94.666 m (82’-6”)	III	II	IX	**Occasional access required**
12244	Lower annulus valve area	94.666 m (82’-6”)	VII	VII	VII	**Occasional access required**
12251	Demineraliser filter access area	94.666 m (82’-6”)	III	IV	VII	**Occasional access required**
12251	Demineraliser filter access area	94.666 m (82’-6”)	III(4)	II	VII	Regular access required
12252	Rad chem lab	94.666 m (82’-6”)	II(5)	II(5)	VII	Regular access required
12253	Pipe chase	94.666 m (82’-6”)	VI	VII	VII	No routine access required
12253	Pipe chase	98.932 m (96’-6”)	VI	VII	VII	No routine access required
12254	SFS penetration room	94.666 m (82’-6”)	VI	VI	IX	**Occasional access required**

Table 24A-2. Auxiliary Building Radiation Zones (cont.)

Number	Name	Elevation	Zone Operations	Zone Shutdown	Zone Accident	Access Requirements
12254	SFS penetration room	98.932 m (96’-6”)	VI	VI	IX	**Occasional access required**
12255	CVS makeup pump room	94.666 m (82’-6”)	V(6)	IV	VII	**Occasional access required**
12255	CVS makeup pump room	94.666 m (82’-6”)	IV	IV	VII	**Occasional access required**
12256	Containment isolation valve room	98.932 m (96’-6”)	VII	VIII	IX	**Occasional access required**
12258	Degasifier column room	94.666 m (82’-6”)	VI	VI	VII	**Occasional access required**
12259	Pipe chase	98.932 m (96’-6”)	VII	VIII	VII	No routine access required
12261	Corridor, main corridor	94.666 m (82’-6”)	II	II	VII	Regular access required
12261	Corridor, end of west alcove	94.666 m (82’-6”)	III	III(7)	VII	**Occasional access required**
12262	Piping/valve room	94.666 m (82’-6”)	V	VI	VII	**Occasional access required**
12264	Chemical waste tank room	89.789 m & 94.666 m (66’-6” & 82’-6”)	V	V	VII	No routine access required
12265	Waste monitor tank room C	89.789 m & 94.666 m (66’-6” & 82’-6”)	IV	IV	VII	**Occasional access required**
12268	WLS pump room	94.666 m (82’-6”)	V	V(8)	VII	**Occasional access required**
12269	Pipe chase	98.932 m (96’-6”)	VII	VIII	IX	No routine access required
12271	WLS pump room	94.666 m (82’-6”)	V	V	VII	**Occasional access required**
12272	SFS pump room A	94.666 m (82’-6”)	IV	IV	VII	**Occasional access required**
12273	SFS HX room A	94.666 m (82’-6”)	V	V	VII	**Occasional access required**
12274	SFS pump room B	94.666 m (82’-6”)	IV	IV	VII	**Occasional access required**
12275	SFS HX room B	94.666 m (82’-6”)	V	V	VII	**Occasional access required**

Table 24A-2. Auxiliary Building Radiation Zones (cont.)

Number	Name	Elevation	Zone Operations	Zone Shutdown	Zone Accident	Access Requirements
12300	Corridor	100.0 m (100’)	I	I	IV	No restrictions on access **Access required in accident**
12301	Division A, I room	100.0 m (100’)	I	I	IV	No restrictions on access
12302	Division C, I& C room	100.0 m (100’)	I	I	IV	No restrictions on access **Access required in accident**
12303	Remote shutdown room	100.0 m (100’)	I	I	VI	No restrictions on access
12304	Division B, I&C penetration room	100.0 m (100’)	I	I	VII	No restrictions on access
12305	Division D, I&C penetration room	100.0 m (100’)	I	I	VII	No restrictions on access
12306	Valve/piping penetration room	100.0 m (100’)	I	I	VII	No restrictions on access **Access required in accident**
12306	Valve/piping penetration room platform	102.515 m (108’-3”)	I(9)	I(9)	VII	No restrictions on access
12311	Corridor	100.0 m (100’)	I	I	V	No restrictions on access
12312	Division C, RCP trip switchgear Room	100.0 m (100’)	I	I	VI	No restrictions on access
12313	Division C, I&C penetration room	100.0 m (100’)	I	I	VII	No restrictions on access
12321	Non-IE equipment penetration room	100.0 m (100’)	I	I	VII	No restrictions on access
12341	Middle annulus, northeast	100.0 m & 102.184 m (100’ & 107’-2”)	III(23)	II(23)		**Occasional access required**
12341	Middle annulus, southeast	100.0 m & 102.184 m (100’ & 107’-2”)	V	IV		**Occasional access required**

Table 24A-2. Auxiliary Building Radiation Zones (cont.)

Number	Name	Elevation	Zone Operations	Zone Shutdown	Zone Accident	Access Requirements
12341	Middle annulus, west	100.0 m & 102.184 (100’ & 107’-2”) m	III	III		**Occasional access required**
12341	Middle annulus, northeast	105.334 m (117’-6”)	III(22)	II(22)		**Occasional access required**
12341	Middle annulus, west	105.334 m	III	III		**Occasional access required**
12351	Maintenance floor staging area	100.0 m & 102.184 m (100’ & 107’-2”)	II(10)	II	VIII	Regular access required **Access required in accident**
12351	Maintenance floor staging area	105.334 m (117’-6”)	II(10)	II	VIII	Regular access required
12352	Personnel hatch	100.0 m & 102.184 m (100’ & 107’-2”)	III	II	IX	Occasional operation/regular shutdown
12354	Middle annulus access room	100.0 m & 102.184 m (100’ & 107’-2”)	VII	VI	VII	**Occasional access required** **Access required in accident**
12361	Corridor	100.0 m & 102.184 m (100’ & 107’-2”)	II	II	VII	**Occasional access required**
12362	RNS HX room	100.0 m & 102.184 m (100’ & 107’-2”)	V	VI	VII	**Occasional access required**
12363	Waste monitor tank room A	100.0 m & 102.184 (100’ & 107’-2”) m	IV	IV	VII	**Occasional access required**
12363	Waste monitor tank room A pump	105.334 m (117’-6”)	IV	IV	VII	Double height room
12365	Waste monitor tank room C	98.932 m (96’-6”)	V	V	VII	**Occasional access required** **Access required in accident**
12365	Waste monitor tank room C access platform	102.184 m(107’-2”)	V	V	VII	Occasional access required

Table 24A-2. Auxiliary Building Radiation Zones (cont.)

Number	Name	Elevation	Zone Operations	Zone Shutdown	Zone Accident	Access Requirements
12371	Rail car bay/filter storage area	100.0 m & 102.184 m (100’ & 107’-2”)	II[11,12,13]	II[11,12,13]	VII	Regular access required
12371	Rail car bay/filter storage area	105.334 m (117’-6”)	II[11,12,13]	II[11,12,13]	VII	Regular access required
12371	Rail car bay/filter storage area over waste disposal container (WDC) hatch	105.334 m (117’-6”)	IV[14]	IV[14]	VII	**Occasional access required**
12372	Resin transfer pump/valve room	100.0 m & 102.184 m (100’ & 107’-2”)	VII	IX	VII	No routine access required
12373	Spent resin tank room	100.0 m & 102.184 m (100’ & 107’-2”)	IX	IX	VII	No routine access required
12374	Waste disposal container area	100.0 m & 102.184 m (100’ & 107’-2”)	VII	IX	VII	No routine access required
12400	Control room vestibule	105.334 m (117’-6”)	I	I	IV	No restrictions on access
12401	Main control room	105.334 m (117’-6”)	I	I	IV	No restrictions on access
12404	Lower main steam isolation valve (MSIV) compartment B	105.334 m (117’-6”)	III	I	IX	No restrictions on access
12405	Lower VBS B&D equipment room	105.334 m (117’-6”)	I	I	VIII	No restrictions on access
12406	Lower MSIV compartment A	105.334 m (117’-6”)	III	I	IX	No restrictions on access
12411	Corridor	105.334 m (117’-6”)	I	I	VII	No restrictions on access
12412	Electrical penetration room, Div. A	105.334 m (117’-6”)	I	I	VII	No restrictions on access
12421	Non-IE equipment/penetration room	105.334 m (117’-6”)	I	I	VII	No restrictions on access
12422	Reactor trip switchgear 2	105.334 m (117’-6”)	I	I	VII	No restrictions on access

Table 24A-2. Auxiliary Building Radiation Zones (cont.)

Number	Name	Elevation	Zone Operations	Zone Shutdown	Zone Accident	Access Requirements
12423	Reactor trip switchgear 1	105.334 m (117’-6”)	I	I	VII	No restrictions on access
12451	Stairwell	105.334 m (117’-6”)	II	II	VIII	Regular access required
12452	VFS penetration room	105.334 m (117’-6”)	II	II	IX	Regular access required
12454	VFS/SFS/PSS penetration room	105.334 m (117’-6”)	VI	VI	IX	**Occasional access required**
12461	Corridor	105.334 m (117’-6”)	II	II	VII	Regular access required
12462	Cask washdown pit	105.334 m (117’-6”)	III(15)	III(15)	VII	**Occasional access required**
12463	Cask loading pit	98.932 m (96’-6”)	V	V	VII	**Occasional access required**
12463	Cask loading pit	100.0 m & 102.184 m (100’ & 107’-2”)	V(16,17)	III	VII	**Occasional access required**
12463	Cask loading pit	110.774 m (135’-3”)	III(17)	IV	VII	**Occasional access required**
12471	WSS valve/piping area	105.334 m (117’-6”)	VIII	VIII	VII	No routine access required
12472	New fuel storage pit	105.334 m (117’-6”)	II(20)	II(20)	VII	**Occasional access required**
12501	VBS MCR/A&C equipment room	110.744 m (135’-3”)	I	I	VI	No restrictions on access **Access required in accident**
12504	Upper MSIV compartment B	110.744 m (135’-3”)	I	I	VIII	No restrictions on access
12505	Upper VBS B&D equipment room	110.744 m (135’-3”)	I	I	VI	No restrictions on access
12506	Upper MSIV compartment A	110.744 m (135’-3”)	I	I	VIII	No restrictions on access
12541	Upper annulus, southwest	110.744 m (135’-3”)	III	II	IX	**Occasional access required**
12541	Upper annulus, southwest	116.154 m & 118.440 m (153’ & 160’-6”)	IV	II	IX	**Occasional access required**
12553	Personnel access area	110.744 m (135’-3”)	II	II	IX	Regular access required

Table 24A-2. Auxiliary Building Radiation Zones (cont.)

Number	Name	Elevation	Zone Operations	Zone Shutdown	Zone Accident	Access Requirements
12553	Personnel access area airlock	110.744 m (135’-3”)	III	II	IX	Regular access required
12554	Security room	110.744 m (135’-3”)	II	II	VIII	Regular access required
12554	Security room stairwell	110.744 m (135’-3”)	II	II	VIII	Regular access required
12555	VES air storage area	110.744 m (135’-3”)	II	II	IX	Regular access required
12556	Operating deck staging area	110.744 m (135’-3”)	III	II	IX	Regular access required
12561	CCS valve room	110.744 m (135’-3”)	II	II	VII	Regular access required
12562	Fuel-handling area	110.744 m (135’-3”)	II(18)	II(18)	VII	Regular access required
12562	Fuel-handling area	116.154 m & 118.440 m (153’ & 160’-6”)	II(18)	II(18)	VII	Regular access required
12563	Spent fuel storage pit	98.932 m (96’-6”)	IX	IX	VII	No routine access required
12563	Spent fuel storage pit	100.0 m & 102.184 m (100’ & 107’-2”)	IX	IX	VII	No routine access required
12563	Spent fuel storage pit	105.334 m (117’-6”)	IX	IX	VII	No routine access required
12563	Spent fuel storage pit	110.744 m (135’-3”)	II(19)	II(19)	VII	Regular access required
12563	Spent fuel storage pit	116.154 m & 118.440 m (153’ & 160’-6”)	II(19)	II(19)	VII	Regular access required
12564	Fuel transfer canal	100.0 m & 102.184 m (100’ & 107’-2”)	IV	IX	VIII	Occasional access when empty
12564	Fuel transfer canal	105.334 m (117’-6”)	IV	IX	VIII	Occasional access when empty
12564	Fuel transfer canal	110.744 m (135’-3”)	II(19)	II(19)	VIII	Regular access required

Table 24A-2. Auxiliary Building Radiation Zones (cont.)

Number	Name	Elevation	Zone Operations	Zone Shutdown	Zone Accident	Access Requirements
12564	Fuel transfer canal	116.154 m & 118.440 m (153’ & 160’-6”)	II[19]	II[19]	VIII	Regular access required
12601	North elevator mech room	116.154 m & 118.440 m (153’ & 160’-6”)	I	I	VII	No restrictions on access
12661	Elevator mech room	116.154 m & 118.440 m (153’ & 160’-6”)	II	II	VII	Regular access required
12691	North auxiliary building roof	116.154 m & 118.440 m (153’ & 160’-6”)	I	I	VII	No restrictions on access
12692	East auxiliary building roof	116.154 m & 118.440 m (153’ & 160’-6”)	II	II	VII	**Occasional access required**
12693	South auxiliary building roof	118.440 m & 124.384 m (160’-6” & 180’)	II	II	VII-IX	**Occasional access required**
12701	PCS valve room	118.440 m & 124.384 m (160’-6” & 180’)	V	II	VII	**Occasional access required**
12702	Shield building roof, north	118.440 m & 124.384 m (160’-6” & 180’)	II	II	IX	**Occasional access required**
12702	PCS air cooling diffuser	118.440 m & 124.384 m (160’-6” & 180’)	V	II	IX	**Occasional access required**
12702	Shield building roof east (and west)	118.440 m & 124.384 m (160’-6” & 180’)	V	II	IX	**Occasional access required**

Notes:

1. Room 12152: Radiation may exceed the Zone II level locally during sampling.
2. Room 12161: Zone III dose rates may occur with the degasifier out of service.
3. Rooms 12171 and 12172: May be as high as Zone VII dose rates in the event of degasifier failure.
4. Room 12251: Radiation may exceed the Zone III level during filter replacement operations.
5. Room 12252: Radiation may exceed the Zone II level with the presence of radioactive sources.
6. Room 12255: Zone V during reactor coolant degasification operations using makeup pumps in the CVS semi-closed loop configuration.
7. Room 12261 (alcove): Zone IV dose rates may occur in the immediate vicinity of the opening to Room 12262 during shutdown conditions.
8. Room 12268: Zone IV contribution from spent fuel in the vertical position in the up-ender.
9. Room 12306: Blowdown piping may reach Zone II levels with concurrent fuel cladding defects of 0.25 percent and SG tube leakage of 1935 litres per day (500 gpd).
10. Room 12351: Zone III dose rates will occur within ~1.2 m (4.0 feet) of the opening to Room 12363, unless a shielded door is employed.
11. Room 12371: During spent resin disposal container transfer or loading, Zone VII dose rates may occur within this room.
12. Room 12371: During spent fuel transfer and/or transportation cask handling or loading operations, Zone V dose rates may occur within the room.
13. Room 12371: Due to radiation from the SFP, Zone IV dose rates may occur in the northwest corner of this room. If freshly discharged assemblies are loaded near the south edge of the SFP, Zone V dose rates may be possible.
14. Room 12371: Over the WDC hatch, Zone VII dose rates may occur in this location when the hatch to Room 12374 is open.
15. Room 12462: The cask washdown pit can be as high as Zone 5 during cask handling/washdown operations.
16. Room 12463: The underwater spent fuel assembly is at least 1.52 m (5.0 feet) from the south, east, and north walls.
17. Room 12463: During underwater spent fuel assembly transfer operations, this area can be as high as Zone IX. When a loaded cask (with lid in place) is present, dose rates may be as high as Zone V.
18. Room 12562: This area may have dose rates as high as Zone V during spent fuel transfer cask-handling operations. Dose rates as high as Zone III may occur during spent resin handling operations.
19. Room 12564: Zone II dose rates occur at all accessible locations that lie above the SFP water surface.
20. Room 12472: Zone III dose rates may occur during resin transfer.
21. Room 12168: Zone VI dose rates may occur with the degasifier out of service.
22. Room 12341: Zone IV dose rates may occur near the fuel transfer tube hatch during fuel transfer.
23. Room 12362: During cask movement Zone V Levels May exist in this area

Table 24A-3. Annex Building Radiation Zones

Number	Name	Elevation	Zone Operation	Zone Shutdown	Zone Accident	Access Requirements
40300	Security	100.0 m (100’)	I	I	VI	No restrictions on access
40301	Access corridor	100.0 m (100’)	I	I	VI	No restrictions on access **Access required in accident**
40302	Security	100.0 m (100’)	I	I	VI	No restrictions on access
40303	Corridor	100.0 m (100’)	I	I	VI	No restrictions on access **Access required in accident**
40304	Toilet	100.0 m (100’)	I	I	VI	No restrictions on access
40305	Security	100.0 m (100’)	I	I	VI	No restrictions on access
40306	Security	100.0 m (100’)	I	I	VI	No restrictions on access
40307	Battery room No. 1	100.0 m (100’)	I	I	VI	No restrictions on access
40308	Battery charger room No. 1	100.0 m (100’)	I	I	VI	No restrictions on access
40309	Battery room No. 2	100.0 m (100’)	I	I	VI	No restrictions on access
40310	Battery charger room No. 1	100.0 m (100’)	I	I	VI	No restrictions on access
40311	Corridor	100.0 m (100’)	I	I	VII	No restrictions on access **Access required in accident**
40312	Corridor	100.0 m (100’)	I	I	VII	No restrictions on access
40313	Office	100.0 m (100’)	I	I	VII	No restrictions on access
40314	Office	100.0 m (100’)	I	I	VII	No restrictions on access

Table 24A-3. Annex Building Radiation Zones (cont.)

Number	Name	Elevation	Zone Operation	Zone Shutdown	Zone Accident	Access Requirements
40316	Computer room L1/2	100.0 m (100’)	I	I	VII	No restrictions on access
40317	Computer room L13	100.0 m (100’)	I	I	VII	No restrictions on access
40318	ALARA briefing room and operational support centre	100.0 m (100’)	I	I	VII	No restrictions on access
40320	Women’s change room	100.0 m (100’)	I	I	VII	No restrictions on access
40321	Janitor closet	100.0 m (100’)	I	I	VII	No restrictions on access
40322	Men’s change room	100.0 m (100’)	I	I	VII	No restrictions on access
40323	Water heater room	100.0 m (100’)	I	I	VII	No restrictions on access
40324	Drying area (men)	100.0 m (100’)	I	I	VII	No restrictions on access
40325	Shower room (men)	100.0 m (100’)	I	I	VII	No restrictions on access
40326	Non-RCA entry exit area	100.0 m (100’)	I	I	VI	No restrictions on access **Access required in accident**
40327	Health physics office	100.0 m (100’)	I	I	VI	No restrictions on access
40340	Demineralised water deoxygenating room	100.0 m (100’)	I	I	VI	No restrictions on access
40341	Temporary electrical supply room	100.0 m (100’)	I	I	VI	No restrictions on access
40350	RCA entry exit area	100.0 m (100’)	II	II	VI	Regular access required **Access required in accident**
40351	PC pickup and suitup	100.0 m (100’)	II	II	VI	Regular access required
40352	Corridor	100.0 m (100’)	II	II	VI	Regular access required

Table 24A-3. Annex Building Radiation Zones (cont.)

Number	Name	Elevation	Zone Operation	Zone Shutdown	Zone Accident	Access Requirements
40354	HP counting room	100.0 m (100’)	II	II	VI	Regular access required
40355	Decontamination room	100.0 m (100’)	II	II	VI	Regular access required
40356	Lobby to annex building 12351	102.184 m (107’-2”)	II	II	VIII	Regular access required
40357	Containment access corridor	102.184 m (107’-2”)	II	II	VIII	Regular access required
40358	Hot machine shop	102.184 m (107’-2”)	III	III	VI	**Occasional access required**
40359	Pump seal shop	102.184 m (107’-2”)	III	III	VI	**Occasional access required**
40360	Decontamination room	100.0 m (100’)	II	II	VI	Regular access required
40361	Lobby to 40357	102.184 m (107’-2”)	II	II	VI	Regular access required
40361	Radwaste building access corridor	100.0 m (100’)	II	II	VI	Regular access required
40370	Toilet	100.0 m (100’)	I	I	VII	No restrictions on access
40371	Conference room	100.0 m (100’)	I	I	VII	No restrictions on access
40372	Conference room	100.0 m (100’)	I	I	VII	No restrictions on access
40373	Corridor	100.0 m (100’)	I	I	VII	No restrictions on access
40374	Corridor	100.0 m (100’)	I	I	VII	No restrictions on access
40375	Conference room	100.0 m (100’)	I	I	VII	No restrictions on access
40376	Kitchen	100.0 m (100’)	I	I	VII	No restrictions on access
40377	Toilet	100.0 m (100’)	I	I	VII	No restrictions on access
40378	Office area west	100.0 m (100’)	I	I	VII	No restrictions on access

Table 24A-3. Annex Building Radiation Zones (cont.)

Number	Name	Elevation	Zone Operation	Zone Shutdown	Zone Accident	Access Requirements
40379	Office area east	100.0 m (100’)	I	I	VII	No restrictions on access
40400	Corridor	105.334 m (117’-6”)	I	I	VI	No restrictions on access
40401	Toilet	105.334 m (117’-6”)	I	I	VI	No restrictions on access
40402	Corridor	105.334 m (117’-6”)	I	I	VI	No restrictions on access
40403	Control support area	105.334 m (117’-6”)	I	I	VI	No restrictions on access
40404	Toilet	105.334 m (117’-6”)	I	I	VI	No restrictions on access
40405	Rest area kitchen	105.334 m (117’-6”)	I	I	VI	No restrictions on access
40406	Conference room	105.334 m (117’-6”)	I	I	VI	No restrictions on access
40407	Conference room	105.334 m (117’-6”)	I	I	VI	No restrictions on access
40408	Office for Nuclear Regulation room	105.334 m (117’-6”)	I	I	VI	No restrictions on access
40409	Conference room	105.334 m (117’-6”)	I	I	VI	No restrictions on access
40410	Computer room A	105.334 m (117’-6”)	I	I	VI	No restrictions on access
40411	Computer room B	105.334 m (117’-6”)	I	I	VI	No restrictions on access
40412	Shift turnover room	105.334 m (117’-6”)	I	I	VI	No restrictions on access
40413	Electrical switchgear room No. 1	105.334 m (117’-6”)	I	I	VI	No restrictions on access
40414	Electrical switchgear room No. 2	105.334 m (117’-6”)	I	I	VI	No restrictions on access
40442	Boric acid batching room	108.00 m (126’-3”)	I	I	VI	No restrictions on access
40500	North air-handling equipment room	110.74 m (135’-3”)	I	I	V	No restrictions on access
40501	Air intake plenum No. 1	110.74 m (135’-3”)	I	I	V	No restrictions on access

Table 24A-3. Annex Building Radiation Zones (cont.)

Number	Name	Elevation	Zone Operation	Zone Shutdown	Zone Accident	Access Requirements
40503	Lower south air handling equipment room	110.74 m (135’-3”)	I	I	VI	No restrictions on access
40504	Air intake plenum No. 2	110.74 m (135’-3”)	I	I	VI	No restrictions on access
40505	Security room	110.74 m (135’-3”)	I	I	VI	No restrictions on access
40550	Staging and storage area	110.74 m (135’-3”)	II	II	IX	Regular access required
40551	Containment air filtration exhaust room A	110.74 m (135’-3”)	III	III	IX	**Occasional access required**
40552	Containment air filtration exhaust room B	114.097 m (146’-3”)	III	III	IX	**Occasional access required**
40600	Lift machinery room	117.069 m (156’)	I	I	VI	No restrictions on access
40601	Upper south air handling equipment room	117.069 m (156’)	I	I	VI	No restrictions on access
40602	Air intake plenum No. 3	117.069 m (156’)	I	I	VI	No restrictions on access

Table 24A-4. Radwaste Building Radiation Zones

Number	Name	Elevation	Zone Operation	Zone Shutdown	Zone Accident	Access Requirements
50300	Electrical mechanical equipment room	100.00 m (100’)	I	I	VII	No restrictions on access
50350	Mobile systems facility	100.00 m (100’)	II	II	VII	No restrictions on access
50351	Waste accumulation room	100.00 m (100’)	IV	IV	VII	**Occasional access required**
50352	Packaged waste storage room	100.00 m (100’)	IV	IV	VII	**Occasional access required**
50353	HVAC equipment room	100.00 m (100’)	III	III	VII	**Occasional access required**
50354	Truck staging area	100.00 m (100’)	II	II	VII	No restrictions on access

Table 24A-5. Outside Building Radiation Zones

Number	Name	Elevation	Zone Operations	Zone Shutdown	Zone Accident	Access Requirements
Outside	Outdoors west of Room 12471	105.334 m (117’-6”)	III(1)			Normal access not possible

Note:

1. This dose rate, which occurs off the building west wall, near the southwest corner, at elevations between 7.3 and 9.75 m (23 and 32 ft), only occurs during spent resin sluicing operations. At other times, the dose rate is Zone I.

APPENDIX 24B
AP1000 ANNUAL OCCUPATIONAL DOSE ASSESSMENT

24B.1 Methodology

Baseline collective doses were determined for individual tasks within the following overall categories:

- Reactor operations and surveillance
- Routine maintenance
- ISI
- Special maintenance
- Waste processing
- Refuelling

These gave the total doses in each category with none of the dose reduction methodologies incorporated in the AP1000 design as shown in Table 24B-1. The total collective dose of 1.68 person-Sv is high and represents historical data before improvements were made in operational practices to reduce worker doses. The information on doses from the individual tasks in Reference 24.40 was, therefore, used only for the relative contributions to the total.

The baseline case for the total collective dose to workers from outages was taken from the recent history of two Westinghouse reactors (Prairie Island 1 and 2), each generating 522 MWe. The first reactor commenced commercial operation in 1973 and the second in 1974. They represent a standard two-loop Westinghouse nuclear power plant.

The rolling average annual collective doses recorded during outages at the Prairie Island reactors have shown a steady improvement over the years from 1670 person-mSv between startup and 1990, to 894 person-mSv between 1996 to 2003 (Reference 24.22). The average collective dose from Prairie Island units 1 and 2 from 1996 to 2003 has been used in Reference 24.40 as being representative of doses received when modern practice radiation dose control procedures are applied during outages. The latest information on collective dose from the Prairie Island units (Reference 24.22) shows that the rolling average collective dose is continuing to fall. In addition, the collective dose for 2007 (62.8 person-Sv) gives a clear indication of the operational dose when there is no refuelling outage.

To estimate the distribution of the total collective dose among the work categories, the fraction of the total collective dose in each category from 1995 to 1997 was averaged as, shown in Table 24B-2. The fractions were applied to the mean collective dose of 894 person-mSv, as shown in Table 24B-1.

The dose from each subtask within each work category was then determined and adjustment factors were applied to take account of the differences between the AP1000 design and existing Westinghouse PWRs.

24B.2 Component Reduction Adjustment

The amount of work to be carried out, and therefore the dose incurred, will be affected by the number of components, which has been significantly reduced in the AP1000 design compared with previous Westinghouse reactors. A component adjustment factor has, therefore, been determined based on the number of components of each type in the AP1000 design, as shown in Table 24B-3.

The number of components in the AP1000 design is slightly higher than in the AP600 design but this has been taken into account in the adjustment factor.

24B.3 Crud Reduction Adjustment

A number of techniques have been used in Reference 24.40 to assess the benefits of the reduction of cobalt concentration and zinc injection on the dose rate from crud by comparing plant dose rates and corrosion calculations. Some changes, such as the use of zinc additions following SG replacement, were accompanied by other changes, such as electropolishing SG channel heads and use of low-cobalt tubing. Therefore, an exercise was undertaken in Reference 24.40 to normalise the dose reductions achieved to take account of additional changes so that a reduction factor could be estimated for zinc addition. The dose reduction factors identified from the normalisation study can be summarised as follows:

- Use of low-cobalt tubing in the SGs:
    - Comparison of plants with replacement SGs with low-cobalt tubing with plants with normal cobalt content SG tubing: average reduction factor 0.70
    - Results of corrosion studies and analysis: reduction factor calculated as 0.82
    - A reduction value of 0.76 was adopted as the average of the two values
- Use of no-cobalt valves:

– Results of corrosion studies and analysis: reduction factor calculated as 0.87

- Zinc addition to RCS:
    - Addition of zinc to plants after eight or nine cycles reduced dose rates by about 50 percent
    - Comparison of dose rates from piping in similar plants, one of which added zinc following SG replacement, gave a reduction factor of 0.26
    - As the data are only for one or two cycles of zinc addition from startup of a new plant or a plant with replacement SGs, a reduction factor of 0.40 was assumed

The effect of zinc addition alone makes a significant difference to the dose rates from crud deposition. Therefore, it is considered that a more detailed description of the determination of this value in Reference 24.40 is required.

The addition of zinc to the RCS reduces the corrosion rate and subsequent transport of the major materials of construction in the RCS. Until recently, the effect of zinc on plant dose rates was available only from plants that added zinc while in their ninth or later cycle. By this time, the component corrosion films have been somewhat stabilised and the effect of coolant additives is diminished. Nonetheless, plant data indicated that dose rates would be reduced by about 50 percent after about four cycles of zinc addition (Reference 24B.1).

The Angra 2 plant was designed by Siemens before various stellite reduction methods were incorporated in the Konvoi plants (Reference 24B.2). At the time of preparation of Reference 24.40, zinc addition had continued for two cycles. Comparison of piping dose rates with those on similar plants such as the KWG Ghronde plant that did not undergo stellite reduction (Reference 24B.3) enabled the effects of zinc injection to be assessed. Dose rates were determined from interpolation of data presented in a figure in Reference 24B.4.

Cycle of Operation	Ghronde	Angra 2	Ratio, Angra/Ghronde
1	49.2	8.7	0.18
2	68.1	11.6	0.17

The next comparison involved identifying a number of plants where a range of dose reduction techniques had been incorporated and comparing doses after and before SG replacement where the replacement SGs had electropolished channel heads (Reference 24B.5). A total of 14 plants were included; 4 did not have electropolished channel heads and, of the remaining 10, 8 used normal coolant chemistry while Farley 1 and 2 were operated with zinc injection before and after SG replacement. The dose reduction ratios achieved in each plant were normalised to take account of the other dose reduction techniques applied, which gave the following dose reduction ratios.

Source Reduction Technique	Dose Rate Reduction Factor	Code
High vs. low-cobalt impurity fuel grid nickel braze	0.80	FGNB
High vs. low-cobalt fuel grids (Inconel vs. Zircaloy)	0.72	FGIZ
High vs. low-cobalt impurity SG tubing	0.70	ISGT
Varying vs. constant coolant pH	0.86	CCpH
Overall reduction	0.35	All

By dividing the ratio of doses before and after SG replacement by the relevant ratio, based on one or more of the dose reduction factors above, the dose reduction ratio resulting from electropolishing the channel heads can be determined. The comparison of the dose reduction factor achieved by using electropolished channel heads on plants with zinc injection to the factor on plants with normal coolant chemistry gives the reduction factor achieved by means of zinc injection.

The dose reduction factors on plants with normal coolant chemistry in Reference 24.40 are as follows:

SG Replacement Plants with Electropolished Channel Heads – Normal Coolant Chemistry				
Plant	**Elements of Normalisation**	**Normalisation Factor**	**Ratio Before Normalisation**	**Ratio After Normalisation**
Braidwood 1	ISGT (0.70)	0.70	0.47	0.67
Byron 1	ISGT (0.70)	0.70	0.52	0.74
Catawba 1	ISGT (0.70)	0.70	0.21	0.30
McGuire 1	FGNB (0.80) ISGT (0.70)	0.56	0.14	0.24
McGuire 2	FGNB (0.80) ISGT (0.70)	0.56	0.26	0.46
Harris	ISGT (0.70)	0.70	0.33	0.47
Summer	FGNB (0.80) ISGT (0.70)	0.56	0.34	0.61
South Texas 1	ISGT (0.70)	0.70	0.58	0.82
Mean:				**0.54**

The dose reduction factors on plants with zinc injection before and after SG replacement in Reference 24.40 are as follows:

SG Replacement Plants with Electropolished Channel Heads – Zinc Addition Coolant Chemistry				
Plant	**Elements of Normalisation**	**Normalisation Factor**	**Ratio Before Normalisation**	**Ratio After Normalisation**
Farley 1	All	0.35	0.05	0.13
Farley 2	FGIZ (0.72) ISGT (0.70)	0.50	0.04	0.08
Mean:				**0.11**

For comparison, the dose reduction ratios before and after normalisation on plants where the channel heads in the replacement SGs were not electropolished in Reference 24.40 are as follows:

SG Replacement Plants with Nonelectropolished Channel Heads – Normal Coolant Chemistry				
No. Anna 1	All	0.35	0.41	1.18
No. Anna 2	All	0.35	0.49	1.40
Ringhals 2	All	0.35	0.36	1.03
Ringhals 3	FGNB (0.80) ISGT (0.70)	0.56	0.55	0.99
Mean:				**1.15**

The average normalised ratio in the plants with electropolished channel heads and normal coolant chemistry is 0.54. These results indicate a beneficial effect of electropolishing, which on the average results in a dose rate about one-half of that for plants without electropolishing. The long-term dose rate trends in the plants indicate a levelling. This suggests a continuing benefit of electropolishing.

The range of the normalised ratios in plants with electropolishing (0.24 to 0.82) indicates that all factors affecting the dose rates have not been taken into account. One reason for the higher values noted in Braidwood 1 and Byron 1 could be due to the longer cycle length after SG replacement compared with that before. A reason for the South Texas 1 higher value could be due to limited data after SG replacement.

The low normalised ratios in plants that use zinc addition illustrate a significant effect on the channel head dose rates. The absolute channel head dose rates in the two plants were 6.2 and 3.4 Sv/h, the lowest observed in any Westinghouse plant after one cycle of operation. The average normalised value of 1.15 for plants without electropolishing also indicates that not all the factors have been taken into account in the normalisation factors, but that the dose rate trend is similar to that before replacement; thus, confirming the dose rate reduction effect of electropolishing. The effect of zinc addition can be estimated by comparison of the average effect in the Farley plants to that in the other plants with electropolished channel heads. On an overall basis, the average effect is 0.11/0.54 = 0.20, or essentially the same as that obtained from the Angra 2 evaluation. Another estimate of the effect can be obtained by excluding the values from the three high plants (see above) and using the average of the remaining five (0.42). This will yield a zinc addition effect of 0.11/0.42 = 0.26.

Since there are only data from one or two cycles of zinc addition in a “new” plant, on a conservative basis, a zinc reduction factor of 0.40 will be assumed in this calculation note. If more data becomes available, the factor can be updated.

As the Prairie Island reactors have an energy density of 93.5 kW/litre compared with 109.7 kW/litre for the AP1000 design, a correction was applied for the increase in core flux that increases the activation of corrosion products.

The overall effects on the source term relative to the Prairie Island plant were determined to be the following:

- Low-cobalt tubing 0.76
- No-cobalt valves 0.87
- Power density 1.17
- Zinc addition 0.4
- Product of above 0.31

In addition, electropolishing of the SG channel head was determined to provide a further reduction factor of 0.5 for work specifically related to this area of the SG.

The factor applied to each task contribution to the total dose in each work category was determined according to whether the dose was from general background, in which case the factor of 0.31 was appropriate, or from specific components. In the latter case, a conservative reduction factor of 0.62 (2 x 0.31 to allow for crud traps) was applied in combination with the component reduction factor, as shown in Appendix 24A, Table 24A-4.

24B.4 Dose Estimates

The doses from each of the following work categories, excluding refuelling, were calculated:

- Reactor operations and surveillance
- Routine maintenance
- ISI
- Special maintenance
- Waste processing

Other assumptions are shown in the comments in the relevant tables.

Because of the major differences in design between pumps and the reactor head and upper internals on the AP1000 design compared with previous reactors and the use of robotics for many operations, it was not appropriate to scale doses from the following:

- RCP inspection
- Refuelling
- SG sludge lancing
- SG secondary-side inspection
- SG EC tube inspection
- SG ISI

Specific JEM calculations were carried out in Reference 24.42 for refuelling, as shown in Appendix 24C, and in Reference 24.44 for other operations, as shown in Appendix 24D.

24B.5 Results

The contributions from each task within each category are shown in the following:

- Table 24B-4, Dose Estimate for Reactor Operations and Surveillance
- Table 24B-5, Outage Dose from Routine Maintenance
- Table 24B-6, Outage Dose from In-Service Inspection

- Table 24B-7 Outage Dose from Special Maintenance
- Table 24B-8, Annual Dose from Waste Processing
- Appendix 24C

The ISIs include periodic examinations that are not carried out at each outage. While it would not be appropriate, for comparison against the numerical targets, to average such exposures out over the inspection interval, it would also give a falsely high collective dose to include all periodic examinations in 1 year. Therefore, the highest collective dose contribution from a periodic ISI has been included.

The total annual dose in the year with the highest contribution from ISI is shown in Table 24B-9 as 239.0 person-mSv. Collective dose in years where no refuelling outage takes place and in years where the periodic ISI dose is small will be lower.

24B.6 References

24B.1 "PWR Operating Experience with Zinc Addition and the Impact on Radiation Fields 1003389," Electric Power Research Institute, 2003.

24B.2 "Experience with Zinc Injection in European PWRs 1003378," Electric Power Research Institute, 2002.

24B.3 Garbett, K., "Overview of the Impact Of Stellite Removal on Radiation Fields in KWU PWRs," Fourth Water Chemistry Conference for Nuclear Reactor Systems, October 1986.

24B.4 Streit, K., "The Impact of Water Chemistry upon Primary Circuit Component Integrity," International Atomic Energy Agency Workshop, November 2003.

24B.5 "Radiation Field Control Manual 1003390," Electric Power Research Institute, 2004.

Table 24B-1. Breakdown of Historical Collective Dose

Overall Categories	Original Dose in Outage Year from (Reference 24.42) (person-mSv)	Average % of Prairie Island Dose per Category (1995-1997)	Prairie Island Average Dose in Outage Years 1996-2003 (person-mSv)
Reactor operations and surveillance	263	9.27	82.9
Routine maintenance	245.7	16.14	144.3
ISI	297	27.26	243.7
Special maintenance	629.2	25.28	226
Waste processing	72	2.6	23.2
Refuelling	170	19.46	174
Total	**1676.9**	**100**	**894.1**

Table 24B-2. Fractions of Collective Dose in Each Work Category for Prairie Island Reactors 1995-1997

Work Category	Collective Dose (person-mSv)			% Contribution			
	1995	1996	1997	1995	1996	1997	Mean
Reactor operations and surveillance	108.81	93.24	149.74	10.67	8.48	8.67	9.27
Routine maintenance	209.76	187.04	187.38	20.56	17.01	10.85	16.14
ISI	250.22	273.15	559.95	24.53	24.84	32.41	27.26
Special maintenance	238.82	300.33	433.97	23.41	27.31	25.12	25.28
Waste processing	11.4	42.65	48.2	1.12	3.88	2.79	2.60
Refuelling	201.21	203.36	348.29	19.72	18.49	20.16	19.46
Total	**1020.22**	**1099.77**	**1727.53**	**100**	**100**	**100**	**100**

Table 24B-3. Adjustment Factors for Reduction in the Number of Components and Crud Reduction Techniques

Component Type	Component Reduction Factor[1]	Crud Activity Reduction Factor[2]	Overall Component Reduction Factor
All valves	0.4	0.62	0.25
Manual valves	0.37	0.62	0.23
Safety class valves	0.61	0.62	0.38
Pumps	0.43	0.62	0.27
HXs	0.56	0.62	0.35
Demineralisers	0.63	0.62	0.39
Filters	0.63	0.62	0.39

Notes:

1. This represents the ratio of the number of components in the AP1000 design to the number in the previous generation Westinghouse reactor plants.
2. The crud reduction factor of 0.31 has been doubled for components to allow for unidentified crud traps where the total reduction may not apply.

Table 24B-4. Dose Estimate for Reactor Operations and Surveillance

Task Description	Dose (Reference 24.42)		Normalised to PI 1996-2003 Data (person-mSv)	Nominal Adjustment Factor	AP1000 Design Collective Dose Contribution (person-mSv)	Comments
	person-mSv	%				
Patrols and inspections	100	38.02	31.52	0.31 for 1/2 of time	20.6	Assume 1/2 of dose is at power (no adjustment)
Valve line-ups (manual)	10	3.80	3.15	0.37	1.2	0.62 adj. factor x 0.37 for fewer valves
System flushing and testing	8	3.04	2.52	0.31	0.8	
Health Physics						
Job coverage	35	13.31	11.03	0.31 for 2/3 of time	6.0	Assume 1/3 of dose is at power (no adjustment)
Routine surveys	30	11.41	9.46	0.31	2.9	
Decontamination of equipment and work areas	50	19.01	15.76	0.31	4.9	
Calibration of instrumentation	20	7.60	6.30	0.31	2.0	
Chemistry sampling	10	3.80	3.15	0.31	1.0	
Health physics subtotal					**16.7**	
Totals	**263**	**100**	**82.9**		**39.3**	

Table 24B-5. Outage Dose from Routine Maintenance

Task Description	Dose (Reference 24.42)		Normalised to PI 1996-2003 Data (person-mSv)	Nominal Adjustment Factor	AP1000 Collective Dose Contribution (person-mSv)	Comments
	person-mSv	%				
Valve adjustment/repacking	50	20.33	29.33	0.25	7.3	0.62 adj. factor x 0.40 for fewer valves
Auxiliary pump overhaul	50	20.33	29.33	0.27	7.9	0.62 adj. factor x 0.43 for fewer pumps
RCP maintenance and inspection	46	18.70	26.98	0	0.0	Not necessary for AP1000 design RCPs
SG sludge lance	22	8.94	12.90	N/A	12.8	
Demineraliser resin changeout	25	10.16	14.66	0.39	5.7	0.62 adj. factor x 0.63 for fewer demins.
Filter replacement	20	8.13	11.73	0.39	4.6	0.62 adj. factor x 0.63 for fewer filters
Calibrate/repair electrical components	15	6.10	8.80	0.31	2.7	
Miscellaneous work	10	4.07	5.87	0.31	1.8	Includes RCP inspection: Appendix 24D, Table 24D-1
SG secondary -side inspection	8	3.25	4.69	N/A	1.9	SG secondary-side inspection JEM: Appendix 24D, Table 24D-3
Totals	**246**	**100.00**	**144.30**		**44.8**	

Table 24B-6. Outage Dose from In-Service Inspection

Task Description	Dose (Reference 24.42)		Normalised to PI 1996-2003 Data (person-mSv)	Nominal Adjustment Factor	AP1000 Design Collective Dose Contribution (person-mSv)	Comments
	person-mSv	%				
Valve bodies and bolting	100	33.67	82.05	0.25	20.5	0.62 adj. factor x 0.40 for fewer valves
SG primary-side inspections	57	19.19	46.77		7.5	SG EC tube inspection JEM: Appendix 24D, Table 24D-4
RV and RVCH	37	12.46	30.36		20.0	Note 1
RCS loop piping and supports	18	6.06	14.77	0.31	4.6	
SG shell	17	5.72	13.95		4.3	SG ISI: Appendix 24D, Table 24D-5 (highest year)
Other piping	35	11.78	28.72	0.31	8.9	
HX shells	13	4.38	10.67	0.35	3.7	0.62 adj. factor x 0.56 for fewer HXs
Pressuriser shell	12	4.04	9.85	0.31	3.1	
Pumps	4	1.35	3.28	0.27	0.9	0.62 adj. factor x 0.43 for fewer pumps
Tank shells and supports	3	1.01	2.46	0.31	0.8	

Table 24B-6. Outage Dose from In-Service Inspection (cont.)

Task Description	Dose (Reference 24.42)		Normalised to PI 1996-2003 Data (person-mSv)	Nominal Adjustment Factor	AP1000 Design Collective Dose Contribution (person-mSv)	Comments
	person-mSv	%				
Filter housing and supports	1	0.34	0.82	0.39	0.3	0.62 adj. factor x 0.63 for fewer filters
Total	**297**	**100.00**	**243.70**		**74.5**	
Total (Highest year)					**60.2**	Note 2

Notes:

1. It is assumed that the RV and RVCH will be inspected at intervals of 5 years or every third outage (Reference 24.40). The dose from each inspection is estimated to be 10 mSv.
2. The ISIs on the RV, head, and SGs will not be expected to be undertaken in the same year. Therefore, the highest year dose is the year in which there is an outage with the RVCH ISI.

Table 24B-7. Outage Dose from Special Maintenance

Task Description	Dose (Reference 24.42)		Normalised to PI 1996-2003 Data (person-mSv)	Nominal Adjustment Factor	AP1000 Design Collective dose Contribution (person-mSv)	Comments
	person-mSv	%				
Plant upgrades/modifications	150	23.85	53.90	0	0.0	No upgrades are assumed
Valve repairs	110	17.49	39.52	0.25	9.9	0.62 adj. factor x 0.40 for fewer valves
SG primary-side inspections	107	17.01	38.45	0	0.0	Included in ISI under SG primary-side inspection
Auxiliary pump repairs	95	15.10	34.13	0.27	9.2	0.62 adj. factor x 0.43 for fewer pumps
Electrical repairs	40	6.36	14.37	0.31	4.5	
RCP repairs and inspections	40	6.36	14.37	0	0.0	No repairs/inspections are assumed
SG tube plugging	28	4.45	10.06	0	0.0	Included in ISI under SG primary-side inspection
Repairs to tanks, HXs, piping	25	3.97	8.98	0.31	2.8	No credit taken for fewer HXs
SG secondary-side repairs	14	2.23	5.03	0.31	1.6	
Pressuriser repairs	12	1.91	4.31	0.31	1.3	
CRDM repairs	8	1.27	2.87	0.31	0.9	
Totals	**629**		**226.00**		**30.1**	

Table 24B-8. Annual Dose from Waste Processing

Task Description	Dose (Reference 24.42)		Normalised to PI 1996-2003 Data (person-mSv)	Nominal Adjustment Factor	AP1000 Design Collective Dose Contribution (person-mSv)	Comments
	person-mSv	%				
Radioactive waste handling	40	55.56	12.89	1	12.9	
System adjustment/repairs	25	34.72	8.06	1	8.1	
System operation (sampling, valve adjustments, monitoring)	5	6.94	1.61	1	1.6	
Laundry operations	2	2.78	0.64	1	0.64	Laundry assumed to be offsite
Totals	**72**	**100.00**	**23.20**		**23.2**	

Table 24B-9. Total Dose in a Year with an Outage

Overall Categories	Dose (person-mSv)	%
Reactor operations and surveillance	39.3	16.49
Routine maintenance	44.9	18.82
ISI	60.2	25.26
Special maintenance	30.1	12.64
Waste processing	23.2	9.46
Refuelling (Appendix 24C)	41.3	17.32
Total	**239.0**	

APPENDIX 24C
REFUELLING DOSE ESTIMATE

24C.1 Introduction

The collective dose to the group of workers undertaking the refuelling operations has been estimated using the JEM system, which uses a Microsoft Excel spreadsheet to estimate worker doses (Reference 24.42). The dose calculation is based on dose rates at existing plants, modified as appropriate for the reduction in crud as a result of the design and operating regime of the AP1000 plant and other design changes and durations of tasks based on the preliminary AP1000 plant refuelling outage schedule.

24C.2 Overview of Refuelling Operations

Prior to the plant shutdown, new fuel assemblies must be inspected and placed into the new fuel storage area or staged in the spent fuel pool. Generally, the new fuel arrives at the plant anywhere from a few months to a few days prior to the start of a refuelling. At this time, the fuel handling tools and equipment in the SFP are checked and repaired as necessary.

When the plant has been shut down, radiation surveys and equipment checks are performed inside containment. These checks include a survey of the fuel transfer system, RM, and surrounding structures.

When the equipment checks have been completed, preparation of the RVCH begins with the disconnection of the seismic supports and removal of RVCH insulation. The CRDM and DRPI electrical cables are then disconnected and the cable bridges are swung clear. The in-core instrument bullet-nose assemblies that include the in-core thermocouple connections are then disconnected at eight locations near the top of the vessel head. The RVCH vent and reactor vessel level instrumentation system (RVLIS) are also disconnected at this time.

When the RVCH has been prepared for removal, the RV studs are de-tensioned and removed. Next, stud hole plugs are inserted into the vacant stud holes, and by this point in the refuelling, the quick opening transfer tube closure has been opened. After all equipment has been removed from the cavity, the head lift begins. The RVCH is transferred from the RV to the head storage stand located on the operating deck. During the movement of the head, the refuelling cavity is flooded. Next, the CRDM drive shafts are unlatched and the upper internals lift rig is attached to the upper internals. The lift rig is equipped with features that move the thimble support plate such that the in-core instrumentation can be moved with the upper internals package. The upper internals are then removed and placed on their storage stand.

At this point, fuel unloading operations commence. At some point during the fuel unloading, the old RVCH O-rings are removed and inspected, and new O-rings are installed if necessary.

The fuel movement procedure can be summarised as follows:

- The RM is positioned over a fuel assembly. The hoist is then lowered until the grippers engage in the upper nozzle of the fuel assembly. The used fuel assembly is then lifted and placed in the up-ender for transfer to the SFP.

- The carriage containing the used fuel assembly is then lowered from the vertical position to a horizontal position by the up-ender. The carriage is then transferred through the transfer tube to the SFP via the conveyor system.

- On the SFP side of the transfer tube, the carriage is rotated by the SFP up-ender device to the vertical position. The assembly is then removed from the carriage by the fuel-handling machine and placed in a spent fuel storage rack. This process continues until all of the fuel is moved to the SFP.

- New fuel is lifted from its storage area and placed into the SFP elevator. The elevator is lowered to the bottom of the pit. Then the fuel-handling machine is used to carry the assembly to the transfer carriage. The fuel-handling machine releases the new fuel assembly and the carriage is lowered to the horizontal position by the SFP up-ender. The carriage is then transferred to the refuelling cavity via the conveyor system where it is raised to a vertical position by the cavity up-ender. The new fuel assembly is now ready to be moved by the RM.

- The new assemblies and reload assemblies to be replaced are moved to the RV and placed in their proper core location.

Fuel transfer continues until all of the fuel assemblies in the reactor core have been replaced with new fuel or reload assemblies. When the operation is complete, the core is mapped with an underwater camera to ensure that the assemblies are in their proper locations.

Following this inspection, the RV upper internals are reinstalled and the thimble support plate is lowered into position. The CRDM drive shafts are latched and a drag test is performed on each roc cluster control assembly (RCCA).

The cavity water level is then drained to the RV flange elevation. The RV flange is remotely cleaned and inspected.

The reactor head is placed on the vessel and the in-core instrument bullet-nose fittings are reconnected.

After cavity cleaning, the stud hole plugs are removed and the stud holes are cleaned and lubricated. The RV studs are threaded into the vessel and the tensioning sequence completed. The tensioning equipment is then removed from the cavity. The RVCH vent is re-attached and the head insulation reinstalled. Finally, the cable bridge is swung back into position and the cable connections are re-established.

24C.3 Nominal Dose Rates and Radiation Zones

The dose rates used in the calculation of the refuelling doses (Reference 24.42) are shown in Table 24C-1. The order of the zone numbering in the original calculation has been reversed to avoid confusion with the radiation zoning system in Table 24-7. The approximate relationship between dose rates used in this calculation and the radiation zones in Table 24-7 are shown in Table 24C-1 for comparison.

The dose rates are based on the location of the operations and the dose rates used in the original refuelling JEM (Reference 24.44):

- Zone VI was increased from 5 to 7.5 mSv/h based on the change in location from the maximum outside the IHP to that outside the flange during raising and lowering of the head and/or during flange cleaning.

- Zone V was increased from 0.5 to 1 mSv/h based on a change in location from a typical location near the flange with the head raised to the estimated dose rate in the work area where the in-core instrument stack "quick-disconnects" are made.

- The typical Zone IV location was changed to a location near the RV flange since the in-core thimbles are no longer retracted into the area above the top of the head. The dose rate is increased slightly from 0.02 to 0.025 mSv/h.

- The dose rate for Zone III of 0.01 mSv/h does not change from the previous value. However, since the in-core thimbles are no longer retracted into the area above the top of the head, the location is defined as that in the area where the cable tray CRDM connectors and CRDM fan connectors are located.

- Zone II was previously defined as the area where thimble work was done above the top of the head. In addition, it was the value used as the maximum value during fuel movement. Since the in-core thimbles are no longer retracted into the area above the top of the head, the primary work location is considered to be that on the manipulator crane and/or SFP bridge deck during fuel movement. From Reference 24.25 this area is such that a conservative exposure rate is 0.025 mSv/h.

- Zone 1 is on the operating deck where the dose rate is considered to be 0.01 mSv/h. This value does not change from the value used in the previous analysis. It is considered to be an effective dose rate and variations are to be expected, e.g., at edge of the refuelling cavity/SFP, with a high level of activity in the water, or near the reactor head on the storage stand. However, the operating deck radiation fields during refuelling at current operating plants are typically 0.01 mSv/h or less.

24C.4 Other Assumptions in the Job Evaluation Model

The estimate of the collective and individual doses from refuelling is based on a group of 8 workers on a rolling 4-shift basis (32 workers) and one supervisor.

The individual dose calculation assumes that one member of the group of workers undertakes tasks within each dose rate zone. Where the overall duration of the task is more than a single shift, this is overpessimistic.

24C.5 Results

The results of the JEM calculation in Reference 24.42 are shown in Table 24C-2 rearranged and converted to SI units. The mean and maximum individual doses are shown in Table 24C-3.

The total collective dose is 41.29 person-mSv incurred during 722 working hours. The split in man-hours, collective dose, and maximum individual dose among the tasks is as follows:

Task Category	Total Man-Hours	Collective Dose (person-mSv)	Maximum Individual Dose (mSv)
Job preparation	106	1.105	0.600
Reactor disassembly	148	14.155	2.016
Fuel movement	196	2.329	0.540
Reactor assembly	256	23.525	2.016
Job cleanup	16	0.175	0.040
Totals	**722**	**41.29**	

Table 24C-1. Nominal Dose Rates Associated with Refuelling Operations

Zone ID for Calculation from (Reference 24.42) (Reversed)	Description	Dose Rate (mSv/h)	Zone ID Based on Dose Rate
1	Operating deck	0.01	I
2	Above cavity and SFP water	0.025	II
3	Cable tray/CDRM fan connectors	0.1	III
4	RV flange area, head in place	0.25	IV
5	Near IIS stack connections	1	IV
6	RV flange area, head off	7.5	V

Table 24C-2. AP1000 Design Refuelling Dose Model

Task No.	Zone	I		II		III		IV		V		VI		Total (man-hours)	Collective Dose (person-mSv)
	Dose Rate (mSv/h)	0.01		0.025		0.1		0.25		1		7.5			
	Number of Workers (N) Duration of Operation (h)	N	h	N	h	N	h	N	h	N	h	N	h		
1	**Job Preparation**														
1.01	Crane decon/check/maintenance	5	12											60	0.6
1.02	Visual inspection of reactor vessel head/internals	3	4											12	0.12
1.03	Open equipment hatch	3	1											3	0.03
1.04	Move in refuelling equipment	2	6	2	0.5									13	0.145
1.05	Manipulator crane checkout	2	6											12	0.12
1.06	Fuel-handling equipment checkout	2	2	1	2									6	0.09
Subtotals														**106**	**1.105**
2	**Reactor Disassembly**														
2.01	Disconnect HVAC piping							2	0.33					0.66	0.165
2.02	Disconnect/remove CRDM/DRPI cable							2	1.5					3	0.75
2.03	Remove reactor vessel head insulation	2	1							2	0.5			3	1.02
2.04	Remove reactor vessel head vent line	1	0.75	2	0.5	2	0.5							2.75	0.1325

Table 24C-2. AP1000 Refuelling Dose Model (cont.)

Task No.	Zone	I		II		III		IV		V		VI		Total (man-hour)	Collective Dose (person-mSv)
	Dose Rate (mSv/h)	0.01		0.025		0.1		0.25		1		7.5			
	Number of Workers (N) Duration of Operation (h)	N	h	N	h	N	h	N	h	N	h	N	h		
2	**Reactor Disassembly (cont.)**														
2.05	Detension/remove studs	2	10			4	8							52	3.4
2.06	Install stud hole plugs	2	2			2	2	2	2					12	1.44
2.07	Disconnect IIS bullet-nose assemblies	2	1.6					2	1.6	2	1.6			9.6	4.032
2.08	Remove transfer tube blind flange			2	0.5					2	0.5			2	1.025
2.09	Remove equipment from cavity	1	2	4	0.5	2	1							6	0.27
2.10	Clean reactor vessel cavity and reactor vessel head	1	2	1	2	1	2							6	0.27
2.11	Move head package to storage stand	6	1					2	0.5			1	0.08	7.08	0.91
2.12	Fill refuelling cavity	1	8											8	0.08
2.13	Unlatch/verify CRDMs	1	8	2	5									18	0.33
2.14	Install upper internals lift rig	1	4	2	2									8	0.14
2.15	Remove and store upper internals	1	4	2	3									10	0.19
Subtotals														**145**	**14.155**

Table 24C-2. AP1000 Refuelling Dose Model (cont.)

Task No.	Zone	I		II		III		IV		V		VI		Total (man-hour)	Collective Dose (person-mSv)
	Dose Rate (mSv/h)	0.01		0.025		0.1		0.25		1		7.5			
	Number of Workers (N) Duration of Operation (h)	N	h	N	h	N	h	N	h	N	h	N	h		
3	**Fuel Movement**														
3.01	Verify manipulator crane index	1	2	2	0.17									2.34	0.0285
3.02	Fuel-handling system wet checkout	2	6	1	1									13	0.145
3.03	Fuel offload (full core)	2	22	1	11									55	0.715
3.04	Fuel inspection/shuffle fuel inserts	2	33											66	0.66
3.05	Core reload	2	24	1	12									60	0.78
Subtotals														**196**	**2.329**

Table 24C-2. AP1000 Refuelling Dose Model (cont.)

Task No.	Zone	I		II		III		IV		V		VI		Total (man-hour)	Collective Dose (person-mSv)
	Dose Rate (mSv/h)	0.01		0.025		0.1		0.25		1		7.5			
	Number of Workers (N) Duration of Operation (h)	N	h	N	h	N	h	N	h	N	h	N	h		
4	**Reactor Assembly**														
4.01	Install upper internals	1	4	2	3									10	0.19
4.02	Remove upper internals lift rig	1	4	2	2									8	0.14
4.03	Relatch and drag test RCCAs	1	8	2	8									24	0.48
4.04	Drain cavity and hydrolaze walls	1	2.5	6	2.5									17.5	0.4
4.05	Remove and install RV O-ring			1	10	2	5	2	5					30	3.75
4.06	Clean inspect RV flange	1	0.5					1	0.5	2	0.5			2	1.13
4.07	Set RVCH	6	1					2	0.5			1	0.08	7.08	0.91
4.08	Install transfer tube blind flange			2	0.5					2	0.5			2	1.025
4.09	Connect IIS bullet-nose assemblies	2	1.6					2	1.6	2	1.6			9.6	4.032
4.10	Decontaminate refuelling cavity	2	6	4	6	4	6							60	3.12
4.11	Remove stud hole plugs and clean	2	4			2	4	2	4					24	2.88
4.12	Install/tension RVCH studs	2	10			4	8							52	3.4
4.13	Install RVCH vent line	1	0.75	2	0.5	2	0.5							2.75	0.1325
4.14	Install RVCH insulation	2	1							2	0.5			3	1.02
4.15	Connect CRDM and DRPI cables							2	1.5					3	0.75
4.16	Connect HVAC piping							2	0.33					0.66	0.165
Subtotals														**256**	**23.525**

Table 24C-2. AP1000 Refuelling Dose Model (cont.)

Task No.	Zone	I		II		III		IV		V		VI		Total (man-hour)	Collective Dose (person-mSv)
	Dose Rate (mSv/h)	0.01		0.025		0.1		0.25		1		7.5			
	Number of Workers (N) Duration of Operation (h)	N	h	N	h	N	h	N	h	N	h	N	h		
5	**Job Cleanup**														
5.01	Remove refuelling equipment	2	1.5	2	0.5									4	0.055
5.02	Replace equipment hatch	3	4											12	0.12
Subtotals														**16**	**0.175**
TOTALS														**722.02**	**41.29**

Table 24C-3. Mean and Maximum Individual Refuelling Doses by Task

Task No.	Task Description	No. of Men	Collective Dose (person-mSv)	Average Individual Dose (mSv)	Maximum Individual Dose (mSv)
1	**Job Preparation**				
1.01	Crane decon/check/maintenance	5	0.600	0.120	0.120
1.02	Visual inspection of reactor vessel head/internals	3	0.120	0.040	0.040
1.03	Open equipment hatch	4	0.030	0.008	0.010
1.04	Move in refuelling equipment	4	0.145	0.036	0.073
1.05	Manipulator crane checkout	2	0.120	0.060	0.060
1.06	Fuel-handling equipment checkout	3	0.090	0.030	0.070
2	**Reactor Disassembly**				
2.01	Disconnect HVAC piping	2	0.165	0.083	0.083
2.02	Disconnect/remove CRDM/DRPI cable	2	0.750	0.375	0.375
2.03	Remove RVCH insulation	4	1.020	0.255	0.510
2.04	Remove RVCH vent line	3	0.133	0.044	0.070
2.05	Detension/remove studs	6	3.400	0.567	0.900(1)
2.06	Install stud hole plugs	4	1.440	0.360	0.720
2.07	Disconnect IIS bullet-nose assemblies	6	4.032	0.672	2.016
2.08	Remove transfer tube blind flange	4	1.025	0.256	0.513
2.09	Remove equipment from cavity	4	0.270	0.068	0.133
2.10	Clean RV cavity and RVCH	3	0.270	0.090	0.270
2.11	Move head package to storage stand	6	0.910	0.152	0.735
2.12	Fill refuelling cavity	1	0.080	0.080	0.080
2.13	Unlatch/verify CRDMs	3	0.330	0.110	0.205
2.14	Install upper internals lift rig	3	0.140	0.047	0.090
2.15	Remove and store upper internals	3	0.190	0.063	0.115
3	**Fuel Movement**				
3.01	Verify manipulator crane index	4	0.029	0.007	0.024
3.02	Fuel-handling system wet checkout	3	0.145	0.048	0.085
3.03	Fuel offload (full core)	8	0.715	0.089	0.495(2)

Table 24C-3 Mean and Maximum Individual Refuelling Doses by Task (cont.)

Task No.	Task Description	No. of Men	Collective Dose (person-mSv)	Average Individual Dose (mSv)	Maximum Individual Dose (mSv)
3	**Fuel Movement (cont.)**				
3.04	Fuel inspection/shuffle fuel inserts	6	0.660	0.110	0.330[3]
3.05	Core reload	8	0.780	0.098	0.540[2]
4	**Reactor Assembly**				
4.01	Install upper internals	3	0.190	0.063	0.115
4.02	Remove upper internals lift rig	3	0.140	0.047	0.090
4.03	Relatch and drag test RCCAs	4	0.480	0.120	0.280
4.04	Drain cavity and hydrolaze walls	6	0.400	0.067	0.088
4.05	Remove and install RV O-ring	5	3.750	0.750	2.000[4]
4.06	Clean and inspect RV flange	5	1.130	0.226	0.630
4.07	Set RVCH	6	0.910	0.152	0.735
4.08	Install transfer tube blind flange	4	1.025	0.256	0.513
4.09	Connect IIS bullet-nose assemblies	6	4.032	0.672	2.016
4.1	Decontaminate refuelling cavity	8	3.120	0.390	0.810
4.11	Remove stud hole plugs and clean	3	2.880	0.960	1.440
4.12	Install/tension RVCH studs	6	3.400	0.567	0.900
4.13	Install RVCH vent line	3	0.133	0.044	0.070
4.14	Install RVCH insulation	4	1.020	0.255	0.510
4.15	Connect CRDM and DRPI cables	2	0.750	0.375	0.375
4.16	Connect HVAC piping	2	0.165	0.083	0.083
5	**Job Cleanup**				
5.01	Remove refuelling equipment	4	0.055	0.014	0.028
5.02	Replace equipment hatch	4	0.120	0.030	0.040
Totals		**32**	**41.288**	**1.290**	
Maximum individual dose					**2.016**

Notes:

1. The task duration precludes exposure of a single worker at both low and high dose rates. With no worker rotation the maximum dose is 800 μSv.
2. The task duration precludes exposure of a single worker to high and low dose rates for the entire task (three shifts). The maximum individual dose is estimated to be 200 μSv.
3. The task duration precludes exposure of a single worker for the entire task (four shifts). The maximum individual dose is estimated to be 160 μSv.
4. The task manning level precludes a single worker being exposed to low and high dose rates. The maximum individual dose is estimated to be 1.25 mSv.

APPENDIX 24D
DOSE ESTIMATES FOR SPECIFIC TASKS

24D.1 Specific Tasks

There are a number of tasks for which it is not appropriate to scale doses received on other Westinghouse plants. For these operations specific JEM assessments have been undertaken in Reference 24.40. The following tasks are covered:

- RCP inspection
- SG sludge lancing
- SG secondary-side visual examination
- SG EC tube inspection and tube plugging
- SG ISI
- RCP ISI

Two other specific tasks were identified in the occupational dose assessment (Reference 24.40), which is carried out within a specific time or number of outages:

- RVCH inspections – Bare metal examination every third outage or 5 years; nondestructive testing examination of penetrations every fourth outage or 7 years.

- RV Inspections – Every 10 years (around every 6 outages).

A JEM calculation was undertaken for the RVCH inspection, which was carried out in Reference 24.44 (this reference also contains the JEM calculation for the refuelling dose, which has been superseded by Reference 24.42). However, on review, the method adopted involved man-access beneath the RVCH to remove instruments, which resulted in an individual dose of 5 mSv. Further discussion with specialists provided the following information:

On a typical job immediately following the close out of the inspection we tear down and remove the control equipment outside of the headstand (with the head on the stand) and then later when the head is moved back onto the vessel we remove the inspection equipment from inside the stand. For the AP1000 head inspections there will be no planned manual inspections underneath the head and no other planned personnel entries underneath the head while it is on the stand.

Although the inspections can last up to 4 or 5 days, they are performed remotely with the operators stationed outside the containment. During the actual span of the inspection we have very little time spent in containment. As you can see the majority of out of containment time is spent setting up and tearing down equipment.

24D.2 Job Exposure Models

The JEM calculations for inspections are shown in the following tables:

- Table 24D-1, Outage Dose Estimate from RCP Inspection

- Table 24D-2, Outage Dose Estimate from SG Sludge Lancing

- Table 24D-3, Outage Dose from Visual Inspection of SG Secondary Side

- Table 24D-4, Dose Estimate for SG EC Tube Inspection and Tube Plugging
- Table 24D-5, Dose Estimate for SG ISI (10-yr Interval)
- Table 24D-6, Dose Estimate for Canned Motor RCP (The European AP1000 design will use wet-winding pumps; however, the dose from maintenance of canned pumps has been included because it is expected that the maintenance dose from wet-winding pumps will not be significantly higher.)
- Table 24D-8, Reactor Vessel Head Inspection Dose

The same technique was adopted for the RV head inspection dose calculation as for the refuelling dose calculation. Dose rates were determined for various locations, as shown in Table 24D-7 (Reference 24.44); the dose calculation was based on numbers of workers, task durations, and dose rate zones determined by specialists within Westinghouse. The total collective dose of 10.0 person-mSv shows good agreement with doses from actual similar operations on existing plants (Reference 24.44). The highest individual exposure is 5 mSv from removal of the inspection equipment following the J-weld examinations, taking 0.5 hr at 10 mSv/h. However, it is noted in Reference 24.44 that, when it was written in 2005, the J-weld examinations were the first of their kind to be undertaken in the industry and it was expected that, with experience and improvements to equipment and techniques, the doses incurred would be significantly reduced.

There is no JEM calculation for the RV ISI but the total collective dose of 10 person-mSv is based on experience from a number of plants.

Table 24D-1. Outage Dose Estimate from RCP Inspection

Activity	Average Dose Rate (μSv/h)	No. of Workers	Time (hr)	Collective Dose (person-mSv)
Electrical[1]				
Measure insulation resistance to ground	0	1	0.2	0
Measure winding resistance	0	1	0.2	0
Mechanical	**N/A**	**N/A**	**N/A**	**N/A**
Total per pump				**0**
Total four pumps				**0**

Note:

1. Electrical measurements may be made from the RCP switchgear located outside the containment.

Table 24D-2. Outage Dose Estimate from SG Sludge Lancing

Activity	Average Dose Rate (μSv/h)	No. of Workers	Time (hr)	Collective Dose (person-mSv)
Move equipment into containment	40	6	4	0.96
Remove insulation and handhole cover	150	1	0.5	0.075
Complete pre-lance water balance	150	2	1	0.3
Install lance on handhole	150	2	0.5	0.15
Operate water lance	150	2	12	3.6
Complete post-lance water balance	150	2	1	0.3
Remove equipment	40	6	4	0.96
Install handhole cover and insulation	150	1	0.5	0.075
Total per SG				**6.42**
Total two SGs				**12.84**

Table 24D-3. Outage Dose from Visual Inspection of SG Secondary Side

Activity	Average Dose Rate (μSv/h)	No. of Workers	Time (hr)	Collective Dose (person-mSv)
Remove insulation and two manway covers(1)	4	2	2.5	0.02
Inspect separators orifices and feedwater ring(1)	40	1	0.5	0.02
Install two manway covers and insulation and lower water level below handholes(1)	4	2	2.5	0.02
Remove insulation and secondary handhole cover	150	2	0.5	0.15
Photograph support plates	150	2	2	0.6
Install handhole covers and insulation	150	2	0.5	0.15
Total per SG				**0.96**
Total two SGs				**1.92**

Note:

1. Secondary-side water level at the lower deck plate

Table 24D-4. Dose Estimate for SG EC Tube Inspection and Tube Plugging

Activity	Average Dose Rate (μSv/h)	No. of Workers	Time (hr)	Collective Dose (person-mSv)
Move equipment into containment	8	4	4	0.128
Install ventilation equipment	200	1	1	0.2
Remove insulation on both manway covers	150	2	0.2	0.06
Remove both manway covers with handling fixture	200	2	1	0.4
Remove both manway inserts(1)	1200	2	0.1	0.24
Install fixture on manway(1)	1200	2	0.1	0.24
Install universal/robotic arm on manway	200	2	0.25	0.1
Insert nozzle hot and cold leg dams with robotic arm	200	2	0.5	0.2
Replace dam fixture tool with EC end effector on robotic arm (hot leg channel)	200	1	0.25	0.05
Perform EC exam of 3340 tubes (33 1/3%)	4	1	111	0.444
Remove EC end effector and replace with mechanical plugging tool	200	1	0.2	0.04
Insert plugs in three tubes	200	1	0.75	0.15
Transfer robotic arm to cold leg channel	200	2	0.25	0.1
Insert plugs in three tubes	200	1	0.75	0.15
Remove robotic arm	200	2	0.25	0.1
Remove hinged fixture(1)	1200	2	0.1	0.24
Install manway inserts(1)	1200	2	0.1	0.24
Install both manway covers with handling fixture	200	2	1	0.4
Replace insulation both manway covers	200	2	0.2	0.08
Remove ventilation equipment	200	1	0.5	0.1
Move equipment out of containment	8	4	2	0.064
Total per SG				**3.726**
Total two SGs				**7.452**

Note:

1. The dose rates for these operations would be reduced by electropolishing the SG bowl, but no credit was taken. The minimum effect would be a reduction of 0.48 person-mSv per SG or 0.96 person-mSv total. There may be a reduction of some of the other dose rates where the SG bowls make a contribution.

Table 24D-5. Dose Estimate for SG ISI (10-yr Interval)

Activity	Average Dose Rate (μSv/h)	No. of Workers	Time (hr)	Collective Dose (person-mSv)
Move equipment into containment	8	4	4	0.128
Remove/Install Insulation				
Steam nozzle(1)	4	2	0.1	0.0008
Secondary manways(1)	4	2	0.1	0.0008
Feedwater nozzle(1)	40	1	0.1	0.004
3 Upper shell girth welds(1)	20	2	1	0.04
Secondary handhole(2)	150	1	0.1	0.015
3 Lower shell girth welds(1)	150	2	1	0.3
Channel head to tube sheet weld(2)	400	2	0.3	0.24
2 Pump to channel head welds(2)	400	2	0.2	0.16
PXS pipe to channel head weld(2)	400	1	0.1	0.04
Hot leg to channel head weld(2)	400	2	0.2	0.16
Install Ultrasonic Inspection Rig				
3 Upper shell girth welds(1)	20	2	0.3	0.012
3 Lower shell girth welds(1)	150	2	0.3	0.09
Channel head to tube sheet weld(2)	400	2	0.1	0.08
2 Pump to channel head welds(2)	400	2	0.2	0.16
PXS pipe to channel head weld(2)	400	1	0.1	0.04
Hot leg to channel head(2)	400	1	0.3	0.12
Ultrasonic Inspection				
3 Upper shell girth welds(1)	0.4	2	7.5	0.006
3 Lower shell girth welds(1)	0.4	2	7.5	0.006
Channel head to tube sheet weld(2)	0.4	2	3	0.0024
2 Pump to channel head welds(2)	0.4	2	2	0.0016
PXS pipe to channel head weld(2)	0.4	2	0.5	0.0004
Hot leg to channel head(2)	0.4	2	1	0.0008
Dye Penetrant Inspection				
Steam nozzle(1)	4	2	0.2	0.0016

Table 24D-5. Dose Estimate for SG ISI (10-yr Interval) (cont.)

Activity	Average Dose Rate (μSv/h)	No. of Workers	Time (hr)	Collective Dose (person-mSv)
Feedwater nozzle(1)	40	1	0.1	0.004
2 pump to channel head(2)	400	2	0.5	0.4
PXS to channel head(2)	400	1	0.1	0.04
Hot leg to channel head(2)	400	2	0.2	0.16
Visual Inspection				
Secondary manway bolts	4	2	0.1	0.0008
Secondary handhole bolts	150	1	0.1	0.015
Secondary inspection hole bolts	400	2	0.2	0.16
Primary manway bolts	400	2	0.1	0.08
SG Support	400	1	0.1	0.04
Remove equipment from containment	8	4	4	0.128
EC tests Table 24D-4 included in ISI Table 24B-6				
Total (highest year)				**4.257**
Mean per outage (six outages)				**0.71**

Notes:

1. Only 1 SG inspected at every 10 year or 6 outages.
2. Both SGs inspected at each outage.

Table 24D-6. Dose Estimate for Canned Motor RCP ISI

Activity	Average Dose Rate (μSv/h)	No. of Workers	Time (hr)	Collective Dose (person-mSv)
Pump Removal				
Position maintenance cart under pump	20	2	2	0.08
Install walkways and tensioner platform	20	2	2	0.08
Disconnect wiring and piping, attach actuator to pump	20	2	0.5	0.02
Install stud tensioners, remove and store nuts and eight studs	80	2	4	0.64
Lower motor on the cart	900	2	0.5	0.9
Move cart to crane access area, install shields over impeller and on pump casing	150	2	3	0.9
Inspection				
Visual inspection of twenty-four 3 1/2" studs, nuts, and washers	20	2	2	0.08
Ultrasonic Testing (UT) scan and dye penetrant testing of studs	20	2	2	0.08
Remotely conduct visual inspection of casing internal surface	20	2	4	0.16
Pump Installation				
Lower pump and maintenance cart to pump compartment, and position under pump casing	20	2	4	0.16
Remove pump casing shield	150	2	0.5	0.15
Raise motor until seated	80	2	1	0.16
Install walkway and tensioner platforms	20	2	2	0.08
Install eight studs and all nuts in two passes	80	2	4	0.64
Reconnect wiring and piping, detach actuator	20	2	0.5	0.02
Store the maintenance cart	20	2	1	0.04
Total 1 pump				**4.19**

Notes:

1. In the European version of the AP1000 design, it is currently proposed that the canned pumps will be replaced by wet-winding pumps (Reference 24.44). The implications of this change on maintenance doses is not yet known. However, as the motor windings and rotor have a cooling water supply, it is expected that the doses will be no greater than those for the canned pumps. In lieu of specific information, the dose estimate for canned pump maintenance has been used. The times provided for activities are estimates; actual maintenance times may vary.
2. The inspection of one pump is only scheduled for the first cycle of operation. If the RCPs are not removed for maintenance, ISI is limited to external visual inspection and UT scan.

Table 24D-7. Nominal Dose Rates Associated with Reactor Vessel Head Inspection

Zone ID for Calculation (Reference 24.44) (Reversed)	Description	Dose Rate (mSv/h)	Zone ID Based on Dose Rate
1	Operating deck GA	0.01	I
2	Inside stand, without RVCH	0.05	III
3		0.1	III
4		0.25	IV
5	GA adjacent to head	0.5	IV
6	Under RVCH	10	V

Table 24D-8. Reactor Vessel Head Inspection Dose

Task No.	Zone	Work Units	I		II		III		IV		V		VI		Total (man-hr)	Collective Dose (person-mSv)
	Dose Rate (mSv/h)		0.01		0.05		0.1		0.2		0.5		10			
	Number of Workers (N) Duration of Operation (h)		N	h	N	h	N	h	N	h	N	h	N	h		
1	**Outer Head Penetrations – Visual**															
1.01	Set up control/monitoring equipment	1	4	8											32	0.320
1.02	Install inspection robot on reactor vessel head	4			1	4									16	0.200
1.03	Perform inspection	4	2	8											64	0.160
1.04	Remove inspection robot	1			1	0.5									0.5	0.025
1.05	Remove control/monitoring equip.	1	4	8											32	0.320
Subtotals															**144.5**	**1.025**
2	**J-Weld Inspections**															
2.01	Set up control/monitoring equipment	1	4	48											192	1.920
2.02	Install inspection equipment in stand	1			3	18									54	2.700
2.03	Perform inspection	1	2	12							2	1			26	1.240
2.04	Remove control/monitoring equip	1	8	24											192	1.920
2.05	Remove inspection equip. from stand	1			4	6									24	1.200
Subtotals															**488**	**8.98**
Totals															**632.5**	**10.0**

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

None.

LIST OF ABBREVIATIONS AND ACRONYMS

ADS	automatic depressurisation system
AOP	abnormal operating procedure
BEIS	Department for Business, Energy & Industrial Strategy
CCA	Civil Contingencies Act
CCI	core/concrete interaction
COMAH	Control of Major Accident Hazards
CSA	control support area
CVS	chemical and volume control system
DAS	diverse actuation system
DBA	design basis accident
EA	Environment Agency
EOP	emergency operating procedure
GLO	government liaison officer
GTA	government technical adviser
HPME	high-pressure melt ejection
HSWA	Health and Safety at Work Act
IAEA	International Atomic Energy Agency
INES	International Nuclear and Radiological Event Scale
IRWST	in-containment refuelling water storage tank
MCR	main control room
NEA	Nuclear Energy Agency
NEPLG	Nuclear Emergency Planning Liaison Group
NIA	Nuclear Installations Act
OECD	Organisation for Economic Co-operation and Development
ONR	Office for Nuclear Regulation
OSC	operations support centre
PCCWST	passive containment cooling water storage tank
PCS	passive containment cooling system
PCSR	Pre-Construction Safety Report
PORV	power-operated relief valve
PSA	probabilistic safety assessment
RCS	reactor coolant system
REPPIR	Radiation (Emergency Preparedness and Public Information) Regulations
RIMNET	radiation incident monitoring network
RNS	normal residual heat removal system
RSR	remote shutdown room
SAP	safety assessment principles
SAMG	Severe Accident Management Guidelines
SCC	strategic coordinating centre
SCG	strategic coordinating group
SG	steam generator
SLC	site licence condition
TSC	technical support centre
UK	United Kingdom

25 ACCIDENT MANAGEMENT

25.1 INTRODUCTION

It is expected that the design of a nuclear facility built in the United Kingdom (UK) will be robust and meet modern international good practices and thus provide adequate protection against low probability potential accidents (Reference 25.1). The AP1000 plant is designed to be operated so that defence in depth against significant faults or failures is achieved by the provision of several layers of protection, as discussed and demonstrated in Chapters 8 through 14.

Accident management provides the final level of defence to ensure that all reasonably practicable steps have been taken to minimise the radiological consequences of any potential accident. Accident management encompasses emergency and abnormal procedures, severe accident management guidelines, and offsite emergency plans. Emergency and abnormal procedures will dictate steps for the operator to take in order to manage and mitigate an unplanned event in preventing any release of radioactivity to the environment. Severe accident management guidelines will detail steps for the plant staff to follow in diagnosing and mitigating challenges to containment fission boundaries, which may otherwise result in a release of radioactivity to the environment. Offsite emergency plans, recognising a high improbability of radioactive releases, provide guidance to the plant staff and offsite civil authorities in order to protect the general public in the event of a release of radioactivity to the environment.

This chapter describes general arrangements and facilities to facilitate the management of accidents currently considered in the AP1000 UK plant design. Any site-specific arrangements will be described in site-specific Pre-Construction Safety Reports (PCSRs).

25.2 FRAMEWORK FOR EMERGENCY MANAGEMENT

Systematic plant and site-specific arrangements must be made for emergency preparedness and response in case of nuclear and radiological incidents (Reference 25.1).

Principle AM.1 of the Office for Nuclear Regulation (ONR) safety assessment principles (SAPs) (Reference 25.1) states:

> Strategies and plans should be in place to prepare for and manage accidents at the facility and/or site.

The siting, design, construction, and operation of the AP1000 plant is subject to the granting of a nuclear site licence by the ONR and compliance with the conditions attached to the licence.

ONR will only permit the operation of a nuclear facility when it has fully satisfied itself that the licensee has made an adequate safety case and developed appropriate safety standards. The safety case identifies instrumentation needed to monitor the state of the plant and the level of severity of an accident, and any equipment to be used to control the accident or mitigate its consequences. Where additional hardware would facilitate accident management, this is also documented within the safety case. The implementation of these standards significantly reduces the chances of an accidental event occurring and resulting in the uncontrolled release of radioactivity.

The responsibilities of the operator when responding to a nuclear emergency, both in relation to protecting the public and to protecting their own workforce, is governed by a number of acts, principally the Health and Safety at Work Act (HSWA) (Reference 25.2), the Nuclear Installations Act (NIA) (Reference 25.3), and the Radiation (Emergency Preparedness and Public Information) Regulations (REPPIR) (Reference 25.4). Other legislation, such as the Fire and Rescue Services Act (Reference 25.5) and the Food and Environment Protection Act (Reference 25.6), governs the response of specific organisations.

The HSWA places a general duty on all responders to do all that is reasonably practicable to reduce risk, while the Ionising Radiations Regulations (Reference 25.7) contain specific requirements for the protection of employees and the public from radiation.

Site licence condition (SLC) 11 (Reference 25.8) under the NIA (Reference 25.3) requires that there shall be “adequate arrangements”, which must be approved by the ONR, for dealing with any accident or emergency arising on site. These “adequate arrangements” are expected to be detailed in the operator’s site-specific emergency plans and associated documentation. The “adequate arrangements” would likely incorporate procedures for dealing with an accident or emergency to ensure that appropriate measures are available for protecting the public and the workforce. Additionally, these arrangements are expected to be capable of covering a wide range of events, from minor incidents restricted to onsite locations to large incidents or emergencies that could result in a significant release of radioactive material to the environment. It is anticipated that the licensee keeps a record of all such incidents, notifies ONR when appropriate, investigates the cause of each incident, and produces a report of the investigation to ensure that lessons are learned.

The licensee of each AP1000 site in the UK will be required to establish arrangements through emergency plans for managing emergencies arising from activities on the site; these plans are to be submitted to and approved by the ONR in accordance with SLC 11. The ability of the operator to implement such plans must be demonstrated to the ONR and rehearsed regularly to satisfy the requirements of the license. The

REPPIR (Reference 25.4) establishes a framework for the protection of workers and the public through emergency preparedness for a radiation emergency and concentrates on requirements of the emergency phase of any accident at a nuclear site. These regulations place a requirement on the licensee (duty holder) and local authorities to ensure that offsite emergency arrangements are in place and rehearsed regularly, setting out the response to be taken in the event of a release of radioactivity that presents a hazardous condition. These duties include, among other things, the need for hazard identification and risk evaluation and the development and testing of offsite emergency plans. The purpose of the offsite plan is to bring together the emergency arrangements of all offsite agencies involved in the response to a radiation emergency occurring at the premises. A radiation emergency is defined as an event likely to result in a member of the public receiving an effective dose of 5 mSv during the year immediately following the emergency.

The Nuclear Emergency Planning Liaison Group (NEPLG) is a forum that brings together, under the Department for Business, Energy & Industrial Strategy (BEIS) chairmanship, a wide range of organisations with interests in offsite planning for an emergency at civil and defence nuclear sites. NEPLG identifies, discusses, and finds solutions to common problems, and facilitates improvements in planning, procedure, and organisation that would form a framework of advice to the emergency planners. It has produced consolidated guidance documentation detailing the response to an emergency at a nuclear site; i.e., the consequence management of the emergency affecting people and the environment. The response arrangements are designed to be put into effect regardless of the nature of the initiating event, whether it is an accident or a terrorist incident. The NEPLG consolidated guidance also identifies the requirements for onsite and offsite emergency response centres (References 25.9, 25.10, 25.11, 25.12, and 25.13).

The NEPLG consolidated guidance will be taken into account by any prospective site licensee to ensure that members of local emergency planning consultative committees and councils are made aware of the guidance.

The International Nuclear and Radiological Event Scale (INES) is a recognised tool for promptly communicating to the public in consistent terms the safety significance of reported nuclear and radiological incidents and accidents, excluding naturally occurring phenomena such as radon. The INES tool is presented in Reference 25.14.

It is not the intention of this section of the PCSR to detail the incidents and/or failure combinations of systems that would require declaration as a site incident or nuclear emergency. The probabilistic safety assessment (PSA) (see PCSR Chapter 10) identifies incidents and failure combinations that would lead to significant offsite releases; however, the specific definitions of site incident and nuclear emergency declarations will be determined within site-specific operating plans and procedures.

The licensee's emergency arrangements require the declaration of either a "site incident" or a "nuclear emergency", depending on the nature of the event, by a duly authorised person.

The definitions of these two declaration states follow:

- **Site incident** – A hazardous condition that is confined in its effect to within the boundary of the site security fence.

- **Nuclear emergency** – A hazardous condition that results, or is likely to result, in the need to consider urgent countermeasures to protect the public outside the site security fence from a radiological hazard.

A site incident may not call for the full implementation of the operator's emergency plan or the alerting of the offsite emergency services. The possibility of a site incident developing into a nuclear emergency is continuously assessed by staff in the main control room (MCR).

A nuclear emergency is likely to call for the full implementation of the site operator's emergency plan. Active countermeasures may include additional offsite radiation and contamination surveys, the restriction of foodstuffs produced close to the site, sheltering, issuing of potassium iodate tablets to people who work or live close to the incident location, and evacuation of areas immediately adjacent to the site. Such countermeasures will depend upon the severity of the accident.

The ability to implement offsite countermeasures should be based on UK and relevant international advice and will be demonstrated in the safety case. Similarly, assumptions that

the onsite effects will be limited by the implementation of accident management and emergency preparedness arrangements would be demonstrated within the site-specific safety case.

25.3 AP1000 PLANT EMERGENCY MANAGEMENT ARRANGEMENTS

This section identifies the generic emergency arrangements and accident management programmes currently included in the AP1000 UK plant design. Any site-specific arrangements will be described in site-specific PCSRs.

The licensee will develop and maintain an accident management programme specific to the site location and environs, AP1000 design, and safety case. Such a programme is intended to take the form of an emergency plan and shall be informed of the aforementioned regulations and guidance in addition to AP1000-specific attributes and defined emergency actions.

In addition, and as integral to these programmes, the licensee will develop and maintain external emergency arrangements and communications with appropriate governmental and regulatory entities for the purpose of facilitating emergency response to site assistance and informing offsite actions.

It is expected that any emergency plan will be informed from many sources both internal and external to the site. The UK AP1000 PSA (see further Chapter 10) provides one source of information from which an accident management programme can be informed. The fault and accident analysis provides another source of information. These studies highlight the importance of actions as significant responses to a set of design basis accidents (DBAs).

Additionally, the licensee will develop and implement severe accident management guidance using the suggested framework provided in the Framework for AP1000 Severe Accident Management Guidance, (Reference 25.15) and the Executive Volume For AP1000 Severe Accident Management Guidelines (Reference 25.16). The site-specific licence application will consider any differences between the as-built plant and the AP1000 certified design. Any significant impact on the safety case will be determined and evaluated.

If a severe accident occurs, actions to terminate fission product release have been predefined in Reference 25.15 and Reference 25.16. These actions will be incorporated into the accident management programme as it is developed. Table 25-1 provides a link between a desired plant outcome – e.g., a controlled stable core – and the high-level actions required to achieve this. This is supported by Table 25-2, which identifies the strategies for severe accident management and the equipment required.

To further development of the emergency arrangements for the AP1000 plant, such planning will likely include actions for increased environmental monitoring following a major accident and release of radionuclides. Such actions are intended to address surveys of soils and agricultural products as may be required or prudent. Contingency plans will also be developed and integrated with the environmental monitoring programme (Reference 25.17).

25.4 ONSITE EMERGENCY RESPONSE FACILITIES

The operator of any UK AP1000 facility, as a result of the SLCs and/or REPPIR regulations, will address the site response to emergency conditions through both operations emergency procedures (abnormal operating procedures (AOPs), emergency operating procedures (EOPs), and Severe Accident Management Guidelines (SAMGs); see Chapter 13) and coordinated onsite response arrangements and actions. These onsite emergency management actions will be integrated with offsite support organisations, including representation at the

strategic coordination centre and the communications interfaces among plants, public, and external agencies.

In support of the onsite emergency management response arrangements, the UK AP1000 operator will plan for and have available emergency response facilities to coordinate and manage site actions. These facilities are broadly classified as having the following functions:

- Direct accident management and plant recovery control through resources located in the MCR, remote shutdown room (RSR), or at the south auxiliary building diverse actuation system (DAS) panel.

- Incident or emergency technical support through the technical support centre (TSC), including accident management, engineering, and external communications roles.

- Operational support through the operations support centre (OSC), including plant logistical support and offsite radiological monitoring coordination roles.

The MCR provides an engineered protected environment from which operators can safely monitor and control plant processes. The major tasks performed in the control room include monitoring, supervising, managing, and controlling those aspects of the plant processes related to thermodynamic and energy conversion processes under normal, abnormal, and emergency conditions. The principal emergency response function of the MCR is to provide human interface resources that determine the plant state and implement the desired changes to the plant state during normal and emergency operations.

The MCR provides alarms and other information to alert the operator to the need for further investigation. Plant process data displays permit the operator to observe abnormal conditions and define the plant state with suitable controls, enabling the operator to execute plant control and recovery actions. The process data displays and the alarms also provide feedback to enable the operator to observe the effects of the control actions.

Operators in the MCR are also provided with information via the equipment monitoring functions (see Table 25-3) to monitor radiation levels and radioactivity in the environment surrounding the plant and to monitor the habitability of the MCR. From the MCR, staff can monitor plant areas where access may be required to service equipment (necessary to monitor or mitigate the consequences of an accident and estimate the magnitude of the release of radioactive material through identified pathways) and continually assess radioactive releases. Table 25-3 summarises the functions monitored in the MCR that allow the operator to mitigate the consequences of an accident.

The MCR is a controlled environment with habitability systems capable of keeping the environment suitable for prolonged occupancy of up to 11 persons throughout the duration of the postulated accidents. The habitability systems provide the capability to detect and protect MCR personnel from external fire, smoke, and airborne radioactivity. Automatic actuation of the individual systems that perform a habitability systems function is provided. Smoke detectors, radiation detectors, and associated control equipment are installed at various plant locations as necessary to provide the appropriate operation of the systems. In the unlikely event that the normal power source or the heating, ventilation, and air conditioning system becomes unavailable, there are passive systems (batteries, compressed air) to support the MCR for up to 3 days.

Additional information about the MCR and its supporting habitability systems are provided in Chapters 6, 9, and 23.

An additional remote operations emergency response facility is also provided within the adjoining RSR. The RSR is physically and electrically separated from the MCR. In the unlikely event of MCR evacuation, safe shutdown conditions may be established and maintained by the plant operators using the remote shutdown workstation in the RSR. This remote shutdown workstation contains indications and controls that allow an operator to achieve and maintain safe shutdown of the plant following an event when the MCR is unavailable.

As a final level of direct accident management and plant recovery control emergency response facilities, a remote DAS workstation is located in the south side of the auxiliary building. This panel can be used to shut down the reactor, and provides capability for manual actuation of key safety features. The DAS panel is located in the south side of the auxiliary building while both the MCR and RSR are on different levels of the north side of the auxiliary building.

The DAS is described further in Chapter 19.

The MCR, RSR, and the remote DAS workstation are designed in accordance with human factors engineering principles and practices.

Two additional onsite support facilities are designated as part of the emergency response function. Operation of both these facilities is designed to provide additional resources in support of the MCR accident management and recovery responses.

The TSC provides an area and resource for use by personnel providing plant management and technical support to operating staff during an emergency. Activation of this facility relieves the reactor operators of peripheral duties and communications not directly related to accident management operations and prevents congestion in the MCR. The TSC is located in the control support area (CSA) of the annex building. The TSC is shielded and operated at a slight positive pressure with atmospheric filtration. Should habitability be challenged within the TSC due to a lack of cooling or a high radiation level following an accident, the plant management function of the TSC is transferred to the MCR or OSC.

The TSC can accommodate a minimum of 25 people with a floor space of at least 6.97 m^2 (75 ft^2) per person and has voice communication equipment for communication with the MCR, the OSC, and external agencies.

An additional facility, the OSC, is an onsite emergency response facility available to provide a centralised habitable area for operations support personnel and resources. Like the TSC, the OSC is designed to relieve operators of peripheral duties and eliminate personnel congestion in the MCR. OSC managers are responsible for coordinating the assignment of duties and tasks to personnel outside the MCR and TSC in support of plant emergency management operations. These duties may typically involve tasks such as offsite radiation monitoring or sampling, onsite repairs to faulted equipment, or performance of manual valve line-ups. The OSC also provides resources for communicating with the MCR and TSC. This permits the personnel reporting to the OSC to be assigned emergency operations support responsibilities.

It is possible that the TSC and OSC resources could be shared between more than one AP1000 unit on the same site, however, this will be a site-specific issue and will be determined as part of the application for a site-specific licence. The appropriate location, design, and specification of the OSC will be determined as part of the application for the site-specific licence and therefore is not discussed any further within this chapter.

The operator of any UK AP1000 facility, as a result of the SLCs, will be responsible for designing the emergency operations facility, including the specification of the location and communication with the facility in accordance with the AP1000 human factors engineering programme.

25.5 CONCLUSION

This chapter identifies the UK requirements for emergency response to a nuclear incident and emergency. It also identifies the provisions available in the current AP1000 UK plant design to respond to a nuclear incident or an emergency as well as identifying the requirements for contingency plans that will be fully integrated with the environmental monitoring programme. This chapter also confirms that the AP1000 UK plant design facilitates the management of an incident or emergency by the provision of the MCR, TSC, and OSC.

25.6 REFERENCES

25.1 Office for Nuclear Regulation, "Safety Assessment Principles for Nuclear Facilities," Rev. 0, 2014.

25.2 UK Public General Act No. 37, "Health and Safety at Work Act," 1974.

25.3 UK Public General Act No. 57, "Nuclear Installations Act," 1965.

25.4 UK Statutory Instrument No. 2975, "The Radiation (Emergency Preparedness and Public Information) Regulations," 2001.

25.5 UK Public General Act No. 21, "Fire and Rescue Services Act," 2004.

25.6 UK Public General Act No. 48, "Food and Environment Protection Act," 1985.

25.7 UK Statutory Instrument No. 3232, "Ionising Radiations Regulations," 1999

25.8 Office for Nuclear Regulation, "Licence condition handbook", January 2016.

25.9 UK Department for Business, Energy & Industrial Strategy, "Nuclear Emergency Planning and Response Guidance – Preparedness", October 2015.

25.10 UK Department for Business, Energy & Industrial Strategy, "Nuclear Emergency Planning and Response Guidance – Response", October 2015.

25.11 UK Department for Business, Energy & Industrial Strategy, "Nuclear Emergency Planning and Response Guidance – Recovery", October 2015.

25.12 UK Department for Business, Energy & Industrial Strategy, "Nuclear Emergency Planning and Response Guidance – Concept of Operations, October 2015.

25.13 UK Department for Business, Energy & Industrial Strategy, "Nuclear Emergency Planning and Response Guidance – Annexes", October 2015.

25.14 International Atomic Energy Agency, "INES, The international nuclear and radiological event scale", Information Series / Division of Public Information, 08-26941 / E

25.15 Westinghouse Report APP-GW-GL-027, Rev. 0, "Framework for AP1000 Severe Accident Management Guidance," April 2006.

25.16 Westinghouse Report APP-GW-GJP-500, Rev. 0, "Executive Volume For AP1000 Severe Accident Management Guidelines", March 2016.

25.17 Westinghouse Report UKP-GW-GL-790, Rev. 6, "UK AP1000 Environment Report", January 2017.

Table 25-1. AP1000 High-Level Action Relative to Severe Accident Goals (Reference 25.15, Table 5-1)

Goal	Element	High-Level Action
Controlled, stable core	Water inventory in reactor coolant system (RCS)	Inject into RCS Depressurise RCS
	Water inventory in containment	Inject into containment
	Heat transfer to steam generators (SGs)	Inject into RCS Inject into SGs Depressurise SGs
	Heat transfer to containment	Inject into RCS Inject into containment Depressurise RCS
Controlled, stable containment	Heat transfer from containment	Depressurise containment Vent containment
	Isolation of containment	Inject into SGs Depressurise RCS
	Hydrogen prevention/control	Vent containment Pressurise containment Burn hydrogen Depressurise RCS Inject into containment
	Core/concrete interaction (CCI) prevention	Inject into containment Depressurise RCS
	High-pressure melt ejection (HPME) prevention	Inject into containment Depressurise RCS
	Creep rupture prevention	Depressurise RCS Inject into SGs Inject into containment
	Containment vacuum prevention	Do not vent containment Pressurise containment
Terminate fission product releases	Isolation of containment	Inject into SGs Depressurise RCS
	Reduce fission product inventory	Inject into containment Depressurise RCS Depressurise containment
	Reduce fission product driving force	Depressurise containment

Table 25-2. Summary of High-Level Severe Accident Management Strategies for AP1000 UK Plant (Reference 25.15, Table 5-2)

Action	Purpose (Positive Impact)	Other Considerations (Negative Impacts)	Equipment
Depressurise containment	Remove decay heat from containment Prevent overpressurisation Mitigate containment fission product leakage Alleviate equipment and instrumentation challenges due to harsh conditions Increase containment water inventory	Hydrogen flammability Containment vacuum of venting Fission product release if venting	Passive containment cooling system (PCS) with water from passive containment cooling water storage tank (PCCWST) or other source Fan coolers Containment vent through normal residual heat removal system (RNS) to spent fuel pit
Pressurise containment	Create inert atmosphere so that hydrogen cannot burn Prevent containment vacuum from failing containment structure	Removal of hydrogen will eventually be needed More oxygen for hydrogen to burn Possible failure to isolate pathway used for pressurisation	Containment heat sinks Fan coolers Automatic depressurisation system (ADS) valves Instrument air
Intentionally burn hydrogen	Let hydrogen burn while containment failure is not a risk to prevent future containment challenge	Pressure and temperature spike	Hydrogen igniters including alternate power source
Vent containment	Avoid containment failure due to overpressurisation Hydrogen burn	Radiological releases Potential future concerns with containment failing from subatmospheric loads No guarantee that vent pathway will be able to reclose	RNS suction line from RCS to spent fuel pool (with ADS valves or other openings between RCS and containment)

Table 25-2. Summary of High-Level Severe Accident Management Strategies for AP1000 UK Plant (Reference 25.15, Table 5-2) (cont.)

Action	Purpose (Positive Impact)	Other Considerations (Negative Impacts)	Equipment
Mitigate fission product release	Reduce release for fission products to atmosphere	Hydrogen burn Containment flooding Hydrogen build-up in lower compartments	Containment fan coolers Containment spray SG water inventory RCS ADS valves Containment isolation Flood containment
Inject into RCS	Restore core cooling (immediate and long term) Scrub fission products Prevent or delay vessel failure	Creation of hydrogen Creep rupture of SG tubes	Core makeup tank Accumulators In-containment refuelling water storage tank (IRWST) RNS Chemical and volume control system (CVS)
Inject into containment	Create inventory in sump for recirculation Submerge lower head of RPV to prevent failure Cool core debris Prevent limit CCI Prevent basemat melt through Reduce flammable gas production Prevent HPME Reduce fission product inventory	Ex-vessel steam explosions Hydrogen generation	Gravity drain of IRWST RNS injection of cask loading pit Spent fuel system injection into refuelling cavity
Inject into SGs	Heat sink Cover SG tubes to prevent creep rupture Scrub fission products Make SGs available to depressurise	Thermal shock of SG tubes Fission product release from leaking tubes Creep rupture of SG tubes (if SG is first depressurised, creating large pressure differential)	High pressure: Main feedwater Startup feedwater Low pressure: Condensate Firewater Service water

Table 25-2. Summary of High-Level Severe Accident Management Strategies for AP1000 UK Plant (Reference 25.15, Table 5-2) (cont.)

Action	Purpose (Positive Impact)	Other Considerations (Negative Impacts)	Equipment
Depressurise RCS	Facilitate injection into RCS Establish long-term heat transfer path Prevent HPME Prevent creep rupture Isolate containment due to SG tube leaks Long-term hydrogen control Reduce fission product inventory	Short term hydrogen release and burn Containment pressurisation	ADS Auxiliary pressuriser spray Head vent CVS letdown SG cooling
Depressurise SGs	Facilitate injection into SGs Create heat transfer with RCS Depressurise RCS	Loss of SG inventory SG fission product release Creep rupture of SG if large differential pressure is created	SG power-operated relief valve (PORV) Steam dump

Table 25-3. Summary of Functions Monitored in the MCR to Mitigate the Consequences of an Accident (Type E Variables)

Function Monitored	Variable
Containment radiation	Containment area high-range radiation level
Area radiation	CSA radiation level
	Primary sampling station area radiation level
Airborne radioactivity released from plant	Turbine island vent discharge radiation level
	Plant vent radiation level
	Plant vent air flow
	Main steam line radiation level
	Boundary environs radiation
	MCR supply air radiation level
Environs radiation and radioactivity	Site specific
Meteorology	Site specific
Accident sampling	Primary coolant
	Containment air
MCR filtration flow	MCR passive filtration induced flow rate

TABLE OF CONTENTS

TABLE OF CONTENTS (cont.)

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS AND ACRONYMS

ALARP	as low as reasonably practicable
ANP	advanced nuclear plant
AOOs	anticipated operational occurrences
BAT	best available technique
BDS	steam generator blowdown system
BRIMS	British Radwaste Information Management System
BS	British Standard
CCTV	closed-circuit television
CEC	cavity enclosure container
CPS	condensate polishing system
CVS	chemical and volume control system
CWS	circulating water system
DF	decontamination factor
EA	Environment Agency
EPRI	Electric Power Research Institute
FWS	feedwater system (main and startup)
GALE	gaseous and liquid effluents computer programme
GDA	generic design assessment
GDF	geological disposal facility
GNS	Gesellschaft für Nuklear-Service mbH
HAZOP	hazard and operability studies
HEPA	high-efficiency particulate air
HHISO	half-height ISO (containers)
HI-STORM	Holtec International dry storage cask system for spent fuels
HI-TRAC	Holtec International transfer cask or shuttle cask for HI-STORM
HLW	high-level waste
HRGS	high-resolution gamma spectrometer
HVAC	heating, ventilation, and air conditioning
ILW	intermediate-level waste
IMS	integrated management system
ISO	International Organisation for Standardisation
IWS	integrated waste strategy
LFE	learning from experience
LLW	low-level waste
LLWR	low-level waste repository
LoC	letter of compliance
LRGS	low-resolution gamma spectrometer
MCR	main control room
MEU	mobile encapsulation plant
MPC	multipurpose canister
NDA	Nuclear Decommissioning Authority
NRC	Nuclear Regulatory Commission
ONR	Office for Nuclear Regulation
PCSR	Pre-Construction Safety Report
PSS	primary sampling system
PWR	pressurised water reactor
PXS	passive core cooling system
QA	quality assurance
RCA	radiologically controlled area
RCDT	reactor coolant drain tank
RCS	reactor coolant system

LIST OF ABBREVIATIONS AND ACRONYMS (cont.)

RF	release fraction
RNS	normal residual heat removal system
RPVH	reactor pressure vessel head
RWMC	radioactive waste management case
RWM	Radioactive Waste Management
RXS	reactor system
SCV	secondary containment vessel
SFS	spent fuel pool cooling system
SG	steam generator
SGS	steam generator system
SKB	Svensk Kärnbränslehantering AB (Swedish Nuclear Fuel and Waste Management Company)
SSC	system, structure, or component
UK	United Kingdom
US	United States
VAS	radiologically controlled area ventilation system
VFS	containment air filtration system
VHS	health physics and hot machine shop ventilation system
VLLW	very low-level waste
VLS	containment hydrogen control system
VRS	radwaste building HVAC system
VTS	turbine building ventilation system
VVM	vertical ventilated module
WGS	gaseous radwaste system
WLS	liquid radwaste system
WRS	radioactive waste drain system
WSS	solid radwaste system
ZIRLO™	zirconium alloy

26 RADIOACTIVE WASTE MANAGEMENT

26.1 INTRODUCTION

The management of radioactive waste, which may be gaseous, liquid, or solid, from operational and decommissioning phases, spans all the stages in the life cycle of the AP1000 design.

A safety case for radioactive waste management should consider not only generation and immediate management or treatment, but also longer-term storage and ultimate disposal. It must also address longer-term safety and environmental issues associated with a particular waste stream (e.g., safety during onsite storage pending final offsite disposal). The aim is to demonstrate that treatment of the AP1000 plant radwaste can be undertaken safely and does not pose a significant risk either to workers or to members of the general public. Please note that for completeness, non-radioactive waste is also addressed in a number of sections below.

This chapter of the Pre-Construction Safety Report (PCSR) is part of the generic design assessment (GDA) for the AP1000 design. This GDA precedes the assessment that will be put forward by potential operators for an installation at a specific site. In some parts of the chapter, especially those related to the management of solid radwaste, the design described is specific to the GDA; the operator may propose a different radwaste strategy.

This chapter considers in turn the gaseous, liquid and solid waste streams. It describes how the proposed reactor design and operation minimise the generation of radioactive waste. It also describes how each type of waste is handled at the reactor site, using the best available techniques (BAT) to minimise current and future impacts, and considers the disposability of the solid radioactive waste. The waste systems are described in further detail in Chapter 6. The chapter builds upon and references many underlying documents. In particular it draws on the Environment Report (Ref. 26.1), the integrated waste strategy (IWS) (Ref. 26.2), the radioactive waste management case (RWMC) evidence reports for intermediate-level waste (ILW) (Ref. 26.3) and high-level waste (HLW) (Ref. 26.4), and the AP1000 Nuclear Power Plant BAT Assessment (Ref. 26.5).

Issues related specifically to decommissioning are handled in Chapter 27. Many of the issues related to operation are described in detail in the Environment Report (Ref. 26.1). Normal discharges to air and water and proposed discharge limits are summarised in Section 26.5 below and detailed in the Environment Report.

Achieving the optimum balance between corrosion, mechanical performance under irradiation, and the generation of activation products such as Co-60 and Ni-63 in radioactive waste is a complex issue that spans several technical areas. For example, the behaviour of activated corrosion products in the primary circuit (and hence the activity in the ion exchange resins and also in the oxide films of out-of-neutron-flux primary circuit components) depends on the primary circuit chemistry, which is covered in Chapter 21. It also depends on the corrosion properties of materials used in the circuit and in the fuel assemblies (Chapters 15 to 23), while the elemental and isotopic composition of the materials used affect the rates at which activation products are generated under neutron irradiation.

This chapter demonstrates that the wastes arising from the proposed generic design and management of the AP1000 design pose no unacceptable risks.

This chapter starts with a summary of the AP1000 design waste management facilities, and then outlines the radioactive waste management strategy. Some general information on discharges to air and water is followed by detailed descriptions (Sections 26.6, 26.7, and 26.8) of the systems for processing gaseous, liquid and solid wastes, including their discharge or disposability. Having described the systems, their responses to external and internal hazards are collated in Section 26.9. A brief description of record-keeping is followed by some overall conclusions.

26.2 SUMMARY OF AP1000 DESIGN WASTE MANAGEMENT FACILITIES

The generic AP1000 design site contains the following groups of buildings (Ref. 26.2, Section 2.1).

26.2.1 Nuclear Island

The nuclear island comprises the reactor containment vessel, the concrete shield building that surrounds the containment vessel, and the auxiliary building. The auxiliary building contains mechanical and electrical equipment plus the main control room, handling areas for fresh fuel, spent fuel, liquid and gaseous radwaste, and main steam and feedwater isolation valve compartments, and the rail car bay where the mobile encapsulation unit (MEU) will be placed during treatment of ILW.

26.2.2 Non-Nuclear Island

The non-nuclear island comprises the following:

- The annex building, including the main personnel entrance, the health physics area, ancillary diesel generators and fuel supply, technical support centre, and various heating, ventilation, and air conditioning (HVAC) systems

- The turbine building, housing the main steam turbine, the generator, and the makeup water purification system

- The diesel generator building, housing two diesel generators and their associated HVAC equipment

- The radwaste building incorporates the GDA facilities necessary to handle the solid low-level waste (LLW) arisings from AP1000 plant operations and maintenance. This includes equipment for treating, packaging, and assaying LLW and for clearing very low-level waste (VLLW). The radwaste building also includes the holdup and monitoring tanks that are part of the liquid waste system, devices for waste monitoring and radiological characterisation, and three truck bays wherein mobile waste-handling equipment may be parked and connected.

Figure 26-1 shows the buildings of the nuclear and non-nuclear islands.

26.2.3 Waste Storage Facilities

The waste storage facilities are not shown in Figure 26-1. They are not part of the standard plant and will be selected by the operator. For the GDA cast, they include the following:

- A dry-storage system for spent fuel (which is the only HLW produced by the AP1000 design). This could be used to retain spent fuel after the AP1000 plant is decommissioned. The United Kingdom (UK) Nuclear Decommissioning Authority (NDA) is currently investigating the credible options for dealing with spent fuel (Ref. 26.6).

- An ILW store. The first phase of the store would accommodate the arisings expected from the first 20 years of operation; subsequent extensions would accommodate further 20-year increments. The ILW store could be used to retain ILW after the AP1000 plant is decommissioned. The NDA is currently exploring options for managing ILW (Ref. 26.7).

- The LLW buffer store, designed for half-height International Organisation for Standardisation [1] (HHISO) containers that have been filled in the radwaste building. In the event that the national LLW repository (LLWR) is temporarily unable to accept disposals, the combined capacity for HHISO containers in the buffer store and the radwaste building can accommodate up to 2 years' arisings of LLW, including arisings from possible abnormal events. Note that the HHISO containers stored within the radwaste building are those being filled. No full HHISO containers will be stored in the radwaste building.

26.3 STATEMENT OF THE SAFETY CASE

Before considering the detailed strategy and operations, it is helpful to consider the preliminary safety statement. The summary in this section has been taken from the UK AP1000 Radwaste Preliminary Safety Statement[2] (Ref. 26.8, Sections 8 and 9). Although the full set of risks to be considered include both the longer-term risks posed by the radioactive wastes and discharges as well as the immediate risks that arise from operating the radioactive waste management facilities, this section concentrates on the immediate risks. The longer-term risks are covered in more detail by the sections dealing with disposability, particularly Section 26.8.6.

The following sections present a summary of the acceptability of the treatment of AP1000 plant radwaste by comparison with appropriate safety criteria.

---

1. Formally International Organisation for Standardisation (ISO); these containers are universally known as ISO containers.
2. The hazard and operability study (HAZOP) 1 study report (Ref 26.46) and the Preliminary Safety Statement (Ref 26.8) were performed on a preliminary design of the waste processing equipment in the radwaste building. Since these reviews took place, a number of design improvements have been made to the radwaste building. These design improvements have had the effect of improving the safety within the radwaste buildings and therefore the conclusions from these reviews are still valid for conservative purposes of GDA. However, they will need to be readdressed at the site-specific stage.

26.3.1 Normal Operations

26.3.1.1 Compliance with Criteria (Normal Operations)

It is expected that the operations for the treatment of AP1000 plant radwaste will not result in a significant dose uptake to operators. The radiation levels within the auxiliary building where radwaste processing will take place and the ILW store are expected to be low, on the order of 0.5 μSv/hr (0.05 mrem/hr) or less.

The estimated dose rate for the radwaste building is 2.5 to 7.5 μSv/hr (0.25 to 0.75 mrem/hr). The estimated contact dose rate for the MEU is 1 μSv/hr (0.1 mrem/hr) (Ref. 26.9, Section 3.9.2.3). The contact dose rate of the ILW store external wall is designed to be 0.5 μSv/hr (0.05mrem/hr).

The expected dose uptake during normal operations will be confirmed upon completion of the dose budget assessment. Compliance with normal operations criteria cannot be confirmed until these are available. The detailed plan for showing compliance with normal operation criteria will be part of site licensing.

26.3.1.2 As Low As Reasonably Practicable Demonstration (Normal Operations)

The following measures will be implemented to ensure that the predicted dose uptake to operators and members of the public is as low as reasonably practicable (ALARP):

- The MEU will provide shielding and will be operated remotely to minimise the potential operator dose uptake during encapsulation operations.
- The MEU, overpack, and ILW store will all be provided with interlocks to ensure that appropriate shielding is in place during package import/export operations.
- HVAC systems will be provided for the auxiliary building, radwaste treatment facility, the mobile encapsulation plant, and the ILW store to minimise the potential for inhalation of airborne contamination.
- Operations within the facilities will be undertaken in accordance with approved procedures, which will identify any specific precautions required during the operations to minimise the dose uptake.
- Awareness of potential hazards by administrative, operational and supervisory staff will be a first line of defence against unnecessary radiation exposure and will be ensured through appropriate training of staff.
- Analysis of abnormal behaviour and incidents on the plant will be undertaken to anticipate and prevent hazards and to confirm that the reliability of plant items is acceptable.
- If any equipment, component or system failure is revealed, the risk of undertaking a repair compared with its remaining in the failed state will be assessed and a decision will then be made on whether or not the failure requires immediate repair.
- Detection systems will be employed within the auxiliary building, radwaste building and ILW store to alert operators to high dose rates so that the operators can undertake immediate evacuation before any significant dose uptake occurs.

26.3.2 Accident Conditions

26.3.2.1 Compliance with Criteria (Accident Conditions)

A detailed hazard identification process was undertaken in support of the treatment of AP1000 plant radwaste and is presented in Chapter 9. The hazard identification process identified numerous fault sequences associated with the treatment of AP1000 plant radwaste. Owing to the preliminary nature of the design of the solid radwaste treatment, a deterministic assessment rather than a probabilistic safety assessment was used to assess the hazards.

All of the identified fault sequences had adequate safeguards.

26.3.2.2 As Low As Reasonably Practicable (Accident Conditions)

The hazard assessment and the fault schedule presented in Chapter 9 give an assessment of the safeguard provision against all credible design basis hazards for the treatment of AP1000 plant radwaste. However, one area that the hazard assessment and fault schedule do not address is the space in which the radwaste operations are to take place.

Part of the reason that this has not been assessed to date is that systems related to solid radwaste management, for example, for treatment, storage, and transportation, could be shared at the utilities option. This is already the case for several existing pressurised water reactors (PWRs). Better utilisation of space could be implemented by dedicating each of the multiple radwaste buildings to treating specific types of waste generated across the site. For example, one radwaste building could include equipment to treat site compactable waste, another to package site metallic waste, and so forth. Alternatively, a separate building could be constructed for treating site solid radwaste. Also, sharing of facilities would allow for operating experience (for example, the same workers) to be shared across the AP1000 plants on a site.

As a result, it has been determined that it would be most appropriate to address the hazard of space available for the radwaste treatment and processing operations, ensuring that ALARP criteria are implemented during detailed design, once the utility has decided upon its preferred method. The UK regulators have agreed with this approach.

It is therefore considered that the risks associated with the treatment of AP1000 plant radwaste have been reduced to ALARP criteria so far as is reasonable to date and will be considered further during detailed design.

26.3.2.3 Methodology Review

The methods to be employed in the treatment of radwaste arising from the AP1000 plant need to be in accordance with current standards, and the methodology needs to be in accordance with best practices in the nuclear industry.

The preliminary safety statement for solid radwaste treatment was developed using up-to-date standard techniques, including a comprehensive hazard identification study in the form of a hazard and operability studies (HAZOP). This was subsequently developed into a thorough hazard listing, and the accident scenarios of significance were carried forward into a fault schedule, where they were quantified.

Each fault in the fault schedule was compared with nuclear industry approved benchmark criteria, which were derived from the accident dose criteria appropriate to the preliminary safety statement. Any shortfalls were considered by the ALARP assessment.

Applying ALARP to reduce normal operation doses and accident risks to as low as reasonably practicable is in line with the most recent current standard industry guidance.

The safety statement in the Radwaste Preliminary Safety Report (Ref. 26.8) demonstrated, in line with current standards, the following:

- There would be sufficient control at all times of hazards.
- All reasonable steps would be taken to eliminate or mitigate hazards, irrespective of time-at-risk arguments.
- Contingency plans had been developed to deal with fault conditions should they deteriorate further.

These methods, used to produce the safety statement, are considered to be in accordance with current standards (Ref. 26.8, Section 8).

26.4 RADIOACTIVE WASTE MANAGEMENT STRATEGY

This section provides a brief overview of the purpose and content of the IWS. To save later repetition, the section includes comments on generation, minimisation and accumulation that relate to all three types of waste (gas, liquid, and solid).

26.4.1 Purpose and Future Development of the Integrated Waste Strategy

The IWS described in Reference 26.2 is compatible with both government policy and with the other strategies for the site. The strategic aim is to reduce the risks and environmental impact arising from AP1000 plant operations by minimising the amount of waste produced and accumulated, and ensuring that radioactive waste is put into a passively safe state. The IWS considers both radioactive and nonradioactive waste.

The IWS is based on the expected waste and spent fuel generation and management practices throughout the operation and decommissioning of an AP1000 plant. It builds on the Environment Report (Ref. 26.1), which lists all the radioactive and nonradioactive wastes that are expected to arise during operation and decommissioning, as well as the datasheets for radioactive waste (Ref. 26.10), calculations of the quantities of waste arisings (Ref. 26.11) and the outline of radioactive waste management and disposal (Ref. 26.9). The IWS applies to the generic site and is to be used in the GDA; it identifies the strategic issues relating to waste management and guides the development of waste management plans. During further site-specific analysis, the utility operator of an AP1000 power plant may develop its own strategy, which would change or replace the submitted IWS. This would for example include construction wastes, which are not included in the current IWS.

The IWS feeds into the integrated management system (IMS) for the facility. The IMS, which covers all activities on the site and not just waste management, will include environmental and safety management features and will be accredited to the UK implementation of international standards such as ISO 9001 and ISO 14001. Further details of the requirement for integration of the IWS into an IMS are provided in the AP1000 Integrated Waste Strategy (Ref. 26.2, Section 3.4).

26.4.2 Overview of the Integrated Waste Strategy

The purpose of this section is to demonstrate that the IWS contains all the appropriate information. The various waste management systems are described more fully in the later sections of this chapter.

- The IWS (Ref. 26.2, Section 2.1) includes a description of the generic AP1000 design site.

- The key waste facilities for operation, namely the liquid radwaste system (WLS), gaseous radwaste system (WGS), and solid radwaste system (WSS) are described in the IWS (Ref. 26.2, Section 2.2). The same section of the IWS also includes a description of the management and facilities for spent fuel and a description of the system to control the chemistry and volume of the reactor coolant.

- The high-level objectives for a specific AP1000 design site will be developed by the utility operators. Typically they will address the minimisation of operational hazards from all site operations, the safe and cost effective storage, handling, and treatment of wastes from all aspects of plant operation, and the eventual delicensing of the site following decommissioning and remediation (Ref. 26.2, Section 2.2.11).

- The assumed final end point for a nuclear site (Ref. 26.2, Section 2.2.10) is that the reactor and associated facilities will be decommissioned and dismantled, and the site at least restored to a standard that is suitable for final end use. The spent fuel and ILW storage facilities could be retained until the national HLW and ILW repositories become available, but once the spent fuel and ILW had been transferred to the national repository the onsite storage facilities would be decommissioned and dismantled. The final site end point demonstrated achievable in Chapter 27.4.2 is a fully cleared site suitable for delicensing.

- Waste management policy, including references to UK government waste management policies for England, Scotland, and Wales and Legislative Requirements and Regulatory Expectations, is covered in the IWS (Ref. 26.2, Section 3). Section 3.1.1 presents the proposed waste management hierarchy. The principles (avoidance, minimisation, reducing/recycling, and abatement) that underpin the IWS for the AP1000 design are consistent with UK waste management policy. Figure 3-3 from this section is reproduced as Figure 26-2; it shows the nuclear BAT management factors for optimisation of waste releases.

- An IMS builds on the IWS and can be fully developed only for a specific site (Ref. 26.2, Section 3.3). The IMS will be developed according to the features of the waste management organisation. It will incorporate environmental and safety management features and will identify any research and technology requirements relating to waste management.

- The IWS (Ref. 26.2, Section 4) describes how the strategy was formulated. The section includes the methodology for the strategic options study (Ref. 26.2, Section 4.2): i.e., how options were selected (via dialogue with prospective site licencees, in order to capture the benefits of their experience in operating similar plants). Joint environmental and safety assessments were used to achieve an overall balance between environmental and safety matters. Table 26-1 lists various assumptions and exclusions. The site end point will be site-specific and may be subject to future consultation and the requirements of future UK government policy, but Section 4.5 presents a set of generic working

assumptions. Section 4.7 covers the stakeholder engagement process that is based on independence, transparency, openness, clarity, and accessibility.

- The overview of site waste strategy, which includes a timeline showing what will happen and when, is provided in the IWS (Ref. 26.2, Section 5). The Environment Report (Ref. 26.1, Figures 3.5-1 and 3.5-2) (reproduced in this chapter as Figure 26-3 and Figure 26-4) provides an overview of the AP1000 design solid waste management strategy. The approach is flexible: for example, interim storage facilities for LLW (Refs. 26.12 and 26.13) have been designed to accommodate two years of LLW arisings, in case the route to the LLWR is temporarily unavailable. The gaseous and liquid radwaste systems are shown in Figure 26-5 and Figure 26-6.

- The IWS itself constitutes Section 6 (Ref. 26.2). This includes information that can be used by the utilities to construct RWMCs: details of strategies for managing nonradioactive solid, liquid and gaseous wastes; descriptions of strategies for managing radioactive liquid and gaseous wastes, solid LLW, ILW, and spent fuel; and a description of the strategy for decommissioning waste. In addition, Evidence Reports for RWMCs have been prepared to cover ILW (Ref. 26.3) and HLW (Ref. 26.4). These reports will develop as the design moves into the site-specific phase and will continue to be enhanced throughout the operational lifetime of the new build plant and beyond.

26.4.3 Waste Generation

The Westinghouse waste management plan comprises the systematic identification of the solid waste and gaseous and liquid discharges generated over the operational and decommissioning period of the AP1000 plant (Ref. 26.1, Chapter 3). So far, solid waste inventory estimates have been developed based on operational experience with existing plants. This ensures that the strategy is realistic and is able to cope with the activities and volumes of waste that are expected to be generated (Ref. 26.1, Chapter 3). The annual releases of radioactive air emissions and effluents are based on proprietary calculations determined from the revised gaseous and liquid effluents computer programme (GALE) code (Ref. 26.1, Chapter 3).

Specific information on the generation of gaseous, liquid and solid wastes is included below, in Sections 26.6, 26.7, and 26.8, respectively.

26.4.4 Minimisation of Wastes at Source

During its operating life and decommissioning, an AP1000 reactor will generate solid waste, liquid discharges, and gaseous emissions. Minimising the amount of waste produced at source has two significant safety benefits:

- The final quantity of waste will be reduced, hence reducing the consequences of operating the AP1000 reactor.

- The reduced quantity of waste implies less waste-processing, which reduces operator dose and hence improves safety.

To assist in understanding the waste minimisation procedures used in the AP1000 facility, Westinghouse has produced the UK AP1000 Environment Report (Ref. 26.1) and the AP1000 Nuclear Power Plant BAT Assessment (Ref. 26.5). These documents explain how the quantity and activity of radioactive waste, and its accumulation on the site, are minimised.

Since the start of the AP1000 design process Westinghouse has considered safety, environmental protection and waste minimisation, through concepts comparable to the UK regulatory principles of ALARP, BAT, and the waste management hierarchy, including waste minimisation at source. Efforts were made to gather information from other similar designs, processes and facilities, along with the experience of station operators (Ref. 26.9, Section 2.2.3). This learning from experience (LFE) concept can be found in the Radwaste Treatment Options Study Report (Ref. 26.14, Appendix 3). The Environment Report (Ref. 26.1, Sections 2.3 and 3.5.4) consolidates and summarises the development, layout, and design features of the AP1000 plant, incorporating minimisation and abatement techniques employed for radioactive and nonradioactive wastes. Some examples of ALARP, BAT, and waste management hierarchy principles are given below.

- Figure 26-7 illustrates that the AP1000 design reduces the amount of valves, pipes, and other components compared to previous generations of PWRs. Hence less waste will be generated during maintenance activities (repair and replacement) and decommissioning.

- The AP1000 reactor coolant pump shaft seals, which are a potential source of excessive leakage of reactor coolant, are eliminated altogether through the use of sealless pumps.

- During the removal of core decay heat following an accident, the reactor coolant remains within containment; only decay heat energy is transferred out of containment.

- The Environment Report (Ref. 26.1, Section 3.2) describes waste-minimisation at source measures such as limiting the level of cobalt in reactor internal structures, which reduces the amount of Co-60 produced by activation reactions.

Sections 26.6, 26.7, and 26.8, which describe the gas, liquid, and solid waste systems, contain further information on waste minimisation.

26.4.5 Use of Best Available Techniques

Application of BAT to waste management requires that all reasonable opportunities should be taken for waste minimisation, reuse, and recycling. Where possible, wastes should be declassified by segregation and cleaning to free-release standards.

The descriptions below of the various waste management systems explain the segregation processes and refer to particular instances of BAT in the proposed AP1000 design. One clear use of BAT is the AP1000 design philosophy to minimise waste, as described in Section 26.4.4.

One of the criteria in the engineering process undertaken for the proposed AP1000 generic design solid waste management facilities was that the plant design should be ergonomically arranged for ease of transfer to ensure that the solid waste management system collects and stores radioactive wastes within shielding to maintain radiation exposure to plant operation and maintenance personnel ALARP (Ref. 26.9, Section 2.2.1).

The AP1000 design IWS is consistent with the waste hierarchy shown below, as well as the key BAT management factors for optimisation of releases from nuclear facilities shown in Figure 26-2. These factors correlate closely as follows:

Waste Hierarchy	BAT Waste Management Factor
Avoid	Use low-waste technology
Minimise	Use low-waste technology Efficient use of resources Reduce emissions
Reduce/Recycle	Use low-waste technology Use fewer hazardous substances
Abatement	Reduce emissions

26.4.5.1 Best Available Techniques Assessment for Key Radionuclides

The formation and abatement of key radionuclides has been assessed by Westinghouse for the AP1000 design using forms prepared for this analysis. The BAT forms include the source of the radioactivity, the pathway to the environment from the source, normal and maximum emissions as predicted by Westinghouse, and comparison with emissions from other nuclear power stations (Ref. 26.5, Appendix A).

Specific instances of BAT in the systems for processing gaseous, liquid, and solid wastes are included in the appropriate sections below.

26.4.6 Minimisation of Accumulation of Radioactive Waste

The final element of the AP1000 design waste strategy is to minimise the accumulation of radioactive waste at the reactor site. This means that radioactive waste should either be discharged, as permitted by the discharge limits, or shipped to suitable LLW, ILW, or HLW repositories as soon as possible. Minimising the inventory of waste on the site has similar safety benefits to minimising the amount arising: the reduced quantity of radwaste on the site reduces the radiological risks that arise from the site.

Westinghouse's waste management strategy requires LLW to be shipped for disposal routinely according to schedules agreed to by the plant operator and the NDA (Ref. 26.1, Section 3.5.1.4, and Ref. 26.15). A preliminary application has been made to the LLWR to confirm their acceptance of LLW from an AP1000 reactor. The Acceptance in Principle (D1) forms obtained from the LLWR are presented in UK AP1000 D1 Form Submission (Ref. 26.16) and contain activity estimates based on solid waste activity calculations (Ref. 26.17).

In the cases of ILW and spent fuel, it is expected that AP1000 plant operators will transport the waste offsite as soon as national repositories are available to accept these wastes (Ref. 26.2, Section 3.1.3). The NDA disposability assessment (Ref. 26.15) concluded that, when compared with legacy wastes, there are no new issues that challenge the fundamental disposability of the wastes expected to arise from operation of the AP1000 plant.

26.5 GENERAL INFORMATION ON DISCHARGES OF RADIOACTIVITY TO AIR AND WATER

Before considering the gaseous and liquid radwaste systems separately, it is helpful to present some general information on the proposed discharges of radioactivity to air and water.

The existing methodology used in the GALE code for calculating gaseous radwaste discharges was benchmarked against operating plant data. When significant differences were noted, the algorithms or input parameters for the GALE code were adjusted to obtain reasonable agreement. The representative data for the AP1000 plant were calculated by normalising 2001 to 2004 US plant data to plant power level. The base plant data generally reflect waste management techniques and philosophies that have been incorporated in the AP1000 design. However, using the 2001 to 2004 data is expected to result in conservative values for the AP1000 design because a number of recent AP1000 design improvements are expected to give reduced activity releases. For example:

- Fewer valves and components will result in fewer leakage pathways.
- Reactor coolant pumps without seals result in less leakage into containment.

From the representative annual emissions given here in Table 26-2 and Table 26-3 worst-case annual discharges and indicative discharge limits have been calculated. The calculation method follows Environment Agency (EA) guidelines; the GDA limits have been proposed on the basis of the expected highest “rolling 12-month” discharges within the reactor cycle.

The expected release rates of airborne radioiodine, noble gases, H-3, C-14, Ar-41, I-131, and beta particulates, liquid discharges of H-3, C-14 and “all isotopes without other limits” vary month by month through the reactor cycle. The maximum release rates (in TBq/y) are approximately two-thirds of the proposed limits for radioactive discharges (Ref. 26.18, Table 7-1). The margin provides some contingency to cope with operational occurrences. The proposed limits are reproduced here in Table 26-4; the actual discharge authorisations will be set by the EA and will be site-specific. The report Generic Design Measurement and Assessment of Discharges (Ref. 26.19) provides background detail on how discharges will be measured and assessed.

The proposed monitoring systems for gaseous and liquid discharges are broadly equivalent to monitoring systems currently used in operating UK nuclear power plants. This provides confidence that the AP1000 design monitoring techniques are in line with current best practices in the UK. During the detailed AP1000 design, consideration will be given to any future EA certification requirements for the monitoring of radioactive discharges. This may include sampling and monitoring equipment, qualifications of personnel involved in monitoring, and laboratory accreditation. None of the monitoring requirements require new technology or measurement techniques. This provides confidence that the AP1000 design monitoring techniques can be designed and engineered to demonstrate BAT and meet applicable UK requirements (Ref. 26.1, Section 6.2.1).

26.6 TREATMENT OF RADIOACTIVE AND POTENTIALLY RADIOACTIVE GASES

The strategy for dealing with radioactive gases is the following:

- To contain them as they arise

- To reduce the activity to ALARP and certainly to below the agreed discharge limits, either by decay or by removing the longer-lived radionuclides

- To hold the gases for sufficient time to measure the activity level and demonstrate that they comply with the limits

- Once they have been demonstrated to comply with the limits, to release them to the atmosphere

Avoiding uncontrolled releases and reducing the activity levels in the controlled discharges will reduce the risks to the public.

Starting with how radioactive gases arise in the AP1000 system, this section describes WGS for handling the gases and the ventilation systems for the various buildings. It also specifies the release points and the tables in the Environment Report (Ref. 26.1) that provide exhaustive lists of the gaseous emissions to air, by source, by radionuclide, and by month in the reactor cycle.

Each of the potentially radioactive gaseous discharges is radiologically monitored before being released (Ref. 26.1, Section 3.3).

26.6.1 Sources of Radioactive Gases

During reactor operation, radioactive isotopes of iodine and the noble gases xenon and krypton are created as fission products. All reasonable steps are taken to minimise the failure of the fuel rod cladding and thus minimise the release of radioactive fission products into the coolant (Section 22.1). A defect in the fuel cladding would allow a portion of these radionuclides to be released to the reactor coolant . Hence leakage of reactor coolant may result in noble gases being released to the containment atmosphere.

The principal point at which radioactive species are released from the coolant to the gas phase is the chemical and volume control system (CVS), which controls the chemistry of the reactor coolant. As well as dissolved fission products, tritium produced by activation reactions can accumulate in the coolant. The WLS degasifier removes gases from the coolant and feeds them to the WGS.

Within the containment building, naturally occurring Ar-40 in the atmosphere may be activated to form radioactive Ar-41.

26.6.2 Gaseous Radwaste Treatment System

The WGS is designed to perform the following major functions on an intermittent basis (approximately 70 hours per year):

- Collecting radioactive or hydrogen-bearing gaseous wastes

- Processing and discharging the waste gas while keeping offsite releases of radioactivity within acceptable limits

The AP1000 design WGS is a once-through, ambient temperature, activated-carbon delay system. The radioactive gases entering the system are carried by hydrogen and/or nitrogen gas. This gas stream passes through:

- The gas cooler, where it is cooled to about 4ºC (39ºF) by the chilled water system

- The moisture separator, which collects condensed water vapour (including condensed tritiated water vapour) from the cooled gas and discharges it to the WLS

- An activated-carbon-filled guard bed, which protects the delay beds from abnormal moisture carryover or chemical contaminants

- Two activated-carbon-filled delay beds in series where xenon and krypton are delayed by a dynamic adsorption process; radioactive decay of the fission gases during the delay period significantly reduces the radioactivity of the gas flow leaving the system

- A radiation monitor

The gases are then discharged to the ventilation exhaust duct.

The minimum calculated holdup times are 38.6 days for xenon and 2.2 days for krypton (Ref. 26.1, Section 3.3).

Each of the two delay beds is designed to provide the full required system capacity under design basis conditions. During normal operation, a single bed provides adequate performance. This provides operational flexibility to permit continued operation of the WGS in the event of operational upset in the system that requires isolation of one bed.

The use of a gas cooler, a moisture separator, a guard bed, and delay beds is a common gas treatment system throughout the nuclear power industry.

In the course of demonstrating that this system uses BAT, the BAT assessment (Ref. 26.5, Section 4.3.2.1) provides some further details of equipment and processes.

26.6.3 Ventilation and Filtration Systems

This section gives brief details of the ventilation and air-filtration systems in the AP1000 design that can handle radioactivity. It excludes nonradioactive ventilation systems that exhaust to the atmosphere such as the diesel generator building heating and ventilation system (Ref. 26.5, Table 4.1). This section is based on the Environment Report (Ref. 26.1, Sections 3.3.2 to 3.3.7).

26.6.3.1 Containment Air Filtration System

The containment air filtration system (VFS) is described in Chapter 23 Containment and Nuclear Ventilation Systems, Section 23.3.

The VFS serves the containment, the fuel-handling area, and the other radiologically controlled areas of the auxiliary and annex buildings, except for the hot machine shop and health physics areas, which are served by the Health Physics and Hot Machine Shop Heating, Ventilation, and Air Conditioning System (VHS) described in Section 23.10.

26.6.3.2 Radiologically Controlled Area Ventilation System

The Radiologically Controlled Area Ventilation System (VAS) serves the fuel-handling area of the auxiliary building, and the radiologically controlled portions of the auxiliary and annex buildings, except for the health physics and hot machine shop areas which are provided with a separate ventilation system. The VAS is described in Section 23.8.

26.6.3.3 Condenser Air Removal System

The condenser collects any inward leaks of air and any noncondensable gases contained in the turbine exhaust steam. The condenser air removal system (CMS) removes these gases from the steam side of the three main condenser shells and exhausts them into the atmosphere via the condenser air removal stack.

During normal operation and shutdown, the main condenser has no significant inventory of radioactive contaminants. The noncondensable gases and vapour mixture are not normally radioactive and are discharged to the atmosphere. However, it is possible for the mixture to become contaminated following a steam generator (SG) tube leak. Radiation monitors associated with the steam generator blowdown system (BDS), SG system (SGS) (main steam), and the condenser air removal system determine whether the secondary side is radioactively contaminated. Unacceptable levels of radiation trigger corrective action.

26.6.3.4 Turbine Building Ventilation System

The turbine building ventilation system (VTS) is described in Section 23.13. The system maintains acceptable air temperatures in the turbine building for equipment operation and for personnel working in the building.

26.6.3.5 Radwaste Building Ventilation and Filtration System

The Radwaste Building HVAC System (VRS) system is described in detail in Section 23.9. Air will be extracted from the radwaste building equipment via low-level grilles, conveyed through high-integrity ductwork to high-efficiency particulate air (HEPA) filters and discharged to the main plant exhaust stack. Dedicated HEPA-filtered branches will extract air from the waste-sorting cabinets.

26.6.3.6 Intermediate-Level Waste Store Ventilation and Filtration

The ILW store will be equipped with two HEPA filters in series to remove radioactive particulates present in the ILW building atmosphere.

The stack monitoring system for the ILW store will provide continuous monitoring of stack discharges to atmosphere. Stack monitoring system outputs and signals will be displayed in the central control room (Ref. 26.9, Section 3.7.17.1). The stack monitoring system shall be in accordance with British Standard (BS) 5243 (Ref. 26.21).

26.6.4 Emissions to Air

26.6.4.1 Release Points

Under normal operating conditions, the main plant vent and ILW ventilation stack are the only potential sources of gaseous radioactive emissions. The other emission points act as sources of radioactive air emissions only in abnormal conditions such as a loss of coolant accident or primary-secondary tube leak failure. This system is described in detail in Chapter 23.

The main plant vent is located on the side of the containment building. The Environment Report (Ref. 26.1, Table 3.3-3) shows its dimensions, flow rates, temperature, and stack height.

26.6.4.2 Expected Emissions

Table 26-5 shows expected monthly discharges through the fuel cycle. Table 26-2 gives representative 12-month discharges to air based on months 7 to 18 of the fuel cycle, worst-case annual discharges (taking into account plant ageing and other factors), and calculated annual discharge limits for radioiodines, noble gases and a number of other radionuclides.

The following tables from the Environment Report (Ref. 26.1) provides further comprehensive details of emissions to air, by source, by radionuclide and by month in the reactor cycle.

Table 3.3-6	Expected annual release per building or area of radioiodines to the atmosphere, averaged over the 18-month fuel cycle
Table 3.3-7	Expected annual release per building or area of radioactive noble gases, tritium, and C-14 to the atmosphere, averaged over the 18-month fuel cycle
Table 3.3-8	Expected annual release per building or area of radioactive particulates to the atmosphere, averaged over the 18-month fuel cycle
Table 3.3-11 to 3.3-22	Detailed monthly discharges in gas per building or area of radioiodines, noble gases, H-3, C-14, Ar-41, Co-60, Kr-85, Sr-90, I-131, Xe-133, Cs-137, and other particulates

Table 26-6 compares the annual gaseous discharges from the AP1000 design with the UK PWR Sizewell B and with four Westinghouse PWRs in the US. The table also includes liquid discharges (see Section 26.7.5). Although the balance between gaseous and liquid discharges varies from plant to plant, the total discharge per gigawatt of electrical output from the generic AP1000 design is significantly less than that from Sizewell B and less than or approximately equal to those from the other Westinghouse PWRs.

26.6.5 Best Available Techniques for Gaseous Radwaste Treatment

The BAT for gaseous treatment (Ref. 26.5, Section 4.3.2) is summarised here for four systems: the WGS, VRS, VFS, and VAS.

26.6.5.1 Best Available Techniques for Gaseous Radwaste System

The carbon delay beds in the WGS have been designed as a folded serpentine configuration. Although this configuration may have larger total void volumes than a straight configuration, long void channels are less likely to form in the carbon and hence contact between the gas and solid is increased. The serpentine configuration also minimises the space requirements. The number of legs in the beds has been chosen to optimise the balance between reducing discharges, which is favoured by increasing the number of legs, and minimising solid radioactive waste arisings, which is favoured by reducing the number of legs (Ref. 26.1, Section 3.3.5.1).

26.6.5.2 Best Available Techniques for Systems

BAT analyses for ventilation and filtration systems are discussed in Chapter 23, Appendix 1.

26.7 LIQUID RADWASTE SYSTEM

The strategy for dealing with radioactive liquids at a coastal site is to do the following:

- Contain the liquids as they arise
- Reduce the activity to ALARP and certainly to below the agreed discharge limits, e.g., by filtration or ion exchange
- Monitor the activity level and demonstrate that it complies with the agreed limits
- Release the effluents to sea

The WLS is designed to control, collect, process, handle, store, and dispose of liquid radwaste generated as the result of normal operation, including anticipated operational occurrences.

This section describes the WLS, how it operates and how it represents the application of BAT. It is based on the Environment Report (Ref. 26.1, Section 3.4).

26.7.1 Sources of Liquid Radwaste

There are several possible sources of liquid radwaste, as shown below (Ref. 26.1, Section 3.4.1). Table 26-7 shows the volumes that are expected to arise, per day (normal and maximum) and over the life of the plant.

Reactor Coolant System Effluents

The effluent subsystem receives borated and hydrogen-bearing liquid from two sources: the reactor coolant drain tank (RCDT) and the CVS. The RCDT collects leakage and drainage from various primary systems and components inside containment. Effluent from the CVS is produced mainly as a result of reactor coolant system (RCS) heatup, boron concentration changes, and RCS level reduction for refuelling. The RCS effluents contain dilute boric acid at concentrations up to 2700 ppm. This borated water is the principal input in terms of volume and activity.

Floor Drains and Other Wastes with High Suspended Solids

Floor drains and other wastes are collected by various building floor drains and sumps and routed to one of two waste holdup tanks each with a volume of 57 m^3 (2013 ft^3). They potentially have high suspended solid contents.

Detergent Wastes

Detergent wastes coming from the plant hot sinks and showers as well as some cleanup and decontamination processes are routed to the chemical waste tank, which has a volume of 29 m^3 (1024 ft^3).. Detergent wastes are typically high in dissolved solids but very low in radioactivity.

Chemical Wastes	Chemical wastes collected from the laboratory and other relatively small-volume sources are collected in the chemical waste tank where they may, if appropriate, be combined with detergent wastes. They may comprise mixed nonhazardous, hazardous, and radwastes or other radwastes with high dissolved-solids content. These wastes are generated at a low rate.
SG Blowdown	SG blowdown is normally nonradioactive and is accommodated within the BDS. However, if SG tube leakage results in significant levels of radioactivity in the SG blowdown stream, this stream is redirected to the WLS for treatment before release. In this event, one of the waste holdup tanks is drained to prepare it for blowdown processing.

26.7.2 Liquid Radwaste Treatment System

Figure 26-6 shows the WLS. The liquid radwaste is collected in the following five tank systems:

- Reactor Coolant Drain Tank
- Effluent holdup tanks
- Waste holdup tanks
- Chemical waste tanks
- Monitor tanks (treated liquid radwaste)

Effluent is radiologically monitored before being discharged (Ref. 26.1, Section 6.2.1).

26.7.2.1 Degasification of Reactor Coolant System Effluent

The RCS effluents, cooled if necessary, pass to the vacuum degasifier to remove hydrogen and dissolved radioactive gases before storage in the three effluent holdup tanks. The stripped gases are vented to the WGS.

The contents of the effluent holdup tanks may be:

- Recirculated and sampled
- Recycled through the degasifier for further gas stripping
- Returned to the RCS via the CVS makeup pumps
- Directed to the monitor tanks for discharge
- Passed through the filtration and ion exchange treatment system

26.7.2.2 Pre-Filtration

The contents of the effluent holdup tanks and waste holdup tanks are normally passed through a treatment system comprising an upstream filter followed by four ion exchange resin vessels in series and a downstream filter.

A pre-filter is provided to collect particulate matter in the effluent stream before ion exchange. The pre-filter is particularly important for removal of solids present in effluent collected from the floor drains, which are directed to the waste holdup tanks.

26.7.2.3 Deep Bed Filtration

The deep bed filter is a stainless steel vessel containing a layered bed of activated charcoal above a zeolite resin. The activated charcoal provides an adsorption media for removal of trace organics and provides protection for the ion exchange resins from contamination with oil from the floor drain wastes. Moderate amounts of other chemical wastes can also be routed through this vessel.

The top layer of activated charcoal collects particulates and, being less dense than the zeolite, can be removed without disturbing the underlying zeolite bed. This minimises the production of solid waste. The lower layer of the deep bed filter is clinoptilolite zeolite, which possesses an affinity for caesium.

The decontamination factors for deep bed filtration (100 for both caesium and rubidium) are included in Table 26-8 which collects together the factors for filtration and ion exchange.

26.7.2.4 Ion Exchange

Four ion exchange beds are provided following the deep bed filter. The ion exchange vessels are stainless steel, vertical, cylindrical pressure vessels with inlet and outlet process nozzles plus connections for resin addition, sluicing, and draining. The process outlet and flush water outlet connections are equipped with resin retention screens designed to minimise pressure drop. The design flow provides an adequate margin for processing a surge in the generation rate of this waste.

The ion exchange media will be selected by the plant operator to optimise system performance according to prevailing plant conditions. Typically, the first bed will contain a cation exchange resin, and the second two beds will contain mixed bed resins. Any of these vessels can be manually bypassed and the order of the last two can be interchanged, so as to provide complete usage of the ion exchange resin.

The ion exchange beds operate in the borated saturated mode. This means that the boric acid present in the reactor coolant effluent passes through the ion exchange beds without reduction in concentration.

The cation filter removes caesium, rubidium and other cations (with assumed decontamination factors of 10) but not iodine; the mixed waste ion exchangers have decontamination factors of 10 to 100 for iodine and 2 to 100 for other ions. These factors are compiled in Table 26-8.

26.7.2.5 After Filter

This filter is provided downstream of the ion exchangers to collect particulate matter such as resin fines. The unit is constructed of stainless steel and has disposable filter cartridges.

26.7.2.6 Monitor Tanks

Treated effluent is discharged to the six monitor tanks located in the radwaste building. Information on the design of the monitor tanks and their secondary containment can be found in Tables 3.4-2 and 3.4-3 of the Environment Report (26.1).

The total tank volume allows up to approximately 42 days' storage during normal power operations. The storage period is reduced during the short periods associated with higher discharge rates resulting from boron dilution near the end of core life and during RCS heat-up following refuelling. The worst case for the storage period is a few days. This would result from the unusual case of a shut-down shortly after an outage with little time between the first outage and restart. As the time between the first outage and the second restart increases, the storage time increases.

The release of treated liquid waste from any monitor tank to the environment is permitted only when sampling of the subject tank's contents indicates that such a release is permissible. If the effluent does not meet the permissible limits, it can be returned to a waste holdup tank or recirculated directly through the filters and ion exchangers.

A radiation monitor is located on the common discharge line downstream of the WLS monitor tanks. These radiation monitors will provide a signal to terminate liquid radwaste releases if the discharge concentration in the line exceeds a predetermined set point.

Effluent meeting discharge limits for radioactivity is pumped from the monitor tanks in a controlled fashion to the cooling water return from the circulating water system (CWS). The cooling water stream provides a substantial dilution of the discharged effluent before release to the environment.

26.7.2.7 Potential to Bypass Ion Exchange

Routine bypass of the WLS ion exchangers is not expected. However, the WLS is designed to be flexible and capable of handling a relatively wide range of inputs, including both high-grade water (from reactor effluents) and low-grade water (floor drains).

Each collection tank (effluent holdup tank, waste holdup tank) typically will be stirred and sampled prior to processing. Analysis of the sample from a specific batch of liquid will allow the operator to determine the optimum processing technique.

When processing a batch of reactor effluents, all WLS ion exchangers and filters are expected to be in service. However, when processing effluent from floor drains from the waste holdup tanks it is possible that some batches may be very low in radioactivity. For example, actuation of the fire water system in the radiologically controlled area of the plant could lead to a significant volume of uncontaminated fire water being collected by the WLS. In this case it may be acceptable and preferable to bypass one or more of the WLS ion exchangers in order to maximise the life of the media, thereby minimising solid radwaste arisings and associated occupational radiation exposure.

In all cases, processed water downstream of the WLS ion exchanger or filter train is collected in a monitor tank and is sampled prior to discharge to the environment.

26.7.2.8 Use of Mobile and Temporary Equipment

The WLS is designed to handle most liquid effluents and other expected events using installed equipment. However, for events occurring at a very low frequency, or producing effluents not compatible with the installed equipment, temporary equipment may be brought into the truck bays of the mobile treatment facility in the radwaste building.

Connections are provided to and from various locations in the WLS to these mobile equipment connections. This allows the mobile equipment to be used in series with installed equipment, as an alternative to it with the treated liquids returned to the WLS, or as an ultimate disposal point for liquids that are to be removed from the plant site for disposal elsewhere.

The radwaste building truck bays and lay-down space for mobile equipment, along with the flexibility of the numerous piping connections to the WLS, allow the plant operator to incorporate mobile equipment in an integrated fashion.

The connection of temporary lines between permanent plant radwaste storage tanks and mobile radwaste receptors (e.g., radwaste containers or mobile radwaste treatment systems) is a very common and well-understood process in operating nuclear power plants.

A dewatering return line, identical to the resin supply line, allows for dewatering equipment also to be tested prior to resin-handling operations, to ensure that process equipment has been properly aligned and all connections are firm. The automatic line flushing controller includes provisions for flushing the temporary lines connected to mobile waste receptors once resin-handling operations are complete.

Plant procedures are expected to incorporate best practices for the assembly of temporary piping systems connected to mobile waste receptors, including:

- Integration of standard plant procedures and procedures generated by the owner/vendor of mobile waste receptor through a step-by-step walkthrough
- Colour-coding of temporary lines and unique identifier tags indicating to which components each hose will be attached
- Including step-by-step signoffs and independent verification at each appropriate step of equipment set-up and operation
- Visual verification and hydraulic testing of waste flow paths with primary water to confirm piping arrangement and end connections prior to radwaste transfers
- Verification of procedure(s) for abnormal events during operations

Temporary equipment may also be used to clean up the condensate storage tank if it becomes contaminated following SG tube leakage. This use of temporary equipment is similar to that just described, except that the equipment is used in the yard rather than in the radwaste building truck bays.

These provisions to use mobile and flexible technology properly interconnected with permanent systems allow for evolving state-of-the-art methods to be applied to waste processing throughout the life of the plant. Using such methods has the potential to reduce risks from operating equipment, operator doses, and doses to the public.

Mobile systems are currently available in the US and have been proposed for use in Europe and the UK. In 2005, the Electric Power Research Institute (EPRI) undertook a review of LLW mobile processing and treatment systems for advanced nuclear plant (ANP) designs. In this review, they identified a number of known mobile technologies that are or could be applicable to a LLW management programme for an ANP. Skid or transporter container-mounted units that currently exist include:

- Tubular ultrafiltration
- Reverse osmosis units
- Ion exchange vessels
- Drum/paddle dryers
- High-velocity vacuum dewatering
- Activated carbon beds
- Solidification systems This list is not exhaustive. In Europe, the use of mobile treatment facilities for liquid radioactive waste generated from the dismantling of submarines in Russia has been proposed and preliminary designs drawn up (Ref. 26.25). In the UK, mobile plants have been targeted at solidification of wastes including sludges (Ref. 26.26). A transportable intermediate-level waste solidification plant was commissioned in 2003 at Trawsfynydd, which is currently being used to treat approximately 80 percent of the wet ILW at the site.

The mobile units typically are transported and operated in shielded containers with controls located outside of the container. Shielded containers are used to provide protection to operators and to enable the containers to meet transport regulations as they are moved between sites.

26.7.2.9 Detergent Waste

Detergent wastes are collected in the chemical waste tank. They have low concentrations of radioactivity and contain soaps and detergents not compatible with the ion exchange resins. If their activity is low enough, then they can be discharged without processing. When detergent waste activity is above acceptable limits and processing is necessary, the waste water may be transferred to a waste holdup tank and processed in the same manner as other radioactively contaminated waste water, if the installed equipment is suitable to do so. If onsite processing capabilities are not suitable for the composition of the detergent waste, then processing can be performed using mobile equipment.

The mobile equipment would comprise a concentration step (e.g., evaporation or reverse osmosis) to reduce the volume of waste to the extent necessary to allow an encapsulation plant to immobilise the concentrate in a cementitious grout. The encapsulated waste would be shipped to the LLWR. The condensed evaporator distillate or reverse osmosis permeate would be transferred to a waste holdup tank for further processing in the WLS or transferred to a monitor tank for sampling and discharge.

26.7.2.10 Chemical Waste

Chemical wastes are normally generated at a low rate (0.03 m^3/day (1.06 ft^3/day) [Ref. 26.1, Table 3.4-1]) and collected in the chemical waste tank. These wastes are only collected: no processing is provided. Provisions have been made to allow for chemical addition to the tank for pH or other adjustment. When combined with the radioactive sink and shower drains, the chemical wastes may be sufficiently dilute to be discharged without processing.

If the mixed liquid is not dischargeable or if the constitution of the chemical waste means that mixing is inadvisable, special processing will be required. Piping is provided to permit processing by mobile equipment brought into the radwaste building truck bays. Following such processing, the fluid may be returned to the WLS holdup tank for further processing and discharge, discharged directly, or transferred for further processing elsewhere.

Drainage of chemicals to the chemical waste tank will be controlled by procedure, ensuring that no incompatible waste streams are mixed. The chemicals to be used in the laboratory will be decided on by the utility operator.

26.7.2.11 Sludge

Sludge is not expected to accumulate significantly on the bottoms of liquid waste treatment tanks. These tanks are designed to minimise sludge formation by including provisions to slope the effluent holdup tank from one end to the other into a dirt pan section where particulate material can collect. The vertical tanks are sloped to the low point where particulates will be collected. The discharge pump suction is taken from the dirt pan or low point for drawing waste water out of the tank, thus performing a self-cleaning action. The tanks are also fitted with oversized manways that allow for access should any additional cleaning be necessary for tank maintenance or during decommissioning.

26.7.3 Disposability of Liquid Wastes

The waste from the chemical waste tank will be immobilised in cementitious grout using a mobile plant. In order to reduce the volume of waste requiring encapsulation, the waste will be dewatered e.g., by use of an evaporator, to the extent necessary to form a suitable grout mix. The resulting evaporate is encapsulated, typically in a 200-litre (7.06 ft^3) drum.

The completed waste packages are loaded into HHISO containers for shipment to the LLWR. Evaporator distillate is condensed and returned to the WLS.

Encapsulation is a simple and proven means of dealing with mobile LLWs. It is acceptable to the LLWR, and it meets the LLWR's current conditions on the physical nature of the waste form and the expected activity level (Ref. 26.27).

26.7.4 Best Available Techniques for Liquid Radwaste Treatment

The BAT optioneering considered for WLS (Ref. 26.1, Section 3.4.4, and Ref. 26.5, Section 4.3.3.1) is summarised below. Other options may be possible.

26.7.4.1 Ion Exchange Versus Evaporation

Liquid radwastes may be treated by ion exchange (to remove contamination, enabling the remaining liquid to be discharged) or by evaporation (to reduce the volume of contaminated liquid).

In Europe, many nuclear reactors are located on major rivers and not on coastal sites. It is common for these reactors to be equipped with evaporators to minimise the radioactive liquid discharges. However, the standard AP1000 design does not have evaporators based on considerations shown in the Environment Report (Ref. 26.1, Section 3.4.4.1).

Including evaporators would contradict the AP1000 design overriding principles of safety and simplicity. Compared to a traditional evaporator-based liquid radwaste system, the ion-exchange AP1000 system provides effectiveness and simplicity, and will tend to minimise operator doses and solid radwaste arisings. The complexity of the traditional evaporator design leads to significant maintenance with associated occupational radiation exposure and also allows more opportunity for operator errors. The relatively passive nature of the ion-exchange-based AP1000 system provides effective operation with lower

maintenance, lower operator doses, simpler operation, and at lower capital and operating costs.

The fact that the generic site for the AP1000 design is a coastal site and not a river site also lessens the value of using evaporators for minimising the discharge of boric acid. Unlike river water, seawater already contains significant boron concentrations.

The ion exchange treatment process has been shown to effectively control offsite discharges. This is the reason that the proposed WLS treatment system using ion exchange beds and filtration rather than evaporation is a BAT (Ref. 26.5, Section 4.3.3.1.1).

26.7.4.2 Enriched Boric Acid Versus Natural Boric Acid

Boron-10 in the form of boric acid is used for reactivity control in the AP1000 design.

The boron in natural boric acid contains approximately 20 percent boron-10, whereas the boron in enriched boric acid contains 60 percent boron-10. Because the same amount of the boron-10 isotope is required regardless of whether it is provided in the enriched or natural form, using enriched boric acid means that the total concentration of boron required in the RCS could be reduced by a factor of three. This would permit the quantity of lithium hydroxide (an alkali used to control the pH of the coolant, balancing the weak boric acid) to be similarly reduced, resulting also in a reduction on the amount of tritium produced from neutron activation of lithium-6 and so providing a safety benefit.

However, it is also possible to reduce the production of tritium from the lithium hydroxide by enriching the lithium hydroxide in lithium-7 (and reducing correspondingly the amount of lithium-6), while retaining the larger lithium hydroxide inventory required to balance the natural boric acid. Because the generation of tritium from boron-10 is the same for both options, adjusting the isotopic composition of the lithium to reduce the tritium generation from lithium hydroxide by a factor of three or more will ensure that the total tritium generation is at least as low as for the system with enriched boric acid. Moreover, enriched boric acid is approximately 200 times more expensive than natural boric acid (Ref. 26.1, Section 3.4.4.2). Therefore, using natural boric acid and lithium hydroxide that is enriched in lithium-7 provides a more cost-effective method of reducing the tritium generated in the RCS than using enriched boric acid.

Using “gray rods” for mechanical shim control, rather than relying on chemical shim control via boric acid, also helps to reduce tritium production and thereby increase safety.

26.7.4.3 Cartridge Filtration Versus Cross Flow Filtration

The WLS incorporates an after-filter downstream of the ion exchangers to collect particulate matter such as resin fines. The radioactive particulate load in the WLS influent is already reduced by passage through the pre-filter, deep-bed filter, and three ion-exchange beds before the after-filter. Using cartridge filters offers a low-pressure system that is suitable for the low flow rates (~8 m^3/day (282.5 ft^3)) associated with the WLS. The filters are readily replaceable and treated as LLW.

Cross-flow filtration techniques of microfiltration, ultrafiltration, nanofiltration, and reverse osmosis potentially offer more effective particulate removal efficiency than cartridge filtration. All of these techniques use membrane processes that segregate a liquid that permeates through a membrane from a concentrate that is retained. The driving force of the process is the pressure difference across the membrane. However, these processes have a number of disadvantages, including a more complicated system with probable higher

maintenance and operator doses, the requirement for higher pressures, and increased radwaste from decommissioning.

On balance, the proposed use of cartridge filters is BAT for filtration after the ion-exchange beds (Ref. 26.5, Section 4.3.3.1.3).

26.7.5 Liquid Discharges

Process liquids are normally discharged to one of the six monitor tanks shown in Figure 26-6. The release of treated liquid waste from any monitor tank to the environment is permitted only when sampling of the subject tank's contents indicates that such a release is permissible (Ref. 26.5, Section 4.3.3, and Ref. 26.1, Section 3.4.3.6).

Table 26-9 shows expected monthly discharges through the fuel cycle. Table 26-3 gives representative 12-month liquid discharges based on months 7 to 18 of the fuel cycle, worst-case annual discharges (taking into account plant ageing and other factors), and calculated annual discharge limits for tritium, carbon-14, and a number of other radionuclides.

Table 26-6 shows that the normalised total annual liquid radioactive discharges from the AP1000 reactor are significantly less than those from Sizewell B and from comparable recently-built Westinghouse PWRs in the US.

The following tables in the Environment Report (Ref. 26.1) provide comprehensive details of liquid emissions by source, by radionuclide, and by month within the reactor cycle:

Table 3.4-6	Expected annual release per building or area of radioactive liquid effluent discharges, averaged over the 18-month fuel cycle, all radionuclides.
Table 3.4-7 to Table 3.4-18	Detailed monthly liquid discharges per building or area of H-3, total non-H-3, C-14, Fe-55, Co-58, Co-60, Ni-63, Sr-90, Cs-137, Pu-241, and other particulates.

26.8 SOLID RADWASTE SYSTEM

Gaseous and liquid radioactive wastes need containment and decontamination until they can be proven to meet authorised discharge limits. Solid wastes, on the other hand, are easier to control physically but are more diverse. They will contain the radioactive contamination that has been removed from the gas and liquid wastes, and will include highly radioactive material such as spent fuel. Division into LLW, ILW, and HLW recognises that the different types of solid radwastes need different handling.

Storing waste in a passively safe configuration minimises the need for active safety systems and thus reduces risk. The desire to process waste into a passively safe form must be balanced against the likelihood that delaying processing would reduce operator dose, and it does not foreclose any future management options.

An option to store solid LLW, ILW, and HLW arising from the AP1000 reactor has been developed to ensure that these wastes are managed in compliance with UK regulatory and legislative requirements. The Environment Report (Ref. 26.1) will serve as the basis for the following sections, and the Radioactive Waste Arisings, Management and Disposal report (Ref. 26.9) is used as a supporting reference to provide information and to demonstrate how

the solid waste management strategy defined by the IWS (Ref. 26.2) is to be implemented. The following sections provide detail on how the principle of passive safety will be addressed.

After outlining the overall strategy for dealing with solid radwastes, this section considers the sources of solid radwaste, and then describes how each category of waste is handled at the AP1000 plant and comments on the ultimate disposability of the waste. The section concludes with a consideration of BAT for solid radwaste. Where appropriate, the descriptions consider in turn LLW, ILW, and HLW. The hazard analysis builds on the information here; but, because it is also relevant to gaseous and liquid wastes, it is presented in Section 26.9.

26.8.1 Strategy for Solid Radwastes

The strategy for solid radwastes utilises the waste hierarchy through storage and decontamination techniques designed to reduce the activity of the waste as far as reasonably practicable. The description below is based on that given in the Environment Report (Ref. 26.1, Section 3.5.1).

Westinghouse expects that the LLW, ILW, and spent fuel waste streams will be capable of being disposed in NDA facilities and has selected waste forms, treatment processes and containers accordingly.

Uncertainties and risks relating to the achievement of this strategy will be identified as the strategy is implemented and managed by documenting and discussing them with the utility customers and the EA. The main uncertainties, risks and assumptions in this strategy are associated with radioactive waste and spent fuel disposal at NDA facilities. The NDA is not presently able to provide information on the spent fuel packages that it will accept; therefore, Westinghouse will assume that current practices for spent fuel packaging, as well as LLW and ILW packages, remain acceptable once the AP1000 plant is built and operating. This includes container designs and sizes, and acceptable waste forms.

Nearby facilities, where and when available, will be used to the extent practical to minimise the environmental impact of transport. During site operations, communications will be maintained to assess onsite and offsite interdependencies, such as those between the AP1000 plant and offsite disposal facilities.

Figure 26-3 shows the AP1000 design solid radwaste management strategy. This strategy will include:

- Waste minimisation
- Avoidance of the unnecessary introduction of waste into the environment
- Waste characterisation and segregation
- Collection and retention of data on the waste and waste packages
- Consideration of options in a BAT assessment
- Communications with interfacing facilities and stakeholders
- Assurance that steps in the management of waste are compatible
- Characterisation of risks and uncertainties

26.8.2 Sources of Solid Wastes

26.8.2.1 Operational Solid Wastes

Solid LLW includes dry active wastes, general trash, and mixed wastes as a result of normal plant operation, including anticipated operational occurrences (AOOs) i.e., events that are anticipated to occur at least once in the plant lifetime. Section 26.8.2.2 discusses the inclusion of condensate polishing system (CPS) resins as LLW.

ILW arises from the periodic replacement and maintenance procedures, e.g., replacement of filters. The bounding design case is that the filter and resin wastes are in contact with high coolant activity associated with 0.25 percent fuel failure. Modern PWR fuel is considerably more reliable than this, and it is possible that the filter and resin activity levels will be low enough for them to be disposed as LLW.

The only source of HLW is spent fuel, i.e., fuel that is no longer efficient in creating electricity because its fission process has slowed. However, it is still thermally hot, highly radioactive, and potentially harmful. The reference 18-month equilibrium cycle feeds (and discharges) 64 fuel assemblies every 18 months. On average, this means that approximately 43 assemblies per year are discharged and stored in the spent fuel pool storage area. Each fuel assembly consists of 264 fuel rods. The fuel rods consist of uranium dioxide ceramic pellets contained in cold-worked and stress-relieved zirconium alloy (ZIRLO™) tubing, which is plugged and seal-welded at the ends to encapsulate the fuel.

The solid radwastes comprise the following:

LLW
compactable paper, tape, clothing, plastic, elastomers
noncompactable metallic items, glass, wood
condensate polisher spent resin
dry granular carbon
HVAC filter – granulated charcoal
compressible rigid plastic – gaskets, valve packing, insulation
HVAC filter – uncompacted fibreglass or metal
electro-deionisation unit – resin/membrane module
heat exchanger insulation
filter – pleated polyester
wet granular particles – sludge
waste oil
mechanical pump seal – silicon carbide
pump diaphragms – Buna n
degasifier separator – canned pump
resin transfer screw pump

ILW
ion exchange resin
gray rod cluster
wet granular carbon
filter cartridge – metallic cylinder
control rods
neutron Source Rods

HLW
spent fuel

In addition, the possible replacement of SGs or the reactor pressure vessel head (RPVH) would generate large one-off items (see Section 26.8.11).

The Environment Report (Ref. 26.1, Table 3.5-1 and Appendix A) gives detailed breakdowns of the volumes of these wastes. The volumes are comparable with those from existing plants. Table 26-10 shows that solid discharges from the AP1000 plant are much lower than those from existing nuclear power plants and other UK reactors.

26.8.2.2 Justification of Spent Ion Exchange Resins as Intermediate-Level Waste

This short section explains why the AP1000 reactor spent ion exchange resins are identified as ILW.

The expected activity of primary spent ion exchange resin is 78.1 TBq/y (2111 Ci/y) . The expected volume is 7.79 m^3/y (275.1 ft^3/y) (Ref 26.11, Section 6.1). As the density of resin is of the order of 1 t/m^3 (62.43 lb/ft^3), the implied specific activity of 10.0 TBq/m^3 (7.7 Ci/ft^3) clearly exceeds the LLW threshold of 12 GBq/te beta/gamma (0.15 mCi/lb beta/gamma). Thus, the primary resins are classified as ILW.

A secondary ion exchange resin waste stream comprising condensate polishing resins also arises within the AP1000 design. Under normal operating conditions, the condensate polishing resin will be nonradioactive and will be discharged as nonradioactive waste. Under abnormal conditions (e.g., SG tube failure), there may be a transfer of primary circuit activity into the secondary circuit. The amount of activity transferred will be very small, and the activity of the CPS resin will not exceed the limits for LLW. To be conservative, the waste disposability assessment and the waste arisings tables in the Environment Report (Ref. 26.1, Appendix A1) list the condensate polishing resin as LLW.

26.8.2.3 Decommissioning Wastes

The basic AP1000 design principles minimise the creation of radwaste during operations and decommissioning. The AP1000 reactor was designed to have fewer valves, pipes, and other components so less waste will be generated during maintenance activities such as repair and replacement (see Figure 26-7). This reduction in components also leads to lower quantities of waste being generated during decommissioning. The level of cobalt in reactor internal structures is limited to below 0.05 weight percent, and in primary and auxiliary materials to less than 0.2 wt. percent (Ref. 26.1, Section 3.5). This reduces the production of Co-60, which is typically the radionuclide with highest activity in activated metal components. Surfaces, including steel wall and floor surfaces, will be sealed to prevent penetration and to facilitate decontamination.

The wastes generated during decommissioning comprise the following materials (Ref. 26.1, Section 3.5.10), which are described more in detail in Chapter 27.

Small-Volume Components

The small-volume components at decommissioning include various electrical equipment, filters, electro-deionisation units, and skids. These wastes are classified as LLW.

Large-Volume Components

The large-volume components include the reactor head, which is not expected to require replacement during the operational period of the AP1000 plant. The quantities of ILW and

LLW large-volume component wastes generated during decommissioning are shown in Table 26-11.

It is assumed that the reactor vessel is disposed intact and is not decontaminated. No benefit would be gained from decontaminating the reactor vessel, as most of the dose would come from activation of vessel materials. Techniques may be developed in the future that would allow the decontamination of the reactor vessel without significant dose uptake to the operators. This would subsequently allow the reactor vessel to be cut up in a way similar to the method outlined for the reactor pressure vessel head (Ref 26.1, Section 3.5.7.1). This will be assessed as part of the individual site's decommissioning plan.

Decontamination of the reactor systems could be accomplished with some piping modifications to bypass the reactor vessel, as well as with the use of existing filter and demineraliser vessels.

Waste from Decontamination Operations

The following systems may become contaminated during normal and shutdown operations for maintenance and disposal purposes:

- BDS
- CVS
- Startup feedwater system (FWS)
- Primary sampling system (PSS)
- Passive core cooling system (PXS)
- RCS
- Normal residual heat removal system (RNS)
- Reactor system (RXS)
- Spent fuel pool cooling system (SFS)
- SGS
- Containment hydrogen control system (VLS)
- WGS
- Liquid radwaste system
- Radioactive waste drain system (WRS)
- Solid radwaste system

The plant areas that house these systems have the potential to become contaminated in the event of an accidental release of radioactive material. Decontaminated materials are expected to be handled in the hot machine shop, the cask washdown pit, or the area where the decontaminated equipment is located. Drains are located throughout the plant at various locations, including the rooms where decontaminated materials are handled, in case an unexpected spill occurs in an area where contaminated materials are handled. The spill can thus be flushed with water and drained for waste processing. Ultimately, the correct method of handling the spill will depend on the situation, and the utility will be responsible for making the appropriate decision about how to clean it up.

For the decontamination procedure for specific equipment or areas, see the decontamination considerations report (Ref. 26.55).

The only plant area with the potential to become activated is structural module CA-04, which surrounds the reactor.

The AP1000 decontamination equipment facilities provide decontamination capabilities for decontamination of the above systems.

The plant is designed to have a decontamination glovebox, a high-pressure demineralised water sprayer, and a dry ice pellet blaster located in the hot machine shop (Room 40358) for the decontamination of components and equipment that have become contaminated (Ref. 26.29).

The high-pressure demineralised water sprayer and dry ice pellet blaster are portable units that can be used to decontaminate equipment in situ if required. If the component can be transported to the hot machine shop, a decontamination basin is available for decontamination if the component is too large for the decontamination glovebox. If a component is too large for the decontamination basin, other areas such as the cask washdown pit can be used in conjunction with the portable decontamination units.

Waste produced during decontamination operations will be minimised utilising the waste hierarchy. The decontamination of the AP1000 plant has been simplified through a number of design features, e.g., controlling the spread of contamination, minimising the potential for cracks and crevices in large pools and pits, sloped tank bottoms, and coated surfaces.

The routine operation of systems designed to capture radioactivity throughout the operational life of the plant (e.g., WLS, WGS, WSS, CVS, and SFS) has the benefit of reducing the accumulation of activity in the pipes, vessels, and components to be decommissioned (Ref. 26.55).

Discharge and disposability assessments will be carried out as part of the BAT/ALARP assessments required when selecting the optimum chemical decontamination agents. Until these assessments have been made, it is not possible to assess the expected reduction in contamination levels that will be achieved during post-operational cleanout and decommissioning.

Achievable decontamination factors vary widely between techniques and between different applications of the same technique. Operator experience, treatability studies, and monitoring are all important in determining the achievable decontamination factors. Some examples of decontamination factors achieved on decommissioning projects have been published (Ref. 26.30).

Typical secondary wastes that may arise from utilising decontamination techniques include effluent, ion exchange resins, filters, abrasives, dross, used tools, and personal protective equipment. The decontamination waste streams will be treated, recycled, or disposed of in ways that are consistent with the techniques described in the Integrated Waste Strategy (Ref. 26.2) and the Environment Report (Ref. 26.1). The volume of decontamination waste is expected to be insignificant when compared with other operational or decommissioning wastes.

Dry Active Waste

The compactable dry active waste created during decommissioning operations (e.g., rags, overalls, gloves, and packaging) is LLW and is estimated to be generated at a rate of 135 m^3 (4767 ft^3) per year. This volume can be reduced fivefold to 27 m^3 (953.5 ft^3) per year using a low-force compactor. Assuming an accumulated decontamination operation of 3 years, the dry active LLW generated during decommissioning would be 81 m^3 (2860 ft^3) (see Table 26-11). The use of supercompaction could reduce this number further.

Demolition Waste

Only a very small fraction of demolition waste (rubble) is likely to be considered LLW, with the majority being nonradioactive or made nonradioactive during the decontamination process. The estimate of LLW demolition waste includes 2165 m^3 (76460 ft^3) of concrete and 158 m^3 (5580 ft^3) of steel (Ref. 26.1, Appendix A6).

The LLW demolition waste includes waste from the demolition of modules within containment. These modules are steel structures, some with concrete-filled wall sections, which would be cut into transportable pieces with little volume increase.

The demolition waste also includes 199 m^3 (7028 ft^3) of concrete in the vicinity of the core. This represents a 1.5-m (4.92 ft) thickness of concrete around the reactor vessel cavity, which may contain enough activation products to be treated as LLW. This is originally a concrete monolith, but when broken up and packaged, it will contain significant voidage. The Environment Report (Ref. 26.1, Section 3.5.10) estimates that the actual packaged LLW volume will be 400 to 600 m^3 (14130 to 21190 ft^3), implying 50 to 67 percent voidage.[3]

The total ILW decommissioning waste associated with large-volume components and waste from decontamination operations is estimated to be about 800 m^3 (28250 ft^3). The total LLW associated with decommissioning large- and small-volume components, compactable dry active waste and demolition waste is estimated to be about 5500 to 6000 m^3 (194200 to 211900 ft^3).

The management of decommissioning waste is being planned with the expectation that the LLW, ILW, and spent fuel waste streams will be capable of being disposed in NDA facilities. This is consistent with the conclusions of the Disposability Assessment (Refs. 26.15 and 26.31) carried out by the Radioactive Waste Management (RWM) of the NDA.

26.8.3 Minimisation of Solid Wastes

Philosophy and General Techniques for Minimisation

Over the past 15 years, Westinghouse has made several design decisions to reinforce the concepts of safety through simplicity, ALARP, and BAT (Ref. 26.5). Examples of the decisions related to waste minimisation, waste generation, and waste disposal are described in more detail in the Environment Report (Ref. 26.1, Section 2.6) and the BAT assessment (Ref. 26.5, Section 4.1.3). These techniques aim to minimise waste generation and to meet the design requirements with the lowest radioactive effluent, lowest risk for accidental loss or leakage, high reliance on proven technology, lowest risk for public or operator radiation exposure, and lowest overall plant cost. Some examples follow:

- Reduction of containment penetrations, which reduces the risk for containment leakage
- AP1000 design improvements that have eliminated the requirement to pump borated makeup water continuously into the RCS or to include complicated water processing systems in the design
- Use of demineralisers for the treatment of the borated radioactive letdown water

3. For comparison, close-packed spheres in an infinite space have 26 percent voidage.

- A zinc addition subsystem to reduce water stress corrosion cracking and crud-induced power shift, as well as the potential release of active corrosion products into the WLS

The design of the AP1000 plant also takes into account prevention of contamination by using secondary containment systems for the AP1000 plant chemical storage tanks (Ref. 26.1, Section 2.9.4, Table 2.9-6). Some of the plans need to be reviewed during site-specific analysis and designed as necessary to ensure that they will comply with UK guidance (Ref. 26.32). Prevention of radioactive contamination is also minimised by using system, structure, and component (SSC) designs and operational procedures that limit leakage and/or control the spread of contamination. In this regard, the spent fuel pool and connected pools are examples of structures designed to eliminate unidentified leakage to the groundwater. These are documented more fully in the Environment Report (Ref. 26.1, Section 2.9.5). Westinghouse prepared a document (Ref. 26.33) to demonstrate that these practices are consistent with the United States (US) Nuclear Regulatory Commission (NRC) Regulatory Guide 4.21 (Ref. 26.34), which is considered good practice for this area.

Further principles that minimise the production of LLW, ILW, and HLW follow.

Low-Level Waste

LLW is minimised by the following activities (Ref. 26.1, Section 3.5.4.1):

- Good housekeeping
- Appropriate operating procedures
- Segregation
- Volume reduction
- Sealed surfaces (including steel wall and floor surfaces) to prevent penetration and to facilitate decontamination
- Limiting the amount of material brought into containment
- Training all staff allowed to enter radiologically controlled areas (RCAs)
- Provision of waste facilities immediately outside of the RCAs, for the disposal of unnecessary packaging materials
- Provision of tool stores within the RCAs to prevent contamination of clean tools brought in from outside
- Testing filter performance to ensure filters are only replaced when necessary
- Provision of radwaste advice on radiation work permits

Intermediate-Level Waste

ILW is minimised by the following activities (Ref. 26.1, Section 3.5.4.2):

- Optimum operation of the reactor in terms of power generation per tonne of fuel

- Selecting fuel with minimal potential for fuel defects, thereby minimising the radioactive isotope contamination of the primary cooling water circuit, reducing the load being treated by the ion exchange resin beds and hence the volume of ILW
- Received fuel being carefully inspected for any imperfections
- Minimisation of plant shutdowns
- Use of gray rods (low-density neutron absorbers) for mechanical shim control rather than relying on coolant chemistry
- Use of sealless coolant pumps eliminates seal leaks and creation of radioactive waste water
- Selection of materials of construction with a composition low in cobalt
- Use of zinc addition for corrosion control
- Selections of ion exchange media to give an optimum decontamination factor, which will minimise the number of ion exchange media changes required and reduce the waste volume
- Flexibility in routing effluent through the different ion exchange beds to optimise resin uptake
- Testing filter performance to ensure filters are only replaced when necessary
- Segregation procedures to prevent dilution of ILW streams by mixing them with LLW streams
- Formulation trials to determine an optimum blend ratio for the conditioning matrix producing the optimum number of waste packages
- Suitable operating procedures

High-Level Waste

The fuel economics and the amount of spent fuel are closely correlated. Both are optimised when the fuel cycle is designed with fuel being discharged from the reactor as close as is reasonable to the licensed discharge burnup limit. Westinghouse fuel is designed and verified for 62 GWd/MTU maximum burnup for the lead rod (Ref. 26.35), which translates to a batch average burnup of approximately 50 GWd/MTU.

The proposed 18-month fuel cycle will help to support the design intention of minimising spent fuel. This is based on an assumed 97 percent capacity factor and a 21-day refuelling outage, giving a cycle length of approximately 510 effective full power days. Although an annual cycle would give slightly fewer spent fuel assemblies over the life of the plant (2517 versus 2653), the number of shutdowns would increase from 40 to 60. The vast majority of Westinghouse customers (i.e., the utility operators) choose the longer fuel cycle (Ref. 26.1, Section 3.5.4.3).

26.8.4 Handling of Solid Radwaste

In contrast to handling the gaseous and liquid systems, handling the solid radwastes focuses on appropriate segregation and then on packaging the wastes in a way that is suitable for long-term storage, transport and disposal. Figure 26-4 is a plan of how solid radioactive waste is handled on the generic AP1000 design site: LLW goes to the radwaste building, whereas ILW and HLW go to the auxiliary building.

The engineering aspects of the AP1000 design were developed to ensure the design of the solid waste management facilities fulfilled the functional requirements and criteria defined in the Radioactive Waste Arising, Management and Disposal report (Ref. 26.9, Sections 2.2.1 and 3). These activities were managed by a quality management system operated in accordance with the applicable international standards:

- A final waste form conforming to current regulatory requirements that can be produced, handled, and managed on site and stored safely
- A workable design based on currently available technology of appropriate maturity
- A design that can be accommodated within the confines of the generic site
- A design that demonstrates ALARP principles
- A design that demonstrates BAT principles
- A design that is safe, for which potential hazards have been identified and for which the appropriate mitigation measures have been incorporated
- The plant design is ergonomically arranged for ease of transfer and ensures that the solid waste management system collects and stores radioactive wastes within shielding to maintain radiation exposure to plant operation and maintenance personnel ALARP
- A design compliant with UK regulations, codes, and standards
- 60-year operational capacity
- 100-year design life of spent fuel store and ILW store

The design of AP1000 and the process used to select radwaste treatment equipment provide flexibility to the operator in case the utility decides to reassess solid waste treatment to consider the latest developments in technology and different packaging arrangements (Ref. 26.1, Section 3.5.1.3). For example, one of the benefits of using a mobile encapsulation plant for ILW is that the technology can be updated as required in line with developing best practices (Ref. 26.9, Section 3.3.2.3) in order to reduce doses to operators and/or the general public.

The Radioactive Waste Arisings, Management and Disposal report (Ref. 26.9, Section 3.8) covers the radiological areas classification in terms of radiation and contamination zoning.

The following sections describe how waste is classified and segregated, and the onsite treatment of LLW, ILW, and HLW.

26.8.4.1 Segregation of Waste

In order to facilitate safe and effective management of radioactive waste, the waste should be characterised and segregated according to their activity and other physical and chemical properties.

Segregation ensures that lightly-contaminated waste (e.g., LLW) remains separate from higher-activity waste that may require more packaging and more costly deep geological disposal. Characterisation ensures that the physical, chemical, radiological and biological properties of particular waste packages are assessed and recorded, enabling the packages to be managed appropriately.

The radwaste building contains facilities (buffer/marshalling area) for segregated storage of various categories of solid LLW prior to processing (Ref. 26.2, Section 2.1.1.3). Also within the buffer/marshalling area will be a dedicated space for the decay storage of waste if and when required.

The WSS is designed to be able to segregate solid wastes by activity level and by physical and chemical characteristics, and also to segregate clean wastes originating in the RCA (Ref. 26.2, Section 2.2.3). Figure 26-3 and Figure 26-4 outline the segregation steps.

26.8.4.2 Waste Characterisation

The Letter of Compliance (LoC) process used by NDA RWM advises that waste streams are assessed before disposal. The issued LoC may be conceptual, interim or final, with the later stages requiring more information. A final-stage LoC advises that details of the physical, chemical, radiological, and biological properties of the waste, whereas a conceptual assessment would require only a general description of the waste (e.g., including assessed radionuclide inventory and whether or not it will contain organic material) along with a description of the methods proposed to characterise the waste fully.

The design of the waste management system will ensure that the required information is captured as described in the Radioactive Waste Arisings, Management and Disposal report (Ref. 26.9, Section 3.3.7).

Waste will be categorised for treatment as conventional or radioactive. Radioactive wastes will be categorised as VLLW, LLW, ILW, and HLW. They will be further characterised and (kept) segregated according to their required treatment, as determined by chemical composition, compactability, and radionuclide inventory.

26.8.5 Solid Waste Storage

In addition to the nuclear and non-nuclear islands buildings, there are facilities for the onsite storage of solid LLW, ILW, and HLW generated during AP1000 plant operation. These are described below.

26.8.5.1 Low-Level Waste Handling and Storage

The LLW store is located within the boundary of the licensed site to the rear of the radwaste building (Ref. 26.1, Section 2.3.6.1). This store comprises the LLW buffer and the radwaste building, which includes the waste accumulation room. The radwaste building also holds monitoring tanks containing processed effluent that are ready for release to the environment (Ref. 26.1, Section 3.4.3.6). The mechanical aspects and facilities of the radwaste building

and associated design requirements are detailed in Radioactive Waste Arisings, Management and Disposal report (Ref. 26.9, Sections 3.4.5 and 3.2.1.3).

LLW is bagged, collected manually, and transported to the buffer/marshalling area of the waste accumulation room. The waste is packaged in HHISO containers. A forklift truck specifically designed for container handling will be used to move the HHISO containers from the radwaste building to the buffer store. HHISO containers will be handled within the radwaste building by the overhead crane. The HHISO container will be transported by road to the LLWR at Drigg for final disposal (Ref. 26.1, Section 3.5.9.1).

The AP1000 plant design includes provisions for the decontamination of any contaminated material that may arise from equipment replacement parts, tools and other metallic, plastics, or cloth parts and materials that may arise from outage activities. Any of these materials that can initially be classified as ILW are intended to be decontaminated to an LLW category.

The waste management strategy requires LLW to be shipped for disposal routinely according to schedules agreed to by the plant operator and the UK NDA. A facility will be available to store LLW during periods (up to 2 years) when waste cannot be received by the LLWR (Ref. 26.11).

Facility Design

The radwaste building is a non-seismic building with portable-shielding and lockable doors to minimise unauthorised entry and inadvertent exposure. This structure contains no systems essential for maintaining nuclear safety, but is designed for wind and seismic loads in accordance with the Uniform Building Code. The foundation of each building is a reinforced concrete mat (Ref. 26.9, Section 3.2.1.2).

Access to the radwaste building work areas by authorised personnel is assumed to be via the annex building change and health physics rooms, in which personnel will change into “clean conditions” protective clothing. Departure from the radwaste building will be via the change rooms, in which the protective clothing will be removed and placed in contaminated clothing containers (Ref. 26.9, Section 3.4.6).

The Waste Accumulation Room 50351 in the radwaste building is used to buffer, store, sort, and process incoming packaged LLW. Personnel ingress to and egress from this room will be via the subchange in the northwest corner.

The LLW buffer store is a covered area comprising a concrete hard-standing area with a steel-framed canopy (Ref. 26.9, Section 3.2.1.3).

Reserve Storage Capacity

Separate areas are reserved for the storage of several items, such as empty waste disposal containers (Ref. 26.9, Section 3.2.1.3).

Plant Availability

It is anticipated that LLW processing will be required all year round. Plant availability within the radwaste building will be 52 weeks per year at 5 days per week with a 7.5 hour working day. Multishift working will be possible, if required, depending on chosen campaign requirements (Ref. 26.9, Section 3.3.8).

Control System

The requirements for security systems for the radwaste building will be determined during the detailed design associated with the specific site (Ref. 26.9, Section 3.7.11). The facilities within the radwaste building will generally be manually operated, with an appropriate level of interlocks incorporated to prohibit mal-operation (Ref. 26.9, Section 3.3.6.2). Closed-circuit television (CCTV) cameras will be positioned to allow operations in the radwaste building to be monitored (Ref. 26.9, Section 3.7.10).

Transfer, Inspection, Maintenance and Monitoring of Waste Packages

Waste packages are handled in the LLW processing area, giving consideration to the radiation protection, environment and safety aspects (Ref. 26.1, Section 3.5.9.1). One example of the safety procedures is that LLW will be sorted under controlled conditions through the use of glove boxes (Ref. 26.1, Section 3.5.7.1).

HHISO containers will be handled within the radwaste building by the overhead crane and moved to the buffer store using a forklift truck specifically designed for container handling (Ref. 26.9, Section 3.2.1.3). The HHISO container will be transported by road to the LLWR at Drigg for final disposal (Ref. 26.1, Section 3.5.9.1).

Instruments monitor and control the process variables associated with LLW processing. This includes radiometric measurements within LLW handling equipment. Assaying of LLW drums to ensure that compliance with the site discharge criteria can be demonstrated uses a low-resolution gamma spectrometer (LRGS) located within the radwaste building. The LRGS will be located in an area of low background activity, or additional shielding will be installed to ensure that measured count rates are attributable to emissions from the waste drum. The LRGS will be integrated with the package tracking system (Ref. 26.9, Sections 3.7.15.2 and 3.7.17). Once drums have demonstrated that they meet quality assurance (QA) requirements, they are placed in a HHISO container positioned within the radwaste building (Ref. 26.9, Section 3.4.5.4).

Package Type

The waste package used for LLW is one that is currently accepted by the LLWR. As such, it has been designed to comply with the current requirements for handling, retrieval, transport, storage, and disposal (Ref. 26.9, Section 3.3.2.2).

26.8.5.2 Intermediate-Level Waste Handling and Storage

ILW is stored within suitable contamination-zoned and shielded areas of the auxiliary building prior to treatment in the MEU. Maintenance, control console, shielding, ventilation, safety, and seismic qualification of the MEU are discussed in the Radioactive Waste Arisings, Management and Disposal report (Ref. 26.9, Sections 3.4.3 and 3.9.2), together with the waste tracking system.

Once the ILW is encapsulated in waste packages acceptable to RWM (e.g., 500-litre (17.66 ft^3) drum, 3 m^3 (105.9 ft^3) drum and box), the boxes and drums will be transported to an onsite ILW store. During transport to the ILW store, the waste package (drum or box) will be placed in an overpack, which will provide shielding in order to limit exposure to operators and the public. A self-propelled trailer will be used to move the waste packages to the ILW store along designated routes. During transfer, the package is to be suitably shielded to ensure dose uptake to personnel is ALARP. Based on the expected resin load and the assumed dose levels, the overpack shielding required for a single processed ILW package is steel of 0.19-m

(0.62 ft) thickness or concrete of 0.63-m (2.1 ft) thickness (Ref. 26.9, Sections 3.4.7.3 and 3.9.2).

Inside the ILW store, the packages will be placed and recovered using an overhead crane. The packages will be stored until a national ILW repository becomes available.

The first phase of construction will provide an ILW store suitable for 20 years of ILW production. The ILW store will be designed for a total inventory of 60 years of operational waste arisings from one AP1000 unit. The ILW store has a 100-year design life and could be used to retain ILW after the AP1000 plant is decommissioned and until the national ILW repository becomes available (Ref. 26.9, Section 3.4.7, and Ref. 26.1, Section 3.5.8.2).

Facility Design

The auxiliary building is designed to withstand the effects of natural phenomena. The ILW store is a reinforced concrete structure (Ref. 26.1, Sections 2.3.1 and 2.3.6.2), consisting of a waste package reception area and a shielded vault serviced by a certified nuclear crane. Figure 26-8 shows plan and section views of the ILW store. Further details are found in the Radioactive Waste Arisings, Management and Disposal report (Ref. 26.9, Section 3). A seismic assessment has determined that the AP1000 plant ILW store does not need to be seismically qualified from a radiological consequence perspective (Ref. 26.8, Section 6.8.3.1 and Ref. 26.9, Section 3.4.7.11). For response to external hazards, see Section 26.9.2..

The ILW storage facilities are designed to minimise unauthorised intrusion and to provide radiation shielding. The requirements for store shielding are listed below.

The assessment of shielding thickness addresses both onsite doses to workers and offsite doses to members of the public, in accordance with the assessment criteria discussed in the Radioactive Waste Arisings, Management and Disposal report (Reference 26.9, Section 3.9.3.1). The assessment considers two source terms:

- Store populated only by 3 m^3 (105.9 ft^3) RWM-compliant drums
- Store populated only by 500 litre (17.66 ft^3) RWM-compliant drums, placed in standard stillages

For the dose rates to the public, there are two site boundary distances considered for the generic site:

- The assumed distance to the site boundary is 200 m (656.2 ft).

- The distance from the site boundary to the nearest dwelling is a further 80 m (262.5 ft) (a total of 280 m (918.6 ft)).

The shielding and dose requirements imply that the walls of the ILW store should be constructed of 1 m (3.3 ft) thick concrete and the roof of 0.74 m (2.42 ft) thick concrete, both with minimum density 2.35 te/m^3 (146.7 lb/ft^3) (Ref. 26.9, Section 3.9.3).

In-store and encapsulation equipment will be modular, and components will be regularly or routinely replaced rather than being designed for the full 100-year storage period. All components that are subject to wear are located in such a manner that will allow easy access, removal and replacement with the minimum of disturbance to adjacent components (Ref. 26.9, Section 3.4.7.7).

Reserve Storage Capacity

The basic module for ILW storage accommodates 20 years of arisings. It may be expanded or duplicated as required to meet the necessary 60-year capacity (Ref. 26.9, Section 3.4.7.2). The vault sizing is also discussed in the Radioactive Waste Arisings, Management and Disposal report (Ref. 26.9, Section 3.4.7.5). In this section, it is stated that the store will initially be sized to contain the waste arising from nominally 20 years of operation of the AP1000 plant, minimising the initial capital expenditure. The actual rate and quantity of waste arising from operation will inform the planning and sizing of future store extensions. The onsite ILW store could be used as interim storage for the AP1000 plant decommissioning waste. If the national ILW repository is available before the end of AP1000 plant operations, ILW decommissioning waste could be shipped direct to the repository without interim storage onsite. Having the national ILW repository available before the end of AP1000 plant operations will also allow for the decommissioning and dismantling of the onsite ILW store using the decommissioning facilities created for the AP1000 plant. In this case, the onsite ILW store will be emptied and all stored waste packages shipped to the repository. Waste arisings from the dismantling of the ILW store will be similar in nature to the ILW, LLW, and conventional waste arising from AP1000 plant decommissioning. ILW packages will be shipped directly to the national ILW repository (Ref. 26.2, Section 6.9.3.1).

Control System

The requirements for security systems for the ILW store (e.g., building access turnstiles, swipe card systems, intruder alarm, and/or audio listening systems) will be determined during the detailed design associated with the specific site (Ref. 26.9, Section 3.7.11).

The ILW store will have a dedicated control console. More detail on the operating modes (normal and manual modes and recovery mode, intended to be used following equipment failure) can be found in the Radioactive Waste Arisings, Management and Disposal report (Ref. 26.9, Sections 3.3.6.2 and 3.4.7.4). The primary control positions for controlling process operations will typically be local to the process and will be provided (where possible) with direct viewing of the main operations, supported by CCTV where appropriate. The CCTV cameras are described in the Radioactive Waste Arisings, Management and Disposal report (Ref. 26.9, Section 3.7.10).

The operators within the control room will be suitably shielded from both packages in the vault and the import/export area (Ref. 26.9, Section 3.4.7.4).

Transfer, Inspection, Maintenance and Monitoring of Waste Packages

The ILW storage requirements and procedures to ensure safety, radiation protection, transportability, stock control, and ability to retrieve waste packages are provided in the Environment Report (Ref. 26.1, Section 3.5.8.2):

- The ILW store incorporates a receipt area with waste package assay equipment and a shielded vault serviced by a certified nuclear crane. The packages will be transferred into the receipt area via a shielded door and then transported by the crane to a position in the store vault determined using the tag information.

- The package position will be recorded in the control log for ease of future retrieval. The packages will be placed in the store layer by layer to limit the potential topple height of stored packages. The layers will be constructed from the furthest point of the store working back to the receipt area.

- The chosen transfer path for placing/retrieving a package will be such to minimise the effective drop height.

- The store design and operation will be such to enable retrieval and visual examination of individual packages. CCTV within the import/inspection area will be used to facilitate this.

- The same facilities used during placement of the ILW packages into the store will be used to ship the ILW packages.

Some of these topics are also covered in Radioactive Waste Arisings, Management and Disposal (Ref. 26.9, Sections 3.4.2.3 and 3.4.7).

Instruments monitor and control the process variables associated with ILW processing. These include radiometric measurements within the ILW import/export equipment and general area monitoring. ILW packages will be assayed using a high-resolution gamma spectrometer (HRGS) located within the ILW store building before they are transferred to the ILW store vault and before they are sent to the repository. The HRGS will be located in an area of low background activity or will have additional shielding applied to ensure that measured count rates are attributable to emissions from the waste drum. The HRGS will be integrated with the package tracking system (Ref. 26.9, Section 3.7.16.1). The LRGS (in the radwaste building) and HRGS ensure that compliance with the site discharge criteria can be demonstrated (Ref. 26.9, Section 3.3.7).

Remedial action strategy for ILW packages is considered when external damage or defects are found (Ref. 26.9, Sections 3.4.3.3 and 3.4.7.1). All ILW packages will be visually inspected during handling and, if defects or external damage are found, the package will be flagged as “rogue”. A rogue package may arise from:

- Overfill of a package during encapsulation, causing spillage and contamination to the outer surface

- Malfunction during lidding, causing an unsealed package

- Corrosion or damage to the package, resulting in a containment failure

Any rogue package will be transferred to a secondary containment vessel (SCV). The SCV is a container of similar design to the RWM packages that is sized to fit over the RWM 3 m^3 (105.9 ft^3) box or drum. If an ILW package is found to be rogue as a result of QA inspections, it will be inserted into an SCV, lidded, and positioned in the store as normal. A small batch of empty SCVs will be stored within the radwaste building until required.

Overpacking of failed ILW packages was chosen for the purpose of GDA, ensuring that operator dose uptake is ALARP. Currently, no area or equipment exists to conduct structural repair/remedial work on a nonconforming or failed waste package. This option may be developed by the licencee during site-specific detail design.

A suitably shielded crane maintenance area is to be provided containing facilities to radiologically monitor and manually decontaminate equipment by means of swabbing. Maintenance access to this area will be assessed, as will the identification of routes for import and export of any maintenance items and materials. The maintenance requirements will be in line with the Lifting Operations and Lifting Equipment Regulations 1998, as well as other applicable regulations (Ref. 26.9, Section 3.4.7.7).

Package Type

The BAT optioneering study (Ref. 26.14) has determined that the waste packages should be RWM-compliant types in order to meet the expected conditions for acceptance for the national ILW repository. As such, they will comply with the requirements for handling, retrieval, transport, storage, and disposal. The in-store and encapsulation equipment, such as the MEU, four-drum stillages, and the nuclear crane will be suitable to engage and handle these RWM waste packages (Ref. 26.9, Sections 3.4.3.3, 3.4.7.2, and 3.4.7.12).

Continued Safe Storage of ILW

The ILW store is to be fully independent and capable of functioning beyond decommissioning of the AP1000 plant (Ref. 26.9, Section 3.4.7.15). In making the GDA, RWM assumed that interim storage was required for a period of 100 years (Ref. 26.31, Section 5.1.1). This is consistent with the 100-year lifetime assumed in the NDA's UK Radioactive Higher Activity Waste Storage Review (Ref. 26.36, Section 1.5.3).

It is envisaged that when an ILW repository becomes available, the ILW packages will be removed from the store and monitored again with the HRGS before being sent to the repository. If the HRGS result of a package indicates the radionuclides in the package have decayed such that the package could be LLW, the package will be temporarily placed in an LLW storage area. The LLW disposal facility will be contacted to ensure the appropriate records are prepared for LLW disposal at that time.

Figure 26-9 (reproduced from report on long-term storage of AP1000 ILW and spent fuel in the UK (Ref 26.56)) outlines the management plan for the ILW facilities. Because the precise timescales depend on decisions still to be taken (e.g., on approval to build new power stations or an opening date for a final disposal facility), the diagram shows the sequence and parallelism of events rather than explicit dates.

26.8.5.3 High-Level Waste Storage

After spent fuel is removed from the reactor, it will be stored in the fuel storage pool. Details of the fuel storage pool can be found in Section 6.10.3.

Because spent fuel is not expected to be reprocessed, Westinghouse has proposed using the Holtec International dry storage cask system for spent fuels (HI-STORM) 100U to dry-store the spent fuel once it has been removed from the storage pond for the operational period of the plant and beyond. The HI-STORM 100U system consists of three primary components:

- HI-STORM 100U underground vertical ventilated module (VVM)
- Multipurpose canister (MPC), each of which contains 32 spent fuel assemblies
- Holtec International transfer cask for HI-STORM (HI-TRAC), which holds the MPC during loading operations

Figure 26-10 shows the HI-STORM 100U system and its components. Once the spent fuel assemblies have reached the acceptable limits for heat generation (currently assumed to be about 100 years), and assuming that the national geological disposal facility (GDF) is available, they will be transported from their dry cask storage to the GDF.

The RWMC evidence report for HLW (Ref. 26.4, Section 10) outlines the currently best understood and proposed conditioning and disposability options for spent fuel. The packaging

plant for handling the AP1000 plant spent fuel will be designed with features to ensure that the risks and detrimental effects to the public and the environment as well as plant operators are ALARP. More detailed information can be found in Section 26.8.6.3 of this PCSR and in the Environment Report (Ref. 26.1, Section 3.5.9.3).

In order to demonstrate within the GDA that the packaging of spent fuel from AP1000 plant operations is achievable and safe, further information is presented below relating to:

- An outline of the current option for packaging of AP1000 plant spent fuel for dry storage
- A description of spent fuel repackaging system as a way of demonstrating that the necessary technology exists for packaging fuel for the GDF. Information relating to the GDF proposed for Sweden (this incorporates many features expected in the UK GDF) and from other countries

The availability of the necessary technologies for packaging spent fuel, the research undertaken by Svensk Kärnbränslehantering AB (SKB) in Sweden and other organisations worldwide such as Holtec International in the US, Gesellschaft für Nuklear-Service mbH (GNS) in Germany and the conclusions of the NDA spent fuel disposability report give confidence that the packaging of spent fuel from an AP1000 reactor is achievable and safe within GDA.

Facility Design

The dry spent fuel storage is a seismically qualified below-ground dry-storage facility that provides radiation shielding for the spent fuel (Ref. 26.1, Sections 2.3.6.3 and 3.5.8.3). For example, the HI-STORM 100U underground VVM provides for storage of a Holtec MPC in a vertical configuration inside a subterranean cylindrical cavity entirely below the top-of-grade. The principal function of the VVM structure is to provide the biological shield and cooling facility.

Transfer, Inspection, Maintenance and Monitoring of Waste Packages

HLW packages will be transported from the spent fuel cooling pond in their dry cask storage Holtec MPC to the HLW store using an appropriate transport vehicle. The Holtec MPC is one option that can be used for the interim storage, transport and final disposal of the AP1000 plant spent nuclear fuel. There are various other systems under development that could also be used for the interim storage, transport, and/or disposal. It may also be possible to place the AP1000 plant spent fuel directly into an RWMC disposal canister, once removed from the cooling pond, if the canister is designed for such a purpose.

Once the spent fuel assemblies have reached the acceptable limits for heat generation, they will be transported from their dry cask storage to the national GDF once it is available. During transport, each waste package will be placed in an overpack to provide radiation shielding and also to ensure the integrity of the waste during a road accident. The total weight of the waste package will be within appropriate limits for transport on UK roads when necessary. It is envisaged that transport of packaged spent fuel would be undertaken using a disposal canister transport container. This is an RWM transport container concept that provides two layers of shielding (Ref. 26.1, Section 3.5.9.3).

The assessment undertaken by NDA assumed that spent fuel packages would be overpacked for disposal (Ref. 26.1, Section 3.5.9.3).

Package Type

The decision on how to package spent fuel for storage is one that will be taken up by a future licencee. Two options, the MPC and a Castor cask, are discussed in more detail below. Once the package has been selected, compliance with requirements for handling, retrieval, transport, storage, and disposal can be assessed. However, sufficient information is available already on the various options to indicate that spent fuel may be stored safely.

The MPC was proposed for use at Yucca Mountain and is a single package equally suitable for onsite storage, transport, and permanent disposal in a future repository. It can hold up to 32 PWR assemblies. The MPC lid provides sufficient structural capability to permit the loaded MPC to be lifted by threaded holes in the MPC lid (Ref. 26.1, Section 3.5.8.3). The Environment Report (Ref. 26.1, Section 3.5.8.3) presents more information regarding the three main components of the dry storage system. As indicated above, the MPC can be accommodated in the HI-STORM 100U system.

A Castor V/21 cask containing 21 spent PWR assemblies (with burnups in the range 30 to 35 GWd/MTU) has been in storage at the Idaho National Environmental and Engineering Laboratory since 1985. A series of examinations was undertaken in 1999 and early 2000 to investigate the integrity of the Castor V/21 cask. The findings of those inspections (Ref. 26.37) concluded that there is no evidence of significant degradation of the Castor V/21 cask systems important to safety from the time of initial loading of the cask in 1985 up to the time of testing in 1999. Although the burnup of this fuel is lower than that expected for the AP1000 plant fuel, these findings provide some confidence that the Castor cask would also be a suitable container for long-term fuel storage. A 2008 NRC fact sheet (Ref. 26.38) also commented that dry spent fuel storage in casks is considered to be safe and environmentally sound. More information regarding the long-term storage of spent fuel can be found in the report on long-term storage of AP1000 ILW and spent fuel in the UK (Ref. 26.56)

The licencee is responsible for selecting a spent-fuel storage system and should undertake further work to ensure that it meets the requirements for handling, retrieval, transport, storage, and disposal. The evidence above indicates that it will be possible to meet the requirements for safe long-term interim storage of spent fuel.

26.8.6 Disposal of Solid Radwaste

26.8.6.1 Waste Acceptance Criteria for Disposal

Acceptance criteria will be established by the operator for admitting waste to the storage facility, as well as the final repository, and arrangements implemented to ensure radioactive wastes will meet the acceptance criteria. Relevant factors were described previously, and are summarised below.

Sections 26.8.5.1 and 26.8.5.2 of this chapter describe the compatibility of LLW and ILW packages with handling, transport, and storage requirements, including their suitability for retrieval and transport following the expected storage periods. These sections also address briefly the arrangements for examination, testing and auditing of LLW and ILW packages.

Waste packages will be monitored to demonstrate the absence of surface contamination before being placed in storage. In the case of LLW, the waste package will be decontaminated using manual cleaning cloths or swabs. The decontamination waste will be handled and disposed of with other LLW (Ref. 26.9, Section 3.4.5.4). The ILW package

decontamination processes within the store will be undertaken if required. Dry methods such as swabbing are preferable, as they eliminate liquid effluents (Ref. 26.9, Section 3.4.7.14).

26.8.6.2 Disposability of Low-Level Waste

Westinghouse has sought assurance from the LLWR that the expected LLW streams will be disposable. Table 26-12 compares the total activity in the LLW packages that will be transported to the LLWR with the activity triggers for acceptance (Ref. 26.39). For each of the listed activity groups, the waste packages meet the LLWR conditions for acceptance. Moreover, the LLWR has agreed in principle to accept the relevant waste (Ref. 26.16).

The acceptance in principle from the LLWR (Ref. 26.16) includes the immobilisation of approximately 0.5 m^3 (17.7 ft^3) of waste oil per year. The preferred option for the disposal of this waste stream is incineration at the Tradebe (formerly Pyros) incinerator at Fawley (Refs. 26.40 and 26.41).

The acceptance in principle from the LLWR was obtained in the event that this was deemed impractical, and the waste could be immobilised and shipped to the LLWR. The same treatment would be applied to the condensate polishing resins that had been in place during the 30-day leak from the primary to secondary circuits, even if this is considered highly unlikely to occur.

Incineration has also been identified as a potential disposal route for 3.85 m^3 (136 ft^3) per year of condensate polishing resins. Normally these will be nonradioactive. However, calculations have shown that both 7-day and 30-day tube leaks would lead to activity levels that exceed the criteria for acceptance at the incinerator (Ref. 26.17). For the 7-day leak, a storage and decay period of 3 years would enable the waste to meet the acceptance criteria. If this were deemed impractical, the waste could be immobilised in cementitious grout and shipped to the LLWR. The same treatment would be applied to the resins that had been in place during the 30-day leak, although such a leak is considered highly unlikely to occur.

26.8.6.3 Nuclear Decommissioning Authority Disposability Assessment of Intermediate-Level Waste and Spent Fuel

The RWM of the NDA has investigated the disposability of ILW and spent fuel. RWM produced a disposability assessment report (Refs. 26.15 and 26.31), which raised a number of issues. The RWMC evidence reports for ILW (Ref. 26.3) and spent fuel (Ref. 26.4) (which were not available when the RWM work started) address a number of the issues.

26.8.6.4 Further Evidence on Spent Fuel Disposal

The geological disposal facility proposed for Sweden incorporates many features expected in its UK counterpart. The Swedish radwaste management organisation SKB has undertaken a significant research programme and has proposed a design of canisters for spent fuel disposal (Ref. 26.42, Section 4).

SKB's proposed disposal method is to package the spent fuel in copper canisters and embed the filled canisters within Bentonite clay at a depth of 500 m (1640 ft) in the crystalline bedrock of the GDF. This provides three separate environmental isolation barriers (canister, Bentonite clay, and bedrock) for the spent fuel and prevents contamination from getting into groundwater. The copper canister is nearly 5 m (16.4 ft) long and has a diameter of over 1 m (3.3 ft). The copper shell is 5 cm (0.164 ft) thick. Inside the shell there is an insert of cast iron

for greater strength. The copper shell is highly resistant to corrosion in the environment expected to prevail in the final repository.

SKB has developed a canister laboratory research facility to develop technology for welding the lid and bottom onto the canister, and also to ensure the equipment used in the encapsulation process will achieve the necessary quality and output. SKB is using ultrasound technology and radiography to test welds and canister components and has developed a programme to determine the reliability of different inspection methods (see e.g., Reference 26.43).

SKB has documented current scientific knowledge of the climate-related conditions and processes relevant to the long-term safety of a repository to a level required for an adequate safety assessment (Ref. 26.44).

The encapsulation canister proposed by the NDA in the disposability assessment is similar to the canister used in the facilities being developed by SKB. The entire fuel element is deposited in the encapsulation canister and therefore no additional waste streams (e.g., ILW fuel assembly structural elements) are generated. The SR-Can assessment carried out by SKB (Ref. 26.45 and its many supporting reports) determined that this encapsulation process and associated repository have environmental impacts that are minimised. The packaging plant for handling AP1000 plant spent fuel will be designed with features to ensure that the risks and detrimental effects to the public, environment, and plant operators are ALARP.

The availability of the necessary technologies for packaging spent fuel, the positive comments from the Swedish regulator, the research undertaken by SKB in Sweden and other organisations worldwide such as Holtec International in the US, GNS in Germany and the conclusions of the NDA spent fuel disposability report all give confidence that the encapsulation of spent fuel from an AP1000 reactor is achievable and safe within the terms of GDA.

26.8.7 Best Available Techniques for Solid Radwaste

Following the development of the engineering aspects, the BAT assessment of the solid waste management unit was developed to identify suitable processes for managing the ILW and LLW streams. This is described in the BAT assessment document (Ref. 26.5) and summarised in the Environment Report. The BAT assessment focused on the available and currently proven technologies that have been used in the UK and elsewhere for the treatment of LLW and ILW. Initially, an optioneering process was carried out to identify a set of radwaste treatment options. This, along with the assessment criteria, is described in the Solid Waste BAT assessment report (Ref. 26.14).

The treatment options considered include cement encapsulation of solid ILW and compaction of compactable LLW (Ref. 26.1, Section 3.5.5). Each step in the management of radwaste will be compatible with all other steps, including pre-treatment, treatment, storage, disposal, handling, and onsite and offsite transport. Figure 26-11 summarises the ILW and LLW radwaste treatment options that have been selected following the BAT exercise carried out by Westinghouse. Figure 26-12 and Figure 26-13 give more detail on the initial option screening exercise for LLW and ILW.

Westinghouse proposes that the dry spent fuel storage system be used on the generic AP1000 design site (Ref. 26.1, Section 3.5.6). The selection of the spent fuel storage system can be deferred for a period to allow new techniques to be incorporated, if appropriate (Ref. 26.9, Section 3.2.1.3).

The AP1000 design and the process used for selection of radwaste treatment equipment provide flexibility to the operator to allow for the planning of the use of the most appropriate and efficient systems as they become available (Ref. 26.1, Sections 3.5.7 and 3.5.5.6). For example, the cement encapsulation system is mobile and designed to be easily removed, providing the utility with the option to replace the equipment after operations have started if newer technology has been developed.

The proposed locations of the ILW and spent fuel storage facilities (Ref. 26.1, Sections 2.3.6.2 and 2.3.6.3, respectively) have been selected to minimise the transportation distances between the auxiliary building and the stores and to facilitate safe transfer of waste. Similar constraints were considered in the optioneering exercise for the location of the encapsulation plant (Ref. 26.9, Section 3.4.3.4).

26.8.8 Best Available Techniques Assessment for Nonradioactive Waste Treatment

The nonradioactive waste produced by the AP1000 plant is less significant than the radioactive waste. However, BAT should still be applied to this waste. This section considers briefly the sources of gaseous discharges, liquid discharges and solid waste. It provides the references to the detailed descriptions of how BAT is used to manage the significant (liquid and solid) waste, and some examples of those techniques.

26.8.8.1 Nonradioactive Emissions to Atmosphere

There are only two gaseous nonradioactive emission sources, the mobile encapsulation plant and the standby generators (Ref. 26.1, Section 4.1.1). If powdered grout materials are handled on the mobile encapsulation plant for ILW encapsulation, then local auxiliary building extraction systems and bag filters will be provided to reduce airborne emissions to acceptable levels (Ref. 26.1, Section 4.1.1.1). The contribution of standby diesel generators to the overall thermal rated input and air pollution from the combustion of the gases is minimal, as is air pollution arising from gaseous products of combustion.

26.8.8.2 Nonradioactive Liquid Discharges

Regarding the liquid nonradioactive waste treatment, the IWS (Ref. 26.2, Section 6.5) demonstrates that the treatment systems used to prevent the uncontrolled release of contaminants to the environment make use of current BAT, and ensure that all discharges are ALARP. The nonradioactive waste water systems comprise the waste water system, the sanitary drainage system, the seawater cooling systems, storm water, fire water, and various closed-loop cooling systems such as that for the turbine building (Ref. 26.1, Section 4.2). There may be circumstances that require the development of an impact evaluation and management in the site-specific design.

26.8.8.3 Nonradioactive Solid Wastes

The sources of solid nonradioactive waste are summarised in Table 26-13. The conventional waste management strategy will ensure, to the extent practicable, that techniques will be used to prevent or minimise the production of wastes. Examples are:

- Reusing receptacles, hoses, and other plant consumables, where it is safe to do so
- Using appropriate signage to remind staff of the need to reduce waste
- Reusing HEPA filter boxes

- Providing waste collection facilities in the RCA outside of contamination-controlled areas from which waste can be monitored and, if it is not contaminated, removed from the RCA for disposal as nonradioactive waste

- Learning from operator experience shared between the sites and externally from other organisations in the UK and overseas

Figure 26-14 shows the proposed treatment and disposal of nonradioactive waste.

26.8.9 Management of Orphan Waste

The AP1000 design and processes seek to minimise "orphan"[4] waste, so-called because of their incompatibility with current or developing disposal techniques. A detailed review of AP1000 plant systems and rooms was performed to ensure that creation of orphan waste will be as low as reasonably practicable. This review identified no orphan waste streams (Ref. 26.2, Section 3.1.2).

26.8.10 Processing of Radioactive Waste into a Passively Safe State as Soon as Is Reasonably Practicable

The AP1000 design is aimed to maximise operational flexibility and minimise waiting times. The design and layout of equipment also consider access for installation, operation, recovery, inspection, maintenance, and decommissioning. Any package shall be capable of being retrieved from any position within the store, and at any time, during the 100-year storage period (Ref. 26.9, Section 3.4.7.8).

Incoming LLW will be brought into the facility and temporarily stored in a buffer or marshalling area within the radwaste building until required for sorting (Ref. 26.1, Section 3.5.7.1).

Solid ILW will be encapsulated on a campaign basis when sufficient volume of waste is available to complete an encapsulation run, typically coinciding with refuelling outages after 18 months of operation (Ref. 26.9, Section 3.3.2.3).

The spent fuel assemblies are initially stored in the spent fuel cooling pond to allow radioactive decay to occur and decay heat to be removed before being transferred to dry cask storage (Ref. 26.1, Section 3.5.7.3).

26.8.11 Treatment of Large Solid Items of Radioactive Waste: Steam Generators and Reactor Pressure Vessel Head

Large solid radioactive waste items are not expected to be generated during normal operation of the AP1000 plant. However, as a contingency, the SGs and the RPVH may require replacement. This section describes the arrangements for handling these large items.

The layout of the containment is designed to permit the removal of either steam generator through a temporary opening cut through the top of containment, then through the centre of the passive containment cooling air diffuser. During a steam generator removal operation, the steam generator is lifted from the steam generator compartment by a temporary construction trolley and then through containment by a large mobile crane. It is expected that the SGs will

4. Materials for which no final treatment or disposal route has yet been identified (Ref. 26.2, Table 9-1).

fall into the LLW category. It is intended that these items are handled as they arise and are size reduced, the pieces being decontaminated to the fullest practicable extent. Decontaminated pieces that are no longer radioactive will be released to conventional waste-handling facilities for recycling or disposal. Decontaminated pieces that remain radioactive will be wrapped before placement into HHISO containers and sent for disposal at the LLWR (Ref. 26.9, Section 5.2.3.4).

Decontamination materials are expected to be similar in nature to those already used for operational AP1000 plant LLW arisings as dealt with in the AP1000 plant radwaste building and will be packaged and disposed of in the same manner.

To facilitate this disposal route for large items, a temporary facility would be erected, for example a tent with mobile HVAC equipment and connections to the AP1000 plant power, water, and air systems as necessary. Following processing of the SG, the temporary waste-handling facility would be decontaminated as necessary and dismantled.

The materials used in the construction of the SGs are nickel-chromium-iron alloys and austenitic stainless steel (Section 6.2.2). These materials and their associated activities will meet the current conditions for acceptance at the LLWR, classified as metallic wastes.

If replacement of the reactor pressure vessel head is necessary, treatment of the replaced RPVH will be similar to that for replaced SGs. The replaced RPVH is expected to be LLW and will be handled as it arises. It will be size-reduced and the pieces decontaminated to the maximum extent practicable. Decontaminated pieces that are no longer radioactive will be released to conventional waste-handling facilities for recycling or disposal. Decontaminated pieces that remain radioactive will be wrapped before placement into HHISO containers and sent for disposal at the LLWR.

26.9 RESPONSE TO PROCESS, EXTERNAL AND INTERNAL HAZARDS

This section is relevant to gaseous, liquid and solid radwaste, and builds on the detailed descriptions of the facilities presented in Sections 26.6, 26.7, and 26.8.

26.9.1 Process, External and Internal Hazards for Low-Level Waste

26.9.1.1 Response to Process Hazards

A number of hazards that have been identified associated with the AP1000 plant LLW radwaste treatment operations are described in the UK AP1000 Radwaste Preliminary Safety Statement (Ref. 26.8, Section 6.8.1). These include:

- Spread of contamination
- Loss of containment of packages
- Contaminated wounds

The unmitigated consequences of each of these faults are considered below.

Spread of Contamination

During AP1000 plant radwaste treatment operations, spread of contamination and dose inhalation can occur due to:

- Contaminated packages

- Failure of pipework in the mobile encapsulation plant
- Release of contamination during operations to size-reduce LLW

The spread of contamination will be minimised by the application of well-designed procedures. In addition, the mobile encapsulation plant will be operated remotely. It is therefore considered that the potential dose uptake from inhalation of small quantities of airborne contamination will be negligible, and is therefore not subjected to detailed quantification.

Loss of Containment of Low-Level Waste Package

The inventory of a LLW package is significantly lower than that of the ILW package and the consequences of a loss of containment are consequently smaller. The consequence for a LLW package is calculated as <0.1 mSv (10 mrem) (worker), <0.1 mSv (10 mrem) (public) (Ref 26.8, Table 5.1).

Contaminated Wounds

A contaminated wound can be caused by an operator error during LLW size reduction operations. It is possible that a sharp edge is created during LLW cutting operations and the operator receives a wound from a section that is contaminated. The dose to an operator due to a contaminated wound is estimated in the UK AP1000 Radwaste Preliminary Safety Statement (Ref. 26.8, Appendix B) to be 38 μSv (3.8 mrem), which would be regarded as an event of relatively low significance.

26.9.1.2 Response to External Hazards

A number of preliminary safety reviews have been carried out on the design and operation of the radwaste building (Ref. 26.9, Section 4.1). HAZOP studies were performed to underpin the design of the radwaste building. Some of the issues identified during the HAZOP studies are related to the selection of a specific site and these will be carried forward for full resolution during the detailed design associated with a specific site. The output of the HAZOP 1 study is incorporated into the UK AP1000 Radwaste Process Hazard Study 1 Report (Ref. 26.46) and considers the extreme weather conditions as external hazards.

26.9.1.3 Response to Internal Hazards

The radwaste building will include environmental controls that are part of the main AP1000 plant control systems. These comprise (Ref. 26.9, Section 3.3.5.6):

- Control of the HVAC system (Ref. 26.19 , Section 9.4)
- Fire detection system
- Environmental surveillance and general radiometric display systems

The radwaste building HVAC system is designed to permit periodic inspection of the system (Section 23):

- Each component is inspected prior to installation.

- Components of each system are accessible for periodic inspection during normal plant operation.

- A system air balance test and adjustment to design conditions is conducted in the course of the plant pre-operational test programme.

- Air flow rates are measured and balanced in accordance with the guidelines of the Sheet Metal and Air Conditioning Contractors National Association HVAC systems – testing, adjusting, and balancing.

- Instruments are calibrated during testing.

- Automatic controls are tested for actuation at the proper setpoints.

- Alarm functions are checked for operability.

In addition to the overall radwaste building HVAC system, there is a requirement for a local dedicated air extraction system for the removal of any airborne waste particles above the following working areas:

- Sorting glovebox enclosure
- Size reduction glovebox enclosure
- Decontamination glovebox enclosure
- Large item laydown area

The air extraction system design will be based on established HVAC principles used within the nuclear industry and will incorporate flexible/adjustable overhead extraction hoods at each work area.

There is the potential for fires to occur within the radwaste building. An addressable multizone fire detection and alarm system will be installed throughout the radwaste building. Monitoring devices will include, but not be limited to, smoke and heat detectors, manual call points, and visual or audible alarms. The fire detection system will be designed to meet the requirements of BS 5839 Fire Detection and Alarm Systems (Ref. 26.47). Requirements for a permanently installed fire suppression system will be reviewed during the detailed design phase. These systems are described more fully in Radioactive Waste Arisings, Management and Disposal report (Ref. 26.9, Section 3.7.9).

The consequences of a fire in the radwaste building are considered to be significantly lower than for an ILW fire, due to the lower inventory. The worst-case consequences associated with an LLW fire are therefore considered to be <0.1 Sv (10 rem) (operator) and <0.1 mSv (10 mrem) (public) (Ref. 26.8, Section 6.8.2).

The radwaste building will also be provided with environmental surveillance (e.g., temperature (Section 23.9.1) and general radiometric display systems). The general display system will use gamma monitors and combined airborne alpha/beta monitors, which will provide radiological area monitoring. These monitors will be connected to annunciators located adjacent to the main personnel access door into the radwaste buildings. Alarms will be provided for both high gamma and instrument fault conditions. Alarms will be repeated in the AP1000 plant central control room (Ref. 26.9, Section 3.7.17).

The monitor tanks located in the radwaste building contain a radiation monitor on the common discharge line downstream. These radiation monitors will provide a signal to terminate liquid radwaste releases if the discharge concentration in the line exceeds a predetermined set point (Ref. 26.1, Section 3.4.3.6). The radwaste building is also designed to contain any liquid spills from the liquid waste monitor tanks. These provisions include a

raised perimeter and floor drains that lead to the WLS waste holdup tanks (Ref. 26.1, Section 2.3.5, and Ref. 26.9, Section 3.4.5.2). All floor drains are grouted into the surrounding concrete to ensure that any leakage will be collected in the floor drain rather than bypassing the drain (Ref. 26.1, Section 2.9.5.4).

26.9.2 Process, External and Internal Hazards for Intermediate-Level Waste

26.9.2.1 Response to Process Hazards

A number of hazards have been identified associated with the AP1000 plant radwaste treatment operations. These include (Ref. 26.8, Section 6.8.1):

- Spread of contamination
- Loss of containment of packages
- Loss of containment of overpacks
- Increased external dose

The unmitigated consequences of each of these faults are considered in the subsequent sections.

Spread of Contamination

During AP1000 plant radwaste treatment operations, spread of contamination and dose inhalation can occur due to:

- Contaminated packages
- Failure of pipework in the mobile encapsulation plant

The spread of contamination will be minimised by the application of well-designed procedures. In addition, the mobile encapsulation plant will be operated remotely. It is therefore considered that the potential dose uptake from inhalation of small quantities of airborne contamination will be negligible, and is therefore not subjected to detailed quantification.

Loss of Containment of Packages

A number of faults have been identified that have the potential to damage the ILW package in the auxiliary building. These include:

- Dropping an empty package during crane movement
- Control failure of the lid grapple resulting in damage to package lid
- Control system, mechanical or power failure, or operator error resulting in the mobile encapsulation plant shield door impacting a package
- Control system, mechanical failure, or operator error resulting in a package impacting the mobile encapsulation plant shield door
- A package, driven in incorrect direction due to control failure or operator error, falls off the mobile encapsulation plant rails

- Control system failure or mechanical failure of the grout fill head results in impact to a package

- Control system failure or operator error results in the overpack door impacting a package

The bounding consequences of a loss of containment of an ILW package in the auxiliary building can be calculated using a release fraction (RF) of 1E-5, which is appropriate for a single RWM 3 m^3 (105.9 ft^3) box/drum dropped from 25 m (82 ft) (Ref. 26.48). This is judged to be a pessimistic value as no package will be dropped by as much as 25 m (82 ft) but it allows an upper bound of the consequences of an impact to be determined. In addition, the building will provide a decontamination factor (DF) of 10 for releases to the public. The consequences of a loss of containment of an ILW package in the auxiliary building are therefore calculated as (Ref. 26.8, Section 6.8.1.2 and Appendix B):

- Public = Dose × RF/DF = 7.57E1 * 1E-5/10 = 7.57E-5 mSv (7.57E-6 rem)
- Worker = Dose × RF/DF = 3.72E5 * 1E-5/1 = 3.7 mSv (0.37 rem)

It should be noted that this worker dose is considered to be pessimistic, as there will be no operator present in the auxiliary building during encapsulation operations.

A number of faults have been identified that have the potential to damage the ILW package in the ILW store, which include:

- Control failure or operator error resulting in a package being impacted by overpack or by the ILW store inner shield door

- Control failure or operator error resulting in package toppling from receipt conveyor

- Control failure or operator error resulting in impact between crane and package

- Control failure or operator error resulting in crane/package impact with ILW internal structures

- Control failure or operator error resulting in crane impacting stored packages

- Crane failure/lifting beam failure resulting in a dropped load

- Crane failure resulting in crane collapse

- Remote operation of crane resulting in increased potential for operator error

- Toppling of packages due to seismic activity

The unmitigated consequences of the loss of containment of a single ILW package in the import/export bay of the ILW store are considered to be identical to those calculated above for a loss of containment within the auxiliary building (i.e., 7.57E-5 mSv (7.57E-6 rem) [public], 3.7 mSv (0.37 rem) [worker]).

There is the potential for multiple packages in the ILW store to be toppled by a seismic event that does not result in collapse of the ILW store. However, the public consequences of this event will be bounded by the consequences of total collapse of the ILW store, which is considered separately (see Section 26.9.2.2). The operator consequences will be minimal as there is no operator access to the ILW store vault (Ref. 26.8, Section 6.8.3.1).

Collapse of the crane resulting in loss of containment of multiple packages can only occur in the ILW store vault, i.e., remote from the operator. It is therefore considered that loss of a single package in the import/export bay of the ILW store provides a suitably bounding consequence for an operator. For a member of the public to receive a dose of >0.1 mSv (0.01 rem) would require 1300 packages to fall, and this is not credible given that the total number of packages in the ILW store from 60 years of AP1000 plant operations is approximately 1100 (Ref. 26.8, Section 2.1.3.3). It is therefore considered that the dose to a member of the public from crane collapse will be <0.1 mSv (0.01 rem).

Loss of Containment of Overpacks

During the transfer of the package from the auxiliary building to the ILW store, it will be contained in an overpack. There is the potential for this overpack to be damaged in the following facilities:

- Loss of containment of overpack in the auxiliary building
- Loss of containment of the overpack external to the buildings
- Loss of containment of the overpack within the ILW store

There is the potential for a loss of containment of the overpack in the auxiliary building due to the following faults:

- Control system failure or operator error results in package impacting overpack door
- Control system failure or operator error results in external shield door impacting overpack
- Control failure, drive mechanism failure or operator failure results in jacking failure/uneven jacking

The overpack provides an additional DF of 10 over that provided by the package and therefore the potential consequences will be a factor of 10 lower than those identified in the Radwaste Preliminary Safety Statement (Ref. 26.8, Section 6.8.1.2) for the loss of containment of a package. Including the factor of 10 gives estimated doses of 7.57E-6 mSv (7.57E-7 rem) (public) and 0.37 mSv (0.037 rem) (worker).

The following hazards were identified in the HAZOP report (Ref. 26.46) that have the potential to result in a loss of containment of the overpack external to the buildings.

- Vehicle impact into shielded transporter
- Control failure or operator error results in impact between ILW store external shield door and overpack/transporter

The overpack provides an additional DF of 10 over the package, however, the public DF of 10 for a building is no longer applicable; therefore, the potential public consequences will be the same as those identified in the Radwaste Preliminary Safety Statement (Ref. 26.8, Section 6.8.1.2), and the operator consequences a factor of 10 lower than those identified in the same section (Ref. 26.8, Section 6.8.1.2) for the loss of containment of a package, i.e., 7.57E-5 mSv (7.57E-6 rem) (public) and 0.37 mSv (0.037 rem) (worker).

There is the potential for a control failure, drive mechanism failure, or operator error to result in uneven jacking and toppling of an overpack and subsequent loss of containment within the ILW store. The unmitigated consequences of a loss of containment of an overpack in the ILW store are considered to be identical to those calculated above for a loss of containment within the auxiliary building, i.e., 7.57E-6 mSv (public) and 0.37 mSv (worker).

Increased External Dose

There is the potential for an operator to receive an increased external dose uptake from the mobile encapsulation plant and the ILW store.

Faults that have the potential to result in an increased dose rate from the mobile encapsulation plant include:

- Blockage resulting in shine from open mobile encapsulation plant shield door
- Control failure resulting in mobile encapsulation plant shield door being ajar resulting in shine path to operator
- Control system, mechanical or power failure or operator error resulting in the mobile encapsulation plant shield door impacting a package and damaging the shield door
- Control system, mechanical failure or operator error resulting in a package impacting the mobile encapsulation plant shield door
- Control failure, blockage or loss of services resulting in overpack door being open
- Failure to decontaminate pipe after a campaign
- Pipe not sufficiently shielded

The first five faults have the potential to result in an operator receiving an increased external dose uptake from an unshielded package and are considered to bound the dose rate from a pipe.

The unmitigated dose from an unshielded package has been calculated as 23.6 mSv (2.36 rem) to an operator standing 2 m (6.6 ft) from a 3 m^3 (105.9 ft^3) box for 30 minutes (Ref. 26.8, Appendix B). A member of the public 280 m (918.6 ft) from the box would receive 0.1 mSv (0.01 rem) box only if exposed for 140 hours. This is judged to be an incredibly long time, giving the maximum credible dose as <0.1 mSv (0.01 rem).

A number of faults have been identified that have the potential to result in an increased external dose uptake from the ILW Store, which include:

- Control failure or operator error results in both ILW Store shield doors being open.
- ILW store external shield door closes when operator is in the import/export area.
- Control failure or operator error results in impact between ILW store external shield door and overpack/transporter
- Control failure or operator error results in transporter impacting with ILW store
- Control failure or operator error results in ILW shield door error

- Control failure or operator error results in package impacted by overpack or ILW store inner shield door

The unmitigated dose uptake from the unshielded contents of the ILW store has been calculated as 274 mSv (27.4 rem) to the operator and 1.6 mSv (0.16 rem) to a member of the public (Ref. 26.8, Appendix B).

26.9.2.2 Response to External Hazards

A number of preliminary safety reviews, such as HAZOP studies and modern standards reviews, have been carried out to establish the safety issues applicable to the ILW store. These safety reviews have considered the hazards related to and the operability of the store and the seismic aspects of the building (Ref. 26.9, Section 4.1). HAZOP studies were performed to underpin the design undertaken to establish the requirements for the ILW store. Some of the features identified during the HAZOP studies are site-specific, and these will be carried forward for full resolution during the detailed design associated with a specific site.

The external hazards identified during the HAZOP 1 study (Ref. 26.46) included:

- Seismic events
- Extreme weather
- Aircraft crash

Assessments have been carried out of the consequences associated with the design basis earthquake for the ILW store. These assessments concluded that the ILW store does not need to be seismically qualified from a radiological consequence perspective as the unmitigated public offsite doses are less than 1 mSv (0.1 rem). Notwithstanding the above, ALARP arrangements must be implemented. Therefore, if it is reasonably practicable to introduce seismic withstand attributes to the design and construction of the ILW store, then it would be prudent to do so (Ref. 26.8, Section 6.8.3).

Chapter 16 considers whether the design-basis hazards such as wind and snow loading of the ILW store would lead to acceptable behaviour of the generic design in a general UK location. However, owing to the generic nature of the design and the unknown location at which the AP1000 reactor will be constructed, it is not possible to design the ILW store to take account of site-specific extreme weather requirements (Ref. 26.8, Section 6.8.3).

The hazards and risks represented by potential aircraft crashes will be site-specific and dependent on the frequencies of aircraft crashes for different categories of aircraft (light aircraft, helicopters, small transport, large transport, and military combat aircraft). However, given that the public consequences of collapse of the ILW store are below 1 mSv (0.1 rem) (as assessed for the seismic event), it is anticipated that the consequences of an aircraft crash will also be below 1 mSv (0.1 rem) and will not require aircraft impact withstand attributes to be incorporated into the design (Ref. 26.8, Section 6.8.3).

26.9.2.3 Response to Internal Hazards

The auxiliary building will be served by two forced ventilation systems, the containment air filtration system and the radiologically controlled area ventilation system. These systems will control environmental parameters, such as temperature, pressure, and airborne contamination within the building. These systems will be provided with systems to monitor airborne radioactivity and alarms (Ref. 26.1, Sections 3.3.2.2 and 3.3.3).

In addition to this, the auxiliary building will contain radioactive liquid tanks from the WLS (Ref. 26.1, Section 2.9.5.2). Adequate provisions have been made to provide warning of potential overflows through high-level alarms. The consequences of any overflow or leakage are mitigated by the provision of floor drains grouted into the surrounding concrete to ensure that any overflow or leakage will be collected into the building sump, and by sealing surfaces to prevent the uptake of contamination (Ref. 26.1, Sections 2.9.5.2 and 2.9.5.4).

The ILW store will have its own independent ventilation plant. This plant will provide HVAC. The ventilation system design will be based on well-established principles, such as air cascade systems where appropriate, to minimise the possibility of back diffusion of contamination. A list of key assumptions relating to the in-vault environmental conditions will be derived for validation with RWM. This will include identification of the need (or otherwise) for dehumidification and removal of chlorides (given potential coastal locations). The design of the ventilation system will need to include provision for the management of heat generated from stored waste packages (although this is expected to be small, if not negligible) in addition to other heat loads, such as those from plant and equipment. Ventilation will be supplied at low level via a plenum and extracted at high level from the opposite end of the vault. The store will have inlet and outlet HEPA filters in series to remove radioactive particulates present in the ILW building atmosphere. The ventilation system will be consistent with the radiological classification of areas required for the building (Ref. 26.9, Section 3.8).

The generation of effluents arising from ILW store operations will be assessed throughout the design period and reduced or eliminated as far as possible. At a minimum, ventilation stack monitoring systems and associated upstream monitoring systems for ventilation systems will be required. Liquid effluent requirements will be similarly assessed. Should it be determined that decontamination processes are required within the store then “dry” methods (such as swabbing) will be used, thus eliminating liquid effluents (Ref. 26.9, Section 3.4.7.14).

There is the potential for fires to occur within the auxiliary building or the ILW store. In addition there is a fire hazard during transfer of the ILW packages from the auxiliary building to the ILW store. A fire within the auxiliary building has the potential to arise from the following faults:

- Mobile encapsulation plant engine failure
- Electrical fault in the mobile encapsulation plant

In the worst case, it is considered that there is the potential for a single ungrouted package within the mobile encapsulation plant to be consumed within a fire. The release fractions applicable to the release from a drum are specific to the properties of the element being released. The dose due to the release of the activity from a package during a fire that breaches the package is 46.3 mSv (4.6 rem) (public) and 6.83 Sv (683 rem) (worker exposed for 1 minute) (Ref. 26.8, Appendix B).

Assuming that the mobile encapsulation plant and the building both provide a decontamination factor of 10, then the calculated consequences of a fire in the auxiliary building are:

- Public = 46.3/100 = 0.46 mSv (0.046 rem)
- Worker = 6.83 /10 = 0.68 Sv (68 rem)

It should be noted that these consequences are pessimistic, as they assume that the package will fail, resulting in a significant release of activity (Ref. 26.8, Section 6.8.2).

A fire may occur in the ILW store due to a transport engine failure or an electrical failure. The potential for a fire that consumes the entire ILW store inventory was considered and dismissed as not being credible based on the lack of potential ignition sources and any significant flammable inventory and the provision of fire resistant electrical systems. The worst credible consequences therefore arise from a fire involving a single ILW package, which are the same as those calculated above for the auxiliary building, i.e., 0.46 mSv (0.046 rem) (public) and 0.68 Sv (68 rem) (worker) (Ref. 26.8, Section 6.8.2).

An addressable multi-zone fire detection and alarm will be installed throughout the occupied part of the ILW store building. Monitoring devices shall consist of, but not be limited to, smoke and heat detectors, manual call points and connected to visual/audible alarms (Ref. 26.9, Section 3.7.9). The fire detection system will be designed to meet the requirements of BS 5839 Fire Detection and Alarm Systems (Ref. 26.47). Requirements for a permanently installed fire suppression system will be reviewed during the detailed design phase. Radiometric alarms will be provided for both high gamma and instrument fault conditions (Ref. 26.9, Section 3.7.19). Area gamma monitors and combined alpha/beta monitors will be connected to annunciators located adjacent to the main personnel access door into the radwaste or ILW store buildings. Alarms will be provided for both high gamma and instrument fault conditions. Alarms will be repeated in the main control room (MCR) (Ref. 26.9, Section 3.7.17.2).

26.9.3 External and Internal Hazards for High-Level Waste

26.9.3.1 Response to External Hazards

The spent fuel store for the generic site is a seismically qualified facility and comprises spent fuel flasks, flask loading equipment within the AP1000 plant, a suitable transport vehicle, and below-ground storage cells (Ref. 26.1, Section 2.3.6.3).

26.9.3.2 Response to Internal Hazards

As previously mentioned in Section 26.8.5.3 of this chapter, the HI-STORM 100U system consists of three primary components.

HI-STORM 100U Underground Vertical Ventilated Module

The VVM provides for storage of an MPC in a vertical configuration inside a subterranean cylindrical cavity entirely below the top-of-grade (Ref. 26.1, Figure 3.5-18a). The principal function of the VVM structure is to provide the biological shield and cooling facility (Ref. 26.1, Section 3.5.8.3).

The MPC storage cavity is defined by the cavity enclosure container (CEC), consisting of the container shell integrally welded to a bottom plate. The CEC is a closed bottom, open top, thick-walled cylindrical vessel, which has no penetrations or openings. Thus, groundwater has no path for intrusion into the interior space of the MPC storage cavity.

Corrosion mitigation measures commensurate with site-specific conditions are implemented on below-grade external surfaces of the CEC. All external and internal surfaces of the VVM are coated with an appropriate surface preservative. An optional concrete encasement around the coated external surface of the CEC may be added to control the pH at the CEC-to-subgrade interface. A corrosion allowance equal to 3 mm (0.12 inch) on the external surfaces of the VVM in contact with the subgrade is nevertheless assumed in the structural evaluations.

The closure lid is a steel structure filled with shielding concrete and incorporates a specially designed air ventilation system (Ref. 26.1, Section 3.5.8.3).

Multipurpose Canister

The MPC and HI-TRAC in the HI-STORM 100U system are identical to those in the Holtec aboveground system that has been in use for several years.

The MPC is a single package equally suitable for onsite storage, transport, and permanent disposal in a future repository. The MPC is constructed entirely of stainless steel alloy materials with the exception of the Metamic, a fixed neutron absorber, which is contained within the canister for criticality control. The fuel assembly basket contained within the MPC is a honeycomb multi-flanged plate weldment that forms the square fuel cells in the basket. There is complete edge-to-edge continuity between the continuous cells that provides an uninterrupted heat transmission path, making the MPC an effective heat-rejection device.

The top end of the Holtec MPC uses a closure system that includes a lid equipped with vent and drain ports used to remove air and water and to backfill the canister with helium (Figure 26-15a). A closure ring provides a redundant confinement boundary for the MPC lid. The vent and drain ports are covered, helium leak checked, and seal-welded before installing the closure ring. The closure ring is a circular ring that is edge welded to the canister outer shell and lid (Figure 26-15b). The MPC lid provides sufficient structural capability to permit the loaded MPC to be lifted by threaded holes in the MPC lid.

The heat from the fuel stored in the core region of the basket is removed by the thermosiphon (circulatory) action (Figure 26-10). As a result, high-heat-rate fuel[5] can be placed in the core region, surrounded by the cooler (and older) fuel in the periphery. This approach, known as "regionalised" storage, is extremely effective in mitigating the dose emitted from a basket in the lateral direction. The effectiveness of regionalised storage in reducing dose derives from the fact that almost 95 percent of the dose from the basket comes from the peripheral fuel; the inner region fuel contributes very little to the dose (Ref. 26.1, Section 3.5.8.3).

HI-TRAC Transfer Cask, which Holds the MPC during Loading Operations

HI-TRAC is the acronym for Holtec International transfer cask or "shuttle cask" for HI-STORM 100U. HI-TRAC is a slim cylindrical cask with removable bottom and top lids. HI-TRAC can be mounted on top of a HI-STORM 100U overpack to deliver or retrieve an MPC (Figure 26-15c and Figure 26-15d). HI-TRAC is a heavy-walled steel and lead cylinder with a water jacket attached to the exterior of the vessel. The main structural function of HI-TRAC is provided by carbon steel. Water and lead provide the main neutron and gamma shielding functions, respectively (Ref. 26.1, Section 3.5.8.3).

26.10 RECORDS

Good records of the waste characteristics, preserved for whatever timescale is necessary for a particular waste stream or package, will ensure that the waste can be managed safely in the future. The office for nuclear regulation (ONR) requires licencees to make arrangements for recording and preserving all the necessary information (Ref. 26.49).

5. The gamma radiation emitted is approximately proportional to the heat emission rate from the fuel.

The RWM of the NDA has issued a Work Instruction (Ref. 26.50) on generating assessments of the nature and quantity of waste streams. This document includes a description of how to assess the radiochemical and chemical data that should be recorded for each waste stream. It is supported by a report (Ref. 26.51) presenting sets of radionuclide concentrations, known as guidance quantities, that waste producers may use to assess the requirements for recording radionuclide data associated with their wastes. An additional document (Ref. 26.52) gives guidance on assessing which assay methods may be capable of delivering suitable inventory data for radionuclides of interest.

Compliance with the assessments and recommendations made during the NDA RWM LoC process will ensure that the information required now and in the future for the safe management of radioactive waste is recorded.

Waste package inventory records will be completed to maintain an inventory record of each waste package and its location within the ILW store vault (Ref. 26.1, Section 3.5.8.2). These waste package reports will be sent with the ILW packages to the ILW repository (GDF), when it becomes available within the UK. The need for a waste tracking system will be assessed during the detailed design associated with a specific site (Ref. 26.9, Section 3.4.7.13). This system, if needed, will ensure that the location of individual waste packages can be established. This tracking system shall also record data relating to the package, such as reference number, radiological inventory, and production date, in compliance with RWM requirements. The system shall be technology proof, in that any changes in technology shall be easily adopted without losses in data.

An example of the system that is presently used is the British Radwaste Information Management System (BRIMS) (Ref. 26.53). BRIMS is based on an Oracle database and is used by UK radwaste producers to record information about their wastes. In addition to recording the numerical information used to produce the UK Radioactive Waste Inventory (e.g., Ref. 26.54), BRIMS also records contextual information about waste streams.

LLW is planned to be recorded after being sorted, processed, and packaged (Ref. 26.9, Section 3.2.1.3).

26.11 CONCLUSIONS

This chapter of the PCSR provides evidence that:

- Westinghouse has produced an IWS to address the radioactive wastes and spent fuel produced by the AP1000 plant, which is appropriate for the assessment of a generic design.
- The wastes may be contained and cooled where necessary.
- Gaseous and liquid radwaste may be handled safely, with discharges that are ALARP.
- Solid radwastes may be handled safely.
- As far as can be ascertained during the GDA, all wastes are or will be disposable.
- BAT is used throughout.

26.12 REFERENCES

26.1 Westinghouse Report UKP-GW-GL-790, Rev. 6, "UK AP1000 Environment Report", January 2017.

26.2 Westinghouse Report UKP-GW-GL-054, Rev. 1, "UK AP1000 Integrated Waste Strategy", March 2011.

26.3 Westinghouse Report UKP-GW-GL-055, Rev. 2, "UK AP1000 Radioactive Waste Management Case Evidence Report for Intermediate Level Waste", March 2011.

26.4 Westinghouse Report UKP-GW-GL-056, Rev. 2, "UK AP1000 Radioactive Waste Management Case Evidence Report for High Level Waste", March 2011.

26.5 Westinghouse Report UKP-GW-GL-026, Rev. 2, "AP1000 Nuclear Power Plant BAT Assessment", March 2011.

26.6 NDA/RWMD/060, "Feasibility Studies Exploring Options for Storage, Transport and Disposal of Spent Fuel from New Nuclear Power Stations", Nuclear Decommissioning Authority, November 2010.

26.7 Nuclear Decommissioning Authority, "Insight into Decommissioning", Page 6, Issue 4, 2010.

26.8 Westinghouse Report UKP-GW-GL-053, Rev. 1, "UK AP1000 Radwaste Preliminary Safety Statement", February 2010.

26.9 Westinghouse Report UKP-GW-GL-027, Rev. 2, "Radioactive Waste Arisings, Management and Disposal", March 2011.

26.10 Westinghouse Report UKP-GW-GL-057, Rev. 0, "UK AP1000 NDA Data Sheet Submission", February 2010.

26.11 Westinghouse Report UKP-GW-GL-004, Rev. 1, "Process Mass Balance for AP1000 Solid Waste", March 2011.

26.12 Westinghouse Report UKP-GW-GL-017, Rev. 1, "UK AP1000 Radwaste Building Plant Layout", March 2011.

26.13 Westinghouse Report UKP-GW-GL-018, Rev. 0, "UK AP1000 Radwaste Treatment Plant Site Layout", July 2009.

26.14 Westinghouse Report UKP-GW-GL-039, Rev. 0, "Radwaste Treatment Options Study Report", June 2009.

26.15 Nuclear Decommissioning Authority Report LL10568935, "Generic Design Assessment: Summary of Disposability Assessment for Wastes and Spent Fuel Arising from Operation of the Westinghouse Advanced Passive Pressurised Water Reactor (AP1000)", 23 September 2009.

26.16 Westinghouse Report UKP-GW-GL-058, Rev. 0, "UK AP1000 D1 Form Submission", March 2010.

26.17 Westinghouse Report UKP-GW-GL-003, Rev. 0, "Solid Waste Activity Calculation from AP1000", April 2010.

26.18 Westinghouse Report UKP-GW-GL-028, Rev. 2, "Proposed Annual Limits for Radioactive Discharges", March 2011.

26.19 Westinghouse Report UKP-GW-GL-029, Rev. 0, "AP1000 Generic Design Measurement and Assessment of Discharges", February 2009.

26.20 Not used.

26.21 BS 5243:1975, "General principles for sampling airborne radioactive materials", British Standards Institution, September 1975.

26.22 Not used.

26.23 Not used.

26.24 Not used.

26.25 A. Griffith, et al., "Integrated Treatment and Storage Solutions for Solid Radioactive Waste at the Russian Shipyard near Polyarny", Proc. WM'02, 24–28 February 2002.

26.26 Michel Grave and Arthur Willis, "A History of Mobile Solidification in the UK", RWIN Meeting, University of Sheffield, UK, 19 July 2005.

26.27 5-A-015, "Form D1 Application: Licensed AP1000 Operator", LLW Repository Ltd, 9 September 2009.

26.28 Not Used.

26.29 Westinghouse Report APP-GW-GER-100, Rev. 0, "Decontamination Equipment Facilities Report", October 2011.

26.30 EPA-402-R-06-003, "Technology Reference Guide for Radiologically Contaminated Surfaces", US Environmental Protection Agency, 2006.

26.31 Nuclear Decommissioning Authority Document NXA/10897959, "Generic Design Assessment: Disposability Assessment of Wastes and Spent Fuel Arising from the Operation of the Westinghouse AP1000 Part 1, Main Report", 15 January 2010.

26.32 Health and Safety Executive, "The Control of Major Accident Hazards Regulations 2015, L111, Third edition, 2015", 2015.

26.33 Westinghouse Report APP-GW-GLN-098, Rev. 0, "AP1000 Standard Combined License Technical Report 98 'Compliance with 10CFR20.1406'", April 2007.

26.34 Regulatory Guide 4.21, "Minimization of Contamination and Radioactive Waste Generation: Life-Cycle Planning", US. Nuclear Regulatory Commission, June 2008.

26.35 Westinghouse Documents WCAP-10125-P-A and WCAP-10126-NP-A, "Extended Burnup Evaluation of Westinghouse Fuel", December 1985.

26.36 "UK Radioactive Higher Activity Waste Storage Review", Nuclear Decommissioning Authority, March 2009.

26.37 Kenneally, R. M. and Kessler, John H., "Behavior of Spent Fuel and Safety-Related Components in Dry Cask Storage Systems", August 2001.

26.38 Fact Sheet, "Dry Cask Storage of Spent Nuclear Fuel", US Nuclear Regulatory Commission.

26.39 "Conditions for Acceptance by LLW Repository Limited of Radioactive Waste for Disposal at the Low Level Waste Repository (CFA)", Issue 01/08, Nuclear Decommissioning Authority.

26.40 Westinghouse Report UKP-GW-GL-040, Rev. 0 "Pyros Code of Practice Conditions for Acceptance of Radioactive Waste", June 2009.

26.41 Westinghouse Report UKP-GW-GL-041, Rev. 0 "Pyros Request for Letter of Intent", June 2009.

26.42 Svensk Kärnbränslehantering AB, TR-06-21, "Initial State Report for the Safety Assessment SR-Can", October 2006.

26.43 Svensk Kärnbränslehantering AB Information Brochure, "Encapsulation, When, Where, How and Why?", January 2008.

26.44 Svensk Kärnbränslehantering AB, TR-06-23 "Climate and Climate-Related Issues for the Safety Assessment SR-Can", November 2006.

26.45 Svensk Kärnbränslehantering AB, TR-06-09 "Long-Term Safety for KBS-3 Repositories at Forsmark and Laxemar – A First Evaluation Main Report of the SR-Can Project", October 2006.

26.46 Westinghouse Report UKP-GW-GL-052, Rev. 1, "UK AP1000 Radwaste Process Hazard Study 1 Report (HAZOP)", February 2010.

26.47 British Standards Institution Report BS 5839-1:2002+A2:2008, "Fire Detection and Fire Alarm Systems for Buildings. Code of Practice for System Design, Installation, Commissioning and Maintenance", October 2002.

26.48 N/078, "Generic Transport Safety Assessment: Volume 2 – Appendices", Nirex, July 2003.

26.49 "Guidance for Inspectors on the Management of Radioactive Materials and Radioactive Waste on Nuclear Licensed Sites", Health and Safety Executive, Nuclear Safety Directorate, 13 March 2001.

26.50 Nuclear Decommissioning Authority Report RWPR60-WI02, "Radioactive Waste Management – Definition of Nature & Quantities of Waste and Preparation of Waste Package Data Summaries", December 2008.

26.51 N/105, "The Identification of Radionuclides Relevant to Long-Term Waste Management in the United Kingdom", Nirex, November 2004.

26.52 Nuclear Decommissioning Authority Report RWPR60-WI08, "Radioactive Waste Management – Status Report on Data Recording Proposals", December 2008.

26.53 Nuclear Decommissioning Authority Report LL6257831, "The British Radwaste Information Management System (BRIMS) – Meeting the Challenges of the 21st Century", 2005.

26.54 DEFRA/RAS/08.002, NDA/RWMD/004, "The 2007 UK Radioactive Waste Inventory", UK Department for Environment, Food and Rural Affairs, March 2008.

26.55 Westinghouse Report UKP-GW-GL-084, Rev. 0, "UK AP1000 Decontamination Considerations", March 2011.

26.56 Westinghouse Report UKP-GW-GL-085, Rev. 0, "Long Term Storage of AP1000 ILW and Spent Fuel in the UK", March 2011.

Table 26-1. Assumptions and Exclusions for the Integrated Waste Strategy (Ref. 26.2, Table 4-1)

Item	Description
Assumption 1	National LLWR is available within 2 years of site operations commencing
Assumption 2	National ILW repository will be available before the end of the onsite ILW store building design period (before the end of this century)
Assumption 3	National HLW (spent fuel) repository will be available before the end of the design period of the onsite spent fuel store (before the end of this century)
Assumption 4	No major changes in legislation during the operational period of the AP1000 and the associated onsite waste facilities.
Assumption 5	Planning permissions for the spent fuel store and the extensions to the ILW store will be granted.
Assumption 6	No major restrictive changes to discharge limits during the operational period of the AP1000
Exclusion 1	External hazards and events that could cause major disruptions other than those already assumed in the safety case
Exclusion 2	Post-closure monitoring, requirements are not specified here.
Exclusion 3	Post-closure management, requirements are not specified here.
Exclusion 4	Variations in discharge

Table 26-2. Calculated Annual Limits for Air Emissions (Ref. 26.1, Table 6.1-5)

Air Effluent Input	Representative 12-month Plant Discharge (TBq/y)	Worst-Case Plant Annual Discharges (TBq/y)	Calculated Annual Limit (TBq/y)
Radioiodines(1)	5.95E-04	9.82E-04	1E-03
Noble gases(2)	8.099	13.363	13
Tritium	1.867	3.081	3
Carbon-14	0.638	1.053	1
Argon-41	1.323	2.182	2
Cobalt-60	3.22E-06	5.32E-06	5E-06
Krypton-85	4.070	6.716	7
Strontium-90	4.44E-07	7.33E-07	7E-07
Iodine-131	2.07E-04	3.42E-04	3E-04
Xenon-131m	1.76	2.91	3
Xenon-133	1.335	2.203	2
Caesium-137	1.33E-06	2.20E-06	2E-06
Other particulates	1.22E-05	2.01E-05	2E-05
Total beta particulate(3)	1.72E-05	2.84E-05	3E-05
Total	11.928	19.681	20

Notes:

1. Radioiodines include I-131 and I-133.
2. Noble gases include Kr-85m, Kr-85, Kr-87, Kr-88, Kr-85, Xe-131m, Xe-133m, Xe-133, Xe-135m, Xe-135, Xe-137, Xe-138.
3. Total beta particulate includes Co-60 + Sr-90 + Cs-137 + other particulates.

Table 26-3. Calculated Annual Limits for Liquid Emissions (Ref. 26.1, Table 6.1-6)

Liquid Effluent Input	Representative 12-month Plant Discharge (TBq/y)	Worst-Case Plant Annual Discharges (TBq/y)	Calculated Annual Limit (TBq/y)
Tritium	35.09	57.90	60
Non-tritium	7.70E-03	1.27E-02	1E-02
Carbon-14	4.42E-03	7.30E-03	7E-03
Iron-55	6.42E-04	1.06E-03	1E-03
Cobalt-58	5.44E-04	8.97E-04	9E-04
Cobalt-60	3.01E-04	4.97E-04	5E-04
Nickel-63	6.91E-04	1.14E-03	1E-03
Strontium-90	3.24E-07	5.35E-07	5E-07
Caesium-137	3.01E-05	4.97E-05	5E-05
Plutonium-241	1.08E-07	1.78E-07	2E-07
Other isotopes(1)	1.07E-03	1.76E-03	2E-03
Total	35.104	57.922	60

Note:

1. Other isotopes = Non-tritium isotopes – (C-14+ Fe-55+Co-58+Co-60+Ni-63+Sr-90+Cs-137+Pu-241).

Table 26-4. Proposed Annual Discharge Limits for AP1000 Plant (Ref. 26.18, Table 7.1)

Radioisotope	Calculated Annual Limit (TBq/y)	Proposed Annual Limit (TBq/y)
Air Emission		
Radioiodines	1E-03	1E-03
Noble gases	13	13
Tritium	3	3
Carbon-14	1	1
Argon-41	2	2
Cobalt-60	5E-06	–
Krypton-85	7	–
Strontium-90	7E-07	–
Iodine-131	3E-04	3E-04
Xenon-133	2	–
Cesium-137	2E-06	–
Other particulates	2E-05	–
Beta particulates	3E-05	3E-05
Liquid Discharge		
Tritium	60	60
Non-tritium	1E–02	–
Carbon-14	7E–03	7E–03
Iron-55	1E–03	–
Cobalt-58	9E–04	–
Cobalt-60	5E–04	–
Nickel-63	1E–03	–
Strontium-90	5E–07	–
Cesium-137	5E–05	–
Plutonium-241	2E–07	–
Other isotopes	2E–03	–
All isotopes without other limits	5E–03	5E–03

Table 26-5. Predicted Monthly Air Radiation Emissions During 18-month Fuel Cycle (Ref. 26.1, Table 6.1-3)

Month	Predicted Monthly Air Radiation Discharges (TBq)													
	Radio Iodines	Noble Gases	Tritium	C-14	Ar-41	Co-60	Kr-85	Sr-90	I-131	Xe-131m	Xe-133	Cs-137	Other Particulate	Total
1	4.96E-05	0.298	0.132	0.045	0.093	2.69E-07	0.081	3.70E-08	1.73E-05	0.0513	0.090	1.11E-07	1.02E-06	0.568
2	4.96E-05	0.305	0.132	0.045	0.094	2.69E-07	0.085	3.70E-08	1.73E-05	0.0528	0.091	1.11E-07	1.02E-06	0.575
3	4.96E-05	0.312	0.132	0.045	0.094	2.69E-07	0.090	3.70E-08	1.73E-05	0.0546	0.091	1.11E-07	1.02E-06	0.583
4	4.96E-05	0.320	0.133	0.046	0.094	2.69E-07	0.095	3.70E-08	1.73E-05	0.0566	0.091	1.11E-07	1.02E-06	0.592
5	4.96E-05	0.329	0.134	0.046	0.095	2.69E-07	0.101	3.70E-08	1.73E-05	0.0589	0.092	1.11E-07	1.02E-06	0.602
6	4.96E-05	0.339	0.134	0.046	0.095	2.69E-07	0.108	3.70E-08	1.73E-05	0.0616	0.093	1.11E-07	1.02E-06	0.614
7	4.96E-05	0.351	0.135	0.046	0.096	2.69E-07	0.117	3.70E-08	1.73E-05	0.0647	0.093	1.11E-07	1.02E-06	0.628
8	4.96E-05	0.366	0.136	0.046	0.096	2.69E-07	0.127	3.70E-08	1.73E-05	0.0683	0.094	1.11E-07	1.02E-06	0.644
9	4.96E-05	0.383	0.137	0.047	0.097	2.69E-07	0.138	3.70E-08	1.73E-05	0.0727	0.095	1.11E-07	1.02E-06	0.664
10	4.96E-05	0.404	0.138	0.047	0.098	2.69E-07	0.153	3.70E-08	1.73E-05	0.0780	0.096	1.11E-07	1.02E-06	0.687
11	4.96E-05	0.430	0.140	0.048	0.099	2.69E-07	0.171	3.70E-08	1.73E-05	0.0847	0.098	1.11E-07	1.02E-06	0.717
12	4.96E-05	0.463	0.142	0.048	0.101	2.69E-07	0.194	3.70E-08	1.73E-05	0.0932	0.100	1.11E-07	1.02E-06	0.755
13	4.96E-05	0.508	0.145	0.050	0.103	2.69E-07	0.224	3.70E-08	1.73E-05	0.105	0.102	1.11E-07	1.02E-06	0.805
14	4.96E-05	0.570	0.149	0.051	0.105	2.69E-07	0.267	3.70E-08	1.73E-05	0.120	0.105	1.11E-07	1.02E-06	0.875
15	4.96E-05	0.662	0.155	0.053	0.110	2.69E-07	0.330	3.70E-08	1.73E-05	0.144	0.111	1.11E-07	1.02E-06	0.980
16	4.96E-05	0.815	0.165	0.056	0.117	2.69E-07	0.437	3.70E-08	1.73E-05	0.183	0.119	1.11E-07	1.02E-06	1.152
17	4.96E-05	1.117	0.184	0.063	0.130	2.69E-07	0.644	3.70E-08	1.73E-05	0.259	0.136	1.11E-07	1.02E-06	1.494
18	4.96E-05	2.031	0.242	0.083	0.171	2.69E-07	1.269	3.70E-08	1.73E-05	0.492	0.187	1.11E-07	1.02E-06	2.527
Total	**8.93E-04**	**10.001**	**2.664**	**0.910**	**1.887**	**4.85E-06**	**4.662**	**6.66E-07**	**3.11E-04**	**2.1004**	**1.887**	**2.00E-06**	**1.83E-05**	**15.463**

Table 26-6. Comparison of Normalised Annual Gaseous and Liquid Radioactive Discharges from AP1000 Plant with Those from Other Nuclear Power Plants (Ref. 26.1, Tables 3.3.23 and 3.4-21)

Plant	Discharges GBq/y per GW(e)					
	AP1000	South Texas 1	Braidwood 1	Cook 1	Vogtle 1	Sizewell B
Gaseous discharges	10311	7692	561	12571	2184	70115
Liquid discharges	33374	46331	49094	44500	40450	50503
Total	43685	54023	49655	57071	42634	120618

Table 26-7. AP1000 Plant Estimated Operational Liquid Radwaste Arising from System Operations (Ref. 26.1, Table 3.4-1)

System	Waste Description	Waste Class	Physical/ Chemical Description	Normal Daily Volume (m^3)	Max. Daily Volume (m^3)	Volume for Life of Plant (m^3)	Radioactivity
BDS	Steam generator blowdown	LLW	Secondary-side coolant	4.22	42.24	2.22E+06	Included here as LLW but may be nonradioactive
CVS	Boron dilution near EOL	LLW	Borated reactor coolant	6	26	2.52E+02	100% reactor coolant
CVS	RCS heat up	LLW	Borated reactor coolant	85	170	4.08E+03	100% reactor coolant without radiogas
WLS	CVS shim bleed (liquid)	LLW	Diverted reactor coolant/dilute boric acid	1.65	2.94	4.17E+04	100% reactor coolant
WLS	Equipment leaks	LLW	Dilute boric acid	0.34	54.5	1.07E+04	100% reactor coolant
WLS	Floor drains (dirty wastes)	LLW	Dilute boric acid	4.54	21.8	1.01E+05	0.1% reactor coolant
WLS	Sampling-system drains	LLW	Dilute boric acid	0.76	3.79	1.73E+04	100% reactor coolant
WLS	Hand wash/ hot shower	LLW	Grey water	0.76	7.57	4.64E+04	0.037 MBq/m^3
WLS	Equipment and area decontamination	LLW	Detergent waste	0.15	1.51	9.28E+03	0.1% reactor coolant
WLS	Chemical waste	LLW	Spent samples containing analytical chemicals	0.03	0.05	7.10E+02	$\leq$ reactor coolant
WLS	Decontamination fluids	LLW	Liquid with decontamination chemicals	0.0023	0.0047	6.20E+01	37,000 MBq/m^3

Table 26-8. Assumed Decontamination Factors for Liquid Radwaste Ion Exchange Beds (Ref. 26.1, Table 3.4-4)

Resin Type/Component	Iodine	Cs/Rb	Other
Zeolite/deep bed filter(1)	1	100	1
Cation/waste ion exchanger 1	1	10	10
Mixed/waste ion exchanger 2	100	2(2)	100
Mixed/waste ion exchanger 2	10	10(2)	10(2)

Notes:

1. This component is not included in NUREG-0017. DFs are based upon "Reduction of Caesium and Cobalt Activity in Liquid Radwaste Processing Using Clinoptilolite Zeolite at Duke Power Company," by O.E. Ekechokwu, et al., Proc. Waste Management '92, Tucson, Arizona, March 1992, University of Arizona, Tucson.

2. Credit for this DF is not taken in determination of anticipated annual releases.

Table 26-9. Predicted Monthly Liquid Discharges of Radioisotopes During 18-month Fuel Cycle (Ref. 26.1, Table 6.1-4)

Month	Predicted Monthly Liquid Radiation Discharges (TBq)											
	Tritium	Non-Tritium	C-14	Fe-55	Co-58	Co-60	Ni-63	Sr-90	Cs-137	Pu-241	Other Isotopes	Total
1	2.473	1.43E-04	8.14E-05	1.20E-05	1.02E-05	5.62E-06	1.30E-05	5.96E-09	5.66E-07	1.99E-09	1.63E-05	2.473
2	2.481	1.52E-04	8.62E-05	1.27E-05	1.08E-05	5.96E-06	1.37E-05	6.33E-09	5.96E-07	2.11E-09	1.71E-05	2.481
3	2.489	1.61E-04	9.14E-05	1.35E-05	1.14E-05	6.33E-06	1.45E-05	6.70E-09	6.33E-07	2.23E-09	1.81E-05	2.489
4	2.498	1.71E-04	9.73E-05	1.44E-05	1.22E-05	6.73E-06	1.54E-05	7.14E-09	6.73E-07	2.38E-09	1.92E-05	2.499
5	2.509	1.83E-04	1.04E-04	1.54E-05	1.30E-05	7.18E-06	1.65E-05	7.66E-09	7.22E-07	2.55E-09	2.05E-05	2.509
6	2.522	1.97E-04	1.12E-04	1.65E-05	1.40E-05	7.73E-06	1.78E-05	8.25E-09	7.73E-07	2.75E-09	2.20E-05	2.522
7	2.536	2.13E-04	1.22E-04	1.78E-05	1.51E-05	8.36E-06	1.92E-05	8.92E-09	8.36E-07	2.97E-09	2.37E-05	2.537
8	2.554	2.32E-04	1.32E-04	1.94E-05	1.65E-05	9.10E-06	2.09E-05	9.73E-09	9.10E-07	3.24E-09	2.57E-05	2.554
9	2.574	2.55E-04	1.46E-04	2.13E-05	1.81E-05	9.99E-06	2.29E-05	1.07E-08	9.99E-07	3.56E-09	2.81E-05	2.574
10	2.599	2.83E-04	1.62E-04	2.36E-05	2.00E-05	1.11E-05	2.54E-05	1.18E-08	1.11E-06	3.96E-09	3.11E-05	2.600
11	2.631	3.17E-04	1.82E-04	2.65E-05	2.25E-05	1.24E-05	2.85E-05	1.33E-08	1.24E-06	4.44E-09	3.47E-05	2.631
12	2.671	3.61E-04	2.07E-04	3.02E-05	2.56E-05	1.42E-05	3.25E-05	1.52E-08	1.42E-06	5.07E-09	3.96E-05	2.671
13	2.724	4.22E-04	2.41E-04	3.51E-05	2.97E-05	1.65E-05	3.77E-05	1.77E-08	1.65E-06	5.88E-09	4.59E-05	2.724
14	2.798	5.03E-04	2.88E-04	4.18E-05	3.55E-05	1.96E-05	4.51E-05	2.12E-08	1.97E-06	7.07E-09	5.44E-05	2.799
15	2.909	6.25E-04	3.59E-04	5.22E-05	4.40E-05	2.45E-05	5.62E-05	2.63E-08	2.45E-06	8.77E-09	6.73E-05	2.909
16	3.092	8.25E-04	4.74E-04	6.88E-05	5.85E-05	3.23E-05	7.44E-05	3.49E-08	3.23E-06	1.16E-08	8.88E-05	3.092
17	3.453	1.22E-03	7.07E-04	1.02E-04	8.66E-05	4.81E-05	1.10E-04	5.18E-08	4.81E-06	1.72E-08	1.31E-04	3.455
18	4.548	2.43E-03	1.40E-03	2.03E-04	1.72E-04	9.51E-05	2.18E-04	1.03E-07	9.51E-06	3.43E-08	2.60E-04	4.550
Total	50.061	8.70E-03	5.00E-03	7.25E-04	6.14E-04	3.41E-04	8.33E-04	3.70E-07	3.42E-05	1.22E-07	9.44E-04	50.070

Table 26-10. Comparison of AP1000 Plant ILW/LLW Production Against Other UK PWR Plants (extracted from Ref. 26.1, Table 3.5-11)

Reactor Type	ILW and LLW (m^3 per GWy[e])
PWR	430(1)
AP1000	102(2)

Notes:

1. Volumes are for wastes packaged for long-term management based on the probable conditioning method and container type. Station operational and decommissioning wastes are included.
2. Estimated operational waste only.

Table 26-11. Summary of Main Radwaste Arisings from Decommissioned Process Equipment (Ref. 26.1, Table 3.5-10)

Waste Description	Waste Level	Envelope Volume (m^3)	Mass (tonnes)	Notes
Reactor vessel and pressuriser tanks	ILW	388	426	
Pumps – various	ILW	100	327	
Reactor system internals	ILW	*	146	*individual pieces
Process equipment internals – various	ILW	185	291	
Heat exchangers	ILW	9	10	
Filters – various	ILW	6	8	
Pressuriser heaters	ILW	0.05	0.16	
Waste from system decontamination operations (e.g., spent resins and spent filter cartridges)	ILW	~85	~102	Mass based on average density 1,200 kg/m^3
Steam generators/heat exchangers – various	LLW	1,493	1,281	
Reactor integrated head package	LLW	224	118	
Tanks	LLW	808	94	
Ion exchange systems	LLW	15.1	28	
Pumps	LLW	32	16	
Fasteners	LLW	4	15	
Insulation	LLW	22	8	
HVAC filters – various	LLW	35	8	
Adsorbers	LLW	7	4	
Small vessels	LLW	0.02	0.02	
Compacted dry active waste generated during decontamination operations	LLW	81	121	Mass based on average density 1,500 kg/m^3

Table 26-12. Activity Triggers for LLWR

Activity Group	Trigger for Total Activity (GBq)	Trigger for Specific Activity (GBq/t)	Expected Total Activity (GBq)	Expected Specific Activity (GBq/t)
Uranium	9.0E1	9.0E-2	0	0
Ra-226 and Th-232	9.0E0	9.0E-3	0	0
Other alpha	9.0E1	9.0E-2	3.0E-4	1.4E-5
Carbon-14	1.5E1	1.5E-2	3.0E-4	1.4E-5
Iodine-129	1.5E1	1.5E-2	0	0
Tritium	3.0E3	3.0E0	2.0E-4	8.5E-6
Cobalt-60	6.0E2	6.0E-1	1.3E-2	5.4E-4
Others(1)	4.5E3	4.5E0	2.1E-1	9.1E-3

Note:

1. "Others" also includes the cobalt-60 content of the waste stream.

Table 26-13. Summary of Main Solid Nonradioactive Waste Produced by AP1000 Plant (Ref. 26.1, Table 4.3-1)

Description of Waste Radioactive Waste Classification	Frequency	Normal Volume per Unit Frequency (m^3)	Volume per Life of Plant (m^3)
HVAC filters (fibreglass/metal)	various	various	5209
Battery (lead acid)	Once/20 y	360	700
Lube oil	Once/25 y	79.5	159
Reverse osmosis modules	Once/7 y	15.77	135.2
Electrodeionisation/reverse osmosis filter cartridges	Once/6 months	0.39	45.65
HVAC filters (charcoal)	Once/10y	4.86	29.12
Valve packing – compressible rigid plastic	Once/5 y	1.14	13.7
Electrodeionisation (resin/membrane module)	Once/12 y	1.34	6.68
Door/hatch gaskets (fibreglass cloth)	Once/60 y	1.16	1.16
Main feedwater pump seals (silicon carbide)	Once/5 y	0.056	0.68
Heat exchanger gaskets (neoprene)	Once/10 y	0.062	0.37

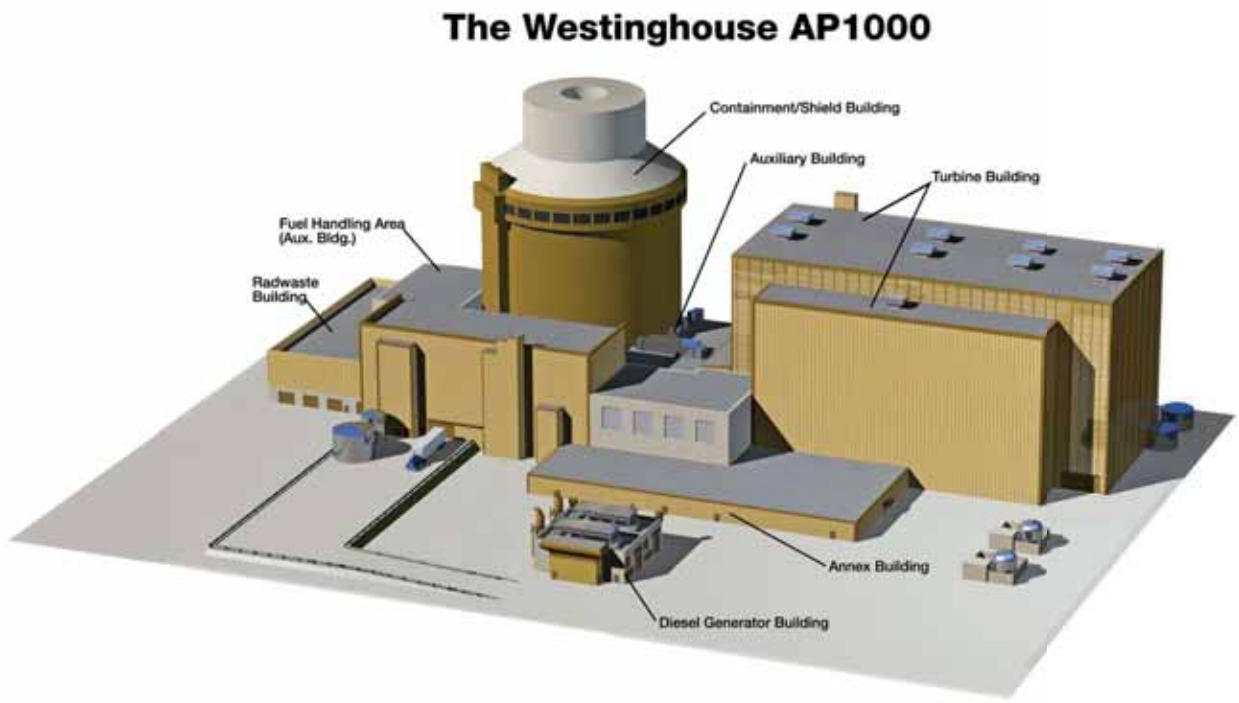


Figure 26-1. AP1000 Design Main Buildings (Ref. 26.2, Figure 2-1)

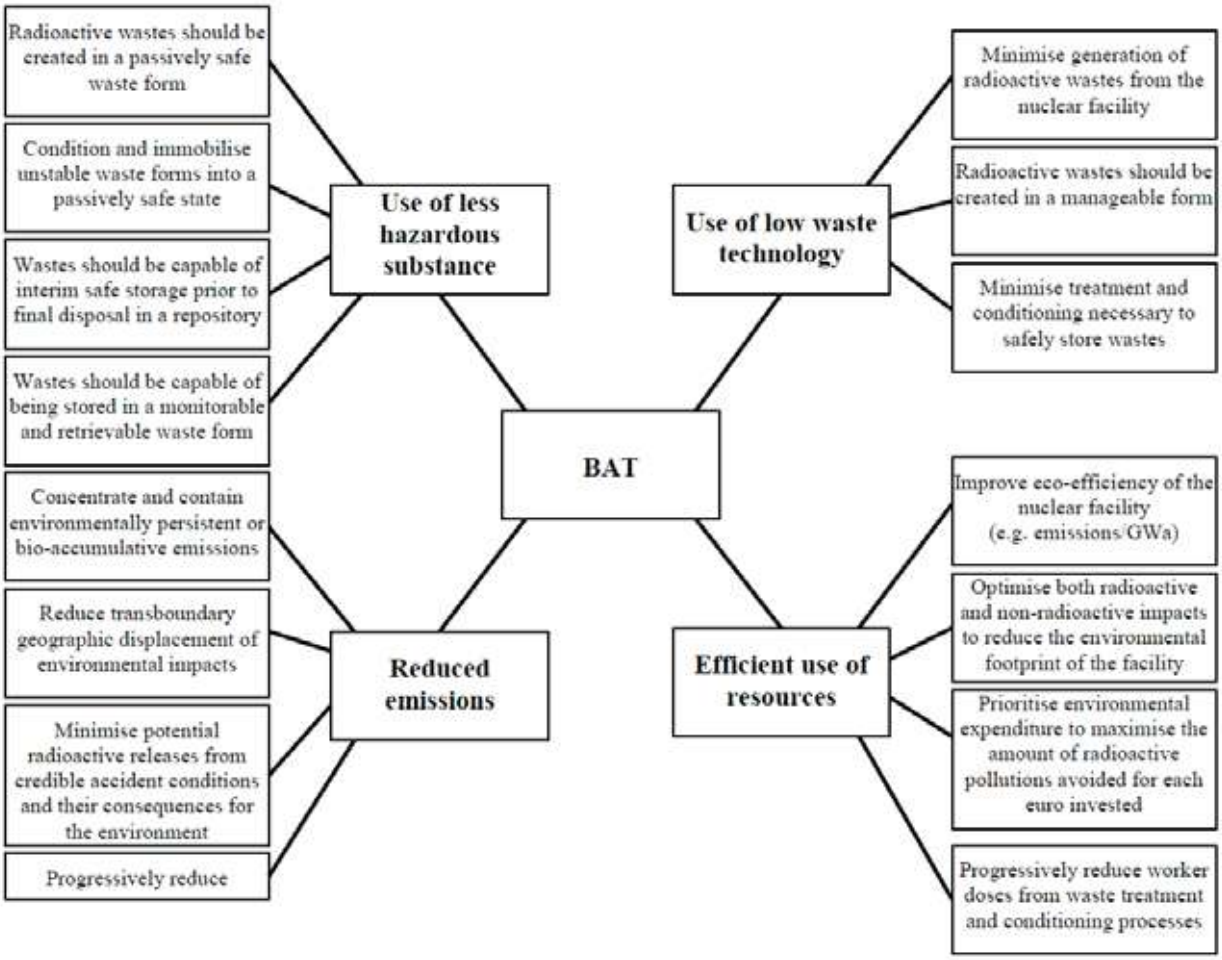


Figure 26-2. Nuclear BAT Management Factors for Optimisation of Releases from Nuclear Facilities (Ref. 26.1, Figure 3.1-2)

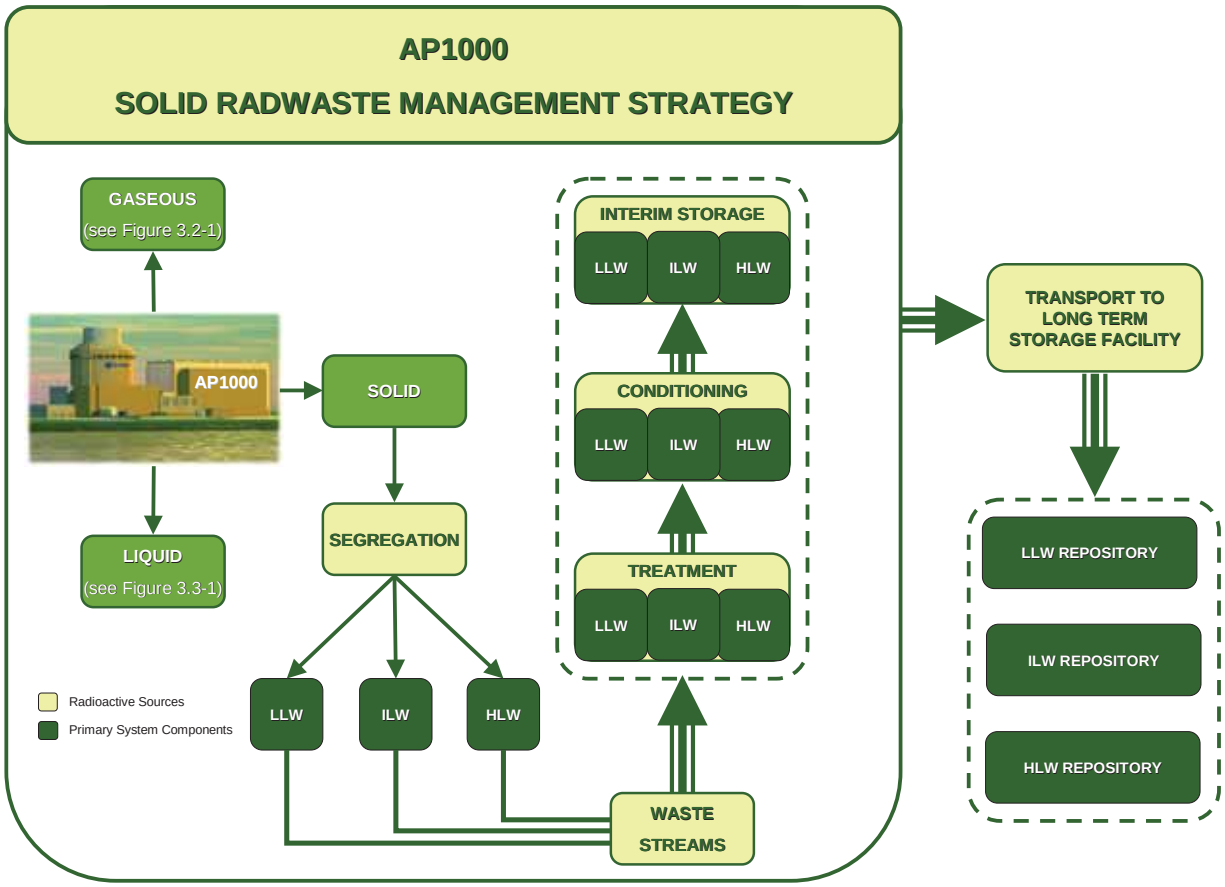


Figure 26-3. AP1000 Design Solid Radwaste Management Strategy (Ref. 26.1, Figure 3.5-1)

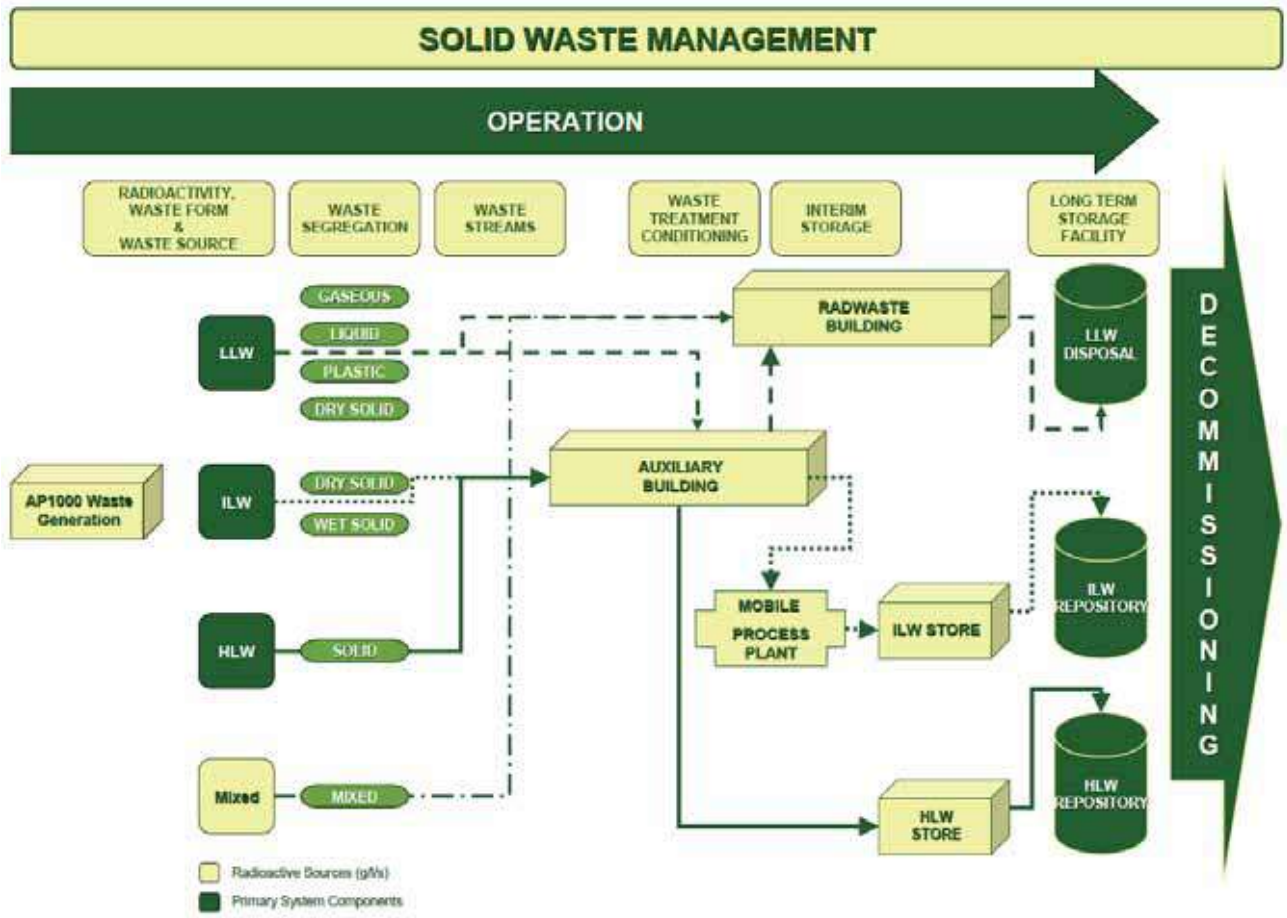


Figure 26-4. AP1000 Design Solid Waste Management (Ref. 26.1, Figure 3.5-2)

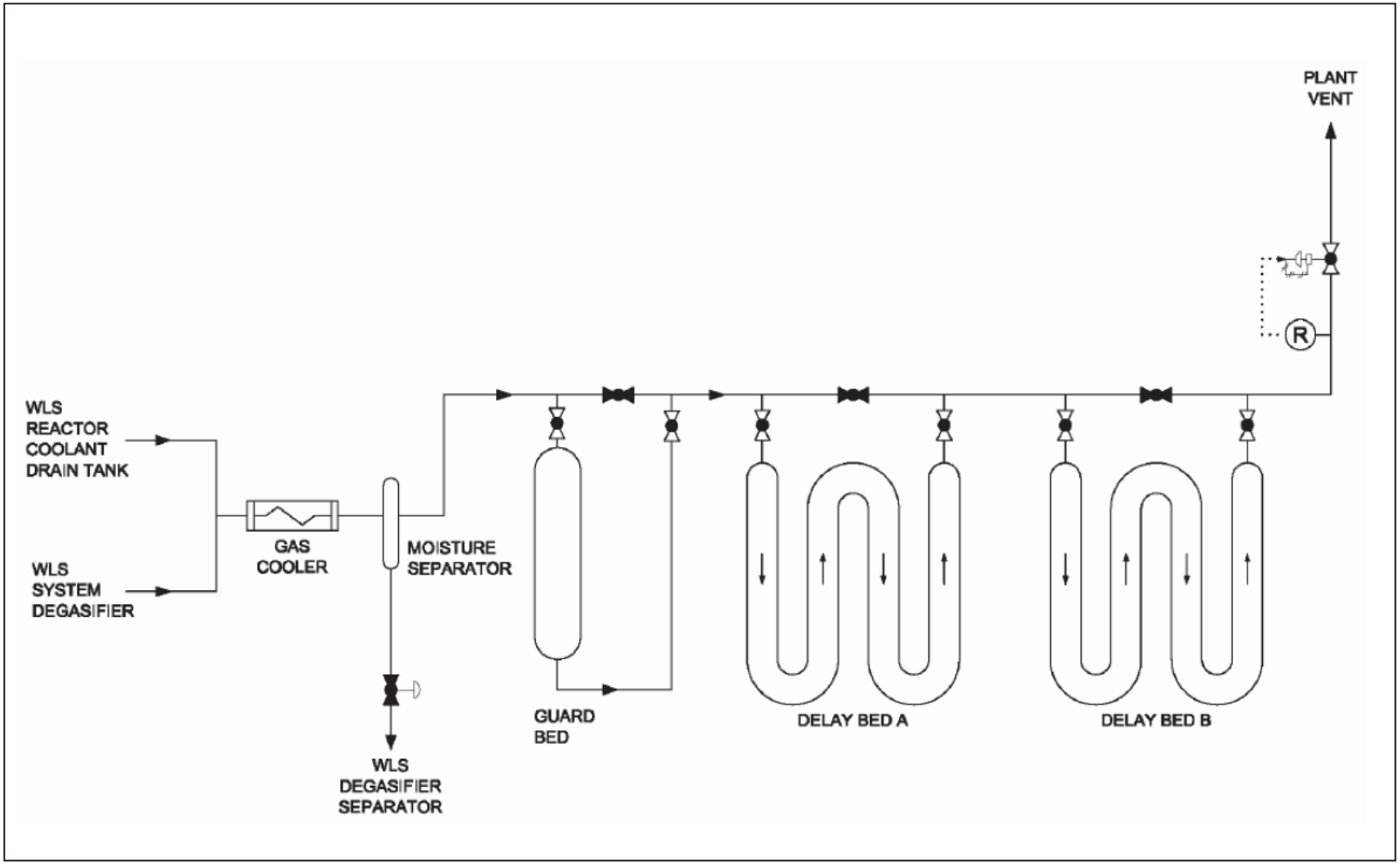


Figure 26-5. AP1000 Design Gaseous Radwaste System (Ref. 26.1, Figure 3.3-1)

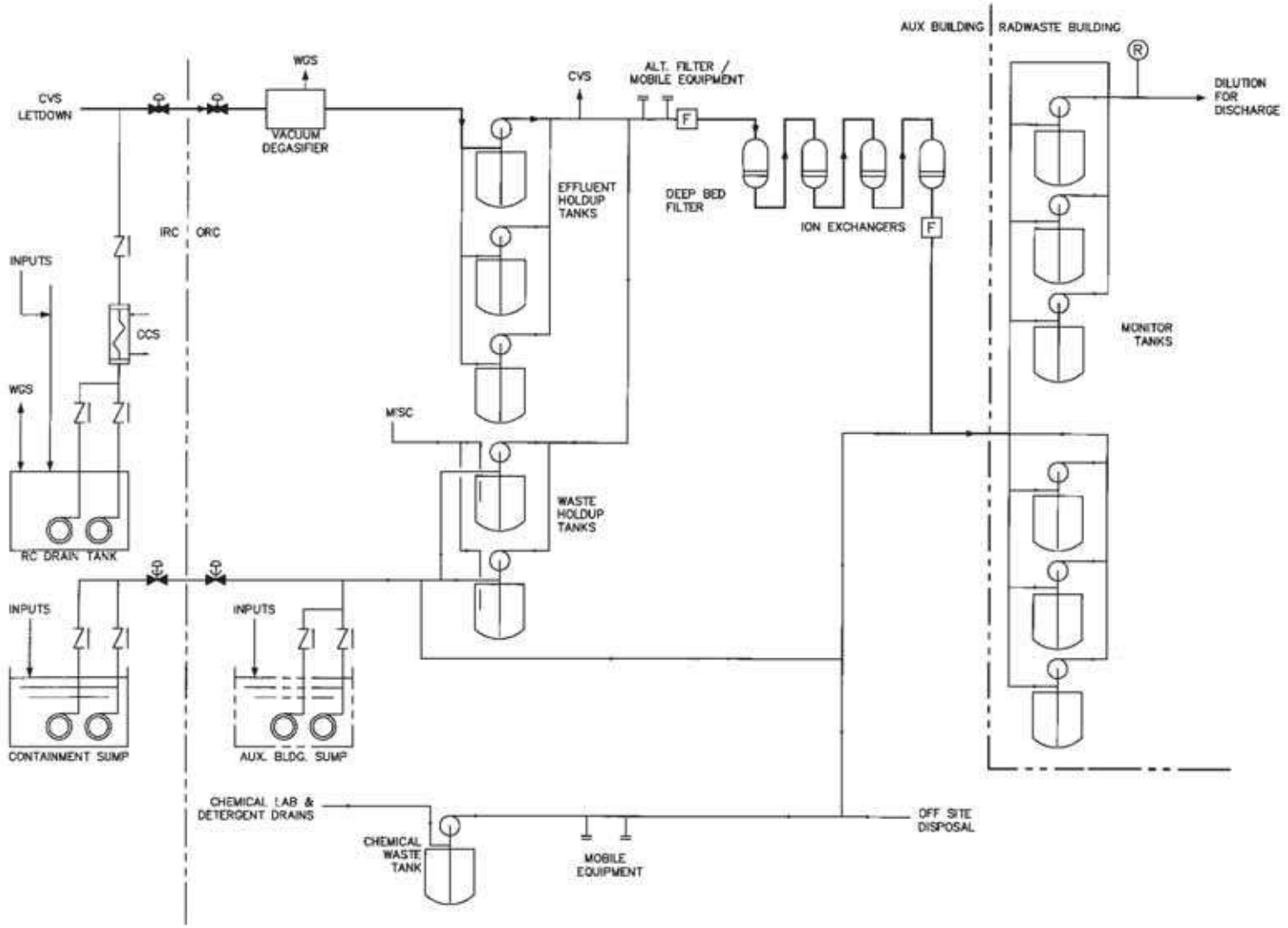


Figure 26-6. AP1000 Design Liquid Radwaste System (Ref. 26.1, Figure 3.4-1)

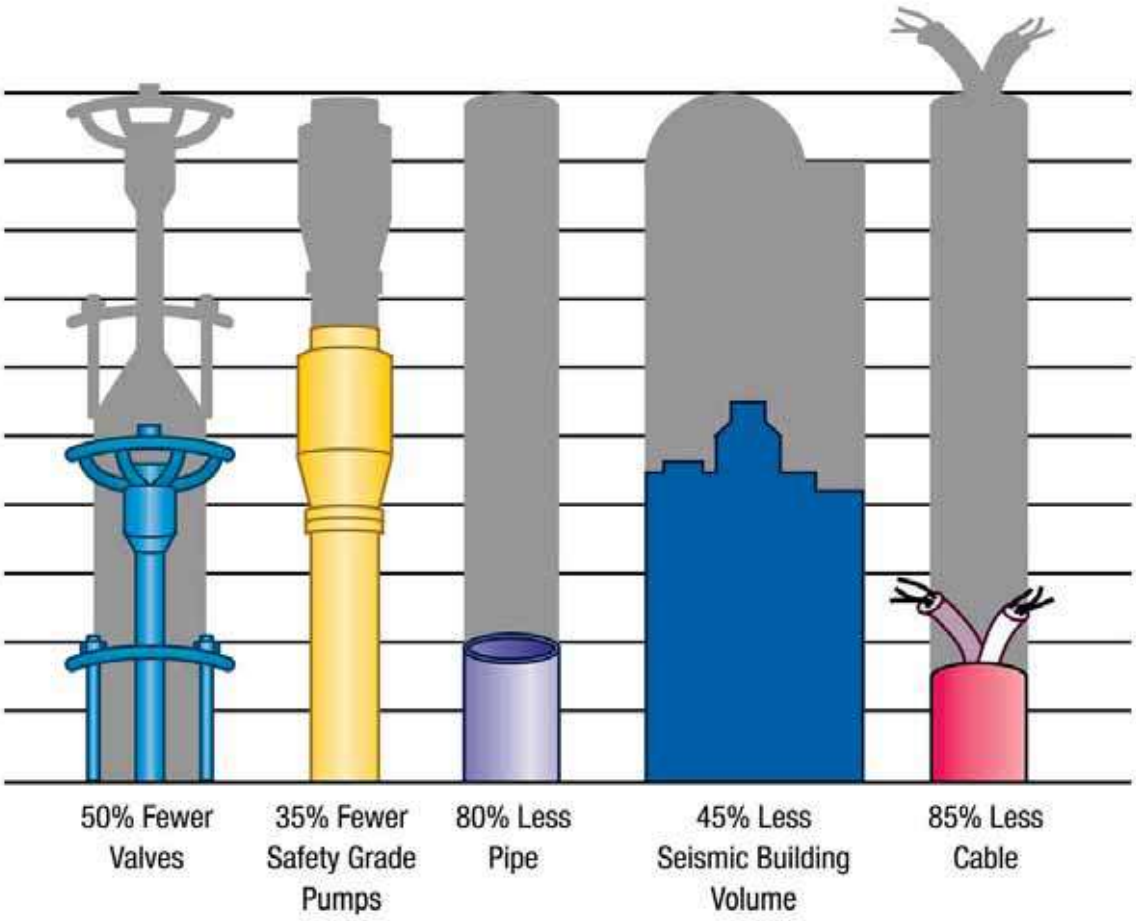


Figure 26-7. Minimisation of Equipment and Materials in the AP1000 Design (Ref. 26.2, Figure 3-2)

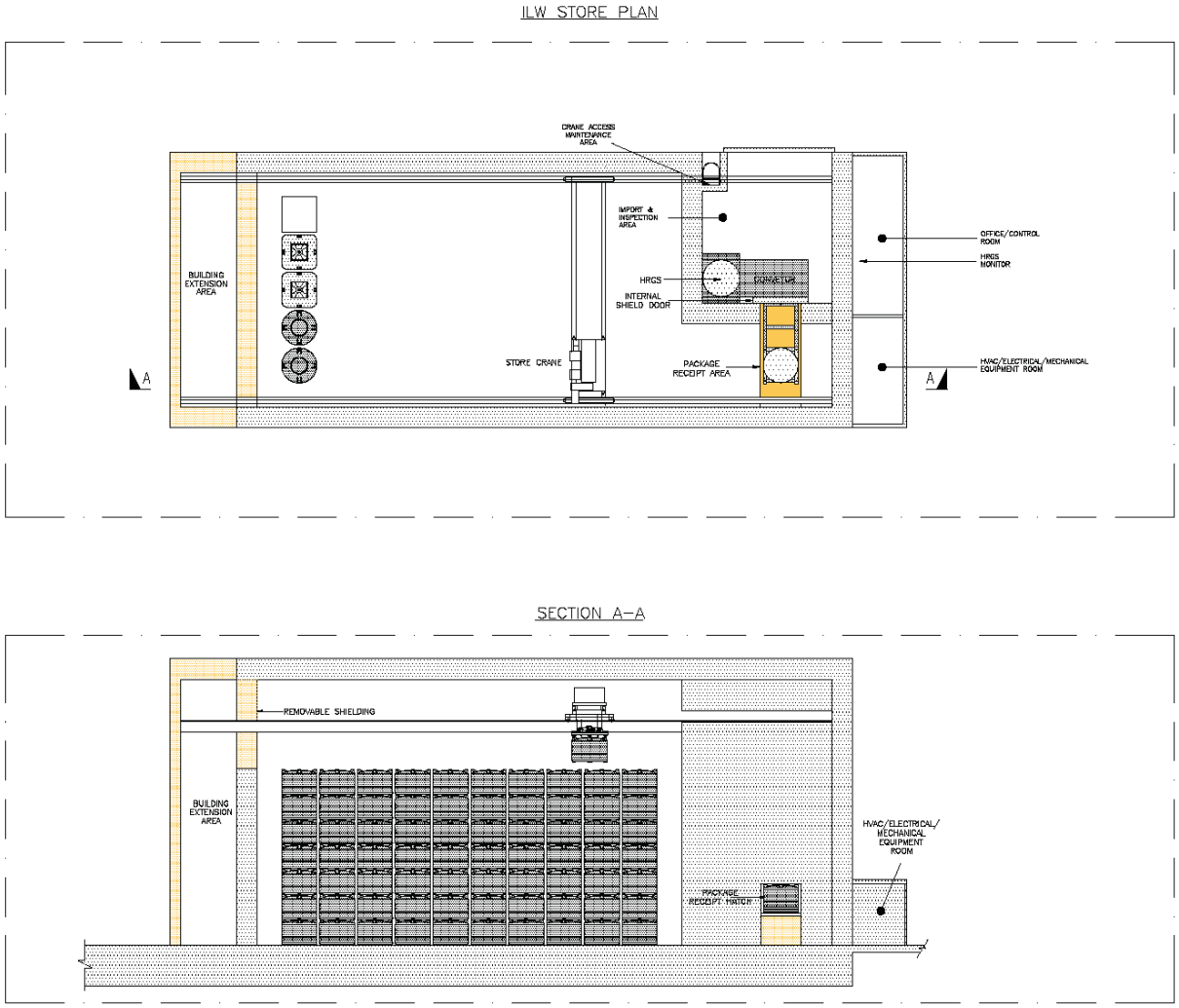


Figure 26-8. Plan and Section Views of the ILW Store

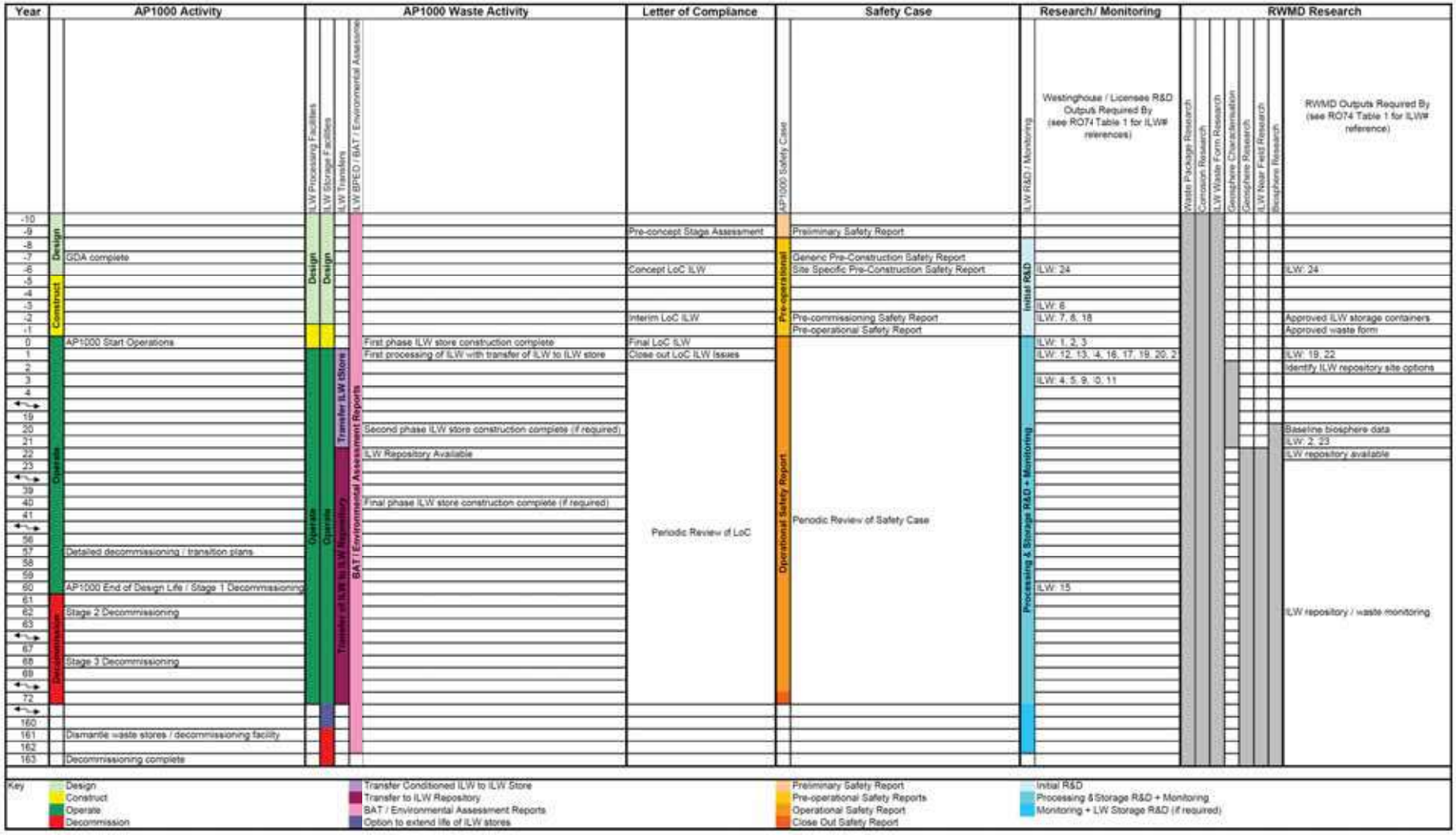
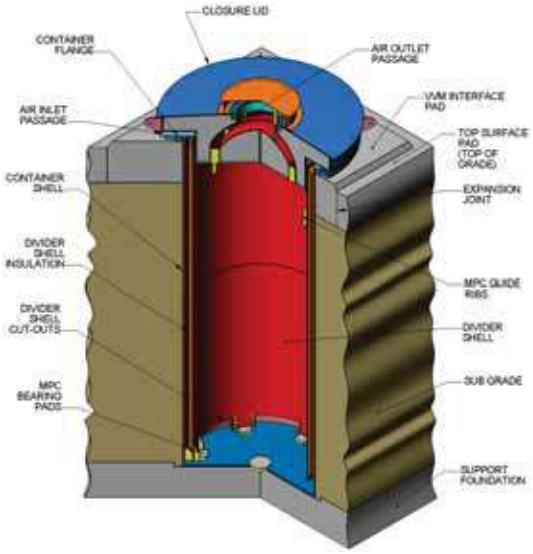
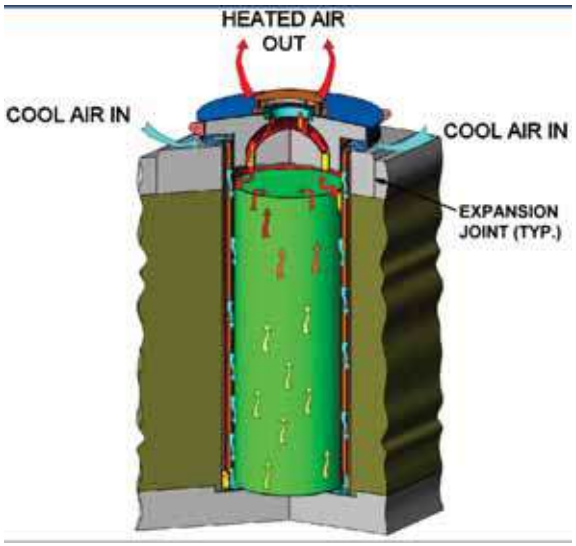


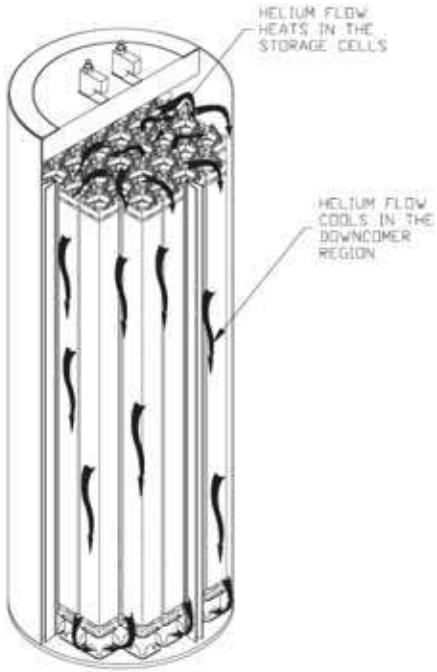
Figure 26-9. ILW Management Facilities Plan



a) Cutaway View of HI-STORM 100U VVM



b) HI-STORM 100U System Air Flow Pattern



c) Heat Rejection in a Holtec MPC through Thermosiphon Action

Figure 26-10. Holtec Spent Fuel Storage System (Ref. 26.1, Figure 3.5-18)

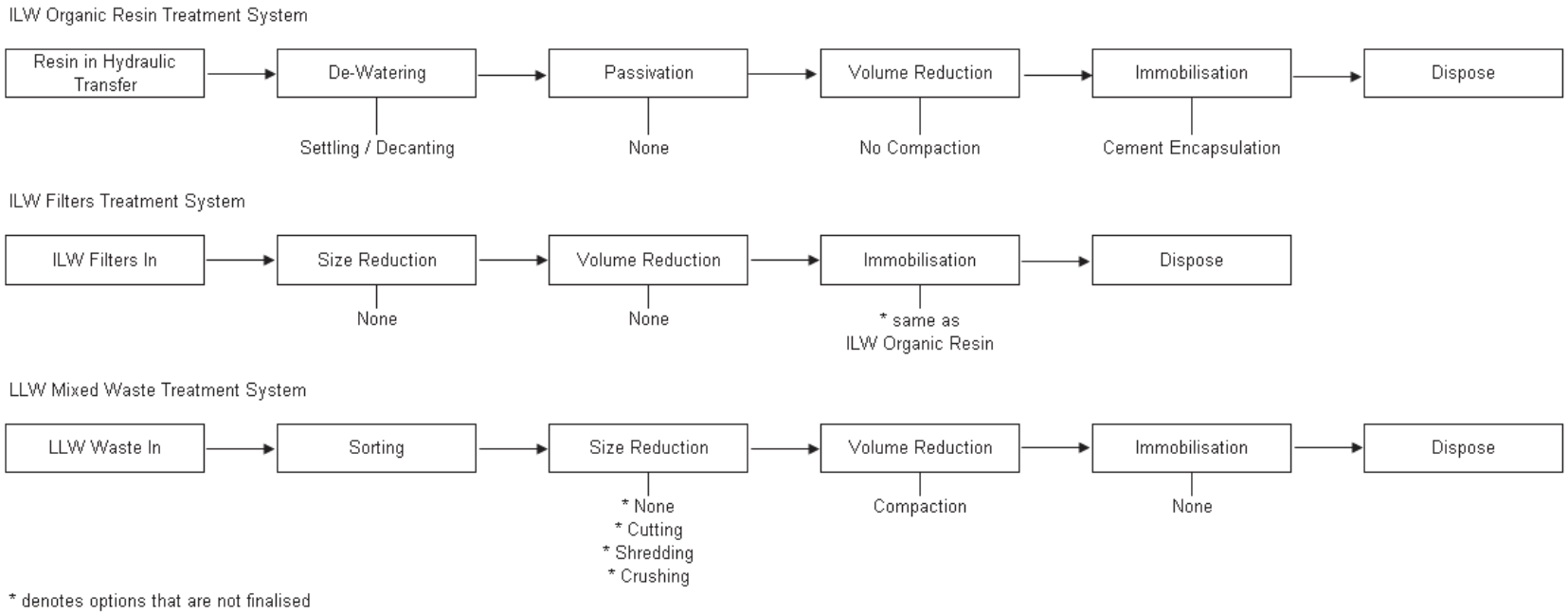


Figure 26-11. Summary of Selected BAT for ILW and LLW Radwaste (Ref. 26.1, Figure 3.5-8)

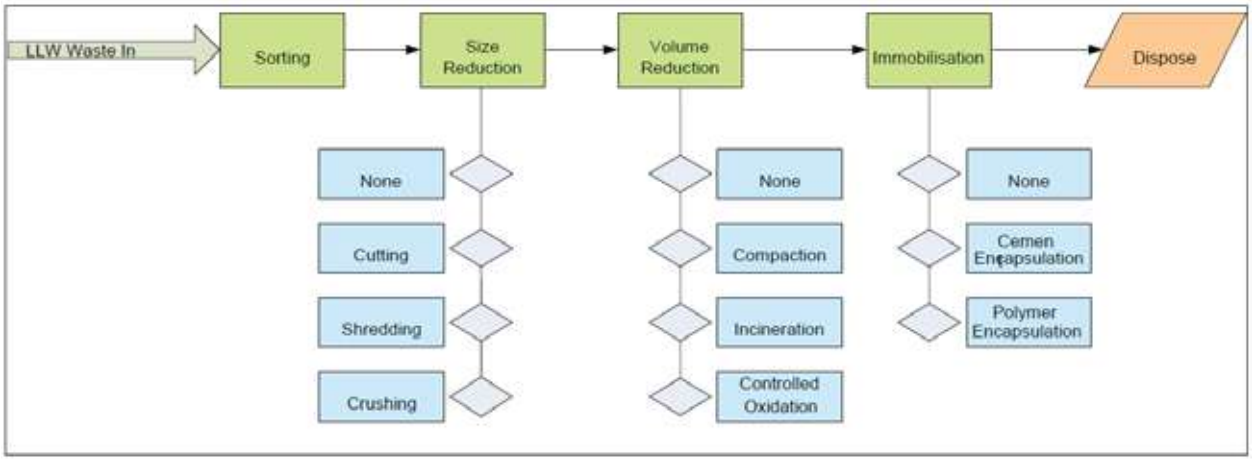


Figure 26-12. LLW Options (Ref. 26.1, Figure 3.5-3)

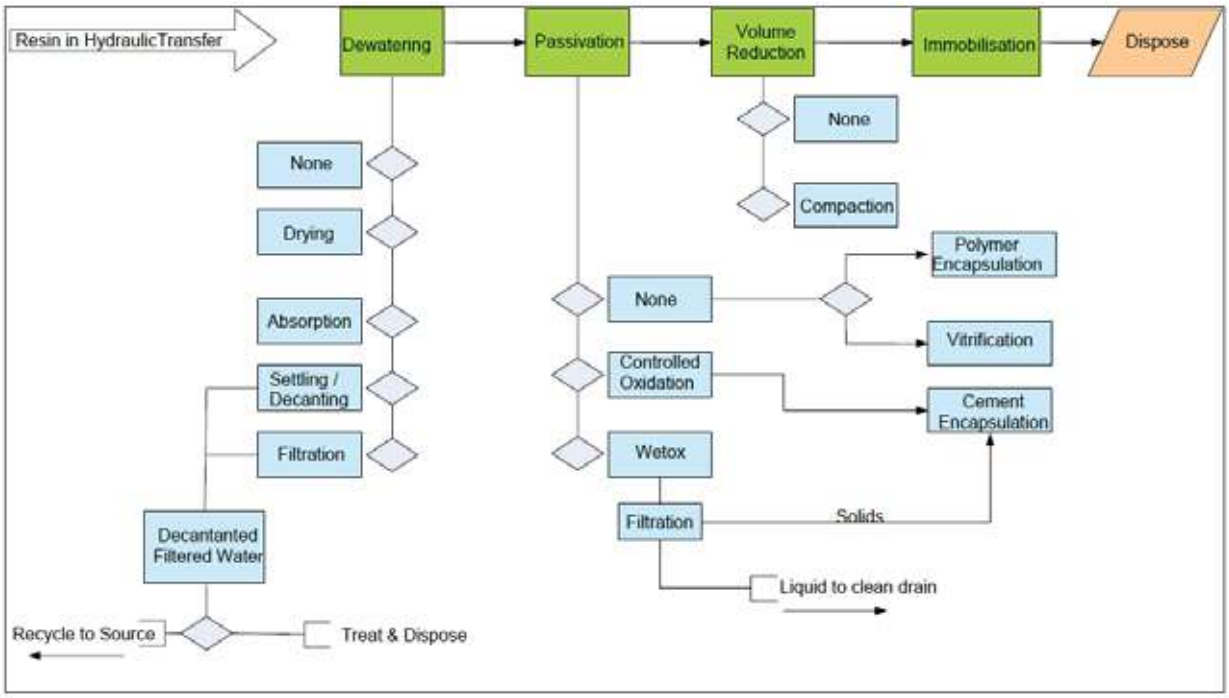


Figure 26-13. ILW Organic Resin Treatment Options (Ref. 26.1, Figure 3.5-3)

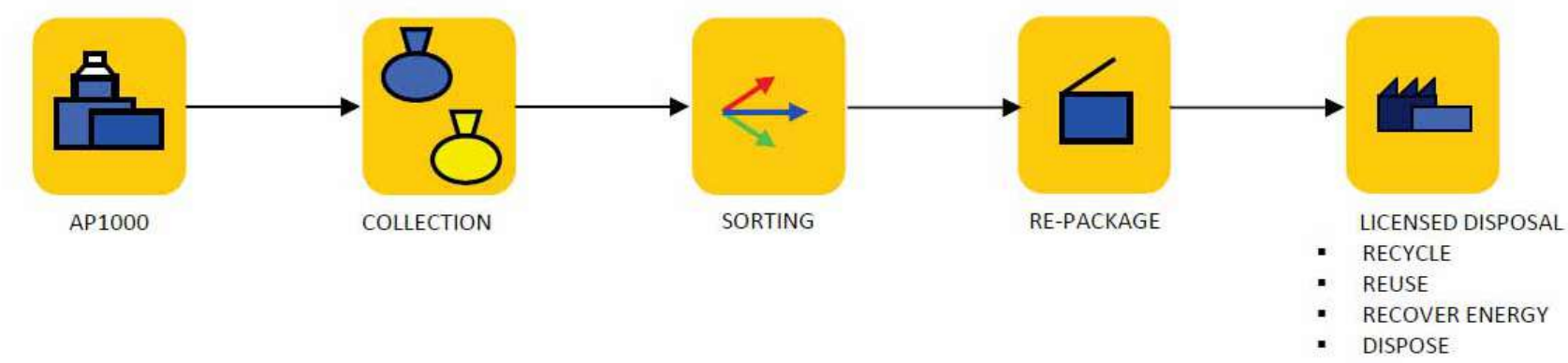


Figure 26-14. Conventional Solid Waste Treatment and Disposal Route (Ref. 26.1, Figure 4.3-1)

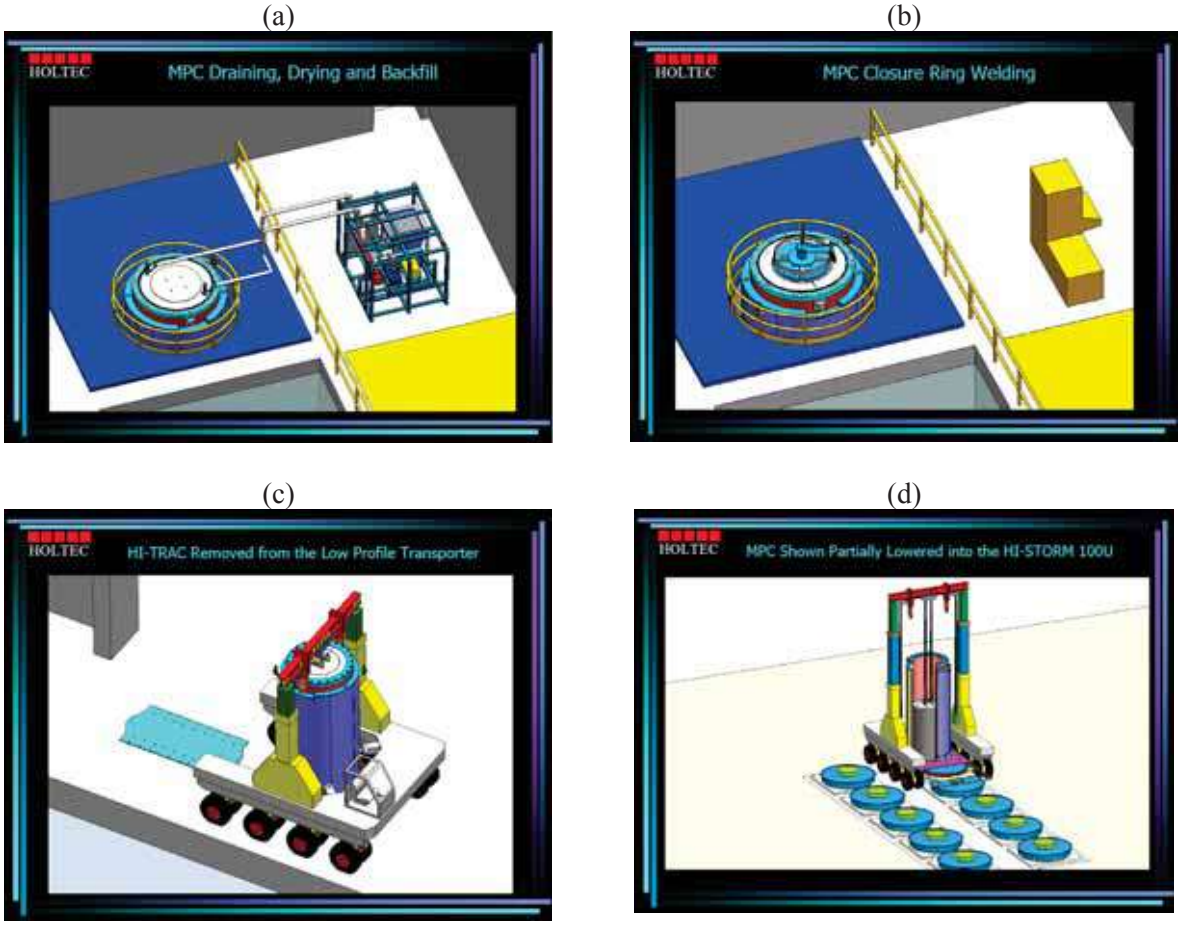


Figure 26-15. Handling Spent Fuel Flasks (Ref. 26.1, Figure 3.5-17)

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS, ACRONYMS, AND TRADEMARKS

ALARP	as low as reasonably practicable
BAT	best available technique
CDM	Construction Design and Management Regulations
DECC	Department of Energy & Climate Change
DPS	decommissioning plant status
EA	Environment Agency
EIADR	Environmental Impact Assessment for Decommissioning Regulations
ESF	emergency safety features
EU	European Union
FSC	final site clearance
GDA	generic design assessment
GDF	geological disposal facility
HEPA	high-efficiency particulate air
HHISO	half-height ISO (containers)
HLW	high-level waste
HVAC	heating, ventilation, and air conditioning
IAEA	International Atomic Energy Agency
ILW	intermediate-level waste
ISO	International Organisation for Standardisation
IWS	integrated waste strategy
LFE	learning from experience
LLW	low-level waste
LLWR	low-level waste repository
MCR	main control room
NDA	Nuclear Decommissioning Authority
NI	nuclear island
ONR	Office for Nuclear Regulation
NEA	Nuclear Energy Agency
PWR	pressurised water reactor
RCP	reactor coolant pump
RPV	reactor pressure vessel
RWM	Radioactive Waste Management
SAP	safety assessment principle
SG	steam generator
SLC	site licence condition
SPHSE	self-priming high solids epoxy
SQEP	suitably qualified and experienced person
SSC	system, structure, or component
UK	United Kingdom
US	United States
WENRA	Western Nuclear Regulators Association

TRADEMARKS

Inconel is a registered trademark of Special Metals Corporation.

27 DECOMMISSIONING AND END-OF-LIFE ASPECTS

27.1 INTRODUCTION

The objective of this chapter is to demonstrate that the generic design of the AP1000 plant can be safely decommissioned at the end of its operational life in accordance with United Kingdom (UK) strategy and regulations. Site-specific issues, including site delicensing, are not discussed as they will be the responsibility of the licensee. Although decommissioning is the last stage in the life cycle of a nuclear facility, licensees are required to make and implement adequate arrangements for the safe decommissioning of the site in accordance with national strategy, site licence condition (SLC) 35 (Reference 27.1).

The AP1000 design incorporates a number of features to facilitate decommissioning and to reduce the risk from decommissioning activities. Steps have been taken to minimise the amount of waste produced. The basis for decommissioning is based on current available techniques; dose management is considered to be as low as reasonably practicable (ALARP). These principles are described in Section 27.2.

Section 27.3 outlines the decommissioning strategy that has been developed for the AP1000 plant, describes the reasoning behind the timing of decommissioning, and provides more detail on the operations that will be carried out during decommissioning. It discusses the factors that affect the timing of decommissioning. Assumptions have been made that will be subject to review over time as detailed site-specific information becomes known. For example, use of the site after operations have ceased and local stakeholders' views will be important factors to consider when final decommissioning plans are being constructed.

A plan for implementing the decommissioning operations has been developed based on the chosen decommissioning strategy. This is described in Section 27.4, where further details on the safety management arrangements and decommissioning operations are given to enable the safe and systematic reduction of hazard from the AP1000 plant after operations finish.

Land remediation is a requirement of the operator and is not considered at this stage. However, anticipated regulator requirements are summarised in Section 27.5.

During generic design assessment (GDA), one single-unit AP1000 plant per site is assumed. Locating multiple plants on a site does not affect the logistics of decommissioning the nuclear island (NI), because each NI on a site will operate independently and can be decommissioned independently. However, if the waste treatment facilities are shared, the decommissioning plan must ensure that the decommissioning waste does not affect units still operating and that the decommissioning waste does not exceed the capacity of the waste facility.

Conclusions and references are presented in Sections 27.6 and 27.7.

27.1.1 Decommissioning Principles

The decommissioning strategy and plan developed in this chapter are based on the following principles:

- Systematic and progressive risk reduction
- Dose minimisation
- Waste minimisation
- Passively safe storage of wastes

Application of these four principles is discussed in the following sections.

27.1.1.1 Risk Reduction

Risk reduction is achieved using a staged approach to decommissioning. Three stages are identified, each one reducing the highest-risk items in turn; all three stages follow International Atomic Energy Agency (IAEA) guidance (Reference 27.2).

Stage 1 is to remove the fuel from the reactor and from the spent fuel pool, following an appropriate period of cooling. Spent fuel is put into dry storage canisters and transported to the onsite spent fuel stores. Checks are carried out to ensure that containment is maintained. After the fuel is removed, the primary circuit is decontaminated using existing primary circuit systems.

In Stage 2, preparatory work will be carried out to enable the remaining decommissioning activities. This includes conversion of the fuel-handling area for processing decommissioning waste; Surveys of the facility will be carried out and decommissioning plans and safety cases will be finalised. Service systems not required for decommissioning activities will be removed

In Stage 3, remaining radioactive materials will be removed in a systematic manner that reduces risk until there are no radiological restrictions on the site. This is the radiological end point for the site.

These three stages of decommissioning are discussed further in Section 27.3. The stages of decommissioning could overlap if appropriate but, for the sake of clarity, are considered as three distinct stages.

27.1.1.2 Dose Minimisation

Dose to decommissioning operators will be reduced to levels that are ALARP. Methods to achieve ALARP include design features to minimise dose; assessing potential options and choosing the arrangements that are ALARP; reducing the dose rate, for example, by decontamination or shielding or remote working; and reducing the time spent close to the source, for example, through modular construction that allows multiple components to be removed together from the reactor and then dismantled in a lower-dose area.

27.1.1.3 Waste Minimisation

The waste management hierarchy is integrated into the design, operation, and decommissioning plans for the AP1000 plant. In line with the requirements of the waste hierarchy, prevention, re-use, and recycling features are incorporated into the design. Decommissioning will be planned so as to avoid the production of unnecessary wastes. The number of approaches that will be used to minimise decommissioning waste are described below.

The integrated waste strategy (IWS) (Reference 27.3) will be reviewed during the operational phase and prior to and during the decommissioning phase to maximise reuse and recycling; disposal will be chosen only if other options are not practicable. The use of new and more appropriate waste routes for the decommissioning phase will be assessed.

A thorough characterisation of the physical, chemical, biological, and radiological properties of the plant will be carried out after defueling and decontamination of the primary circuit. The drivers for this characterisation are to establish plant conditions so that decommissioning

can be carried out safely and waste can be minimised, for example, by decontamination and separation. Operational radiological monitoring records will provide input for the characterisation.

Decontamination will be used where practicable to recover wastes that can, in line with the requirements of the waste hierarchy, be reused, recycled, or disposed of by conventional nonradioactive routes.

Segregation of different waste types will be carried out to allow optimum use of the waste routes available at the time of decommissioning. Segregation, minimisation, and disposal techniques are detailed in the IWS document (Reference 27.3), which will be updated as required by the operator to continuously improve waste minimisation.

27.1.1.4 Passively Safe Storage of Wastes

It is recognised that disposal routes for higher-activity materials will not be available immediately when that waste is processed. Therefore, a period of interim storage on site is envisaged. The waste will be stored on the site in appropriately designed facilities in a passively safe condition; that is, one that will not require active safety systems during the interim storage period. The use of an interim passively safe storage system will not compromise disposability.

27.1.2 Decommissioning End Point

The aim of decommissioning is to remove hazards so that the site does not present an unacceptable level of risk to human health or the wider environment. The end point includes the decommissioning of all facilities, including the interim storage facilities. The physical end point will be determined to a large extent by the future use of the site. In making a decision on the end point, the operators will take into account factors such as the planning conditions and the views of the regulators, local authority, and stakeholders. Therefore, the physical site end point will be determined later by the operator, taking into account local stakeholders' views but subject to the overriding requirement that there is no unacceptable risk to human health or the wider environment. The decommissioning end point is discussed further in Section 27.4.2, where an assumed end point is given for planning purposes.

27.2 DESIGN FOR DECOMMISSIONING

27.2.1 Overview

The design of the AP1000 plant incorporates features that support safe decommissioning, and minimise the amount and category of wastes produced from decommissioning as well as human and environmental impact. These principles are discussed in this section, along with the features incorporated into the design to aid decommissioning and to reduce waste volumes.

27.2.1.1 Design Principles

Regulatory Guidance

The design of the AP1000 plant facilitates and minimises decommissioning and associated waste management operations and costs. The principles underpinning the design are consistent with the UK government policy on decommissioning, the Office for Nuclear

Regulation (ONR) safety assessment principles (SAPs) for Nuclear Facilities and the Environment Agency (EA) Radioactive Substances Regulation – Environmental Principles.

SAP DC.1 states that "facilities should be designed and operated so that they can be safely decommissioned" (Reference 27.4). The adoption of this principle ensures that decommissioning and waste retrieval requirements are incorporated into plant design. Measures that demonstrate the adoption of this principle include the following:

- Design measures to minimise activation and contamination, for example, selection of materials around the reactor to prevent large quantities of long lived radionuclide's forming (e.g., using low cobalt steel)
- Physical and procedural methods to prevent the spread of contamination
- Control of activation (e.g., by control of primary circuit water chemistry)
- Design features to facilitate decommissioning and to reduce dose uptake by decommissioning workers
- Consideration of the implications for decommissioning when modifications to and experiments on the facility are proposed
- Identification of reasonably practicable changes to the facility to facilitate or accelerate decommissioning
- Minimising the generation of radioactive waste

Additionally, SAP RW.2 states that "the generation of radioactive waste should be prevented or, where this is not reasonably practicable, minimised in terms of quantity and activity". This principle may be adopted through specific design provisions, construction methods and commissioning, operational and decommissioning arrangements that avoid the creation of radioactive waste or reduce to the minimum radioactive waste generated throughout the facility lifetime.

As well as the SAPs, the EA Radioactive Substances Regulation – Environmental Principles also provide guidance on how decommissioning and waste minimisation may be incorporated into plant design. Principle DEDP3, Considering Decommissioning during Design and Operation, states that "facilities should be designed, built and operated using the best available techniques (BATs) to minimise the impacts on people and the environment of decommissioning operations and the management of decommissioning wastes" (Reference 27.5). In addition principle DEDP4, Discharges during Decommissioning, states that "aerial or liquid radioactive discharges to the environment during decommissioning should be kept to the minimum consistent with the decommissioning strategy for the site".

The following sections describe how the design of the AP1000 plant addresses these principles.

Minimising the Generation of Radioactive Waste

The current design of the AP1000 plant is the result of a design philosophy and design process that emphasised safety and simplicity. The design process used throughout the development of the AP1000 plant is to create a safe nuclear power plant with costs, radiation exposures and radioactive discharges ALARP.

The AP1000 design minimises the creation of radioactive waste during operations and decommissioning as the AP1000 plant was designed with fewer valves, pipes, and other components so less waste will be generated during maintenance activities (repair and replacement) and decommissioning compared to plants of a similar size. When compared to similar nuclear power plants, the AP1000 plant has roughly 50 percent fewer valves, 35 percent fewer pumps, 80 percent less piping, and 80 percent fewer heating, ventilation, and air-conditioning systems. Considering these characteristics, the decommissioning phase of the AP1000 plant should be shorter and the decommissioning activities may produce smaller quantities of activated/contaminated material that should be treated and conditioned for interim storage and final disposal as radioactive waste. This lends itself to more simple strategies, shorter decommissioning timescales and lower requirements for funding of the decommissioning phase.

In addition to the reduced building volumes and plant inventory, many features have been incorporated into the AP1000 design that are intended primarily to reduce the production of activated corrosion products. Such measures include the selection of materials used in the design and controls imposed upon the construction. A consequence is a reduction of operational radiation exposure during the normal operational life of the plant. A direct result of this is the reduction of the radioactive inventory and a reduction in the residual mass of active materials at the time of decommissioning.

The only effective course of action to reduce activation of fixed structures is to control material composition and attempt to reduce major element concentrations. Each of the materials in and around the core has a major element concentration that cannot be removed. For steels, these include iron and nickel, and for concrete, calcium. Efforts to reduce trace elements are of little benefit since their contribution to the total is minimal in comparison with the contribution from the major elements to the radioactive inventory.

One case where the control of a trace element is appropriate is steel where the reduction in cobalt has significant benefits. Activation of Co-59 produces Co-60, which is the largest contributor to occupational radiation exposure on pressurised water reactors (PWRs). The most highly activated structures in the plant will be the reactor internals. The level of cobalt in these structures has been restricted to below 0.05 percent by weight.

The UK AP1000 Environment Report describes in detail ways in which the AP1000 design minimises radioactive waste generated during operation, in particular (Reference 27.7):

- Section 2.6 gives further examples of AP1000 design decisions related to waste minimisation, waste generation, and waste disposal that reinforce the concept of safety through simplicity, ALARP, and BAT.

- Section 3.2 describes several ways in which the release of radioactive emissions from the AP1000 plant is reduced at source.

- Section 3.3 describes the handling and treatment of gaseous radioactive waste and gives details of the BAT assessments carried out for the treatment of gaseous radwaste.

- Section 3.4 describes the handling and treatment of liquid radioactive waste and gives details of the BAT assessments carried out for the treatment of liquid radwaste.

- Section 3.5.4 describes how waste minimisation, storage and disposal principles have been incorporated into all stages of the AP1000 plant life cycle including design, construction, operation and decommissioning.

- Table 3.1-1, Nuclear BAT Management Factors and AP1000 features, outlines the ways generation of radioactive waste is minimised, resources are used efficiently, emissions are reduced and waste is stored in a passively safe and retrievable form.

Preventing the Spread of Contamination

The AP1000 design provides features for protection against the occurrence, spread, and thus potential personnel exposure to radioactive contamination. The major contributor to the contamination of surfaces is activated corrosion products. The following steps have been taken in the design of the AP1000 plant to limit the generation of corrosion products:

- The injection of zinc acetate into the primary system has the effect of inhibiting general corrosion and primary water stress corrosion cracking. Corrosion rates of the materials can be reduced by up to a factor of three or more with the addition of 20 ppb of zinc.

- Primary circuit water chemistry will be maintained at pH levels of 6.9 to 7.4 to again mitigate the effects of activated corrosion products.

- Primary and auxiliary materials selected for use in the AP1000 plant have a cobalt content of less than 0.2 percent by weight or even lower depending on component. High cobalt stellite alloys are not used in primary circuit components.

The spread of contamination is also limited by a structural design that incorporates a number of structural modules. These are composite structures comprising concrete filled steel plate where face of the steel plate forms the walls of rooms. They are easily decontaminated and prevent the possible leaching of water borne contaminants into the concrete. In the limited areas where there are concrete walls exposed to potential contamination, such walls are coated with a coating that can be decontaminated. All steel surfaces exposed to potential contamination will also be provided with surface finishes that will prevent penetration and facilitate decontamination.

The incorporation of thicker and larger plates in the spent fuel pool also limits the spread of contamination. Where possible, this plate becomes the formwork. This eliminates the potential for voids between the plates and the concrete, which eliminates the potential for unsupported areas of plate and thus potential for high stress areas. The larger plates significantly reduce the amount of welds and particularly in situ welding. In addition, reduction in the weld surfaces reduces the damage to the plate surface finish making decontamination easier. Leaks in the spent fuel pool are primarily associated with welds that have been significantly reduced in quantity in this design. In addition, leak chases are provided. These provide for evidence of leakage and direct any contaminated leakage flow to the waste handling systems. They also prevent the leaching of active fluid into the concrete should a leak occur. The same advantages are also applicable to the refuelling water storage tank and the reactor cavity.

Spread of contamination is also limited by the provision of heating, ventilation, and air conditioning (HVAC) within the secondary containment areas.

The Environment Report (Reference 27.7, Section 2.9.5) gives further details of how the potential for leakage and spread of radioactive contamination from the AP1000 plant is minimised by using structure, system, and component designs and operational procedures. The principles that will be considered in the design of the radwaste and intermediate-level waste (ILW) store buildings with respect to decommissioning are outlined in the

UK AP1000 Radioactive Waste Arisings, Management and Disposal report (Reference 27.8). These include:

- Surfaces exposed to contamination will be minimised wherever practicable, and their surface coatings will be impermeable and readily decontaminated. For example inside containment:
  - Carbon steel and structural modules within the containment are coated with either inorganic zinc with an epoxy top coat or self-priming high solids epoxy (SPHSE).
  - Where practical, miscellaneous carbon steel items (such as stairs, ceilings, gratings, ladders, railings, conduit, duct, and cable tray) are hot-dip galvanised.
- Steel surfaces subject to immersion during normal plant operation (such as sumps and gutters) are stainless steel or are coated with SPHSE applied directly to the carbon steel without an inorganic zinc coating.
- Exposed concrete surfaces inside containment are coated with an epoxy sealer to help bind the concrete surface together and reduce dust that can become contaminated and airborne.
- Floors subject to heavy traffic or contaminated liquid spills are coated with self-levelling epoxy or SPHSE floor coating.
- The plant will be designed for the containment and recovery of possible spillage of active material.
- To prevent the spread of airborne contamination during operations, the ventilation system will be designed using depression gradients, such that the flow of air is from areas of low contamination to areas of potentially high contamination.
- Cabinets (e.g., sample cabinets) will be of robust construction and made as small as practicable, where used whilst still fulfilling their design function.
- Both internal and external surfaces of cabinets will be smooth and free from cracks, sharp edge projections and recesses, where contamination could collect.
- All cabinets will be vented via the active ventilation system and maintained at a depression, to prevent the potential spread of airborne contamination to the operating areas.

Design Features that Facilitate Decommissioning

As well as minimising decommissioning waste and contamination, the AP1000 design incorporates features which facilitate decommissioning. These are described later in Section 27.2.2.3.

In addition to the design features which minimise waste, reduce contamination and facilitate decommissioning, the plant containment and structures will be designed to retain their integrity for the expected operational life and the subsequent decommissioning period. The life of the radwaste building will be extended beyond the assumed 60 year operation period to allow the building to be used to support decommissioning. The operational period for the ILW store building is 100 years.

27.2.1.2 Operation and Maintenance Principles

Regulatory Compliance

Ultimate responsibility for plant operation and maintenance will belong to the licensee. When operating the plant the licensee must follow regulatory requirements that are informed by the policy and regulatory guidance provided by the UK government, ONR, EA, and international bodies such as the IAEA.

As Low As Reasonably Practicable

The licensee should ensure that the principle of ALARP is considered in all operational and maintenance tasks which are important to safety, radioactive waste management and decommissioning.

Best Available Technique

The licensee should ensure that the principle of BAT is adopted in the management of radioactive substances and radioactive waste to provide an optimal level of protection to human health, wildlife, organisms and the wider environment. The implementation of BAT during operations should result in reduced amounts of waste and radioactive contamination to be dealt with during decommissioning.

Operation and Maintenance

The licensee will need to establish preventive maintenance programmes to ensure the continual safe operation of the AP1000 plant. These programmes will include surveillance, inspection and maintenance of systems, structures, or components (SSCs) in accordance with appropriate safety margins, engineering practices and quality levels.

The way in which a plant is operated and maintained will also have a significant impact on the decommissioning strategies that can be implemented and the nature and amounts of waste that will have to be dealt with. For example, the operational procedures and good housekeeping must ensure that radioactive contamination does not spread throughout the plant and that provision is made to carry out maintenance with the minimum spread of contamination. It is also important that the plant is decontaminated throughout its operating lifetime, as this will minimise the potential operator dose uptake during decommissioning operations.

To ensure a high level of plant safety as the plant ages, the licensee should develop an inspection and maintenance programme to manage SSC ageing effectively and proactively. As the plant ages, there is an increased probability of both single component failures and common-cause failures. Operating experience has shown many SSC failures have occurred as a result of ageing mechanisms such as general and local corrosion, erosion–corrosion, radiation and thermal embrittlement, fatigue, creep, vibration and wear (Reference 27.9). These failures can affect plant safety through abnormalities of process systems. The programme should cover the entire lifetime of the plant including the decommissioning period which may extend over many years. The objective is to provide for the timely detection and mitigation of significant ageing effects in nuclear power plant SSCs important to plant safety and reliability during operation and decommissioning (Reference 27.10).

Waste Minimisation

The basic AP1000 design principles that minimise the creation of radwaste during operations and decommissioning are well established (Reference 27.7 and 27.8). These principles, which include good housekeeping, optimisation of plant shutdowns, waste segregation and volume reduction, should be followed by the licensee.

The operational procedures used by the licensee should take into account waste minimisation and best practice to prevent additional secondary waste arisings during operation of the plant. This will ensure that all wastes can be disposed of by already proven or planned routes when the plant is eventually decommissioned.

The onsite waste inventory should be minimised before decommissioning by the prompt transfer of waste to the available national waste disposal repositories, if these are available and have capacity to accept new build waste. Some ILW and high-level waste (HLW) may have to be transferred to onsite waste stores before this transfer is possible.

Plant Modification

If the licensee should modify the plant during the operational life, then the effect on decommissioning, such as future access, should be taken into consideration.

Data Collection, Record Management and Corporate Memory

SAP DC.6 states that "Documents and records that may be required for decommissioning purposes should be identified, prepared, updated, retained, and owned so that they will be available when needed" (Reference 27.4).

The adoption of this principle requires the licensee to develop robust data collection and record management procedures to handle the large amount of monitoring, process equipment and maintenance information that needs to be retained to facilitate decommissioning. This includes records of any design or materials changes and any extensive maintenance or refurbishment work carried out. These records are important to document the plant condition prior to the transition from operation to decommissioning and to ensure minimal loss of corporate memory before the decommissioning phase begins.

27.2.1.3 Learning from Experience Principles

National and International Experience

International experience is an important source of information on best practice. Learning from experience (LFE) is published by international organisations (e.g., IAEA, Western European Nuclear Regulators Association (WENRA), Nuclear Energy Association (NEA), European union (EU)), regulatory bodies (e.g., ONR, NRC), and in scientific and technical publications and conference proceedings. Westinghouse and the licensee will monitor these resources as part of their normal business practice. Relevant information will be appropriately recorded.

The IAEA has established a decommissioning network, which will bring together organisations with specific experience and competence in decommissioning and that are willing to share their experience with other organisations.

Licensee Experience

The licensee will likely have accumulated its own operating and decommissioning experience from operating and decommissioning other nuclear power plant facilities. The licensee will use this experience together with experience gained from the specialist decommissioning contractors that it employs to inform the decommissioning of the AP1000 plant.

Westinghouse Experience

Westinghouse will engage with the licensee with the LFE processes which Westinghouse has in place, for example the Corrective Action Process and the Lessons Learned database. The decommissioning of early Westinghouse PWR plants and the first AP1000 plants (e.g., China and US) that are likely to be decommissioned ahead of any UK plants will provide LFE resources that can be made available to the licensee to assist in their decommissioning plans. The requirements to alert and involve licensees in the discussion and resolution of learning events, which have relevance to safety or the environment, is built into the Westinghouse management arrangements.

27.2.2 Design Features for Decommissioning

27.2.2.1 General

The most effective time to minimise the decommissioning hazards and liabilities is during the design phase. Westinghouse has designed a number of features into the AP1000 plant that reduce the hazards associated with decommissioning and the liabilities that must be managed after the end of operations. These features are grouped into two categories:

- Minimising the volume and activity of waste
- Enabling decommissioning

The following sections describe each specific design feature incorporated into the AP1000 plant that minimises decommissioning liabilities, facilitate the decommissioning operations, and minimise the dose to operators.

27.2.2.2 Reducing Waste Volumes and Activity by Design

Minimising Materials

A very effective method of reducing decommissioning liabilities is to minimise the amount of materials and number of components that have to be decommissioned. At the design stage, Westinghouse reviewed the components used in previous designs and made significant reductions in materials without compromising safety or operational performance. Compared with similar nuclear power plants, the AP1000 plant has approximately 50 percent fewer valves, 35 percent fewer pumps, 80 percent less piping, and 80 percent fewer HVAC systems. As a result, the decommissioning phase of the AP1000 plant should be shorter and the decommissioning activities will produce less activated and contaminated material that must be treated and conditioned for interim storage and final disposal as radioactive waste. This should result in less decommissioning work to carry out and ultimately produce less waste to dispose of during decommissioning. A reduced dose may also result from having to decommission fewer components, which may result in less time working in active areas. The use of lower numbers of components also minimises the number of potential leakage pathways.

Selecting Materials for Low Activation

Activation of steels can have a significant impact on decommissioning liabilities, as activation products increase dose rates around the plant and can increase the category of waste. Westinghouse took an effective course of action during the design phase that reduces dose for decommissioning operations by carefully selecting materials to control composition and attempting to reduce activation products. In particular, a significant effort has been made to reduce cobalt-based alloys and/or lower the acceptable level of cobalt in the materials.

Reducing the amount of cobalt in structural materials is an example of the particular benefits of materials selection. Activation of Co-59 produces Co-60, which is the largest contributor to occupational radiation exposure on PWRs. The most highly activated structures in the plant will be the reactor internals. The level of cobalt in these structures has been restricted to below 0.05 percent by weight, thus reducing Co-60 production. Other primary and auxiliary materials selected for use in the AP1000 design have cobalt content of less than 0.2 percent by weight. Additionally, for the steam generator (SG) tubes, adoption of 690TT allows a reduction in cobalt generation because of the reduction in nickel content, and cobalt in 690TT for the SG tubes is limited to 0.015 percent by weight. Use of stellite alloys for hard facing of valves and other components has been significantly reduced.

Each material in and around the core has elements that generate problematic activation products, and these cannot always be eliminated. For steels, these include iron and nickel, and for concrete, calcium. Even where these materials cannot be eliminated, steps have been taken to minimise the quantity present, including simplifying the design and reducing the number of components.

Minimising Corrosion

Activated corrosion products are the major contributor to the contamination of surfaces in the primary circuit. The following steps have been taken in the design of the AP1000 plant to limit their generation:

- The injection of zinc acetate into the primary system has the effect of inhibiting general corrosion and primary water stress corrosion cracking. Corrosion rates of the materials can be reduced by up to a factor of three or more with the addition of 20 ppb of zinc.

- Corrosion products and other contaminants will be removed by the chemical and volume control system during the operational phase, which will reduce contamination levels and dose for operators during decommissioning.

- Primary circuit water chemistry will be maintained at a pH between 6.9 and 7.4 to again mitigate the effects of activated corrosion products.

Decontaminating Primary Circuit

The majority of the primary circuit is designed in stainless steel with limited use of Inconel™. At this time, an oxidative process system has been identified for the decontamination of potentially active or contaminated piping circuits although other processes (e.g., oxidative/reductive processes) may be considered. Decontamination factors of up to ten for stainless steel and two to three for Inconel are expected for the initial phases.

This method of decontamination will require the provision of dedicated reagent tanks, pumps, and associated equipment. It may be possible to use existing operational plant and equipment.

This gives the operator the option to decontaminate the primary circuits before dismantling if the conditions at the time suggest that it would represent the ALARP option.

Selecting Surface Materials

The AP1000 structural design incorporates a number of structural modules that are plate structures filled with concrete, the whole acting as a composite structure. They present a steel plate face forming the walls of rooms. In addition, concrete surfaces that will potentially be exposed to contamination will be covered with steel plates that can be decontaminated. Where these steel surfaces could be exposed to potential contamination, they will be provided with surface finishes to facilitate decontamination. This is an improvement over existing PWRs, where a large amount of concrete is exposed to contamination that is more difficult to decontaminate. The outer steel surface also prevents the possible transfer of waterborne contaminants into the concrete.

Reducing Leakage Pathways

The AP1000 design has a number of design features to reduce leakage pathways. Reducing the number of leakage pathways reduces the spread of contamination and thus potentially the amount of radioactive waste produced, as well as the amount of work and dose for decommissioning operatives. The measures for reducing leakage pathways are discussed below.

Penetrations through the primary containment are designed to be leaktight assemblies whilst allowing pipes and cables to pass through the containment vessel boundary. Very often, in previous designs, they are the sites of small leakage pathways and so have been minimised in the AP1000 design.

One of the fundamental design objectives for passive cooling of the AP1000 reactor is to isolate containment during a design basis accident so that only energy passes through the containment boundary, not fluids. This minimises the number of penetrations and reduces design, inspection, and maintenance burdens, and, therefore, waste arisings that could result from these activities.

Penetrations have been minimised by implementing a variety of innovative techniques:

- Service systems in containment, for example, component cooling water or compressed air, are split and routed inside containment, resulting in only one supply or return penetration for each service.

- Some intermittent services with common fluids share common penetrations. For example, both chilled water and hot water heating services to HVAC in containment share common penetrations since they will not be used at the same time. The fire protection water and containment spray supply systems also share a common penetration.

- Instrumentation and control penetrations are reduced by taking advantage of digital data highway technology. Multiplexing cabinets are located such that instrumentation and control signals share a common highway penetration in lieu of multiple individual signal penetrations.

All floor drains in radioactive areas are grouted into the surrounding concrete to provide secondary containment: this ensures that any leakage will be collected in the floor drain and

not bypass the drain, therefore potentially reducing the spread of contamination should the drain leak. This reduces the amount of work and waste during decommissioning.

The spent fuel pool and connected pools are designed to eliminate unidentified leakage to the groundwater. The design includes construction using high-quality modular techniques, reduced numbers of welds using advanced welding techniques, welds equipped with leak chases, and a zoned pool leak detection system. To the extent possible, these pools are located entirely inside the auxiliary and containment building, so that any theoretical leakage from the tanks would accumulate in the building, reducing the potential spread of contamination and decommissioning liabilities. Further details can be found in the Environment Report (Reference 27.7, Section 2.9.5.5).

27.2.2.3 Features Enabling Decommissioning

The AP1000 design includes the following features that enable decommissioning to be carried out more quickly, more safely, and to minimise dose to operators.

Modular Dismantling Philosophy

The AP1000 plant is designed and built in modules, which aids the construction and quality of build, and makes decommissioning easier. Modules can be removed in a similar manner to the way that they were installed, although some segmentation of modules may be required to facilitate lifting operations due to the additional weight of concrete added during the construction process. The decommissioning sequence depends on the way the individual modules interact to provide the overall structural integrity of the facility during decommissioning. Some individual modules can be partly decommissioned in parallel if individual modules are structurally independent, and can be separated and removed to the waste processing area for further dismantling, decontamination, packaging and disposal. This allows some of the decommissioning to be carried out away from the original position and source of dose, in a facility designed and built specifically for dismantling, decontamination, size reduction, and packaging for disposal. This approach reduces risk and dose to operators.

Polar Crane Available for Decommissioning

The polar crane in the containment is designed for lifting large items from the reactor such as the SGs, reactor coolant pump (RCP) motor/impeller assemblies, and reactor vessel head to a place where they can be set down and prepared for transfer to the waste facility. It will be available for lifting these large reactor components during the decommissioning phase. In addition, an auxiliary hook can be used for assisting with large lifts or on its own for lifts of smaller components.

Reactor Pressure Vessel

The AP1000 design is such that the reactor pressure vessel (RPV) can be removed in one piece. This should significantly reduce the doses received by decommissioning staff and reduce costs. Further processing such as decontamination and size reduction would be required to make the RPV suitable for disposal in the UK. This will be done in a specifically designed facility should the operator choose to use this option.

Logistics of Waste Movements

Once the polar crane has lifted items or minor modules for transfer to the waste processing facility, they must be removed from the plant. The plant has been designed with pathways that facilitate the movement of equipment. These routes will be used during decommissioning

operations to install decommissioning equipment and they will allow for removal of whole plant items and modules as they are being decommissioned.

Floor slabs of the auxiliary building and shield building are strengthened and structurally connected, providing not only seismic protection but also allowing movement of the heavier modules and plant items.

Heating, Ventilation, and Air-Conditioning Systems Support Decommissioning

During operations, facilities at risk of potential contamination are provided with ventilation systems that provide extraction and filtration. The ventilation systems will also be used in facilities where there is a contamination risk during decommissioning. This will provide local ventilation to reduce airborne contamination, thus reducing the spread of contamination and the risk of internal dose to operators.

It is expected that local modifications to the HVAC system will be required during the decommissioning phase. This will depend on the operating experience, decommissioning plans, and safety case developed closer to the time by the operator.

Operational Shielding Suitable for Decommissioning

Operational shielding has been designed in a way that will facilitate decommissioning operations. Some examples are described below.

The shield building is a structure that surrounds the containment vessel and provides shielding for the containment vessel and other radioactive systems located in the containment building. This will be maintained during the decommissioning phases to reduce doses to decommissioning staff. Some modifications to the shielding are expected to allow access for decommissioning equipment and revised shielding assessments will be carried out as part of the decommissioning safety case. These changes are not expected to adversely affect the protection offered by the shielding. Any modifications made to shielding will ensure that doses to decommissioning staff will be ALARP.

The shroud that provides shielding to the control rod drive mechanism can be used for removal of the system during decommissioning to reduce dose to operators.

Removable shielding is provided for piping systems that require inspection during the operational phase. This will allow quick access for size reduction and isolation of pipework during decommissioning. The removable shielding can also be reused on other sections of pipework, thus reducing dose to decommissioning operators.

Shielding is provided to separate equipment such as demineralisers and filters from nonradioactive equipment. Uncontaminated items can therefore be removed with minimal dose to operators when making space to decommission the radioactive equipment.

Shielding provided between radiation sources and access areas for operations will continue to be used during decommissioning.

Equipment that requires minimal maintenance is enclosed in shielded compartments. Removable access hatches are fitted to allow access for decommissioning whilst maintaining shielding around the components.

Shielding is provided to manually operated valves that can become contaminated, and will reduce dose to operators during decommissioning.

Recovery of Residual Operational Waste

The AP1000 plant is designed so that operational wastes such as those from the condensate polishing plant can be removed and processed in the waste handling building during the operational phases. Some operational wastes, such as the residue of operational wastes in vessels, will have to be removed during decommissioning. The shielded hatches that allow access to the vessels for maintenance during operations can also be used for decommissioning; either by providing access for remotely operated tooling or allowing man access if dose rates within the vessels permit.

Isolation and Decommissioning of Sections of the Plant

The plant design allows sections of plant to be isolated and decommissioned independently of others where appropriate. In particular service systems will be provided with isolation valves to allow areas to be decommissioned and taken out of service without affecting ongoing service supplies needed elsewhere. Also, prior to decommissioning, a new electrical supply to the ILW store will be installed which will also supply the radwaste building. This will allow the main NI to be dismantled whilst retaining the use of the radwaste building.

27.3 DECOMMISSIONING STRATEGY OF THE AP1000 DESIGN

27.3.1 Introduction

This section provides a high-level decommissioning strategy appropriate to this stage of the approval process. At the appropriate time, it can be used as the basis of a standalone decommissioning strategy document. This decommissioning strategy document will be updated by the operator at appropriate intervals agreed upon with the regulator, or after significant changes, to ensure that it remains current as required under SLC 35 (Reference 27.1). The decommissioning strategy document is also subject to periodic regulator review (ONR and EA) as may be required by government policy (Reference 27.11) and SLC 15 (Reference 27.1).

This strategy is consistent with UK government regulations, policies, and strategies; and with IAEA guidelines on decommissioning nuclear power plants (Reference 27.2).

This section gives details on the activities that will be carried out during decommissioning, and the sequence and duration of those activities.

Timing of decommissioning is an operator’s decision but a number of factors will affect the choice between immediate and deferred decommissioning. The sensitivity of the decision to those factors is discussed. One of the significant factors in deciding when to decommission is the predicted use of the site after operations, which also affects the site end point and land remediation strategy. Each of these in turn is influenced by local stakeholders as well as regulatory requirements. Stakeholder engagement and the site end point are therefore also considered in this section. Planning and other matters related to implementation of the strategy are discussed in Section 27.4.

27.3.2 Generic Decommissioning Strategy

27.3.2.1 General

The IAEA has recognised the following three primary decommissioning strategies in developing IAEA safety standards (Reference 27.2):

- **Immediate dismantling** – Dismantling begins soon after shutdown of the plant (typically within 5 years) with radioactive material being removed.

- **Deferred dismantling or safe enclosure ("safe store")** – Those parts of the facility containing radioactivity are processed or brought into a condition such that they can be stored and maintained safely (e.g., liquids are drained from the system and irradiated fuel and operational waste materials removed). The facility is placed in long-term storage (for, say, 50 years) before final dismantling.

- **Entombment** – As with the deferred dismantling option, liquids and waste are removed. The remaining radioactive material is encased onsite (normally in concrete). Essentially, the site becomes a near-surface waste repository.

All the options above could be implemented for the AP1000 plant. The strategy of entombment is, however, highly unlikely to be acceptable to the public for nuclear power plants in Western Europe as it is effectively onsite disposal of HLW, which is not in line with declared government policy.

The choice therefore lies between prompt and deferred decommissioning. However, whichever option is adopted, spent fuel would be discharged from the core and kept in an interim store onsite at the end of station operation before disposal once a facility is available.

The factor that influences the two considered options, immediate or deferred decommissioning, is effectively a choice about timing. The advantages and disadvantages of immediate or deferred decommissioning are considered with respect to the AP1000 design below in Sections 27.3.2.2 to 27.3.2.6. Unless deferral can be substantiated, then immediate decommissioning is the default position.

27.3.2.2 Radioactive Waste Minimisation and Operator Exposure

Deferring decommissioning may be the most appropriate option if it allows primary circuit materials to decay to the point where waste volumes or categories are reduced, or dose to operators is significantly reduced.

Waste generation will be minimised in an AP1000 due to material selection. For example, the level of cobalt in reactor internal structures is limited to below 0.05 weight percent, and in primary and auxiliary materials to less than 0.2 weight percent, however, there is still some activation of the steel producing Co-60 in the RPV. Some concrete will also become activated, for example from module CA-04. It is expected that decommissioning of the RPV will have to be delayed for at least 8 to 10 years after cessation of plant operations to allow activity levels to drop sufficiently so that the dismantled components can be transported within the regulations applicable at that time. This delay will allow the Co-60 to decay by approximately two half-lives and the dose due to this nuclide to reduce by a factor of approximately four. Remote decommissioning methods, however, will still be required for the RPV decommissioning whether an immediate or deferred decommissioning strategy is chosen.

The inventories of activated materials for the AP1000 plant after 10, 50, and 100 years have been determined (see Appendix 27A, Table 27A-1). The data show that the reduction in activity in the period between 10 and 50 years after shutdown is relatively modest; clearly, the categorisation of the activated waste materials is unlikely to change significantly in that time.

It is concluded that, from the perspective of radioactive waste minimisation and operator radiation exposure, there is no significant benefit to be gained by deferring decommissioning.

27.3.2.3 Radioactive Waste Management and Available Disposal Routes

Disposability of Intermediate-Level Waste and Spent Fuel

The ILW and the spent fuel from the AP1000 plant at a burnup of 65 GWd/t have been assessed to be disposable in the UK (Reference 27.12). In addition, the low-level waste repository (LLWR) has agreed in principle to accept low-level waste (LLW) from AP1000 installations (Reference 27.13).

It is recognised that spent fuel will have to be allowed to cool for 100 years before it can be placed in the geological disposal facility (GDF). This is allowed for in the design.

The GDF is not yet available but the current plan is for it to be available for disposal of waste from this generation of nuclear power plants. The AP1000 design allows for passive safe storage of ILW and spent fuel until the proposed GDF becomes available.

The unavailability of the GDF at the end of the AP1000 plant operation should not delay immediate decommissioning of the reactor as the design allows for passive safe storage of ILW and spent fuel, and other wastes can be disposed of as they arise. However, the decommissioning strategy and timing of decommissioning should be reviewed if changes to either of the repositories' plans occur.

As the disposability of the spent fuel and ILW is effectively neutral in determining the decommissioning timeframe, immediate decommissioning, as the default position, remains the preferred option.

27.3.2.4 Maintenance of the Organisation and Corporate Memory

Immediate dismantling is advantageous because the workforce and management structure, and hence the corporate memory, will essentially be in place, allowing work to flow from operations to decommissioning without loss of that corporate memory.

The spent fuel store decommissioning will have to be deferred until the fuel has cooled sufficiently to be disposed of and therefore requires maintaining the organisation for a considerable period, 100 years or more. This period exceeds the decommissioning period for the AP1000 reactor itself, and so does not affect decommissioning of the power plant.

There may or may not be a substantial delay to waste store decommissioning. However, delaying reactor decommissioning (where corporate memory helps) to aid store decommissioning (where corporate memory will be much less of an issue) is not advantageous.

Based on this criterion, prompt reactor decommissioning is therefore favoured.

27.3.2.5 National and International Experience

There is a wealth of international experience now developing on the timing of decommissioning and actual decommissioning. This international experience suggests that prompt decommissioning is preferred for PWRs (Reference 27.14, Summary of Session 3).

The advantages of prompt decommissioning include the availability of an existing workforce with detailed knowledge of the plant, continuation and maintenance of the organisation, and corporate memory. Prompt decommissioning is consistent with sustainability. The most compelling reasons for deferral are considered to be immature waste management and disposal facilities and inadequate funding.

Current international practice for PWRs calls for prompt decommissioning strategies.

27.3.2.6 Conclusion of Technical Arguments on Generic Decommissioning Strategy

Based on the considerations of the various technical factors discussed above, it is concluded that the bulk of the plant and facilities will be subject to immediate decommissioning at the end of operations. However, the spent fuel and ILW will be placed into passive safe storage, spent fuel so that it can cool sufficiently to allow transfer to the GDF and ILW until the GDF becomes available.

27.3.2.7 Stakeholder Engagement and Decommissioning End Point

In addition to the technical arguments on the preferred decommissioning strategy set forth above, it is important to consider nontechnical arguments. These are likely to focus on the future use of the site and the views of a variety of stakeholders, and will develop with time. It is inappropriate to forecast these arguments at this point, but they will be taken into account by the operator closer to the time when operations cease.

27.3.3 Stages of Decommissioning

The decommissioning strategy is designed for progressive and systematic reduction of hazard, and this is achieved through a number of stages of decommissioning. The three stages of decommissioning are summarised as follows (Reference 27.3); they could overlap if appropriate but, for the sake of clarity, are considered as three distinct stages.

27.3.3.1 Stage 1

The principal activities to be accomplished during Stage 1 are as follows:

- Maintenance of buildings and systems until dismantling
- Removal of fuel from the reactor to the spent fuel pool and disposal per the established practices
- Removal of radioactive inventory from the reactor system and non-decommissioning service systems
- Contamination mapping
- Post-operational clean out and in-situ decontamination (e.g., chemical decontamination of potentially active or contaminated circuits) of non-decommissioning service systems and reactor system

- Establishment of new radiation control areas based on the above actions as work progresses
- Review configuration of service systems (e.g., electrical, piping, HVAC, radwaste, drainage, monitoring) and plan for their use/modification in decommissioning activities
- Removal of fuel from the spent fuel pool to the spent fuel store

It is expected that this phase of work will last 10 years.

27.3.3.2 Stage 2

The principal activities to be accomplished during Stage 2 are as follows:

- Modification of existing service systems and installation of temporary service systems to meet decommissioning requirements (e.g., shielding, monitoring, ventilation systems)
- Removal of radioactive inventory from the spent fuel pool system and fuel handling system
- Dismantling of non-radioactive, non-decommissioning service systems from the turbine building and disposal/recycling of inert waste
- Post-operational clean out and in-situ decontamination of spent fuel pool system and fuel handling system
- Conversion of fuel handling area, within the auxiliary building, into an interim waste storage, decontamination, waste reduction, packaging, and processing area for ILW
- Contamination mapping of radioactive, non-decommissioning service systems
- Dismantling of potentially radioactive, non-decommissioning service systems
- Ex-situ decontamination of dismantled radioactive, non-decommissioning service systems (e.g., in decommissioning building, spent fuel pool, fuel handling area, hot machine shop, radwaste building)
- Treatment, packaging and disposal of waste from potentially radioactive, non-decommissioning service systems
- Contamination mapping of potentially radioactive systems in containment

It is expected that this phase of work will last 6 years.

27.3.3.3 Stage 3

The principal activities to be accomplished during Stage 3 are as follows:

- Dismantling of reactor system. Assessment of activity levels of dismantled equipment and secure protection for transportation to waste handling areas
- Removal of radioactive inventory from residual radioactive systems in containment

- Contamination mapping of other potentially radioactive systems, the containment building, and shield building
- Dismantling of decommissioning service, non-radioactive systems from turbine building and yard. Replacement with temporary decommissioning service systems, as required
- Decontamination of dismantled reactor system ex-situ (e.g., in decommissioning building, spent fuel pool, fuel handling area)
- Post-operational clean out and in-situ decontamination of other radioactive systems in containment, the containment building (including cutting, processing, and removal of active concrete in the containment building), and the shield building
- Removal of radioactive inventory from residual radioactive systems in auxiliary building
- Disposal/recycling of inert waste from non-radioactive systems from turbine building and yard
- Packaging and disposal of radioactive waste from reactor system
- Post-operational clean out and in-situ decontamination of residual radioactive systems in auxiliary building
- Dismantling and removal of residual radioactive systems from containment
- Dismantling and removal of containment building, shield building, and turbine building,
- Ex-situ decontamination of dismantled radioactive systems from containment, and the dismantled active components of the containment building and shield building
- Disposal of inert waste from dismantled turbine building
- Dismantling and removal of remaining non-radioactive, decommissioning service systems and residual radioactive systems in the auxiliary building
- Dismantling and removal of remaining potentially radioactive, decommissioning service systems and the auxiliary building, radwaste building, decommissioning building, and LLW store. Replace with temporary systems as required.
- Ex-situ decontamination of potentially radioactive, decommissioning service systems and the auxiliary building, radwaste building, decommissioning building, and LLW store.
- Treatment, packaging, and disposal of radioactive waste from dismantled radioactive systems from containment and the dismantled active components of the containment building and shield building
- Disposal/recycling of inert waste from dismantling non-radioactive, decommissioning service systems and residual radioactive systems in the auxiliary building
- Dismantling and removal of temporary decommissioning service systems, wastewater system, annex building, and diesel generator building

- Treatment, packaging and disposal of radioactive waste from potentially radioactive decommissioning service systems, including temporary service systems.

- Disposal/recycling of inert waste from temporary decommissioning service systems, wastewater system, annex building, and diesel generator building

- Maintenance of ILW and HLW stores

It is expected that this phase of work will last 6 years.

This sequence of decommissioning works is presented in Figure 27-3.

27.3.3.4 Interim Waste Stores

The interim waste stores will be decommissioned and dismantled once all decommissioning waste has been removed from the stores and transported to the appropriate national repository or offsite waste storage facility if the repository is not available.

27.4 DECOMMISSIONING PLANNING AND IMPLEMENTATION FOR THE AP1000 DESIGN

27.4.1 Planning Overview

This section gives greater details on the implementation of the decommissioning strategy based on an assumed plant status at the end of the operational phase and an assumed target end point for decommissioning. The decommissioning operations, waste management, and safety management arrangements are also described in this section.

The operator will be responsible for updating decommissioning plans as required if UK legislation or best practise changes or if there are any changes to the assumptions made in this document.

At appropriate periods in the future, detailed decommissioning plans will be developed by the operators. During the preparation of these detailed decommissioning plans, the operator will also develop or revise the following documents prior to decommissioning operations:

- Detailed decommissioning plans (for individual plant/facilities)

- Decommissioning safety cases

- Health physics and environmental monitoring strategies

- BAT and ALARP studies (including decommissioning waste routes and waste minimisation strategies)

- Environmental impact assessment and environmental statement as required by The Environmental Impact Assessment for Decommissioning Regulations (EIADR)

- Decommissioning hazard identification

- Radioactive waste management case

- The IWS (Reference 27.3)

27.4.2 Assumed Target Decommissioning End Point

The main objectives of decommissioning any industrial site, including a nuclear power plant, are as follows:

- To ensure that the decommissioned site does not present unacceptable risks to human health or the wider environment
- To allow the release of the site for future use (e.g., for redevelopment or use as open space)

It has been assumed for the purposes of the plan that, as a minimum, the decommissioning operations would include the following:

- Removal of all hazardous materials (including wastes)
- Dismantling of plant/machinery
- Demolition of structures to 1 m below ground level

To achieve these objectives, the overriding requirement would be the safe removal of radioactive materials (to include spent fuel, radioactive wastes, and activated plant components).

The intended decommissioning end point and the subsequent management of contaminated land, if appropriate, will be addressed by the licensee as part of their update of the Decommissioning Strategy document. The assumed target decommissioning end point is described below:

- Plant and equipment will be decontaminated and radioactive materials removed and disposed of via the appropriate route.
- Structures will be de-planted and demolished during final site clearance (FSC).
- Buildings will be removed to a depth of 1 m below ground level.
- Roads, car parks, underground services, and similar structures, will be removed.
- The active drains and outfall will be removed and foul and surface water drains will be removed if less than 1 m below ground level.
- Basements, if present, will be demolished to 1 m below ground level and any remaining subsurface structures punctured to assist drainage.
- Land requiring remediation will be identified and treated appropriately.
- Ground will be appropriately landscaped, and land drains installed if required.
- After FSC, the site will be released from its Nuclear Site Licence if it is deemed appropriate.

It is noted that the eventual end use will be subject to consultation and rationalisation with UK government policy at the time and may also be subject to conditions attached to the original planning consent.

27.4.3 Assumed Plant Status at the End of Operational Life

The status of the facility at the end of its operational life and therefore the start of the decommissioning phase, the decommissioning plant status (DPS), has been assessed.

In determining the DPS, a number of assumptions have been made about the operations of the plant:

- The reactor will be operated for 60 years.
- Plant SSC will have been well maintained during its operational life through the implementation by the licensee of an effective inspection and maintenance programme
- All necessary plant support facilities (e.g., power, utilities, cooling, shielding, ventilation systems, effluent treatment, drainage, security) will be operational and maintained.
- Chemical inventories onsite will be at low levels and tanks will contain residual unused chemicals.
- Some accumulation of potentially radioactive corrosion products is to be expected in the radioactive water systems.
- Irradiated fuel will be kept in the cooling ponds after defueling. The spent fuel will then be dried and then stored for up to 100 years onsite, at which point it will be disposed of in the GDF.
- Operational ILW will be packaged in a form suitable for disposal offsite. There will be an interim passively safe storage period onsite for the waste.
- LLW will be packaged onsite for disposal. After packaging, waste disposal containers will be sent to appropriate disposal sites. It is assumed that current disposal routes (or routes similar to them) will remain available during the operational and decommissioning phases.
- A repository for spent fuel will be available.
- A disposal facility for ILW will be available.
- Any unplanned operational events that might have occurred during the operating life of the plant will have been fully remediated.
- No significant changes have been made to the design or operation of the plant.
- The radiological conditions of the main items of the plant are those shown in Appendix 27A.
- The radiological and contamination zoning of areas will be the same as that outlined in Chapter 24.

27.4.4 Decommissioning Operations and Waste Management

27.4.4.1 Decommissioning Sequence and Methodology

The stages of decommissioning have been outlined previously in Section 27.3.3. The outline decommissioning methodology for each of these stages and for the decommissioning of the site interim waste stores is outlined in the following sections. This information has been based on Sections 5.1.2 to 5.1.5 of the UK AP1000 Decommissioning Plan (Reference 27.20).

27.4.4.2 Stage 1 Decommissioning

Stage 1 decommissioning addresses:

Maintenance of buildings and systems until dismantling

- Following cessation of power generation operations, all buildings and systems will be maintained as required until they are ready to be dismantled
- Remove fuel from the reactor to the spent fuel pool
- Removal and transport of spent fuel from the reactor to the spent fuel pool as per the processes established at that time. Spent fuel will remain in the spent fuel pool until the heat output from the fuel has reduced sufficiently to meet the requirements for placement in a dry spent fuel storage container.
- Remove radioactive inventory from the reactor system and non-decommissioning service systems
- The radioactive inventory of the reactor system and the non-decommissioning service systems will be removed and treated by the existing plant radwaste systems. The term radioactive inventory refers to the radioactive contents of vessels, tanks, pipes, etc., such as water, chemicals, settled solids, ion exchange resins, and filter cartridges. There will be no removal of fixed contaminated equipment at this stage.

Contamination mapping

- Contamination mapping of all radioactive and potentially radioactive systems will be carried out to ensure that the health and safety risks associated with maintenance and dismantling of the radioactive systems are understood and the decontamination and radioactive waste treatment options can be assessed.
- Post-operational clean out and in-situ decontamination (e.g., chemical decontamination of contaminated circuits) of non-decommissioning service systems and reactor system
- The reactor cavity and radioactive, mechanical and fluid systems that are not required for decommissioning will be decontaminated and cleaned in line with the decontamination strategy described in the UK AP1000 Decontamination Considerations (Reference 27.21). Contaminated piping circuits will likely be decontaminated by an oxidative decontamination process, although other processes (e.g., oxidative/reductive processes) may be considered. The oxidative process involves ion exchange. Anion and cation resins will be used, will become active, and must be treated as active waste. It is anticipated that the AP1000 circuits will be significantly less contaminated due to the

chemistry and the addition of zinc acetate. This method of decontamination will require the provision of dedicated reagent tanks, pump skid, and the like. It may be possible to utilise existing plant equipment or alternatively explore the option of using mobile equipment during the development of the final decommissioning plan. All waste, active or not, will be treated in accordance with the requirements in force at the time of decommissioning. The system will be designed to minimise exposure and limit the potential for active water to leak and contaminate surfaces.

Establishment of new radiation control areas

- At the time the plant enters the decommissioning phase, the existing radiological control areas will remain in place. As work progresses and activity levels permit, the boundaries will be successively reduced.

Review of requirements of decommissioning service systems

- The decommissioning requirements for all service systems will be reviewed. Service systems may need to be modified according to decommissioning work package requirements. The need for temporary service systems will be identified (e.g., electrical, piping, ventilation, monitoring, and shielding systems). The existing plant radwaste systems will remain in use for as long as possible during decommissioning. The treatment of decontamination and active drain reagents may be achieved using the auxiliary building ion exchange facility. The treatment route will be assessed to determine if further treatment units (e.g., neutralising, filtration) will be required to achieve required discharge consents. Final effluent disposal will either be by routing to the site effluent treatment facility, discharge to outfall, or by collection and transfer to a designated waste effluent treatment facility, operated by a contractor. A mobile encapsulation plant will be used as far as practicable for the decommissioning and disposal of solid waste (e.g., high-efficiency particulate air (HEPA) filters, spent resins, etc.). When the auxiliary building and in particular the liquid radwaste facilities are to be decommissioned it will be possible to re-locate the encapsulation plant to either the radwaste building, or the temporary decommissioning structure for further use. The liquid radwaste equipment could then be cleaned, size reduced, and encapsulated if needed. The point at which the existing plant radwaste systems will be decommissioned will be defined in the final decommissioning plan. However, it is assumed it will be during Stage 3.

Removal of fuel from the spent fuel pool to spent fuel store

- Once the remaining spent fuel in the spent fuel pool has cooled sufficiently, the spent fuel assemblies will be transferred from the spent fuel pool to the cask loading pit by the fuel transfer system. Here they will be placed into dry storage canisters which are filled with inert gas and sealed. The sealed canisters will then be cleaned and decontaminated before being transferred to the spent fuel store using an appropriate transport vehicle.

27.4.4.3 Stage 2 Decommissioning

Stage 2 decommissioning addresses:

Modify existing service systems and install temporary service systems to meet decommissioning requirements (e.g., shielding, monitoring, ventilation systems).

Modifying existing service systems and supply temporary service systems to meet decommissioning requirements in line with the plans developed during the Stage 1 review.

Removal of radioactive inventory from spent fuel pool system and fuel handling system.

- The radioactive inventory of the spent fuel pool system and the fuel handling system will be removed and treated by the existing plant radwaste systems. Contamination mapping will be carried out to assess the decontamination and cleaning requirements and the health and safety risks associated with maintenance and dismantling of the radioactive systems.

Dismantling of non-radioactive, non-decommissioning service systems from the turbine building and dispose/recycle inert waste.

- Non-radioactive service systems (for example, circulating water cooling system) that are no longer needed to support decommissioning activities will be dismantled and removed as per the schedule established at that time. Temporary lifting and handling equipment to support plant dismantling will be brought in and installed. The active drain system will remain in operation. All waste is expected to be non-radioactive and will be disposed of/recycled by the procedures in place at that time.

Post-operational clean out and in-situ decontamination of spent fuel pool system and fuel handling system.

- The spent fuel pool, fuel handling system, and other associated areas will be decontaminated and cleaned as required in line with the decontamination strategy described in the UK AP1000 Decontamination Considerations (Reference 27.21). The treatment of decontamination and active drain reagents may be achieved using the existing ion exchange facility as described in Stage 1.

Conversion of the fuel handling building

- All fuel from the reactor and the spent fuel pool will have been removed during Stage 1 of decommissioning. The spent fuel racks will be dismantled and the pool will be cleaned and decontaminated. The HVAC systems will remain in operation. The fuel handling building will then be used as a decontamination and waste reduction area. This building, together with the temporary facility described earlier, will be sufficient to store all of the dismantled equipment removed from the plant during decommissioning. The basic premise is that there is significantly less building volume and equipment and that less of this reduced volume will be active. As items are confirmed as clean, they will be removed from the site and disposed. This facility will be used for processing ILW waste. Items will be reduced in size to accommodate their disposal in the standard waste casks (e.g., radioactive waste management (RWM) boxes and drums (Reference 27.24)) in use at that time for that waste level. Equipment to perform cutting and volume reduction activities will be installed in this building. The reduction process will be designed to minimise personnel exposure, and minimise and contain the generation of dust and the like.

- Contamination mapping of potentially radioactive, non-decommissioning service systems.

- Contamination mapping of all radioactive and potentially radioactive systems will be carried out to ensure that the health and safety risks associated with maintenance and dismantling of the radioactive systems are understood and the decontamination and radioactive waste treatment options can be assessed.

Dismantling of radioactive, non-decommissioning service systems.

- Detailed plans for the dismantling of all major equipment will be developed in the final decommissioning plan. Such plans will include provisions for limiting personnel hazards (see Section 27.4.6.2). Installed in-cell handlers will be used to remove large plant items. Remote in-cell handling equipment will be provided, where there is no man access, to facilitate dismantling of the plant.

- For removal of large plant items and modules, plans will be developed cognisant of the technical guidance such as IAEA Technical Report "Heavy Component Replacement in Nuclear Power Plants: Experience and Guidelines" (Reference 27.25). This report describes the organisational requirements necessary for large and complex removal projects, and describes suitable strategies and sequences for the removal of specific heavy components.

- Examples of outline sequences for removing large items, contaminated items and difficult to access items are provided in Section 5.1.7 of Reference 27.20.

- Before transportation to the LLW or ILW areas, dismantled equipment will be packaged and examined to determine activity levels and to confirm packages are securely protected for transportation. Stations will be set up in the auxiliary and containment buildings to provide this function. Items determined to be clean will be routed to an interim clean storage area where they will await dispatch.

Ex-situ decontamination of dismantled radioactive, non-decommissioning service systems.

- Decontamination of dismantled radioactive components will take place ex-situ in the various facilities provided (e.g., converted spent fuel pool/fuel handling area, the decommissioning facility, the health physics and hot machine shop, the radwaste building).

- Treat, package and dispose of waste from radioactive, non-decommissioning service systems.

- Radioactive waste will be classified, treated and disposed following established procedures for operational LLW and ILW as described in the UK AP1000 Radioactive Waste Arisings, Management and Disposal (Reference 27.8).

Contamination mapping of potentially radioactive systems in containment.

- Contamination mapping of potentially radioactive systems within the containment building will be carried out to ensure that the health and safety risks associated with maintenance and dismantling of the radioactive systems are understood and the decontamination and radioactive waste treatment options can be assessed.

27.4.4.4 Stage 3 Decommissioning

Stage 3 decommissioning addresses:

Dismantling of reactor system. Assess activity levels of dismantled equipment and securely protect for transportation to waste handling areas.

- The reactor system will be dismantled and components will be removed and transported to the waste processing facilities. The activity levels of the reactor pressure vessel should have dropped sufficiently so that the dismantled components can be transported within the regulations applicable at that time. The hot and cold legs will be remotely cut and removed using techniques that minimise personnel exposure. The reactor pressure vessel will be disconnected from its supports, and all piping will have been previously cut and removed. The details of this operation will be included in the final decommissioning plan. A temporary shielding structure will be produced which will cover the reactor pressure vessel and internals during lifting, upending, and transport to the processing facility. The polar crane will be used for the lifting and upending to and on the 135' (41.15m) level. The reactor pressure vessel and its transport shield can then be passed through the new opening to the jacking tower, lowered to the transporter and then taken to the processing facility. These activities can be largely completed remotely.

- An option for the reactor pressure vessel will be to dismember it in situ, package it in the approved containers, and then remove the individual containers. This will require the provision of temporary shielding and cutting processes, which will allow for flooding the reactor vessel compartments to provide additional shielding. Alternatively, reactor vessels in the United States have been disposed intact. The internals will have been removed, decontaminated, wrapped, and taken to the processing area. The transport route will be through the opening provided at the 135' (41.15m) elevation.

Removing radioactive inventory from residual radioactive systems in containment.

- Some of the systems within the containment building are expected to be radioactive (this will have been confirmed by the contamination mapping carried out at the end of Stage 2). The radioactive inventory of these systems will be removed and treated by the existing plant radwaste systems.

Contamination mapping of other potentially radioactive systems and buildings.

- Contamination mapping of the remaining radioactive decommissioning service systems will be carried out prior to commencing cleaning, decontamination, and dismantling of these systems. Contamination mapping of the containment building and shield building, auxiliary building, radwaste building, and the temporary decommissioning facility will also be carried out to assess if any of the structures or concrete are active or contaminated prior to dismantling the buildings.

Dismantling of and removal of non-radioactive decommissioning service systems.

- The non-radioactive decommissioning service systems within the turbine building will be dismantled and removed as per the schedule established at that time. Temporary lifting and handling equipment to support plant dismantling will be brought in and installed. Temporary service systems will be provided to facilitate ongoing decommissioning activities as required.

- Decontaminate dismantled reactor system ex-situ (e.g., in decommissioning building, spent fuel pool, fuel handling area).

- Decontamination of radioactive dismantled reactor components will take place ex-situ in the various facilities provided (e.g., converted spent fuel pool/fuel handling area, the decommissioning building, the health physics and hot machine shop, the radwaste building).

- Post-operational clean out and in-situ decontamination of radioactive systems in containment, the containment building (including cutting, processing, and removal of active concrete in the containment building), and the shield building.

- The radioactive systems within the containment building will be cleaned and decontaminated in line with the decontamination strategy described in the UK AP1000 Decontamination Considerations (Reference 27.21). Active concrete within the containment building will be cut, processed and removed. Concrete is considered to be active no more than 3' (0.9m) from the exposed outer edges. The cutting programme may use a diamond wire sawing technique, which will cut through the steel facing. Any active concrete will be removed under controlled conditions and processed separately. The diamond wire sawing is relatively clean in that dust can be controlled and the limited quantities of water needed can be controlled and maintained within a closed circuit. Typically blocks of concrete are cut and the active pieces removed. The removed pieces are sized for packaging to suit the approved disposal containers. Once the wire is passed around the area to be cut, the machine can be located away from the active area and shielded to minimise personnel exposure. It is anticipated that the only active concrete will be local to the reactor pressure vessel and possibly the spent fuel pool area. The same techniques will be used in both areas. Following the removal of active concrete, the containment and shield buildings will be cleaned and decontaminated as required.

Removal of radioactive inventory from residual radioactive systems in auxiliary building.

- The existing plant radwaste systems in the auxiliary building will be the last radioactive decommissioning service systems to be decommissioned. The radioactive inventory of these systems will be removed and treated by temporary service systems.

Disposing/recycling of active and inert waste.

- As decommissioning progresses, wastes from dismantled non-radioactive systems and non-radioactive wastes segregated from dismantled decontaminated radioactive systems will be disposed/recycled/recovered by the procedures in place at that time. Active wastes will be classified, treated, and disposed following established procedures for operational LLW and ILW as described in the UK AP1000 Radioactive Waste Arisings, Management and Disposal (Reference 27.8). The order in which waste from specific systems will be disposed can be seen in Figure 27.3.

- Post-operational clean out and in-situ decontamination of radioactive decommissioning service systems in auxiliary building.

- The radioactive decommissioning service systems in the auxiliary building will be cleaned and decontaminated in line with the decontamination strategy described in the UK AP1000 Decontamination Considerations (Reference 27.21).

Dismantling and removal of residual radioactive systems from containment.

- The residual radioactive systems within the containment building will be dismantled. Dismantled components will be examined to determine activity levels, securely packaged, and transported to the appropriate waste processing facilities.

Dismantling and removal of containment building, shield building, and turbine building.

- At this point the dismantling of buildings will begin. The removal of the containment building, shield building, and turbine building is a bulk material removal undertaking. This is simplified by the fact that the structures are freestanding and can be systematically removed from the top. The containment building steel pressure vessel will be stable throughout the dismantling process and can support significant weight in terms of access attachments for personnel and cutting equipment. During the removal process, individual sections of plate will need to be stabilised. Waste will be monitored prior to transportation but, as none of it should be active, it is expected that it will go directly to the clean waste areas.

Ex-situ decontamination of dismantled radioactive systems from containment and the dismantled active building components.

- Ex-situ decontamination of dismantled radioactive decommissioning systems and the dismantled active components of the containment building and shield building will take place in the various waste handling facilities (e.g., in the decommissioning building, radwaste building).

Dismantling and removal of remaining radioactive and non-radioactive decommissioning service systems and residual radioactive systems in the auxiliary building.

- The radioactive and non-radioactive decommissioning systems in the auxiliary building will be dismantled and removed as per the schedule established at that time. Temporary lifting and handling equipment to support plant dismantling will be brought in and installed as required. Dismantled equipment will be packaged and examined to determine activity levels and to confirm packages are securely protected for transportation to the waste processing areas.

Decontaminating, dismantling and removal of the auxiliary building.

- The auxiliary building will be systematically removed by cutting through the composite steel/concrete structure. Temporary HVAC together with temporary sealing for openings will ensure that airflow is controlled and inward only. None of this concrete will be active; however, some may be contaminated. Significant areas of the walls are steel faced and can be readily decontaminated. A mobile decontamination unit will be used for this purpose. It is recognised that, due to access considerations, the tanks in the lower auxiliary building may need to be first removed to a local decontamination area and then taken to the processing facility. Such items, due to access considerations, may need to be disassembled prior to removal. This then allows work to decontaminate the walls in the lower auxiliary building to proceed. Explosive removal of concrete has not been considered in the nuclear island. Floor slabs will be supported, cut, and systematically removed to expose the equipment within the rooms. Much of this equipment will be active and will be removed, packaged for local transport, and taken to the waste

processing area. Work to disconnect this equipment, most of which are modules from their systems, will have been previously completed. Dismantled components will be packaged and examined to determine activity levels and to confirm packages are securely protected for transportation to the temporary decommissioning facility.

Decontaminating, dismantling, and removal of the radwaste building.

- Prior to dismantling, the radwaste building will be manually cleaned and decontaminated as required. The building HVAC system will be maintained to minimise dust released and equipment will be manually dismantled and size reduced. The HVAC system will then be decommissioned in a similar manner, and the building cladding removed, followed by demolition of the structure itself. All wastes will be surveyed by Health Physics prior to disposal but it is anticipated this waste will be free release discharge.

Decontaminating, dismantling, and removal of the LLW store.

- The LLW store will be manually cleaned as required. It is not expected to be contaminated but decontamination may be carried out if required. A temporary HVAC system will be provided to minimise dust released and equipment will be manually dismantled and size reduced. All wastes will be surveyed by Health Physics prior to disposal but it is anticipated this waste will be free release discharge.

- Ex-situ decontamination of dismantled radioactive, decommissioning service systems and auxiliary building components.

- Ex-situ decontamination of radioactive components from the decommissioning service systems and the dismantled auxiliary building will take place in the temporary decommissioning facility.

- Treat, package and dispose of radioactive waste from dismantled radioactive decommissioning service systems and buildings.

- All remaining radioactive waste from dismantled radioactive decommissioning service systems and buildings will be treated, and packaged in the temporary decommissioning facility. Waste packages will be examined to determine activity levels and to confirm packages are securely protected for transportation to interim stores/disposal facilities/free-release as appropriate.

- In-situ decontamination and dismantling of the decommissioning building.

- Following processing of radioactive waste from dismantled radioactive decommissioning service systems and buildings, the temporary decommissioning facility will be decontaminated and decommissioned. The HVAC system will be operated while the remaining equipment is cleaned and dismantled, using the mobile decontamination unit. The HVAC system will then be shut down, cleaned, surveyed, etc., with spent filter cartridges being disposed of as ILW waste. All the equipment and structures will be surveyed prior to disposal and it is anticipated it will be LLW or free discharge. Temporary waste handling and processing facilities will be provided.

Dismantling and removal of temporary decommissioning service systems.

- The temporary decommissioning service systems provided to facilitate decommissioning of the existing systems and buildings will be decontaminated and decommissioned.

Dismantled components will be packaged and examined to determine activity levels and to confirm packages are securely protected for transportation to the temporary waste handling and processing facilities. Here the dismantled components will be treated and packaged. Waste packages will be examined to determine activity levels and to confirm packages are securely protected for transportation to interim stores/disposal facilities/free-release as appropriate.

Dismantling and removal of waste water system, diesel generator building, and annex building.

- At this stage, the waste water system, diesel generator building, and annex building will be dismantled. All waste is expected to be non-radioactive and will be disposed of by the procedures in place at that time.

Disposing of radwaste and non-radioactive waste.

- All radioactive waste generated during the final building and systems dismantling will be processed, packaged, and transported to interim storage as described in Section 27.1.1.4. Non-radioactive waste will be disposed of by the procedures in place at that time.

Maintaining ILW and spent fuel stores.

- The interim ILW and spent fuel stores will be required until the respective national repositories are available to receive waste packages for final disposal. In addition to this, spent fuel will need to remain in the spent fuel store until the heat output from the fuel has reduced sufficiently to meet the current RWM criterion for acceptance. Consequently, the ILW and spent fuel stores will need to be maintained until all waste packages have been transported off the site for final disposal.

27.4.5 Decommissioning of Waste Stores

Dismantling of ILW Store

- The store design life is substantially longer than that of the power generation facility and as such the ILW store will be a standalone structure supported by its own services and utilities. If the national ILW repository is available before the end of AP1000 operations, ILW decommissioning waste could be shipped direct to the repository without interim storage onsite. Having the national ILW repository available before the end of AP1000 operations will also allow the decommissioning and dismantlement of the on-site ILW store using the decommissioning facilities created for the AP1000.

- Once all the stored waste packages have been removed from the ILW store to off-site storage (national ILW repository or other appropriate storage facility) the building can be decommissioned. The building HVAC and effluent collection systems will continue to operate to minimise dust and effluent releases. The vault crane will be moved to the maintenance bay for decontamination. It will then be used for the lifting and removal of equipment from the building. Equipment will be decontaminated and the reagents used collected in the effluent collection system. The effluents will be routed to a temporary mobile treatment facility (e.g., filtration, ion exchange, pH neutralisation) before discharge to site drainage. Most of the equipment will be located outside of the vault and is expected to be clean. A Health Physics survey will be carried out and the waste characterised as either LLW or free discharge. Dismantling, cutting, etc., will be

performed manually. Once the equipment has been removed the effluent collection system will be drained and flushed and decommissioned in a similar manner. Any contamination will be removed by scabbling or other suitable techniques (e.g., peelable coatings), and disposed of as LLW or ILW, as required. The HVAC system will then be decommissioned, decontaminated, and surveyed, with spent cartridges being disposed of as ILW using a temporary mobile encapsulation facility. The remaining building structure will be demolished, monitored and anticipated to be free discharge to landfill or, to be used on site as backfill.

Dismantling of Spent Fuel Store

- The on-site spent fuel store will be decommissioned following the transfer of stored spent fuel to the national HLW repository (once available). On-site storage up to 160 years after plant start up may be required to allow all the fuel to decay before shipment to the national HLW repository (see Reference 27.20, Section 10.1.2). The decommissioning facilities created to handle the AP1000 and the ILW store arisings will need to be dismantled and disposed of following a period of decontamination.

- When the HLW repository is available, the spent fuel will be shipped to it and the spent fuel store can be decommissioned. This will require the use of temporary facilities to handle the wastes arising as a result of the dismantlement of the spent fuel store. Based upon the Holtec dry storage system, these wastes will comprise the steel closure lid, steel container and divider shells, the concrete support foundation and top surface pad (Reference 27.7, Section 3.5.8). Holtec's dry storage system materials were selected to ensure no chemical, galvanic, or other reactions among the materials of the HI-STORM 100U System, their contents, and the operating environment. The HLW store comprises a number of subterranean cylindrical steel and concrete cavities (see Section 27.4.5.7.4) which are expected to be free from contamination. This will be confirmed by a survey of surface radioactivity. If necessary, the cavities will be decontaminated and any active waste arising from decontamination will be handled and disposed of as LLW or ILW using a temporary mobile encapsulation facility. Following decontamination, the remaining waste materials will be characterised as either LLW or free discharge.

27.4.5.1 Shielding and Containment

Existing Shielding and Containment

The AP1000 design incorporates significant shielding and containment that is designed to be effective under all conditions anticipated in the plant life cycle.

The containment building is an integral part of the overall containment system with the functions of containing the release of airborne radioactivity following postulated design basis accidents and providing shielding for the reactor core and the reactor coolant system during normal operations. Access to the containment is provided through personnel airlocks and equipment and maintenance hatches. Access to the containment can be controlled by the health physics office in the annex building. The control room is shielded against radiation so that continued occupancy under accident conditions is possible. The fuel handling and storage facility is designed to prevent inadvertent criticality and to maintain shielding and cooling of spent fuel.

The shield building provides shielding for the containment vessel and the radioactive systems and components located in the containment building. During accident conditions, the shield building provides the required shielding for radioactive airborne materials that may be

dispersed in the containment as well as radioactive particles in the water distributed throughout the containment. The cylindrical section of the shield building also protects the containment building from external events and is a key component of the passive containment cooling system.

The auxiliary building provides protection and separation for the seismic Category I mechanical and electrical equipment located outside the containment building. It provides protection for the safety-related equipment against the consequences of internal or external events and it also provides shielding for the radioactive equipment and piping that is housed within the building. Within the auxiliary building, the fuel-handling area is designed to prevent inadvertent criticality, to maintain shielding and cooling of spent fuel and to provide protection for the spent fuel assemblies, the new fuel assemblies and the associated radioactive systems from external events. Also, the fuel-handling area is constructed so that the release of airborne radiation following any postulated design basis accident that could result in damage to the fuel assemblies or associated radioactive systems does not result in unacceptable site boundary radiation levels. Also within the auxiliary building, the control room is shielded against radiation so that continued occupancy under accident conditions is possible.

Certain areas of the annex building, such as the hot machine shop and the control support area are provided with shielding for protection against low level radiation from either internal sources or external sources under accident conditions. This is accomplished by either reinforced concrete walls or reinforced masonry walls.

Wherever possible, the existing shielding and containment in each section of the plant will remain in place until all the active equipment has been removed and all required decontamination has been completed.

Some modifications are expected to the shielding to allow access for decommissioning equipment. Revised shielding assessments will be carried out as part of the decommissioning safety assessment to ensure that any changes meet ALARP considerations.

Temporary Shielding and Containment

Whilst the shielding and containment incorporated into the design of the AP1000 plant will be retained for as long as possible during decommissioning, there will be some requirements for the provision of temporary shielding and containment. These will include:

- Shielding and containment for the temporary decommissioning facility. The facility will be designed to provide the maximum opportunities for remote working during the processing and handling of decommissioning waste in order to reduce personnel exposure.

- A temporary HVAC system and a mobile decontamination unit will be needed for the decommissioning of the auxiliary building.

- A temporary HVAC system and a mobile decontamination unit will be needed for the decommissioning of the temporary decommissioning facility.

- Provision of temporary covers and shielding of open pipe and vessel ends exposed during cutting operations and dismantling.

- A temporary shielding structure will be produced to cover the RPV and internals during lifting, upending, and transport to the processing facility.

- Temporary enclosures and tents with HVAC facilities may be used around dismantling works where there is a risk of generating airborne radioactive material.

Remote Operations

Where possible, dismantling operations for highly radioactive components will be performed remotely in order to reduce the occupational radiation exposure. Remote dismantling operations may take place behind shielding barriers, underwater, in fume hoods and in inaccessible areas.

27.4.5.2 Progressive and Systematic Reduction of the Hazard

Decommissioning plans have been developed that ensure progressive and systematic reduction of the hazard. This is achieved by the three-stage process described in Sections 27.3.3.1 to 27.3.3.3.

Stage 1 Decommissioning

The components of the plant with the highest residual activity are the fuel rods. Removal of the fuel rods from the reactor to the spent fuel pool is the first step of Stage 1 decommissioning. The reactor cavity and other areas that have been directly exposed to the fuel will have the next highest residual activity and consequently decontamination of these areas is the next step of the decommissioning sequence. Residual activity levels will be reduced by removing the radioactive inventory of service systems that are no longer needed for decommissioning.

Contamination mapping of potentially active systems and structures will be carried out to ensure that the health and safety risks associated with maintenance and dismantling of the radioactive systems are understood and the decontamination and radioactive waste treatment options can be assessed. The results of these surveys will inform the selection of cleaning and decontamination processes of the non-decommissioning service systems. The decontamination of active circuits will further reduce residual activity levels prior to the commencement of active component removal.

As decommissioning progresses, the radiological control boundaries will be successively reduced in line with the progressive reduction in hazards.

Throughout the decommissioning process ILW and LLW will continue to be generated. For this reason it is logical to retain the existing plant radwaste systems for as long as possible. Whilst at this stage the precise time at which the radwaste systems will be decommissioned cannot be specified, it is assumed it will be during Stage 3.

As soon as it has cooled sufficiently, the remaining spent fuel will be placed into dry storage canisters and transported to the spent fuel store.

Stage 2 Decommissioning

In order to meet the requirements of decommissioning activities, existing service systems will be modified and temporary service systems will be installed.

As soon as possible, following the removal of the final spent fuel, the radioactive inventory of the spent fuel pool system and fuel handling system will be removed and post-operational clean out and in-situ decontamination will be carried out. This will ensure that residual activity levels are ALARP prior to conversion of the fuel handling building to an ILW waste

processing facility. This is in line with the principle of converting existing parts of the plant to facilitate decommissioning. The spent fuel racks will be dismantled and the pool will be cleaned and decontaminated allowing the area to be used as a decontamination and waste reduction area. Potential hazards associated with these decontamination and waste reduction processes will also be reduced. For example, the volume reduction process will be designed to minimise personnel exposure, and minimise and contain the generation of dust.

Easily removable non-radioactive systems and service systems which are not required for decommissioning will be the first systems to be dismantled. This reduces hazards associated with subsequent decommissioning activities by removing potential obstructions and creating space.

Further contamination mapping will be carried out prior to the dismantling of radioactive, non-decommissioning service systems. At this point, the components with the highest residual activity are the reactor pressure vessel and internals. However, the removal of these components will be deferred to Stage 3 to allow activity levels to drop to the point where the dismembered pieces can be transported within the regulations applicable at that time. The sequence of removal of active non-decommissioned service systems will continue to follow the principle of removing components with the highest residual activity. The sequence for removal of the steam generators is outlined in Section 5.1.7 of the UK AP1000 Decommissioning Plan (Reference 27.20).

Radiation and security controls will be implemented to determine the activity levels of dismantled equipment and to confirm it is securely protected for transportation. This will allow clean equipment to be routed to an interim clean storage area. This will reduce the volume of waste sent to the temporary decommissioning facility, the radwaste building, and the converted fuel handling building. Radioactive components will be transported to the appropriate waste handling area for decontamination, processing, and packaging.

Stage 3 Decommissioning

Contamination mapping of the remaining potentially radioactive systems and buildings will be carried out at the end of Stage 2 and beginning of Stage 3.

By this point the activity levels of the RPV and the internals should have dropped sufficiently to allow them to be removed. The internals will be removed, wrapped, and taken to the processing area for decontamination and processing. The RPV will be removed following the procedure outlined in Section 5.1.4 of the UK AP1000 Decommissioning Plan (Reference 27.20).

Following removal of the RPV, non-radioactive decommissioning service systems will be dismantled and removed and replaced by temporary service systems as required. The non-radioactive systems will be removed first as this work will be easier than the removal of the radioactive systems. The radioactive decommissioning systems will be systematically decommissioned as specified in Section 5.1.4 of the UK AP1000 Decommissioning Plan (Reference 27.20). Residual hazards will be progressively reduced for each system by removing the radioactive inventory, post-operational clean out, in-situ-decontamination, and dismantling and removal of components to the waste processing areas. Here ex-situ decontamination will be carried out as appropriate and the waste will be processed, packaged, and transported to the appropriate interim store or final disposal repository, if available.

At this time the only potential activity or contamination remaining will be in structures and concrete in the containment building, shield building, auxiliary building, radwaste building, and the temporary decommissioning facility. This will have been established by the

contamination mapping carried out at the beginning of Stage 3. Any activated concrete will be removed under controlled conditions and processed separately.

Following the removal of active concrete, the containment building, shield building, and turbine building will be decontaminated in-situ and dismantled. Active and contaminated components from the containment and shield buildings will undergo ex-situ decontamination, processing, packaging, and disposal. It should be noted that the turbine building could be dismantled during Stage 2 as the systems within the building are not expected to be active and will be dismantled and disposed of during the first two years of Stage 2 decommissioning. However, it is expected that the decommissioning of other plant areas that present a greater residual risk will be carried out first and so dismantling of the turbine building will be delayed until the containment and shield buildings are ready to be dismantled.

The last potentially active or contaminated buildings to be dismantled will be the auxiliary building, radwaste building, and the temporary decommissioning facility. This will allow the waste processing and handling facilities in these buildings to remain in service as long as possible. The auxiliary and radwaste buildings will be dismantled first and active waste will be transported to the decommissioning facility for decontamination, processing, and packaging. Temporary decommissioning service systems and a mobile decontamination unit will be provided to facilitate this work. The decommissioning facility will be the last potentially active or contaminated building to be dismantled. It will be decontaminated in-situ prior to dismantling and waste will be classified and disposed of via appropriate routes.

The remaining buildings and systems will all be non-active and will be disposed of by the procedures in place at the time.

When all the active waste has been transferred from the appropriate interim store (LLW/ILW/HLW) to offsite storage, the store will be decommissioned, again following the principle of progressive and systematic reduction of the hazard.

27.4.5.3 Enabling Works

Stage 1 could begin as soon as the plant ceases to generate power, however, there is a need to allow the core barrel radioactivity levels to decay to a level where it can be safely dismantled and packaged in accordance with the requirements in force at that time. It is expected that Stage 1 will last approximately 10 years to ensure that the spent fuel has sufficient cooling time before it is transferred to dry storage. Decommissioning Stages 2 and 3 will be approximately 6 years each. These durations may be reduced and activities implemented in parallel when the final decommissioning plan is generated.

The existing plant radwaste systems will remain in use while Stage 1 and possibly Stage 2 are in progress. The point at which they will be decommissioned will be defined in the detailed decommissioning plan; it is assumed that this will be during Stage 3.

The preferred process for decommissioning is to remove major components and modules for transfer and subsequent processing in the purpose-built waste facility; this is in close proximity to, but away from, the plant. Waste processing and volume reduction activities will be conducted in the reactor building only where necessary. This will provide the maximum opportunities for remote applications for cutting and handling in a facility specifically designed for it. This will also provide opportunities to implement measures to reduce personnel exposure to ALARP.

Before any dismantling work is begun, the fuel handling area within the auxiliary building will be converted to service dismantling, decontamination, and packaging of decommissioning waste. In addition to the fuel handling area a decommissioning facility will be set up large enough to allow storage of at least two SGs, one reactor vessel, and sundry other equipment; and will include a remote handling and waste reduction process area. Equipment to perform cutting, decontamination, volume reduction, and waste packaging activities will be installed in this building.

Throughout the decommissioning process, wastes will be characterised and packaged, with size reduction as necessary. Items will be reduced in size to accommodate their disposal in the standard containers agreed upon with the RWM. The active waste packages will be placed either in passive safe storage (spent fuel and ILW) onsite, or dispatched offsite for disposal at the LLWR. Further details can be found in Section 26.7.2.3 of Chapter 26 and the Radioactive Waste Management Case Evidence Reports for ILW and HLW (References 27.22 and 27.23).

ILW will also be stored and processed in the modified spent fuel handling area in Stage 2. This cannot take place until the last of the spent fuel is removed from the spent fuel pool and the pool has been converted. Stage 1 requires the removal of all fuel from the reactor and the spent fuel area. Once this has been accomplished, the spent fuel racks will be dismantled and the pit will be cleaned and decontaminated. The HVAC systems will remain in operation.

The drainage and ventilations systems may have to be extended or adapted to meet the requirements of the decommissioning process. These changes will be addressed in the detailed decommissioning plans for the individual plant and facilities.

The modified spent fuel handling area, together with the temporary decommissioning facility, will be sufficient to store all the dismantled equipment removed from the plant during decommissioning. With significantly less building volume and equipment, less of this reduced volume will be active. As items are confirmed as clean, they will be removed from the site and disposed of.

27.4.5.4 Decommissioning Operations

The technologies to decommission the AP1000 plant currently exist. However, when the plant is due to be decommissioned, it will be the operator's responsibility to review the techniques available and to select the most appropriate one. The currently recognised techniques for decommissioning and decontamination are summarised below; further details can be found in the Radioactive Waste Arisings, Management and Disposal document (Reference 27.8, Section 5.2.4) and the Decontamination Considerations document (Reference 27.21).

- Decommissioning techniques:
  - Cutting
  - Shearing
  - Demolition
  - Fixing contamination (sealing loose contamination before dismantling)
- Decontamination techniques:
  - Chemical dissolution
  - Electrochemical
  - Abrasion

- Dry surface cleaning
- Wet surface cleaning
- Mechanical surface removal
- Liquefaction
- Degradation

Size Reduction of Large Items

The large solid radioactive waste items that will require decommissioning are the SGs, reactor head and the RPV. A number of options for removing and reducing the size of the SGs have been incorporated into their design:

- Removing the upper noncontaminated sections and lowering the remaining contaminated sections using the polar crane.

- Removing steel work and concrete to allow all of the SGs to be lowered to the ground for size reduction.

- Removing the top of the containment to remove the whole SG using an external crane.

It is expected that the SGs will be radioactive but with an activity level that will fall into the LLW category (as will be case for the other large items). It is intended that these items are handled as they arise and are reduced in size, the pieces being decontaminated to the extent practicable. Decontaminated pieces that are no longer radioactive will be released to conventional waste handling facilities for recycling or disposal. Decontaminated pieces that remain radioactive will be wrapped before placement into half-height International Organisation for Standardisation (ISO) (HHISO) containers and sent for disposal at the LLWR.

Because the upper section of the SGs may have become contaminated during operations, before wastes from these structures are disposed of, decontamination may be appropriate

Decontamination materials are expected to be similar in nature to those previously used for operating AP1000 plant LLW arisings as dealt with in the standard AP1000 plant radwaste building, and so will be packaged and disposed of in the same manner. To facilitate this disposal route, a temporary decommissioning facility will be erected, for example a tent with mobile HVAC. Laydown areas have been provided for protecting and wrapping potentially contaminated equipment prior to transfer to the waste handling facility. The area currently allocated for the temporary decommissioning facility for the GDA site is identified in Figure 27-1, Item 27.

One possible sequence for the decommissioning of the steam generators is outlined in Section 5.1.7 of the UK AP1000 Decommissioning Plan (Reference 27.20).

Other large items such as the reactor vessel, RCPs, and reactor head can be disposed of using techniques similar to those used for SGs, and are therefore not considered further here.

27.4.5.5 Feasibility Reviews

Licensee Reviews

The licensee will carry out feasibility reviews to validate methodology/techniques used in the decommissioning of the AP1000 plant. The initial decommissioning plan will be reviewed

and updated throughout the operational phase; the final decommissioning plan will be reviewed and updated during decommissioning.

Reviews of the arrangements for managing decommissioning activities will also be conducted regularly as part of the licensee's compliance with the construction design and management (CDM) regulations (Reference 27.15). These reviews will ensure that:

- Construction, dismantling and demolition work is carried out, so far as is reasonably practicable, without risk to the health and safety of any person.
- The standard of welfare facilities is adequate for all persons throughout the duration of decommissioning.
- Any structure designed for use as a workplace has been designed taking account of the provisions of the Workplace (Health, Safety and Welfare) Regulations 1992.

Office for Nuclear Regulation Reviews

In accordance with current UK government policy the ONR carries out reviews of certain licensees' decommissioning strategies to ensure that they remain soundly based as circumstances change. Guidance on the quinquennial reviews process is provided in ONR NS-TAST-GD-026 (Reference 27.16).

The licensee will also be regulated by the Nuclear Decommissioning Authority (NDA), a department within the Department of Energy & Climate Change (DECC).

27.4.5.6 Strategy for Safety Systems

27.4.5.6.1 Safety Systems Incorporated in the Design

The AP1000 design incorporates a range of engineered safety features (ESFs) which protect the public in the event of an accidental release of radioactive fission products from the reactor coolant system (Section 6.5). The ESFs include:

- Passive containment cooling system
- Passive core cooling system
- Containment isolation system
- Containment hydrogen control system
- Containment leak rate test system
- Main control room (MCR) emergency habitability systems
- Fission product removal and control systems

Each of these systems will remain active whilst fuel remains in the reactor. The MCR emergency habitability systems will be maintained whilst the control room function is required.

In addition to the ESFs, the AP1000 plant has a number of auxiliary systems that provide safety and support functions during decommissioning:

- Fuel storage and handling
- Water systems

- Process auxiliaries – compressed air, plant gas, sampling systems, drainage, chemical volume control system
- Air-conditioning, heating, cooling, and ventilation systems
- Fire protection system
- Communication system
- Plant lighting system
- Standby diesel generators and diesel fuel oil system

The fuel storage and handling systems will remain operational until all fuel is removed to dry storage. The other systems will remain active during decommissioning while their services are required and the residual risks they are designed to mitigate are still present. Where the above systems cannot be decommissioned progressively, then it may be necessary to bring in temporary equipment to provide these services. These requirements will be assessed in detail in the final decommissioning plan.

The AP1000 plant has Emergency Response Facilities (see Section 25.4) that include the MCR, the operational support centre, and the technical support centre. These areas provide communication and assembly points for staff during an emergency. The technical support centre also provides plant management and technical support to operating staff during an emergency. These facilities will be retained during decommissioning for as long as possible. If necessary, they will be replaced by appropriate temporary facilities to ensure that effective emergency response facilities are available throughout decommissioning.

27.4.5.6.2 Plant Management Safety Systems

In addition to the safety systems incorporated into the design, the licensee will need to implement appropriate plant management safety systems to cover the decommissioning activities. The licensee will be responsible for safety and environmental management of the plant through the operating life and eventual decommissioning of the plant. Westinghouse will liaise with the site licensee, regarding safety and environmental management throughout all phases of the plant life cycle (Reference 27.7).

Westinghouse can support the licensee by providing technical and design information that is relevant to decommissioning and that will assist the licensee in choosing the decommissioning strategy and preparing the initial decommissioning plan, as well as the CDM file for the decommissioning work packages.

It is anticipated that knowledge transfer and the management arrangements developed to support operation of the AP1000 plant will provide the foundations of the arrangements required for the decommissioning process. However, a review of this will be carried out during the creation of the operational management arrangements to ensure that this is true. It is expected that the decommissioning arrangements will be reviewed every 5 years.

27.4.5.6.3 Other Safety Systems Required During Decommissioning

In addition to the plant safety systems incorporated into the design (Section 27.4.5.6.1) and plant management safety systems (Section 27.4.5.6.2), the decommissioning activities may require the modification of safety systems as the dismantling progresses or the addition of

other safety systems for temporary decommissioning facilities. These requirements will be identified in the final decommissioning plan.

27.4.5.7 Decommissioning Waste Management and Disposal

To facilitate safe and effective management of wastes, they will be characterised and duly segregated according to their activity and other physical and chemical properties. This will essentially involve segregation into streams of nonradioactive waste, LLW and ILW, although further segregation within these categories may be necessary to meet the needs of the most appropriate disposal routes. After separation and segregation during decontamination and decommissioning operations, confirmatory monitoring will be undertaken prior to final consignment. The method of operational and confirmatory monitoring will be developed during the detailed decommissioning planning stage.

Application of BAT to waste management requires that all reasonable opportunities should be taken for waste minimisation, reuse, and recycling. Where possible, wastes will be declassified by segregation and cleaning to free-release standards.

27.4.5.7.1 Nonradioactive Wastes

Once segregated, these wastes will be recycled or disposed of via conventional routes. A storage facility for nonradioactive waste is provided in the AP1000 design (Figure 27-1, Item 28).

27.4.5.7.2 Low-Level Wastes

Both the radwaste building (Figure 27-1, Item 5) and the temporary decommissioning facility (Figure 27-1, Item 27) erected for LLW/ILW decommissioning processing, as described in Section 5.1.3 of the UK AP1000 Decommissioning Plan (Reference 27.20), will be used to handle LLW generated during decommissioning.

LLW will be collected and transferred to either the radwaste building or the temporary decommissioning building. The waste will then be processed. This could include decontamination, size reduction, characterisation, and further sorting, repackaging, and immobilisation.

The waste will be packaged in HHISO containers, transported to the buffer store, and finally sent to the LLWR in Cumbria for final disposal. However it is expected that this facility will close during the operating life of the first AP1000 plant. Consequently, any LLW decommissioning waste that will be generated following cessation of operation of the first AP1000 plant will need to be disposed of at a future LLWR that has not yet been specified.

The waste management strategy requires LLW to be shipped for disposal routinely according to schedules agreed to by the plant operator and the UK NDA. The LLW buffer storage area (Figure 27-1, Item 29) will be available to store LLW during periods when waste cannot be received by the LLW disposal facility. This is a covered area comprising a concrete hard standing area with a steel framed canopy. The storage area will have the capability of storing up to 2 years generation of operational LLW. The decommissioning LLW volume may require a larger LLW buffer storage area to accommodate 2 years of generation. If this is the case the storage area and canopy may need to be extended. Due to the construction of the LLW buffer store, it can be dismantled when not needed or relocated to a more convenient location onsite. A final LLW buffer store will only be dismantled upon completion of all radioactive decommissioning activities.

Further information can be found in Section 26.7.5.1 of Chapter 26 of this PCSR and the IWS (Reference 27.3, Sections 6.6 and 6.9).

27.4.5.7.3 Intermediate-Level Wastes

The strategy for dealing with ILW waste arisings is to process the waste into a stable form and then store it onsite in the ILW store.

ILW will be collected and transferred to either the radwaste building or the temporary building before treatment in the mobile encapsulation unit. Treatment could include decontamination, size reduction, characterisation; and further sorting, repackaging, and immobilisation.

Once the ILW has been encapsulated in waste packages acceptable to RWM (e.g., 500-litre drum, 3-m^3 drum and box), the boxes and drums will be transported to an onsite ILW store (see Figure 27-1, Items 21, 25, and 26), where they will be stored in a passively safe condition until a national intermediate-level waste repository becomes available. The ILW store is a reinforced concrete structure consisting of a waste package reception area and a shielded vault serviced by a certified nuclear crane. The seismic assessment has determined that the AP1000 plant ILW store does not need to be seismically qualified from the perspective of radiological consequence. The ILW store will be an independent facility that can remain operational even if the rest of the site has been decommissioned, providing that the essential infrastructure is maintained.

Further information can be found in Section 26.7.5.2 of Chapter 26 and the IWS (Reference 27.3, Sections 6.7 and 6.9).

It has been assumed that ILW will have to be stored onsite until suitable disposal facilities become available. If alternative offsite storage facilities become available, then the potential for their use will be addressed in the IWS and decommissioning strategy documents.

27.4.5.7.4 Spent Fuel

After spent fuel is removed from the reactor, it will be stored in the fuel storage pool. Because spent fuel is not expected to be reprocessed, the HI-STORM 100U System (or another equivalent cask system) is proposed to dry-store it once it has been removed from the spent fuel pool and dried using helium. The spent fuel assemblies will then be transferred from their dry cask storage to the national GDF once it is available, with repackaging carried out as appropriate.

The dry spent fuel storage is a seismically qualified, below-ground dry-storage facility with design features considered to minimise unauthorised intrusion and to provide radiation shielding. The location of the spent fuel store is shown in Figure 27-1, Items 22 to 24. The spent fuel store will be an independent facility that can remain operational even if the rest of the site has been decommissioned, providing that the essential infrastructure is maintained.

It has been assumed that spent fuel will have to be stored onsite until suitable disposal facilities become available. If alternative offsite storage facilities become available, then the potential for their use will be addressed in the IWS and decommissioning strategy documents.

Further information on radioactive waste management can be found in Chapter 26 (in which Section 26.7 addresses the solid radwaste system).

27.4.5.7.5 RWM Disposability Assessment

RWM has concluded that ILW and spent fuel from operation and decommissioning of an AP1000 plant should be compatible with plans for transport and geological disposal of higher activity wastes and spent fuel (Reference 27.12).

RWM expect that these conclusions eventually would be supported and substantiated by future refinements of the assumed radionuclide inventories of the higher activity wastes and spent fuel, complemented by the development of more detailed proposals for the packaging of the wastes and spent fuel and better understanding of the expected performance of the waste packages (Reference 27.12). This information would be developed as part of the detailed site specific decommissioning plan that would be prepared by the licensee during the operational phase of the AP1000 plant.

On the basis of the GDA Disposability Assessment for the AP1000, RWM has concluded that, compared with legacy wastes and existing spent fuel, no new issues arise that challenge the fundamental disposability of the wastes and spent fuel expected to arise from operation of such a reactor (Reference 27.12).

27.4.5.7.6 Volumes of Decommissioning Wastes

The total ILW decommissioning waste associated with large-volume components and waste from decontamination operations is estimated to be about 800 m^3. The total LLW associated with decommissioning large- and small-volume components, compactable dry active waste, and demolition waste is estimated to be about 5500 to 6000 m^3. Further details can be found in Appendix 27A, Tables 27A-2 to 27A-5.

A typical schematic for the treatment of decommissioning waste is shown in Figure 27-2. The management of decommissioning waste is being planned with the expectation that the LLW, ILW, and spent fuel waste streams can be disposed of in NDA facilities.

27.4.5.8 Sensitivity of the Waste Streams to Decommissioning Processes

27.4.5.8.1 Effectiveness of Decontamination

Decontamination processes will be adopted with the aim of changing the classification of the decommissioning waste to the lowest level possible. The aim will be to reduce, where possible, ILW to LLW and LLW to free release material. Effective monitoring of activity pre and post decontamination is important in confirming the waste classification and reducing quantities of ILW and LLW produced during decommissioning.

The mass of decommissioning waste in each ILW and LLW waste classification is sensitive to the effectiveness of the selected decontamination techniques (see Section 27.4.5.9).

27.4.5.8.2 Waste Form

The waste streams produced during decommissioning are sensitive to different decommissioning processes because different processes may result in different forms of waste being produced. For example:

- Different size-reduction processes may generate different amounts of active fines which may produce wastes that require stabilisation or dusts that require filtration.
- Different decontamination processes may produce different solid or liquid secondary wastes (see Section 27.4.5.4).
- For ILW the stabilisation techniques and grout addition rates may vary according to the form of the waste and this will affect the total number of waste packages generated.

27.4.5.8.3 Waste Volume

The waste volume generated during decommissioning is sensitive to the decommissioning processes adopted. For example:

- The adoption of refined cutting techniques (e.g., diamond wire sawing) can remove contaminated concrete to a specific depth of contamination and can be used to minimise the amount of concrete that is classified as radioactive waste.
- Disposal of large items without size reduction may be possible but would result in disposal of a much larger volume of waste.
- The selection of compaction or super compaction will affect the volume of LLW produced.

The mass of the radioactive components that require being decommissioned as identified in the disposability assessment (Reference 27.12) is unlikely to vary significantly as a function of different decommissioning methods. However, the volume of the waste radioactive components is sensitive to the size reduction and packaging techniques that may be employed.

27.4.5.9 Impact of Decontamination on Primary Waste Volumes

Decontamination will be used to reduce the contamination levels of decommissioned materials where BAT and ALARP analyses indicate that it is beneficial. For example, where practicable, decontamination will be used to recover wastes so that they can be reused or recycled. Decontamination may also allow the radiological waste classification of primary wastes to be reduced from ILW to LLW or LLW to free release for disposal by conventional nonradioactive routes. Wastes generated during decommissioning will be segregated into different waste types to allow optimum use of the various decontamination routes available at the time of decommissioning.

The majority of the waste arisings from the decommissioning of small and large volume components, as identified in appendices A3 and A4 of the AP1000 UK Environment Report (Reference 27.7), will undergo swabbing/monitoring to determine their activity and, if necessary, will be subject to decontamination. The aim is to reduce the waste activation level so that it may be reclassified. The wastes will be monitored to assess if this has been achieved

and further decontamination will be carried out if necessary. This process will result in reductions in the volumes of ILW and LLW requiring processing and disposal.

Also, prior to demolition, plant modules will be monitored to assess the contamination levels of the steel and concrete. Decontamination of the modules will be carried out in order to reduce the activation levels from LLW to free release levels where possible. The decontamination will be aided by the use of concrete walls with decontaminable coating and steel surfaces with surface finishes that will prevent penetration of contamination.

No credit has been taken in the disposability assessment (Reference 27.12) for the effect of decontamination on the estimated ILW and LLW arisings. At this stage no estimate has been made of the benefit that decontamination processes may provide in reducing the quantities of ILW and LLW decommissioning waste.

27.4.5.10 Generation of Secondary Wastes

27.4.5.10.1 Liquid Wastes

Some decontamination operations will produce secondary liquid wastes. These may include the following:

- **Detergent wastes** – Wet surface cleaning operations may produce detergent wastes. These will be collected and monitored to assess activity levels. When the activity levels are above acceptable limits, the wastes will be treated through the existing plant radwaste systems but if this is not possible processing will be carried out using mobile equipment. Processing will typically involve a concentration step (e.g., evaporation or reverse osmosis) in order to reduce the volume of waste to the extent necessary to allow an encapsulation plant to immobilise the concentrate in a cementitious grout. The liquids remaining after the concentration step (condensed evaporator distillate or reverse osmosis permeate) will be monitored to assess if further treatment is required prior to discharge.

- **Chemical wastes** – Decontamination processes such as chemical dissolution will produce chemical wastes. These will be collected in the chemical waste tank and pH and other chemical adjustment will take place as required. The wastes will be monitored and if the activity levels are deemed to be above acceptable limits, the waste will be processed using mobile equipment or combined with detergent wastes and processed as detergent waste.

27.4.5.10.2 Solid Wastes

Some decontamination operations will produce secondary solid wastes. These may include:

- **Filters** – Some decontamination and decommissioning operations will produce airborne particulates. These operations include cutting, abrasion, mechanical surface removal (e.g., scabbling) and demolition. These operations will be carried out using the BAT and ALARP techniques so that the amount of dust produced is minimised. However some dust capture by air filtration will be necessary and this will generate spent filters as a secondary waste. The spent filters will be monitored to assess activity levels so they can be processed and disposed of appropriately.

- **Swabs** – Dry surface cleaning will generate contaminated swabs as secondary waste. These will be monitored, classified and disposed of appropriately.

- **Activated resins** – Decontamination of active piping circuits will likely be carried out by an oxidative decontamination process. This involves an ion exchange process using anion and cation resins to absorb activation released by the process. These resins will become active and will be encapsulated in a cementitious grout in a similar way to operational ion exchange resins.

27.4.5.10.3 Quantity of Secondary Wastes

The quantity of secondary wastes that will be generated from the decontamination processes will be dependent on the methods employed and the extent of their use. This will need to be defined as the initial decommissioning plan is developed in detail, but no estimates have been made at this time.

27.4.5.11 Use of Best Available Technique and Waste Management Hierarchy in Decommissioning

27.4.5.11.1 Waste Hierarchy

The licensee will implement the principles of the waste hierarchy (avoid, minimise, recycle/reuse, abate) during decommissioning operations. Throughout the plant operational life and during decommissioning, the AP1000 Integrated Waste Strategy (Reference 27.3) will be reviewed by the licensee to maximise waste reuse and recycling wherever possible.

The AP1000 design includes features that avoid and minimise waste production (Section 27.2.2.2). Decontamination techniques will be selected to minimise the waste produced and to reduce the radiological waste classification during decommissioning (Section 27.4.5.9).

Where waste is produced it will be treated by appropriate techniques (e.g., segregation, size reduction, encapsulation, packaging) to ensure that the waste is in the most appropriate form for disposal.

27.4.5.11.2 Best Available Technique Assessment and Implementation

The plant has design features that avoid the early foreclosure of decommissioning options, and will be operated and maintained, so as to avoid the early foreclosure of decommissioning options which may restrict the implementation of BAT.

The licensee will carry out regular reviews of the methodology/techniques used in the decommissioning of the AP1000 throughout the life cycle of the plant (Section 27.4.5.5). As part of these reviews, the methodology and techniques that are considered to be BAT will be regularly assessed. By deferring the design and construction of the decommissioning facilities towards the end of operations, it will be possible to ensure that the techniques associated with the most up to date BAT assessment are built into the decommissioning facilities that are constructed.

27.4.5.12 Timescale and Programme

The estimated decommissioning timescales for the active facilities are:

- Stage 1 – 10 years
- Stage 2 – 6 years
- Stage 3 – 6 years

The stages of decommissioning could overlap if appropriate but, for the sake of clarity, are considered as three distinct stages.

RWM calculations have indicated that for the limiting irradiation fuel (i.e., at highest burnup), a cooling period of 100 years would be needed to allow disposal in their generic intended design concept. Therefore, the spent fuel may have to be stored in passive safety onsite for that length of time.

ILW will have to be stored onsite in a passively safe state until the future GDF is available to receive ILW.

It has been estimated that a period of 10 years will be required to transfer all the spent fuel to the GDF with another 10 years required to complete decontamination and decommissioning of the spent fuel storage facilities. Similarly, it has been assumed that a period of 10 years will be required to transfer all the ILW to the GDF and to decontaminate and decommission the ILW storage facilities. Given that there is currently a lack of a definitive GDF design and that these timescales will not affect the initial decommissioning programme, these estimates seem reasonable.

This programme of decommissioning works is presented in Figure 27-4.

This programme will be further developed by the operator as the decommissioning strategy and detailed decommissioning plans are reviewed during the lifetime of the AP1000 plant operation.

The passively safe storage facilities for spent fuel and ILW will be designed for 100 years. If after this period there is no GDF (or centralised storage facility) available, or if longer cooling periods are required, then the facilities will be assessed for life extensions and appropriate actions taken to ensure continued safe storage.

27.4.6 Safety Management Arrangements

Organisational safety management arrangements will be the responsibility of the operator. The operator will be responsible for ensuring that organisational arrangements are established and maintained to ensure safe and effective decommissioning of facilities. This responsibility includes a requirement to identify in the safety cases for operation and decommissioning an appropriate management organisation and resource for safe operation and decommissioning. The organisation is likely to change at the end of operations and the start of decommissioning. The organisation should be designed to achieve the activities being undertaken at the time; this organisation may change during the different decommissioning stages and should be reviewed if activities change. The operator is responsible for ensuring that its staff and contractors receive suitable training for roles that they will be required to undertake during decommissioning, which could be different from their previous roles in the operational phase.

The decommissioning safety case will be updated towards the end of reactor operations and before decommissioning starts. It will also be amended as necessary during the decommissioning process to take into account changes in both facilities and hazards. The decommissioning safety case will address existing and new hazards that will be present during decommissioning. The level of detail included will be proportionate to the radiological hazard.

Prior to decommissioning, a fault analysis review will be undertaken. The review will specifically target new faults or operational changes that could arise from decommissioning and is not applicable to current operations.

A review of the hazards that may be encountered during decommissioning should be carried out before decommissioning commences as part of decommissioning planning and safety case preparation. Any changes to the plant required for decommissioning should be substantiated before implementation, and should take into account the following:

- Safety function categorisation
- Examination, inspection, maintenance, and testing arrangements
- Onsite and offsite emergency plans
- Onsite and offsite monitoring programmes

External contractors are likely to be employed during decommissioning operations. The operator will be responsible for maintaining the function of intelligent customer during these operations to ensure that decommissioning operations are carried out safely. The operator is also responsible for ensuring that contractors are suitably qualified and experienced for the work that they are to perform.

The operator will be responsible for determining how these safety arrangements will be managed, but it is likely that the decommissioning arrangements will build upon and be consistent with the operational arrangements.

27.4.6.1 Experience of Decommissioning and Hazards Encountered

Westinghouse has a wealth of experience in nuclear decommissioning, including decommissioning of PWRs as well as other reactor types. Westinghouse will draw upon this experience to assist the licensee to develop a safe and cost-effective decommissioning strategy for the AP1000 plant.

A nonexhaustive list of Westinghouse's global decommissioning experience includes:

- Fort St Vrain (United States (US))
- Vandellos 1 (Spain)
- Zorita (Spain) (PWR)
- CIEMAT Research Facilities (Spain)
- Three Mile Island (TMI) 2 (US) (PWR)
- Yankee Rowe (US) (PWR)
- Trojan (US) (PWR)
- Qinshan (China) (PWR)
- Connecticut Yankee (US) (PWR)
- San Onofre (US) (PWR)
- Shoreham (US)
- Fukushima 2 (Japan)
- Forsmark 1/2/3 (Sweden)
- Oskarshamn 1/2 (Sweden)
- TVO Olkiluoto 1/2 (Finland)
- Chooz A (France) (PWR)
- KNK (Germany)

Past experience indicates that record keeping and plant knowledge are important in facilitating the decommissioning process. The decommissioning plan should reflect that retention of this knowledge base would be a major contributor to a safe, efficient and cost effective decommissioning process.

Westinghouse believes the decommissioning experience accumulated thus far all indicates that the most appropriate philosophy for decommissioning is the same as that embodied in the AP1000 plant construction plan which is to remove components/modules as complete units as far as possible (Reference 27.17).

The first AP1000 plants are under construction in China and the US. It is probable that these plants will reach the end of their operational life before any plant built in the UK. If these plants are subject to immediate dismantling, then there will be lessons learnt from their decommissioning that may benefit the final decommissioning plan required for any UK AP1000 plant.

27.4.6.2 Decommissioning Hazards

27.4.6.2.1 Significant Hazards

The major hazards anticipated during the decommissioning process are industrial and radiological. From past decommissioning experience, these two hazards can interact and complicate each other, for example, inadequate consideration of decommissioning activities during structural design has led to difficulties in retrieving radioactive waste and in some cases hampered sampling to determine the hazardous radiological characteristics.

The major anticipated hazards are as follows:

Radiation Hazards

- Direct radiation
- Radionuclide inhalation/ingestion
- Loss of containment
- Radioactive waste

Industrial Hazards

- Heavy/dropped loads
- Working at height
- Tripping/falling
- Fire
- Noise
- Vibration
- Dust
- Electric shock
- High temperatures
- High pressures
- Enclosed spaces

Toxic Materials

- Residual chemicals
- Decontamination chemicals

- Nonradioactive waste

27.4.6.2.2 Identification of Hazards

Referring to the final decommissioning plan, a decommissioning safety case will be developed by the operator. During decommissioning, the safety case will be updated when necessary to reflect the impact of modifications to the facilities and to address the changing nature of the hazard.

The PCSR uses a number of checklists to identify hazards for consideration in the AP1000 Design Basis Assessment, Probabilistic Risk Assessment, Severe Accident Analysis and assessment of internal and external hazards (see Chapters 9 through 12). Collectively these checklists provide comprehensive and systematic hazard identification. These checklists will be reviewed and hazards assessed for their applicability to the decommissioning operations.

The final decommissioning plan will identify a number of individual decommissioning work packages. The implementation of CDM through the operator's or decommissioning contractor's management system will ensure that the hazards associated with each individual decommissioning work package will be fully evaluated before the project is initiated. A key aim of CDM is to identify hazards early on, so they can be eliminated or reduced at the design or planning stage and the remaining risks can be properly managed.

A survey of radiological and nonradiological hazards will be made as an important input to the safety assessment for decommissioning and for implementing a safe approach during the work. The survey should be conducted to identify the inventory and location of radioactive materials and other hazardous materials. Special attention will be paid during the characterisation of any fissile material that may be left in the plant. Uncertainty about the amounts of fissile material could have severe consequences if assessments for criticality are incomplete or wrong (Reference 27.18).

The radiation and contamination surveys determine the radionuclides, maximum and average dose rates, and contamination levels for inner and outer surfaces throughout the facility. Contamination mapping may then be used to plot the location of the hazards in order to facilitate the development of appropriate safety precautions and to help prioritise the decommissioning works.

Particular decommissioning challenges are associated with removal of heavy components, for example:

- SGs
- Reactor vessel head
- Reactor vessel internals
- Pressuriser
- Reactor coolant piping/recirculation piping

Radiation hazards associated with decommissioning these heavy items may arise during decontamination operations and when the internal active surfaces are exposed during opening or cutting operations. Other radiation exposures may occur during the preparation of containment openings and handling of large items in the designated laydown areas. The safe, hoisting and handling of these large items presents a significant industrial hazard. Lifting engineers will be used to prepare lifting plans to minimise the risks associated with such operations.

The polar crane used during the operation of the site will be retained ready for use during the decommissioning of heavy items. The polar crane structure has sufficient capacity to handle heavy equipment with the addition of a larger capacity hoist module. In addition the polar crane can accommodate the upper assembly of the SGs between the girders.

27.4.6.2.3 Protection Measures

The measures to protect against the significant hazards are similar to the control measures identified in Section 27.4.6.3.

27.4.6.3 Control Measures

The control measures required for each individual decommissioning work package will be developed as part of the final decommissioning plan and related decommissioning safety case and project specific implementation of the CDM. For each activity consideration will be given to:

- ALARP/BAT
- Skills/training
- Written procedures
- Area classification
- Decontamination (chemical/mechanical)
- Access/egress
- Ventilation
- Shielding
- Remote operations/robotics
- Scaffolding/safe lifting/cranes
- Temporary facilities
- Personal protective equipment
- Dose rate/occupancy factors
- Fire safety
- Noise reduction
- Monitoring
- Laydown areas
- Waste treatment/packaging

During Stage 1 decommissioning the first contamination barrier is kept as it was during operation, but the mechanical opening systems are permanently blocked and sealed (e.g., with valves or plugs). This allows the decommissioning and removal of ancillary systems to reduce the hazards from minor systems, whilst making use of radioactive decay in the main hazards to naturally reduce the potential dose uptake from activities.

Equipment will be removed floor by floor such that activities are controlled within a particular plant area and can be easily supervised. Work will be carried out away from access/egress points where practicable. Where such work is unavoidable, consideration will be given to scheduling this work last, again, if practicable. Remaining, contaminated items will then be surveyed, and as before, appropriate systems of work put in place to enable their safe removal.

27.4.6.4 Manual and Remote Tasks

Remote Operations

The decision to select human or robotic decommissioning methods will largely be determined by the outcome of the contamination mapping exercise (see Section 27.4.6.2.2). This information will be used to assess the predicted cumulative dose for the task with the available shielding layout. Other important factors in the selection of human or robotic tasks are design and availability of robotic equipment and the accessibility of the working area.

Where possible, dismantling operations for highly radioactive components will be performed remotely in order to reduce the occupational radiation exposure. For example, removal of the RPV and internals is a task which has been carried out remotely by Westinghouse at several nuclear sites (e.g., Fukushima 2, San Onofre, Yankee Rowe).

Examples of operations that could be done also manually in lower active areas but are typically undertaken remotely in highly active areas include:

- Mechanical, thermal or hydraulic cutting (e.g., diamond wire cutting, band saw, abrasive water jet cutting, plasma arc cutting)
- Grinding, blasting, welding, hammering
- Lifting, jacking
- Disassembly of small components
- Sludge recovery
- Decontamination
- Monitoring (e.g., TV cameras, radiation)
- Handling of radioactive waste (ILW and HLW)

Manual Operations

There will be many manual tasks which need to be undertaken to decommission the facility. It is envisaged that skilled personnel will be engaged to assess, plan and safely execute the required tasks under controlled systems of work. This may include removal of smaller items such as pumps and pipe work and some decontamination and size-reduction operations carried out in the radwaste building, for example.

Manual dismantling may be aided at certain stages by means of the partial or total decontamination of the structures or systems to be dismantled to reduce the level of radiological controls required.

Low activity or clean plant and equipment are assumed to be removed manually, by a suitably qualified and experienced person (SQEP).

Removal of steelwork and concrete structures may involve the use of both SQEP and remotely operated equipment.

27.4.6.5 Industrial Safety Hazards

The industrial safety hazards are identified in Section 27.4.6.2.1 and control measures are shown in Section 27.4.6.3. The anticipated significant nonradioactive hazards may include:

- **Access** – Provisions for items such as access routes/equipment hatches/removable gratings/lifting equipment have been included in the design, and would be subject to routine monitoring and controlled under a written system of work to ensure that unnecessary dose is not accrued by e.g., transient workers.

- **Building integrity** – The buildings will have stood for over 60 years and therefore need to be regularly inspected to ensure their integrity remains, and no unacceptable hazards arise during the decommissioning works. Where new access points need to be provided, assessments will be made to ensure that the building structural integrity is not compromised.

- **Environment** – Environmental conditions (e.g., flood risk) may change over time. Therefore, periodic reviews of external risks to site integrity posed by the environment will be undertaken to assess the impact (if any) on proposed decommissioning activities.

- **Lifting activities** – Lifts will be assessed to determine their potential to impact on safety critical systems should a failure under load occur. It is expected that during decommissioning activities there will be an increased number of lifts compared to operational activities.

- **Manual operations** – Skilled trades such as scaffolding/welding/fitting would be required to do much of the decommissioning work. Controlling the tasks using a safe system of work, pursuant to CDM will ensure that risks to personnel are reduced to tolerable levels. Working at height can pose a particular risk from falls, or dropped objects. A high standard of safety principles and clear expectations will supplement the safe approach to decommissioning.

27.4.6.6 Record Management for Decommissioning

There are specific records that must be maintained during the operational life of the plant for the subsequent decommissioning phase, and the design documents that form a basis for this will be transferred from the vendor to the licensee when the licensee takes plant ownership. This information will include the following:

- A full set of design drawings
- Pre-Operation Safety Report
- A record of regulator discussions and agreements

The operator will be responsible for procuring the plant and for establishing a full set of as-built drawings for the plant. Westinghouse will be available to assist with this and to review any suggested design changes to the plant to ensure that they are not detrimental to the operation and decommissioning of the plant. Further details can be found in the Plant Life Cycle Safety Report (Reference 27.19, Sections 4 and 9.3.5).

During the operational phase of the plant, the operator will be responsible for maintaining records of the plant for use during decommissioning; these records will include the following information:

- Plant modifications
- Operational history
- Incident records
- Radiological surveys
- Radioactive substances and radioactive waste quantities, locations, condition, and ownership, with specific focus at the end of normal operations
- Waste treatment and disposal records
- Safety cases for operations, decommissioning, and waste management
- Regulator interactions and agreements
- The physical condition of the facility, including examination, maintenance, inspection, and testing records

During the decommissioning phase of the project, the operator will be responsible for keeping records of the following:

- The history of decommissioning operations
- Decommissioning reports to show how the objectives of the decommissioning plan, including the planned end-state for the facility, have been achieved
- Waste disposal records

The operator will be responsible for the generation, retention, and ownership of documents and records. The very long timescales involved in the operations and decommissioning of the AP1000 plant will be a major consideration in determining the form and manner in which documents and records are generated and retained.

27.4.6.7 Knowledge from Other Occurrences

As stated above in Section 27.4.3, a number of assumptions have been made when determining the suggested decommissioning strategy. So that the effects on decommissioning of other occurrences can be determined, the plant operators will review the impact of operational events and design changes on decommissioning plant status. These events may have an impact on decommissioning in a number of ways including the following:

- Practicalities of decommissioning such as access and dismantling techniques that can be used
- Dose to operators during decommissioning
- Radiological conditions of the DPS
- Waste volumes

When any significant changes occur, then the plant operator will be responsible for reviewing and updating as necessary the decommissioning strategy, plans, and safety case.

27.4.7 Stakeholder Engagement

The plant operators will be responsible for developing a stakeholder engagement process for decommissioning. This engagement process will be designed to ensure a wide ranging and inclusive consultation on relevant issues. The process will be flexible to allow engagement on any topics determined by the plant operator and should also allow alignment with other stakeholder processes. The stakeholder engagement process developed for the specific site must incorporate:

- Independence
- Transparency
- Openness
- Clarity
- Accessibility

During development, the stakeholder engagement process should consider diverse mechanisms to ensure that information is effectively communicated and that stakeholders have adequate opportunity for engagement. The following are examples of such mechanisms:

- Engagement workshops
- Plant operator website
- Posted information in local public buildings
- Site visitor centre
- Local liaison committee meetings held regularly throughout the year

Because the decommissioning strategy will be a living document developed throughout the life of an operating AP1000 plant, stakeholder involvement will be sought at all pertinent opportunities.

Typical stakeholders could comprise:

- Local authorities and bodies, for example: town, parish, district, and county councils
- Local organisations, for example: landowners' associations, national farmers' union, business associations, local members of parliament, and local residents
- Emergency and health services, for example: Civil Nuclear and County Constabularies, and county fire and rescue services
- Government agencies and regulators, for example: EA, Food Standards Agency, , NDA and ONR.
- AP1000 plant operators

27.5 LAND REMEDIATION

A contaminated land strategy is not required until a specific site has been identified. The operator will be required, however, to provide a strategy that sets out measures to detect radioactively contaminated land and to manage any such land that is identified. This strategy should be integrated with other relevant strategies.

The operator of the plant will be required to establish the following:

- Routine health physics surveys of ground at intervals appropriate to the level of risk in the survey areas.

- Boundary groundwater monitoring. This would include bore holes to intercept all groundwater horizons downstream of any potential contamination sources, and bore holes upstream to give background data. These would be sampled at appropriate intervals.

- Procedures required if spills occur.

If any contamination were to be found, it would need to be characterised, recorded, monitored, controlled, and remediated as appropriate.

27.6 CONCLUSIONS

The design of the AP1000 plant supports safe decommissioning. Steps have been taken to minimise the amount of waste generated during this process. Assumptions have been made about the status of the plant at the end of operations based on the design and operational guidance set out in this document.

The decommissioning strategy identifies the principles on which the AP1000 plant will be decommissioned and describes the reasoning behind the timing of decommissioning, which is proposed to be immediate. Ultimately, however, the operator will review this decision, taking into consideration conditions at the time.

A decommissioning plan has been developed based on this strategy (Reference 27.20). It is based on current available techniques; dose management is considered to be ALARP. The plan meets UK regulatory requirements and international best practice.

The design minimises waste volumes and activities. It is recognised that disposal routes for higher-activity materials will not be available immediately when that waste is processed. Therefore, a period of interim storage onsite is envisaged. The waste will be stored onsite in specifically designed facilities in a passively safe condition. An interim passively safe storage system will not compromise disposability.

27.7 REFERENCES

27.1 Office for Nuclear Regulation, “Licence condition handbook”, January 2016.

27.2 IAEA Safety Guide WS-G-2.1, “Decommissioning of Nuclear Power Plants and Research Reactors,” 1999.

27.3 Westinghouse Report UKP-GW-GL-054, Rev. 1, “UK AP1000 Integrated Waste Strategy,” March 2011.

27.4 “Safety Assessment Principles for Nuclear Facilities, 2014 Edition,” Rev. 0, Office for Nuclear Regulation, 2014.

27.5 Regulatory Guidance Series, No. RSR 1, “Radioactive Substances Regulation – Environmental Principles,” Version 2, UK Environment Agency, April 2010.

27.6 Not used.

27.7 Westinghouse Report UKP-GW-GL-790, Rev. 6, "UK AP1000 Environment Report," January 2017.

27.8 Westinghouse Report UKP-GW-GL-027, Rev. 2, "Radioactive Waste Arisings, Management and Disposal," March 2011.

27.9 IAEA Safety Report Series No. 62, "Proactive Management of Ageing for Nuclear Power Plants," International Atomic Energy Agency, 2009.

27.10 IAEA Safety Report Series No. 15, "Implementation and Review of a Nuclear Power Plant Ageing Management Programme," International Atomic Energy Agency, 1999.

27.11 UK Government Cm 2919, "Review of Radioactive Waste Management Policy – Final Conclusions," Her Majesty's Stationery Office, 1995.

27.12 Westinghouse Report UKP-GW-GL-012, Rev. 0, "Generic Design Assessment: Summary of Disposability Assessment for Wastes and Spent Fuel Arising from Operation of the Westinghouse Advanced Passive Pressurised Water Reactor (AP1000)," October 2009.

27.13 5-A-015, "Form D1 Application: Licensed AP1000 Operator," Shirley Jackson, letter to Allan Carson, 9 September 2009.

27.14 IAEA International Conference on Lessons Learned from the Decommissioning of Nuclear Facilities and the Safe Termination of Nuclear Activities, 11-15 December 2006, Athens, Greece.

27.15 UK Statutory Instrument No. 320, "The Construction (Design and Management) Regulations (S.I. 2015/51)," 2015.

27.16 NS-TAST-GD-026, Nuclear Safety Technical Assessment Guide, "Decommissioning," Rev. 3, Office for Nuclear Regulation, May 2013.

27.17 NEA No. 6924, "Applying Decommissioning Experience to the Design and Operation of New Nuclear Power Plants," Nuclear Energy Agency, 2010.

27.18 IAEA Safety Guide No. WS-G-2.4, "Decommissioning of Nuclear Fuel Cycle Facilities," International Atomic Energy Agency, 2001.

27.19 Westinghouse Report UKP-GW-GL-737, Rev. 2, "Plant Life Cycle Safety Report," March 2011.

27.20 Westinghouse Report UKP-GW-GL-795, Rev. 0, "UK AP1000 NPP Decommissioning Plan," March 2011.

27.21 Westinghouse Report UKP-GW-GL-084, Rev. 0, "UK AP1000 Decontamination Considerations," March 2011.

27.22 Westinghouse Report UKP-GW-GL-055, Rev. 2, "UK AP1000 Radioactive Waste Management Case Evidence Report for Intermediate Level Waste," March 2011.

27.23 Westinghouse Report UKP-GW-GL-056, Rev. 2, "UK AP1000 Radioactive Waste Management Case Evidence Report for High-Level Waste," March 2011.

27.24 Generic Repository Studies, "Generic Waste Package Specification," Vol.1, Nirex Report N/104, 2005.

27.25 IAEA, "Heavy Component Replacement in Nuclear Power Plants: Experience and Guidelines, IAEA Nuclear Energy Series No. NP-T-3.2," International Atomic Energy Agency, 2008.

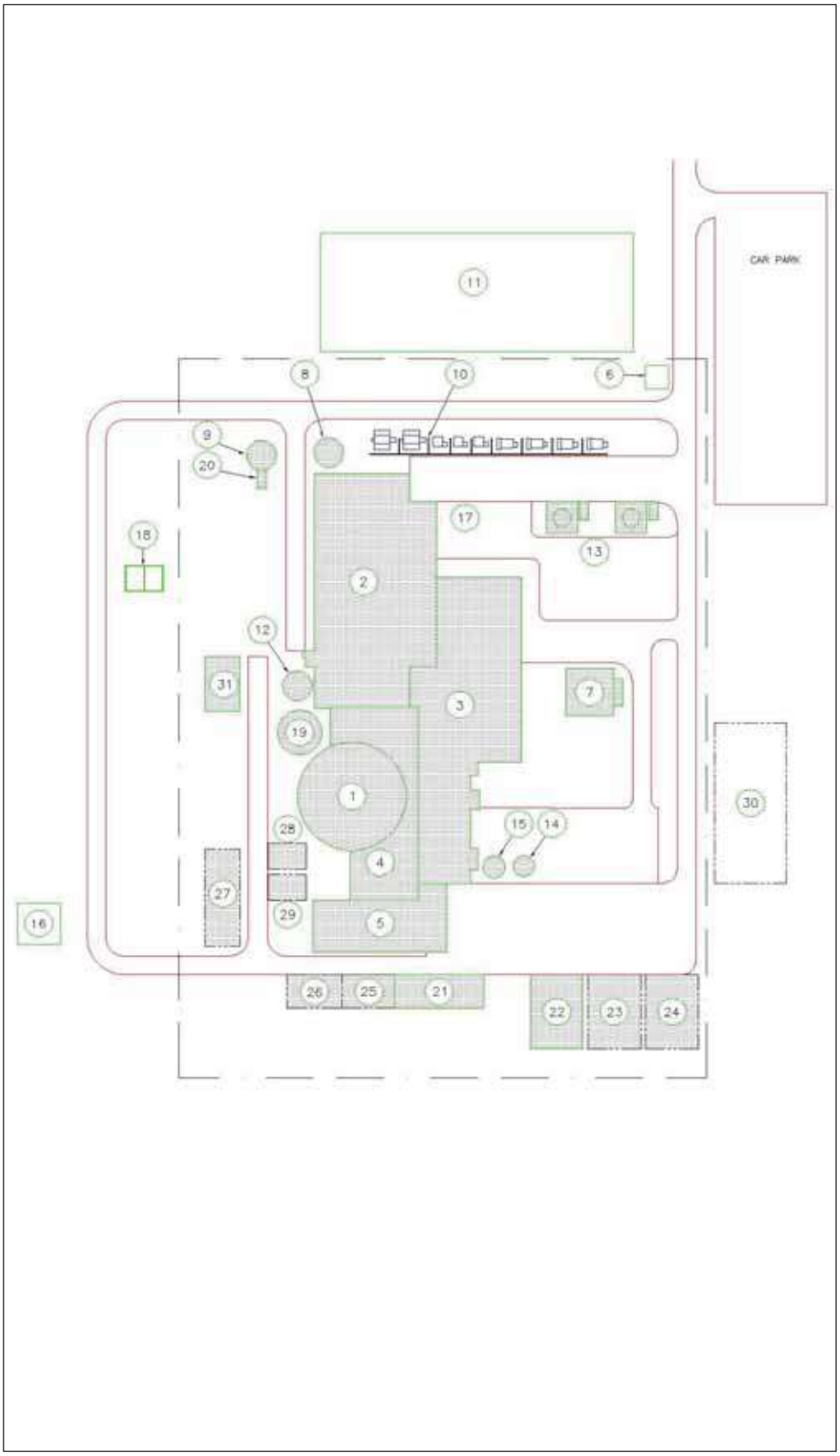


Figure 27-1. Typical AP1000 Design Plot Plan (Page 1 of 2)

Item	Description
1	Containment shield building
2	Turbine building
3	Annex building
4	Auxiliary building (contains fuel handling area)
5	Radwaste building
6	Plant entrance
7	Diesel generator building
8	Fire water/clearwell storage tank
9	Fire water storage tank
10	Transformer area
11	Switch yard
12	Condensate storage tank
13	Diesel generator fuel oil storage tanks
14	Demineralised water
15	Boric acid storage tank
16	Hydrogen storage tank area
17	Turbine building letdown area
18	Waste water retention basis
19	Passive containment cooling ancillary water storage tank
20	Diesel-driven fire pump/enclosure
21	ILW store (20 years)
22	Spent fuel store (20 years' storage)
23	Spent fuel store extension 1 (40 years)
24	Spent fuel store extension 2 (60 years)
25	ILW store extension 1 (40 years)
26	ILW store extension 2 (60 years)
27	Decommissioning facility (future)
28	Storage area for nonradioactive waste
29	Storage area low-level waste
30	Area for contractors' compound
31	Area for storage of large radioactive components

Figure 27-1. Key to Typical AP1000 Design Plot Plan (Page 2 of 2)

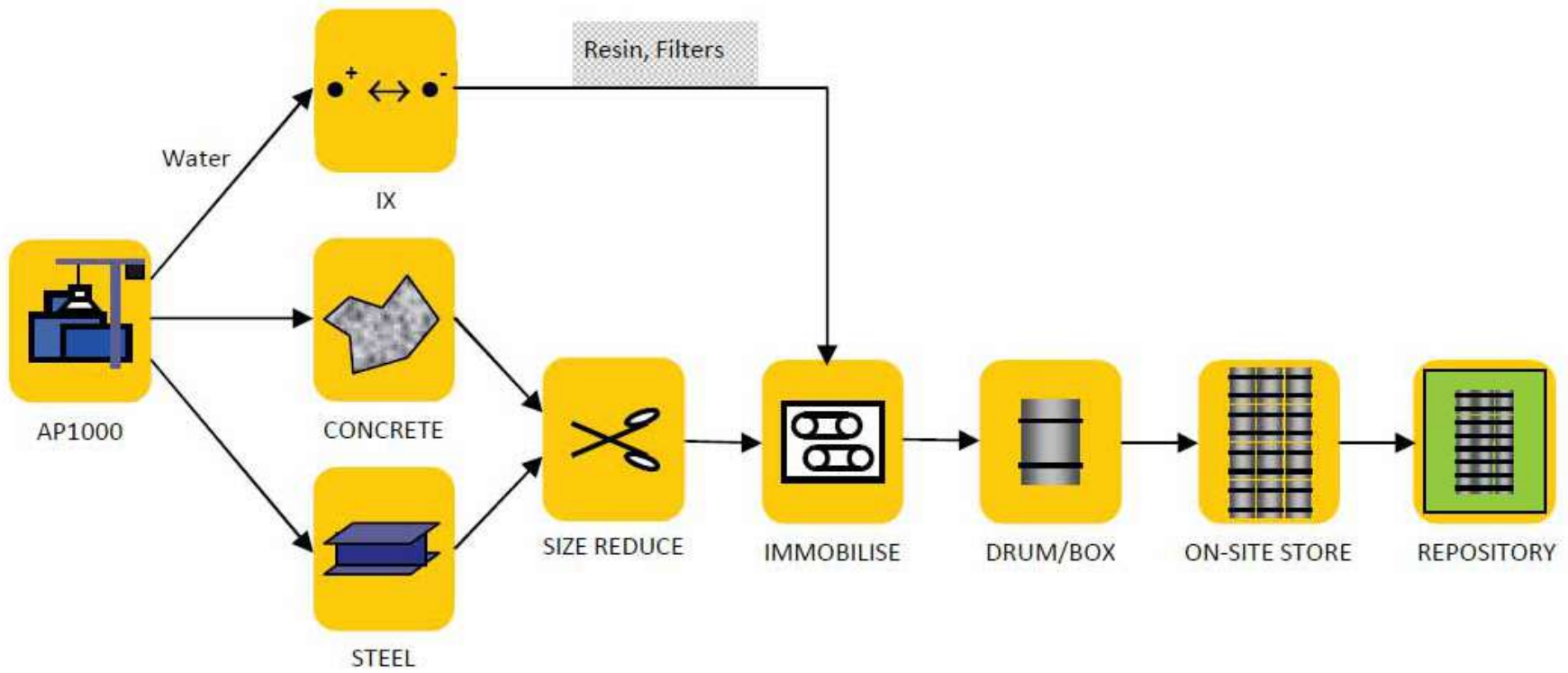


Figure 27-2. Decommissioning Waste Treatment and Disposal

Work Package No.	Work Area Location: Annex Building	Auxiliary Building	Containment	Containment Shield Building	Decommissioning Building	Diesel Generator Building	Turbine Building	Field	Pump Intake Structure	Radwaste Building	Radwaste Store	Various - Services	Yard	System Code	System Description	Type	Decommissioning Service	Activity: HLW	ILW	LLW	Potentially Active	Non-active	Stage 1 (~10 years)	Stage 2 (~6 years)	Stage 3 (~6 years)
1							+							BDS	Steam Generator Blowdown System	MF	n					+	M	SD W	
2							+							CFS	Turbine Island Chemical Feed System	MF	n					+	M	SD W	
3							+							FWS	Main and Startup Feedwater System	MF	n					+	M	SD W	
4							+							GSS	Gland Seal System	MF	n					+	M	SD W	
5							+							HSD	Heater Drain System	MF	n					+	M	SD W	
6							+							MSS	Main Steam System	MF	n					+	M	SD W	
7							+							MTS	Main Turbine System	MF	n					+	M	SD W	
8		+					+							CCS	Component Cooling Water System	MF	n					+	M	SD W	
9							+		+					CWS	Circulating Water System	MF	n					+	M	SD W	
10							+							TCS	Turbine Building Closed Cooling Water System	MF	n					+	M	SD W	
11							+						+	ZVS	Excitation and Voltage Regulation System	EI	n					+	M	SD W	
12							+							CMS	Condenser Air Removal System	MF	n					+	M	SD W	
13							+							HCS	Generator Hydrogen and CO2 Systems	MF	n					+	M	SD W	
14							+							HSS	Hydrogen Seal Oil System	MF	n					+	M	SD W	
15							+							LOS	Main Turbine and Generator Lube Oil System	MF	n					+	M	SD W	
16							+							TOS	Main Turbine Control and Diagnostics System	EI	n					+	M	SD W	
17							+							ZRS	Offsite Retail Power System	EI	n					+	M	SD W	
18		+	+											PSS	PSS Primary Sampling System	MF	y		+	+			M RI CM P M	CM SD DE RW	
19			+											CNS	Containment System	MF	n		+	+			M RI CM P M	CM SD DE RW	
20	+	+	+											CVS	Chemical and Volume Control System	MF	n		+	+			M RI CM P M	CM SD DE RW	
21		+	+											SGS	Steam Generator System	MF	n		+	+			M RI CM P M	CM SD DE RW	
22			+											RCS	Reactor Coolant System	MF	n		+	+			M RI CM P M	CM SD DE RW	
23			+											PXS	Passive Core Cooling System	MF	n					+	M RI CM P M	CM SD DE RW	
24		+	+											RNS	Normal Residual Heat Removal System	MF	n					+	M RI CM P M	CM SD DE RW	
25							+							CPS	Condensate Polishing System	MF	n					+	M HI CM P M	CM SD DE RW	
26		+		+										PCS	Passive Containment Cooling System	MF	n					+	M CM P M	CM SD DE RW	
27			+											IIS	Incore Instrumentation System	MF	n					+	M CM P M	CM SD DE RW	
28							+							CSD	Condensate System	MF	n					+	M CM P M	CM SD DE RW	
29							+							CES	Condenser Tube Cleaning System	MF	y					+	M CM P M	CM SD DE RW	
30		+	+				+							SMS	Special Monitoring System	EI	y					+	M CM M	CM SD DE RW	
31		+	+											PMS	Protection and Safety Monitoring System	EI	y					+	M CM M	CM SD DE RW	
32	+	+	+											DAS	Diverse Actuation System	EI	n					+	M CM M	CM SD DE RW	
33							+							VTS	Turbine Building Ventilation System	MF	y					+	M	MR	SD W
34		+												VES	Main Control Room Emergency Habitability System	MF	y					+	M	MR	SD W
35	+	+					+						+	ZAS	Main Generation System	EI	y					+	M	MR	SD W
36												+		EGS	Grounding and Lightning Protection System	EI	y					+	M	MR	SD W
37							+							DTS	Demineralized Water Treatment System	MF	y					+	M	MR	SD W
38							+							SSS	Secondary Sampling System	MF	y					+	M	MR	SD W
39							+							TSD	Turbine Island Vents, Drains and Relief System	MF	y					+	M	MR	SD W
40		+												ISD	Class 1E dc and UPS System	EI	y					+	M	MR	SD W
41							+							ASS	Auxiliary Steam Supply System	MF	y					+	M	MR	SD W
42							+						+	RWS	Raw Water System	MF	y					+	M	MR	SD W
43							+						+	SWS	Service Water System	MF	y					+	M	MR	SD W
44			+											RXS	Reactor System	MF	n	+					SF M RI CM P M	CM SD DE RW	
45							+								Turbine Building	S	n					+	M	SD W	
46			+											VCS	Containment Recirculation Cooling System	MF	y					+	M CM M	MR	CM RI P SD DE RW
47		+												VUS	Containment Leak Rate Test System	MF	y					+	M CM M	MR	CM RI P SD DE RW
48			+											VLS	Containment Hydrogen Control System	MF	y					+	M CM M	MR	CM RI P SD DE RW
49	+	+												VFS	Containment Air Filtration System	MF	y		+	+			M CM M	MR	CM RI P SD DE RW
50		+	+				+							PLS	Plant Control System	EI	y					+	M CM M	MR	CM RI P SD DE RW
51		+	+											SFS	Spent Fuel Pit Cooling System	MF	y	+	+	+			M CM M	SF RI P MR	CM RI P SD DE RW
52		+	+											FHS	Fuel Handling and Refueling System	MF	y		+	+			M CM M	RI P MR	CM RI P SD DE RW
53			+												Containment Building	S	n		+	+			M CM M		CM P SD DE RW
54				+											Shield Building	S	n					+	M CM M		CM P SD DE RW
55	+	+												VBS	Nuclear Island Nonradioactive Ventilation System	MF	y					+	M	MR	SD W
56												+		VWS	Central Chilled Water System	MF	y					+	M	MR	SD W
57					+									VZS	Diesel Generator Building Ventilation System	MF	y					+	M	MR	SD W
58												+		ELS	Plant Lighting System	EI	y					+	M	MR	SD W
59												+		SES	Plant Security System	EI	y					+	M	MR	SD W
60												+		MHS	Mechanical Handling System	MF	y					+	M	MR	SD W
61												+		CAS	Compressed and Instrument Air Systems	MF	y					+	M	MR	SD W
62												+		FPS	Fire Protection System	MF	y					+	M	MR	SD W
63												+		PGS	Plant Gas Systems	MF	y					+	M	MR	SD W
64		+												OCS	Operation and Control Centres	EI	y					+	M	MR	SD W
65												+		DWS	Demineralized Water Transfer and Storage System	MF	y					+	M	MR	SD W
66													+	ZBS	Transmission Switchyard and Offsite Power System	EI	y					+	M	MR	SD W
67	+	+												VXS	Annex/Auxiliary Nonradioactive Ventilation System	MF	y					+	M	MR	SD W
68												+		VYS	Hot Water Heating System	MF	y					+	M	MR	SD W
69					+									DOS	Standby Diesel Fuel Oil System	MF	y					+	M	MR	SD W
70												+		PWS	Potable Water System	MF	y					+	M	MR	SD W
71	+													ECS	Main AC Power System	EI	y					+	M	MR	SD W
72		+												ESD	Non-Class 1E dc and UPS System	EI	y					+	M	MR	SD W
73					+									ZOS	Onsite Standby Power System	MF	y					+	M	MR	SD W
74												+		EFS	Communication Systems	EI	y					+	M	MR	SD W
75													+	EHS	Special Process Heat Tracing System	EI	y					+	M	MR	SD W
76												+		EQS	Cathodic Protection System	EI	y					+	M	MR	SD W
77												+		DSD	Data Display and Processing System	EI	y					+	M	MR	SD W
78								+						MES	Meteorological and Environmental Monitoring System	EI	y					+	M	MR	SD W
79												+		TVS	Closed Circuit TV System	EI	y					+	M	MR	SD W
80												+		DRS	Storm Drain System	MF	y					+	M	MR	SD W
81												+		RDS	Gravity and Roof Drain Collection System	MF	y					+	M	MR	SD W
82												+		SSD	Sanitary Drainage System	MF	y					+	M	MR	SD W
83		+												WGS	Gaseous Radwaste System	MF	y		+	+			M CM M	MR	CM RI P SD DE RW
84	+													VHS	Health Physics and Hot Machine Shop HVAC System	MF	y					+	M CM M	MR	CM RI P SD DE RW
85												+		RMS	Radiation Monitoring System	EI	y					+	M CM M	MR	CM RI P SD DE RW
86		+							+					WLS	Liquid Radwaste System	MF	y		+	+			M CM M	MR	CM RI P SD DE RW
87		+												WRS	Radioactive Waste Drain System	MF	y		+	+			M CM M	MR	CM RI P SD DE RW
88		+												WSS	Solid Radwaste System	MF	y		+	+			M CM M	MR	CM RI P SD DE RW
89		+												VAS	Radiologically Controlled Area Ventilation System	MF	y		+	+			M CM M	MR	CM RI P SD DE RW
90									+					VRS	Radwaste Building HVAC System	MF	y					+	M CM M	MR	CM RI P SD DE RW
91		+							+						LLW Store	S	y					+	M CM M	MR	CM RI P SD DE RW
92		+	+	+				+						SJS	Seismic Monitoring System	EI	y					+	M CM M	MR	CM RI P SD DE RW
93		+													Auxiliary Building	S	y					+	M CM M	MR	CM RI P SD DE RW
94									+						Radwaste Building	S	y					+	M CM M	MR	CM RI P SD DE RW
95					+										Decommissioning Building	S	y					+	M CM M	MR	CM RI P SD DE RW
96												+		WWS	Waste Water System	MF	y					+	M	MR	SD W
97	+														Annex Building	S	y					+	M	MR	SD W
98						+									Diesel Generator Building	S	y					+	M	MR	SD W
99												+			Temporary Electrical Systems		y					+		MR	SD W
100												+			Temporary Piping Systems		y					+		MR	SD RW
101												+			Temporary Ventilation Systems		y					+		MR	SD RW
102												+			Temporary Monitoring Systems		y					+		MR	SD RW
103												+			Temporary Shielding Systems		y					+		MR	SD RW
104											+				ILW Store	S	y					+		M	
105											+				HLW Store	S	y					+		M	

Key			
Mechanical & Fluid Systems, Components and Equipment	MF	M	Maintain
Electrical & Instrument System	EI	SF	Spent Fuel Removal
Structure	S	RI	Remove Radioactive Inventory
		CM	Contamination Mapping
		P	Post-operational Clean Out / Decontamination In-Situ
		MR	Maintain and Reconfigure to Decommissioning Requirements
		SD	System Dismantling
		DE	Decontamination Ex-Situ
		RW	Radwaste - Classify, Dispose
		W	Waste - Reuse, Recycle, Dispose

Figure 27-3. Outline Decommissioning Sequence

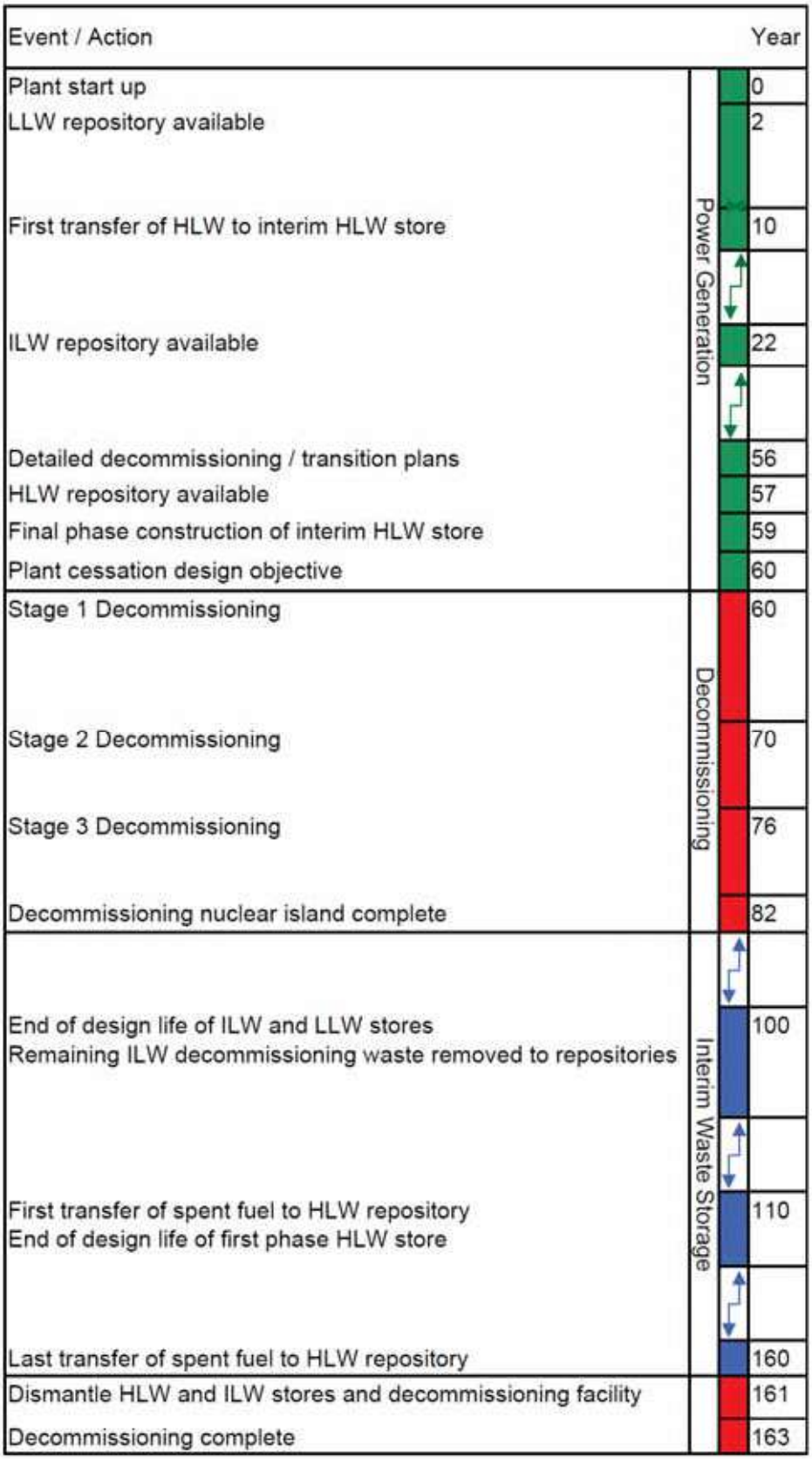


Figure 27-4. Outline Decommissioning Programme

APPENDIX 27A
INVENTORIES OF ACTIVATED MATERIALS AND RADIOACTIVE WASTE ARISINGS

Table 27A-1 summarises the inventory of activated material after 10, 50, and 100 years of decay. A conservative approach has been taken, and basic data regarding activity levels for a typical PWR has been used with the estimated quantities for the AP1000 plant.

Tables 27A-2 to 27A-5 are taken from the Environment Report (Reference 27.7, Table 3.5-10, Appendices A4, A5, and A6) and estimate the radioactive waste arisings from decommissioning.

Table 27A-1. Summary of Inventory of Activated Material After 10, 50, and 100 Years' Decay

Component	Material	Mass (t)	Decay Time (y)	Isotopic Activity (MBq)											Total Activity (MBq)	Mean Specific Activity (MBq/t)
				H-3	Fe-55	Co-60	Ni-59	Ni-63	Nb-93m	C-14	Ca-41	Sm-151	Eu-152	Ho-166m		
Radial Shield																
Baffle, barrel, neutron pads and formers	Stainless steel	66	10		1.3E+10	4.3E+9	9.4E+7	1.5E+10	4.3E+8						3.3E+10	5.0E+8
			50				9.4E+7	1.1E+10							1.2E+10	1.8E+8
			100				9.4E+7	8.0E+9							8.2E+9	1.2E+8
Vessel and vessel cladding	Mild/ stainless steel	333	10	1.8E+6	2.7E+7	7.2E+6	9.3E+4	9.0E+6						4.5E+7		1.4E+5
			50	1.7E+5			9.3E+4	6.6E+6						6.9E+6		2.1E+4
			100	1.1E+5			9.3E+4	4.5E+6						4.7E+6		1.4E+4
Insulation and liner	Stainless/ mild steel	23	10	6.2E+4	9.4E+5	2.6E+5	2.8E+3	2.7E+5							1.5E+6	6.5E+4
			50	6.5E+3			2.8E+3	2.0E+5							2.2E+5	9.6E+3
			100				2.8E+3	1.4E+5							1.5E+5	6.5E+3
Primary shield concrete (including reinforcement)	Concrete and mild steel	1089	10	1.1E+7	1.9E+6	2.9E+5		1.2E+5		3.4E+3	3.5E+4	3.3E+3	6.4E+5	2.2E+3	1.4E+7	1.3E+4
		792	50	1.1E+6				9.3E+4		3.4E+3	3.5E+4	2.5E+3	6.9E+4	2.1E+3	1.3E+6	1.6E+3
		531	100	6.8E+4				6.5E+4		3.4E+3	3.5E+4	1.7E+3	4.2E+3	2.1E+3	1.8E+5	3.4E+2

Table 27A-1. Summary of Inventory of Activated Material After 10, 50, and 100 Years' Decay (cont.)

Component	Material	Mass (t)	Decay Time (y)	Isotopic Activity (MBq)											Total Activity (MBq)	Mean Specific Activity (MBq/t)
				H-3	Fe-55	Co-60	Ni-59	Ni-63	Nb-93m	C-14	Ca-41	Sm-151	Eu-152	Ho-166m		
Upper Axial Shield																
Upper core plate Support columns Upper core support plate	Stainless steel	42	10 50 100	5.7E+6 6.0E+5	7.1E+7	4.4E+7	1.1E+6 1.1E+6 1.1E+6	1.0E+8 7.8E+7 5.5E+7	2.7E+6						2.3E+8 8.1E+7 5.7E+7	5.5E+6 1.9E+6 1.4E+6
Lower Axial Shield																
Lower core plate to lower tie plate	Stainless steel	41	10 50 100	2.6E+7 2.8E+6 1.7E+5	9.1E+8	4.6E+8	1.2E+7 1.2E+7 1.2E+7	1.3E+9 9.7E+8 6.9E+8	2.5E+7						2.7E+9 1.0E+9 7.1E+8	6.6E+7 2.4E+7 1.7E+7

Table 27A-1. Summary of Inventory of Activated Material After 10, 50, and 100 Years' Decay (cont.)

Component	Material	Mass (t)	Decay Time (y)	Isotopic Activity (MBq)											Total Activity (MBq)	Mean Specific Activity (MBq/t)
				H-3	Fe-55	Co-60	Ni-59	Ni-63	Nb-93m	C-14	Ca-41	Sm-151	Eu-152	Ho-166m		
Other Items																
RPV lateral supports RPV support boxes	Mild steel	155	10 50 100	2.8E+5 1.4E+4	4.3E+6	1.2E+6	1.3E+4 1.3E+4 1.3E+4	1.2E+6 4.5E+5 3.1E+5							6.8E+6 4.9E+5 3.3E+5	4.4E+4 3.2E+3 2.1E+3
RPV vertical supports Instrument tubes	Stainless steel															
Loop pipes (2.5 m lengths from nozzles)	Stainless steel	20	10 50 100	4.5E+4 1.0E+4	6.9E+5	1.9E+5	2.1E+3 2.1E+3 2.1E+3	1.9E+5 3.2E+5 2.3E+5							1.1E+6 3.5E+5 2.5E+5	5.5E+4 1.8E+4 1.2E+4

Table 27A-1. Summary of Inventory of Activated Material After 10, 50, and 100 Years' Decay (cont.)

Component	Material	Mass (t)	Decay Time (y)	Isotopic Activity (MBq)				Total Activity (MBq)	Mean Specific Activity (MBq/t)
				Fe-55	Co-60	Ni-63	H-3		
Reactor Building									
RPV head	Steel	1665	10	5.1E+6	1.4E+7	7.4E+6		2.7E+7	1.6E+4
SG			50		7.6E+4	5.9E+6		6.0E+6	3.6E+3
Primary coolant circuit			100			4.3E+6		4.4E+6	2.6E+3
Tanks	Steel	973	10	6.4E+5	1.8E+6	9.3E+5		3.4E+6	3.5E+3
Heat exchangers			50		9.7E+3	7.4E+5		7.6E+5	7.8E+2
Liners			100			5.4E+5		5.5E+5	5.7E+2
Concrete	Concrete	1840	10				1.8E+4	1.8E+4	9.8E+0
			50				2.0E+3	2.0E+3	1.1E+0
			100				1.4E+2	1.4E+2	7.6E-2
Auxiliary Building									
Pumps	Steel	97	10	1.1E+5	2.9E+5	1.7E+5		5.8E+5	5.8E+3
Tanks			50		1.6E+3	1.2E+5		1.3E+5	1.3E+3
Heat exchangers			100			9.3E+4		9.3E+4	9.6E+2
Filters and demineralisers									
Structural steel	Steel	365	10				1.4E+4	1.4E+4	3.8E+1
			50				1.6E+3	1.6E+3	4.4E+0
			100				9.2E+1	1.1E+2	3.0E-1

Table 27A-1. Summary of Inventory of Activated Material After 10, 50, and 100 Years' Decay (cont.)

Component	Material	Mass (t)	Decay Time (y)	Isotopic Activity (MBq)				Total Activity (MBq)	Mean Specific Activity (MBq/t)
				Fe-55	Co-60	Ni-63	H-3		
Concrete	Concrete	2300	10				2.2E+4	2.2E+4	9.6E+0
			50				2.4E+3	2.4E+3	1.1E0
			100				1.4E+2	1.7E+2	7.4E-2
Fuel Building									
Pumps Heat exchangers Filters Liners	Steel	15	10 50 100	2.8E+4	7.9E+4 4.2E+2	4.1E+4 3.2E+4 2.3E+4		1.5E+5 3.3E+4 2.3E+4	1.0E+4 2.2E+3 1.5E+3
Structural steel	Steel	206	10				4.2E+3	4.2E+3	2.0E+1
			50				4.7E+2	4.7E+2	2.2E+0
			100				2.7E+1	3.2E+1	1.6E-1
Concrete	Concrete	530	10				5.1E+3	5.1E+3	2.1E+1
			50				5.6E+2	5.6E+2	2.3E0
			100				3.2E+1	3.8E+1	7.2E-2
Radwaste Building									
Pumps Tanks Heat exchangers Filters and demineralisers	Steel	87	10 50 100	1.4E+5	3.9E+5 2.2E+3	2.0E+5 1.6E+5 1.2E+5		7.4E+5 1.7E+5 1.2E+5	8.7E+3 2.0E+3 1.4E+3

Table 27A-1. Summary of Inventory of Activated Material After 10, 50, and 100 Years' Decay (cont.)

Component	Material	Mass (t)	Decay Time (y)	Isotopic Activity (MBq)				Total Activity (MBq)	Mean Specific Activity (MBq/t)
				Fe-55	Co-60	Ni-63	H-3		
Structural steel	Steel	535	10				1.9E+4	1.9E+4	3.6E+1
			50				2.1E+3	2.1E+3	3.9E0
			100				1.2E+2	1.4E+2	2.6E-1
Concrete	Concrete	2300	10				2.2E+4	2.2E+4	9.6E0
			50				2.4E+3	2.4E+3	1.1E0
			100				1.4E+2	1.7E+2	7.4E-2

Table 27A-2 Summary of Main Radwaste Arisings from Decommissioned Process Equipment

Waste Description	Waste Level	Volume[1]	Mass	Notes
		Cubic Meters	Tonnes	
Reactor Vessel and Pressuriser tanks	ILW	388	426	
Pumps – various	ILW	100	327	
Reactor System Internals	ILW	*	146	*individual pieces
Process Equipment Internals – various	ILW	185	291	
Heat Exchangers	ILW	9	10	
Filters – various	ILW	6	8	
Pressuriser Heaters	ILW	0.05	0.16	
Waste from system decontamination operations (e.g., spent resins and spent filter cartridges)	ILW	~85	~102	Mass based on average density 1200 kg/m^3
SGs/Heat Exchangers – various	LLW	1,493	1,281	
Reactor Integrated Head Package	LLW	224	118	
Tanks	LLW	808	94	
Ion exchange systems	LLW	15.1	28	
Pumps	LLW	32	16	
Fasteners	LLW	4	15	
Insulation	LLW	22	8	
HVAC Filters – various	LLW	35	8	
Adsorbers	LLW	7	4	
Small vessels	LLW	0.02	0.02	
Compacted dry active waste generated during decontamination operations	LLW	81	121	Mass based on average density 1500 kg/m^3

Note:

1. Volume basis may include protruding appendages such as nozzles and brackets allowing the component to fit into an overpack for transport without modification.

Table 27A-3. Estimated Radwaste Arising from Small-Volume Components at Decommissioning

System	Waste Description		Waste Level	Disposability	
	Component	Type		Pre- conditioning	Disposal Route[1]
All systems	Fans, blowers, and drives (122)	Fans	LLW	9	C or B
All systems	Instrumentation elements (3337)	Instruments	LLW	9	C or B
All systems	Wire and cable ac (2498)	ac circuits	LLW	9	C or B
All systems	Wire and cable dc (328)	dc circuits	LLW	9	C or B
BDS	Electrodeionisation units A and B	Ion-migration equipment	LLW	9	C or B
FHS	FHS underwater camera system	Camera	LLW	9	C or B
FHS	Fixed underwater light	Light	LLW	9	C or B
FHS	Portable underwater light	Light	LLW	9	C or B
FHS	Refuelling pool underwater filtration system	Filter	LLW	2 or 15	B or J
FHS	Underwater cameras (4)	Cameras	LLW	9	C or B
VFS	Containment exhaust electric heater (2)	Heaters	LLW	9	C or B
VHS	Health Physics & Hot Machine Shop AHU A	HVAC filter	LLW	2 or 3	B
VHS	Health Physics & Hot Machine Shop AHU B	HVAC filter	LLW	2 or 3	B
WSS	Resin slurry conditions monitor	Camera	LLW	9	C or B
WSS	Resin slurry inlet camera	Camera	LLW	9	C or B
WSS	Resin slurry recirculation camera	Camera	LLW	9	C or B
–	Hot machine shop decon. glove box	Skid	LLW	9	C or B
–	Hot machine shop portable decon. system	Skid	LLW	9	C or B
–	Power transformers (50)	Transformers	LLW	9	C or B
–	Shield below MS59	Plate	LLW	9	C or B

Note:
1. See Table 27A-4 for key of disposal routes.

Table 27A-4. Key for Preconditioning and Disposal Methods

Pre-conditioning Method	
1.	Immobilisation in a cementitious grout within a $3m^3$ RWM approved drum
2.	Immobilisation in a cementitious grout within a $3m^3$ RWM approved box
3.	Compacted (Possible super compaction) into a 200L RWM approved drum and placed into HHISO container
4.	Placed in “baskets” in the RWM (possibly grouted), e.g., 4 m box
5.	Collection and passed to monitoring and sampling tanks with filtration/IX
6.	Passed to WGS delay beds
7.	Collection and storage in oil tanks
8.	Sorted dependent on size/type
9.	Monitoring and swabbing (over period of time) with potential cleaning/decontamination or size reduction
10.	Potential quenching, filtration, chemical treatment, and ion exchange, as necessary
11.	Size reduction and placed in HHISO
12.	Placed in HOLTEC flask
13.	Collect and store
14.	Collect in a chemical waste tank and de-water (cross flow filtration)
15.	Collect in 200L Drum
Disposal Method	
A.	Site ILW store until UK repository becomes available
B.	Sent to LLW repository for storage
C.	Recycle or free issue
D.	Discharge to site drain
E.	Discharge to atmosphere
F.	Incineration
G.	Discharge via site effluent treatment
H.	Underground HLW storage facility
I.	Offsite contractor (e.g., NSG Environmental Ltd)
J.	Send to Inutec for drying and disposal at LLWR

Table 27A-5. Steel and Concrete Rubble from Demolishing Various Modules

Module	Waste Description	LLW/ILW/ HLW/Mixed	Physical/Chemical Description	Waste Form	Steel Mass	Steel Volume[(1)]	Concrete Mass	Concrete Volume[(1)]
					Tonne	m^3	Tonne	m^3
CA01	Concrete/Steel	LLW	Steel framework filled with concrete	Solid	907	118	4315	1796
CA02	Concrete/Steel	LLW	Steel framework filled with concrete	Solid	30	4	142	59
CA03	Stainless Steel	LLW	Reinforced curved tank wall section	Solid	191	25	N/A	N/A
CA04	Concrete/Steel	LLW	Barrel shaped octagonal structure houses reactor vessel	Solid	28	4	478	199[(2)]
	Lead/Titanium	LLW	Lead encased titanium tubes	Solid	4	0	N/A	N/A
CA05	Carbon Steel	LLW	Steel framework filled with concrete	Solid	56	7	268	111

Notes:

1. Demolished volume is based on density of 7700 kg/m^3 for steel and 2400 kg/m^3 for concrete and 11000 kg/m^3 for lead filled titanium tubes. Provisions should be included in storage facilities to accommodate packaged waste that may require two to three times demolished volume. With proper decontamination prior to demolition, most of this waste will be essentially all VLLW.
2. Concrete volume based on the assumption that a concentric section around the reactor vessel cavity in the vicinity of the core will contain enough activation products to be treated as an LLW.

TABLE OF CONTENTS

LIST OF TABLES

None.

LIST OF FIGURES

None.

LIST OF ABBREVIATIONS AND ACRONYMS

ac	alternating current
ALARP	as low as reasonably practicable
BSL	basic safety level
BSO	basic safety objective
C&I	control and instrumentation
CDF	core damage frequency
CIM	component interface module
CMT	core makeup tank
CVS	chemical and volume control system
DAS	diverse actuation system
DB	design basis
DDS	data display and processing system
DRP	design reference point
EA	Environment Agency
EMI	electromagnetic interference
EPRI	Electric Power Research Institute
GDA	generic design assessment
HED	human engineering discrepancy
HF	human factors
HVAC	heating, ventilation, and air conditioning
IAEA	International Atomic Energy Agency
LOCA	loss-of-coolant accident
LRF	large release frequency
MCR	main control room
ONR	Office for Nuclear Regulation
OSC	operational support centre
PCSR	Pre-Construction Safety Report
PLS	plant control system
PLSR	Plant Life Cycle Safety Report
PMS	protection and safety monitoring system
PSA	probabilistic safety assessment
PWR	pressurised water reactor
RCCA	rod cluster control assembly
RCP	reactor coolant pump
RNS	normal residual heat removal system
RSR	remote shutdown room
SAP	safety assessment principle
SFAIRP	so far as is reasonably practicable
SGTR	steam generator tube rupture
SLC	site licence condition
SSC	system, structure, or component
TSC	technical support centre
UK	United Kingdom
WGMS	Westinghouse Global Management System

28 CONCLUSIONS

28.1 Introduction

This chapter summarises the main conclusions from the Pre-Construction Safety Report (PCSR) for the Westinghouse AP1000 nuclear power plant submitted under the Office for Nuclear Regulation (ONR) generic design assessment (GDA) process (Reference 28.1).

28.2 Setting the Pre-Construction Safety Report in Context

Chapter 1 of Volume 1 sets the PCSR in the context of the evolution of the AP1000 design, and of the United Kingdom (UK) regulatory regime in general and the GDA process in particular.

Chapter 1 also introduces the overall safety claims that the implementation of passive safety features and the simplification of the design significantly contribute to the improved safety and reliability of the plant over existing plants; that the AP1000 design, construction, and operation fully meet UK licensing requirements and safety assessment principles (SAPs) (Reference 28.2); and that levels of public, worker, and environmental risk from all modes of operation and all parts of the plant life cycle are as low as reasonably practicable (ALARP).

Chapter 2 then gives an overview of the safety case developed in the subsequent volumes and chapters of this PCSR that demonstrates that these overall safety claims are justified. The structure of the safety case presented in this PCSR is based on the following claims introduced in Chapter 2:

- Safety is managed throughout the plant life cycle.
- Safety is achieved through simple, passive design and defence in depth.
- Design and operation are tolerant to faults and risks are ALARP.
- Engineering solutions are fully substantiated.
- Radiological releases are minimised in normal and abnormal operating conditions.

28.3 Safety Is Managed throughout the Plant Life Cycle

The Westinghouse Global Management System (WGMS) discussed in Chapter 3 ensures that documented quality and safety procedures are in place, and that they are robust, managed, and monitored in accordance with statutory, legal, and regulatory requirements. The WGMS meets the requirements of UK and international regulations and good practice. Post-GDA, the WGMS also ensures that Westinghouse safety management arrangements are appropriately transferred and integrated into the safety management systems of the licensees, who become responsible for safety once the Design Acceptance Confirmation is received from the ONR and a Statement of Design Acceptance is received from the EA. The arrangements ensure that safety-important information is available, as appropriate, throughout the construction, commissioning and operating phases and eventual decommissioning.

An integral part of this process is adapting the safety case presented in this PCSR, which is based on the UK generic site described in Chapter 4 to the actual site(s) where the design is to be built. The Plant Life Cycle Safety Report (PLSR) (Reference 28.3) describes the process by which the knowledge within the AP1000 safety case can be most comprehensively transferred to the potential licensee and outlines the Westinghouse assumption about any licensee's management system. Plant life cycle issues related to engineering (for example,

commissioning, maintenance, ageing, and decommissioning) are addressed in Chapter 7 as discussed below in Section 28.4.

In these chapters, Westinghouse safety management is shown to be a continuous process from design through construction and commissioning to operation and ultimate decommissioning.

28.3.1 Safety Management Conclusions

The principles underlying the management of safety ensure that the design, construction, commissioning, operation, and decommissioning fully meet UK regulatory expectations and best practice and that the public, worker, and environmental risks associated with the above phases of the plant life cycle are ALARP.

28.4 Safety Is Achieved through Simple, Passive Design and Defence in Depth

Volume 2 describes the AP1000 design and operation.

Chapter 5 introduces the engineering principles that underlie the AP1000 design. In particular, it gives the scheme for categorising safety functions and classifying the systems, structures, and components (SSCs) that provide them. This categorisation and classification scheme is the basis on which appropriate codes and standards are applied, how maintenance and testing regimes are determined, and how the equipment is qualified, commensurate with the safety importance of each SSC. The categorisation and classification scheme provides a coherent framework for developing and substantiating the safety case for the design.

Where the AP1000 plant departs from conventional PWRs is in the use of passive means of providing essential safety functions to protect against faults. These passive safety features rely solely on natural mechanisms such as natural convection and driving forces derived from compressed gases rather than active pumped systems; therefore, safety is substantially enhanced. Further, there is no reliance on alternating current (ac) power to bring the reactor to a safe shutdown condition or to keep it there. More conventional active systems provide defence in depth by reducing the probability that the passive safety features will be actuated.

All of these features and their operation are described in Chapter 6. The design described in Chapter 6 draws together information specified by the Design Reference Point (DRP) (Reference 28.4) and supporting safety case information. The information presented in Chapter 6 is used as the basis for all the assessments presented in the PCSR and covers the following:

- Reactor systems
- Steam and power conversion systems
- Normal operations
- Passive safety systems
- Control and instrumentation (C&I)
- Essential electrical systems
- Auxiliary systems
- Containment and ventilation systems
- Fuel handling and radwaste systems
- Civil structures

Chapter 7 discusses how the engineering aspects are managed through the life cycle, including during power operations. It recognises that the AP1000 plant design, build, test and maintenance activities can influence the safety of the AP1000 plant throughout life and that there is a requirement for Westinghouse to work with the operator to ensure the continued safety of the reactor. However, it is also accepted that the delivery of Westinghouse's arrangements post-design acceptance and on a licensed site will be under and in agreement with the licensee's arrangements.

Chapter 7 also outlines the long-term approach to the management of the ageing mechanisms to ensure the plant remains safe and risks remain ALARP for the duration of the plant life cycle. It also sets out the approach to the periodic safety review process.

28.4.1 Design Conclusions

In many respects, the AP1000 reactor is a conventional PWR. However, the above chapters demonstrate that the implementation of passive safety features, simplification of the design, and defence in depth significantly contribute to a high level of safety and reliability.

28.5 Design and Operation Are Tolerant to Faults and Risks Are As Low As Reasonably Practicable

Volume 3 presents the fault and accident analysis that demonstrates the fault tolerance of the AP1000 design and operation. The methodology used is outlined in Chapter 8.

Possible faults have been identified in a systematic, auditable, and comprehensive way for the reference design, including all operating modes of the reactor and all inventories of radioactive material on the site. The list of faults is presented in Chapter 8, Appendix 8A. The list of faults is comprehensive, but some of the individual faults may be bounded by other faults whose behaviour is similar and have similar provision of safety functions.

The fault list also details the hazards arising onsite or offsite (internal and external hazards, respectively).

28.5.1 Design Basis Analysis

The design basis (DB) analysis of each of the fault groups is given in turn in Chapter 9. For each, several faults are identified and analysed that produce the most onerous demand on the design safety systems. The main fault types analysed in Chapter 9 are the following:

- Main steam line break
- Increase in heat removal faults (excluding main steam line break)
- Feed line break
- Decrease in heat removal faults (excluding main feed line break)
- Major mechanical failure of a single reactor coolant pump (RCP)
- Decrease in reactor coolant flow faults (excluding major mechanical failure of a single RCP)
- Reactivity and power distribution faults (excluding control rod ejection)

- Ejection of a rod cluster control assembly (RCCA) from the core
- Inadvertent operation of a core makeup tank (CMT)
- Chemical and volume control system (CVS) malfunction that increases reactor coolant inventory
- Steam generator tube rupture (SGTR)
- Large-break loss–of-coolant accidents (LOCAs)
- Medium-break LOCA
- Small-break LOCA
- Safety injection line break
- CMT line break
- Passive residual heat removal tube rupture
- Reactor coolant leakage
- Large cold leg break in Mode 4 operation
- Loss of normal residual heat removal system (RNS) in Modes 4 and 5 with RCS intact
- Loss of RNS in Mode 5 with RCS open
- Criticality faults during refuelling and spent fuel storage
- Loss of heat removal during refuelling and spent fuel storage
- Dropped fuel cask in loading bay
- Dropped fuel assembly onto other fuel
- Operator falls into flooded refuelling cavity or fuel storage pool
- Water-level fall in refuelling cavity or fuel storage pool (shielding lost)
- Failure of filters in heating, ventilation, and air conditioning (HVAC) system
- Dropped filters
- Reduced HVAC airflow
- Loss of containment of spent resin
- Dropping of radioactive exchangeable items
- Failure of small lines carrying primary coolant outside the containment

The DB response of the system and the corresponding SSCs to the analysed faults in each of these groups demonstrates that the applicable acceptance criteria is met (including the dose targets given in the SAPs, Reference 28.2, Target 4. The set of SSCs required to ensure that the criteria are met are assigned to the appropriate class and the corresponding safety function(s) to the appropriate category, using the scheme described in Chapter 5.

Where the fault falls into the category of frequent faults (initiating event frequency $>10^{-3}$/yr), alternative means of providing the necessary safety functions are also identified to comply with the SAP requirement that frequent faults should have diverse means of providing the necessary safety functions. These faults are analysed to demonstrate that the diverse SSCs listed can mitigate the event and satisfy the applicable acceptance criteria.

Also as part of this process, as required under site licence condition (SLC) 23, limits and conditions are identified which may be candidates for operating rules or which may have operating rules associated with them. Similarly, required operating instructions (e.g., to manually initiate safety systems) are identified. These operating instructions are considered in Chapter 13 as outlined below in Section 28.5.4. Finally, other SSCs are identified that may provide defence in depth and contribute to ALARP.

Chapter 9 demonstrates that, for all but one of the above fault groups, with the identified SSCs operating and identified limits and conditions met, the calculated doses are below the basic safety objective (BSO) for the corresponding DB dose target (SAP Target 4) (Reference 28.2). For the one fault where this is not the case (SGTR), the calculated doses are still well below the basic safety level (BSL) for the corresponding dose target. Further, for all of the fault groups, the risks from all modes of normal operation and fault conditions are shown to be ALARP.

28.5.2 Probabilistic Safety Assessment

The probabilistic safety assessment (PSA) discussed in Chapter 10 takes the same reactor and spent fuel pool fault groups as in Chapter 9 and assesses the progression of events if the safety systems fail or do not operate as designed. Each fault group is assigned an initiating event frequency, normally based on operating experience for other PWRs or from reliability assessments and a set of sequences developed representing the failure of safety systems. Each sequence has a frequency calculated from the initiating event frequency and the reliabilities of the mitigating systems. Consequences for each sequence are calculated from transient or other analyses.

The PSA gives the required analysis of severe accidents (i.e., sequences that lead to offsite doses above the DB dose targets or that lead to damage of the reactor core).

Two main parameters constitute the output of the PSA: the core damage frequency (CDF) and the large release frequency (LRF). For at-power internal events, these are assessed to have values of 1.7×10^{-7}/yr and 1.7×10^{-8}/yr, respectively. Both parameters are several orders of magnitude lower than for conventional PWRs of similar power output. Accidents in shutdown conditions make a contribution to these parameters that are comparable to the at-power values.

The SAPs (Reference 28.2) give a number of probabilistic targets to be met by the plant. The PSA gives the results relevant to internally initiated reactor faults and, as such, makes a major contribution to the demonstration that these targets are met. However, other parts of the fault and accident analysis also make a contribution so the consideration of probabilistic targets is

postponed until Chapter 14 (see Section 28.5.5 below), which gives the overall conclusions of the fault and accident analysis.

28.5.3 Internal and External Hazards

Internal and external hazards and the risks from operator errors and other human factors have been assessed separately.

Internal hazards are those that arise onsite but outside the nuclear systems that have the potential to affect the safety of the AP1000 plant. Internal hazards have been identified in a systematic, auditable and comprehensive way, and the following are assessed in Chapter 11:

- Internal fires
- Internal flood
- Pressure part failure
- Internal explosions
- Internal missiles
- Release of toxic, corrosive, or flammable material
- Dropped loads and load mishandling
- Biological agents
- Onsite transport
- Electromagnetic interference (EMI)

The focus of the Internal Hazard assessment is to demonstrate that the Class 1 SSCs delivering the Category A safety functions are adequately protected from design basis internal hazards or that there is sufficient redundancy that if some equipment is lost, the safety function can still be delivered. Protection from internal hazards of Class 2 SSCs delivering Category A safety functions and providing defence in depth and Class 2 SSCs delivering supporting Category B safety functions have also been assessed, where operation of such Class 2 SSCs is credited. Where relevant, the effect of combined and consequential hazards has been reviewed and assessed.

The assessment in each of the Internal Hazard areas has confirmed that the DB hazard does not prevent the delivery of the Category A safety functions or any supporting Category B safety functions. The conclusion is, therefore, that the AP1000 design is tolerant to faults arising from internal hazards and that the designed safety measures are effective.

External hazards are those naturally occurring and man-made hazards that may arise offsite. Examples include earthquakes, extreme weather, and aircraft crash. The following external hazards for the generic site described in Chapter 4 are assessed in Chapter 12:

- Earthquakes
- External flooding
- Accidental aircraft crash
- External explosion
- Extreme ambient temperatures
- Meteorology
- Extreme wind
- Offsite fire and smoke
- Offsite missiles
- Biological fouling

- EMI and lightning

The majority of the external hazards assessed in this assessment fall within the bounds of the generic site parameters given in Chapter 4 and thus may be regarded as within the DB of the plant. This is mainly due to the inherent robustness of the AP1000 design.

The analysis is similar to that done for internal hazards, and this chapter demonstrates that the delivery of the Category A safety functions by Class 1 SSCs is not compromised by design basis external hazards and that the AP1000 design measures are effective.

A number of site-specific assessment requirements have been identified, which will need to be addressed in any site-specific PCSR, and there are a number of overall site requirements including accident/incident management and emergency preparedness that will need further consideration at the appropriate stage.

28.5.4 Human Factors

Chapter 13 describes how an integrated and managed Human Factors (HF) Engineering programme has been rigorously and systematically applied throughout the concept, analysis and design phases of the Standard AP1000 Plant design. The measured and proportional application of HF processes and methodologies has ensured that the design considers at all times the role of the human operator in the safe and efficient operation of AP1000.

The HF design of the AP1000 Plant has been based upon a set of internationally recognised Standards and Codes and on industry experience and guidance that can be deemed as relevant good practice in the UK.

The difference between the role of the operator in the AP1000 plant and in current plants is one of degree, and not a fundamental change in character. The use of passive safety systems, simplification of the design, and appropriate use of automated systems mean that the operators are responsible for assessing plant status and verifying the availability and operability of, and the need for actuation or termination of the plant's defence in depth and passive safety systems. The HSI includes displays that integrate information to facilitate assessment of plant state and supervisory control of automated and passive systems, and a computerised procedure system that facilitates execution of the AOPs and EOPs. It is therefore easier to place the plant into a safe condition and maintain it in a safe state under post-fault conditions. The Human Factors programme has provided guidance to ensure that functions have been allocated appropriately between automatic systems and human operators. Where operator action is required, the corresponding action is strictly controlled through the use of plant procedures with supervision and verification monitoring from the main control room (MCR) supervisor, and crew performance is governed by the plant conduct of operations. The combined effect of these provisions is to minimise the likelihood of operator errors that might affect plant safety. The design evolution of AP1000 is consistent with the ONR's expectations for the demonstration of ALARP with respect to new commercial reactor designs.

It is recognised that, even with the best design from a human factors perspective, operator errors may still occur. Chapter 13 demonstrates that the risk from operator errors is small and reduced to a level that is ALARP. This demonstration consists of a systematic identification of operator errors, that is, the failure of operators to perform actions required to ensure nuclear safety correctly, and the assessment of these errors to show that their contribution to risk is reduced to levels that are low and ALARP.

The following three types of operator errors identified by the International Atomic Energy Agency (IAEA) are assessed:

- **Type A** – Operator actions that degrade or prevent systems from performing their safety functions (maintenance latent errors)

- **Type B** – Operator actions that induce initiating events (operator induced initiating events and maintenance induced initiating events)

- **Type C** – Post-fault operator actions that prevent the mitigation of the initiating event or make it worse

Human errors of these three types are identified from both the DB analysis presented in Chapter 9 and the PSA in Chapter 10. These errors are screened according to their risk significance, and those considered to be risk-significant are analysed and documented in a uniform and systematic way in accordance with current good human factors analysis practice for the purpose of this PCSR.

Acknowledged gaps in the human factors safety case substantiation for GDA have been identified and will need to be further progressed during the site licensing phase. These shortfall areas are:

- Completion of the resolution process currently in progress for the human engineering discrepancy (HED) and HED issues arising from the HF verification and validation activity conducted for standard AP1000 plant design.

- Completing the plant start-up C&I HF verification activity described in Reference 13.61.

- Complete human error analysis process at a cognitive-level for all screened-in, risk-significant operator actions, as demonstrated on a sample of actions for GDA, and provide these as input into the site PSA.

- Completion of the HF maintenance and maintainability assessments for local plant maintenance, testing, inspection, and surveillance activities.

- Implementation of a site-specific HF integration plan as part of the overall AP1000 programme plan.

The conclusion of the human factors assessment is that, as a consequence of the AP1000 plant operating philosophy, the design, and the human factors programme, the role of the operators in ensuring nuclear safety in the AP1000 plant has been optimized, andthe risk due to human error is reduced ALARP for GDA.

28.5.5 Conclusions from Fault and Accident Analysis

Chapter 14 summarises and consolidates the results of the chapters in Volume 3 (Chapters 8 to 13) so that comparisons can be made with the other SAP targets.

The chapter lists all of the SSCs that have been identified in the fault and accident analysis as being important to safety, giving their classification and performance and reliability claims made in the safety case.

SAP Targets 5 and 7 are probabilistic targets for risk of individual death for workers and public, respectively. Both have the same BSL ($1.0x10^{-4}$/yr) and BSO ($1.0x10^{-6}$/yr). The PSA doesn't give this value explicitly, but Chapter 14 argues that, for reactor faults, the CDF provides a reasonable surrogate and has a value well below the BSO. Other faults only provide a minor contribution to these targets.

Targets 6 and 8 give frequency-dose targets for the plant as a whole for the workforce and public, respectively. Bringing the information together from the various chapters shows that the targets are easily met.

Finally, Target 9 is a societal risk target, giving BSL and BSO for the risk of 100 or more fatalities. Chapter 14 argues that the LRF, which is significantly below the BSO, is a reasonable surrogate for this.

Chapter 14 brings together the various ALARP assessments that have been done in the past and the individual ALARP assessments coming from the fault and hazard assessments in this PCSR to demonstrate that the risks from AP1000 design and operation are ALARP.

During the development of the AP1000 plant, design choices have been made that reduce fault frequencies, removing some faults common to existing plants altogether. The passive design of protection systems and defence in depth contribute significantly to a design that is extremely tolerant to faults.

The designers of the AP1000 plant have sought means of further reducing risk during every part of the design and safety assessment possesses. The designers have also used available tools such as the PSA and severe accident assessment to identify risk-reduction measures that might be reasonably practicable to implement. Many design decisions and design changes have been implemented as a result, which contribute to the overall risk being ALARP.

28.6 Engineering Solutions Are Fully Substantiated

The SSCs that have been identified in the fault and accident analysis as being important to safety, their classification, and the performance and reliability claims made for them in the safety case are listed in the Engineering Schedule in Appendix 15A.

Chapter 15 lists the sources of claims on SSCs in the safety case and the requirements on SSC performance that are implied by them. These requirements come from the following sources:

- Performance requirements from the transient analysis performed as part of the DB assessment
- Survivability and operability requirements arising from the need to operate in normal plant environmental conditions and the environmental conditions following a design basis accident (DBA)
- Reliability requirements from the probabilistic assessment of DB faults and the PSA
- Separation and segregation requirements from the internal hazard assessments
- Seismic qualification requirements arising from the external hazards assessment

- Quality requirements for design, manufacturing, installation, commissioning, maintenance, and testing

- Durability requirements related to expected plant service life

The remaining chapters of Volume 4 (Chapters 16 to 23) provide the evidence that the SSCs identified in the fault assessments can meet the requirements arising from the claims made on them in the safety case through their design and by the way they are tested and maintained throughout the life of the plant.

28.6.1 Civil Engineering

Chapter 16 summarises the generic design information, which is used to justify that the civil engineering structures will withstand the loads arising from normal operations, internal hazards, external hazards, and internal plant faults.

The civil engineering safety case clearly has a dependency on site-specific information. However, the AP1000 international design is based on external hazard data representative of a worst-case site. This leads to structures having robust load resisting systems capable of withstanding the generally more benign UK environments.

The approach to construction acknowledges that the achievement of the design intent has some dependency on the site, as well as the organisations with responsibilities for construction, and that it would be inappropriate for the construction processes to be fully defined before the site-specific PCSR is developed. While still complying with the codes and standards identified in this chapter, choices remain relating to the specification and methods of construction.

The design has taken into account the 60-year design life. It is concluded that there will be no erosion of the capability of the civil engineering structures to withstand the loads required by the nuclear safety case, provided the appropriate maintenance, examination, inspections, and testing are undertaken. Beyond 60 years, it is likely that the nuclear island structures will still need to provide safety functions until such time as decommissioning has removed all the significant nuclear materials. Replacing the nuclear island civil engineering structures is generally not an option, which can be a possibility when considering internal plant; therefore, the nuclear island structures will need to have a working life well in excess of 60 years, with the exception of some of the water storage structures that may no longer be needed following cessation of power operation. The nuclear island is constructed from a combination of reinforced concrete, structural steelwork, and SC-constructed elements. A working life of 120 years is achievable in line with normal civil engineering criteria

It is concluded that the AP1000 design demonstrates that the deterministic justifications of the civil engineering structures are appropriate to their safety function and class, and that the necessary normal and hazard loads will be withstood as required, subject to appropriate investigations and confirmations being provided relevant to a particular site.

28.6.2 Mechanical Engineering

Chapter 17 considers the mechanical systems, which largely provide safety functions to prevent fuel damage and the consequent release of radioactivity. Analysis of these systems has therefore been carried out to review their requirements against three primary safety functions: reactivity control, residual heat removal, and containment.

The role of each mechanical system in normal and abnormal operation is discussed, and the primary safety functions to which the system contributes are identified. A description of each mechanical system is provided that shows how the SSCs that make up the system contribute to the relevant primary safety functions.

The chapter provides evidence that each SSC can meet the requirements placed on it by the safety case in terms of performance and reliability appropriate to its importance for safety as characterised by its safety classification. The evidence consists of design criteria, discussion of applicable codes and standards, and deterministic analysis, as appropriate.

The conclusion of the chapter is that the mechanical design fully meets the requirements of the safety case in that the individual SSCs assessed are designed, manufactured, installed, tested, and maintained according to the appropriate codes and standards and in a manner consistent with their safety importance as identified in the safety case and appropriate to their safety classification.

28.6.3 Essential Electrical Systems

Chapter 18 describes the design of the electrical power systems of the AP1000 plant, including essential supplies, main and standby generation, auxiliary supplies, main export grid connection, and maintenance grid connection.

A distinguishing feature of the AP1000 plant is that it is designed to be able to achieve a safe shutdown without offsite ac power supplies or standby diesel generators; although defence in depth considerations mean that the plant is normally operated and shut down with ac power available.

The AP1000 electrical system fulfils a number of functions that are important to nuclear safety, contributing to the provision of the primary safety functions of heat removal, containment, and criticality control identified in the safety case. It also contributes to defence in depth.

To reflect the relative importance of each function and the system to deliver that function, the AP1000 plant electrical system is classified according to the scheme given in Chapter 5. Chapter 18 references evidence that the electrical system has been designed in accordance with international nuclear safety standards and follows the principles of diversity, redundancy, segregation, defence in depth, and quality of design and equipment commensurate with the classification of the corresponding SSCs and can meet the performance and reliability requirements placed on it by the safety case.

The conclusion of the chapter is that the design of the electrical systems fully meets the requirements of the safety case by supporting the provision of the main safety functions and by providing defence in depth.

28.6.4 Control and Instrumentation

Chapter 19 discusses the AP1000 C&I systems, which form a fundamental part of the safety systems used to shut down the reactor following DB transients and which maintain the reactor in the shutdown state. Provision is made for continued monitoring in the main control room (MCR) and from the remote shutdown room (RSR). The MCR remains habitable following DBA. The C&I systems are also important for the provision of the reactivity control, residual heat removal and containment safety functions and are classified in accordance with their safety importance in the same way as other systems.

The Class 1 protection and safety monitoring system (PMS) is designed to respond automatically so that specified limiting conditions are not transgressed. The Class 2 diverse actuation system (DAS) provides backup to the PMS in actuating Class 1 safety systems. The plant control system (PLS) which is a Class 2 system provides the main closed loop controls necessary for plant operation and mitigation for plant transients in advance of Class 1 system actuation. The data display and processing system (DDS) which is Class 3 provides the plant monitoring and control interface for the duty system and as subset of the systems important to safety. The DAS is included to support the AP1000 design risk goals by reducing the probability of core damage or a severe accident, which potentially results from the unlikely coincidence of postulated transients and postulated common-mode failure in the PMS and the PLS.

Bases of safety justifications have been produced for the principal C&I systems i.e. the PMS, DAS, PLS and DDS. The PMS basis of safety justification refers to lower tier safety justifications where specific aspects of the system are further substantiated.

Three supporting documents have been produced for Chapter 19 to provide further justification and substantiation of the overall C&I architecture and include:

- an ALARP justification
- SAPs Conformance Assessment
- an IEC 61513 safety Life Cycle Conformance Assessment

The conclusion of the chapter is that the design of the principal AP1000 C&I systems will meet the requirements of the safety case by supporting the provision of the main safety functions and by providing defence in depth, once the identified gaps in compliance and the associated compensating measures have been completed.

28.6.5 Structural Integrity

Chapter 20 provides a safety justification of AP1000 components at the design stage in support of the GDA. It provides component safety reports that provide safety arguments to establish that the structural reliability of each major AP1000 primary pressure boundary component (e.g., reactor pressure vessel, steam generators, and pressuriser) is commensurate with the consequences of gross failure.

Assurance that the safety functional requirements of individual components will be met at all times is provided by substantiating structural integrity against appropriate structural reliability targets depending on the structural integrity classification of the component. Detailed substantiation of the safety claims made on each major structural component is provided in the individual component safety reports.

The chapter concludes that the safety arguments presented identify a suitable and sufficient diversity of evidence to substantiate the structural reliability claimed for the AP1000 components addressed.

28.6.6 Reactor Chemistry

Chapter 21 describes the application of chemical controls and treatments in the AP1000 plant design. It also describes and assesses the systems involved in the provision of chemical controls, principally the CVS.

A number of systems in the AP1000 design contain fluids that are essential to their functions, including heat transfer and control of core reactivity. The quality of these fluids and their interactions with system components and materials can substantially impact the reliable and safe operation of the individual systems or the reactor as a whole. Chemical additives are employed to optimise the performance of the fluids and minimise potential negative effects e.g., corrosion of materials. Chemistry is also used as a means to mitigate impacts in accident and fault conditions, principally by controlling levels of radioactivity in the primary and secondary coolant.

To achieve these aims, chemical controls are in place in the primary circuit to provide the following functions:

- Control reactivity of the core to within operating limits (control of boron levels)
- Maintain integrity of the primary circuit and the fuel cladding (control of oxygen levels and pH)
- Minimise build up of radioactivity on plant outside the core region due to the irradiation and transport of corrosion products (control of crud formation and transport)

The detailed chemistry control strategy is the responsibility of the plant operator, but Westinghouse endorses operating within Electric Power Research Institute (EPRI) guidelines on reactor chemistry, which are developed from accumulated industry-wide research and operating experience and are an authoritative guide to best practice. The AP1000 plant is designed to operate safely within these guidelines and the chemistry operating specifications and technical specifications reflect the EPRI standards.

This chapter provides evidence that the AP1000 reactor chemistry and chemistry control systems support the overall safety claims by aiding control of core reactivity, controlling the integrity of the pressure boundary, and controlling the quantity, distribution, and containment of radioactive materials, thereby ensuring safe operation of the reactor.

The conclusion of the chapter is that the chemical controls in the design significantly contribute to safe operation of the plant and reduce releases to the environment in accident conditions.

28.6.7 Fuel Design

Chapter 22 provides a safety justification of the fuel assemblies in the AP1000 reactor. For normal operation, this means that all reasonable steps are taken to minimise the failure of the fuel rod cladding and thus minimise the release of radioactive fission products into the coolant. For fault conditions, the definition of satisfactory performance depends on the frequency with which the fault is expected to occur.

This chapter presents the safety case for the standard fuel element design in the AP1000 PWR. The safety case consists of a justification that the nuclear, thermal, and hydraulic design of the fuel meets the design bases, functional requirements, and safety performance required for normal operation and during transients and in accident conditions.

A number of fundamental safety criteria are defined in terms of the ability to shut the reactor down, avoidance of fuel damage or fuel failure, and limits to release to the environment. The mechanical design of the core components and their physical arrangement, together with the

corrective actions of the reactor control, protection, and emergency cooling systems, ensure that in any fault these criteria are met.

These safety criteria together define a number of safety design bases.

During normal operation, following any operational transient or following any fault expected to occur during the lifetime of the fuel, the following apply:

- The number of clad failures must be small so that the safety criteria are clearly met.
- The fuel and in-core components suffer no deterioration that could prejudice their performance in subsequent, more severe faults.

In addition, a number of design bases for design basis fault sequences have been identified. These safety design bases lead to limiting conditions (for example, minimum departure from nucleate boiling ratio or critical heat flux) within which the fuel can operate safely during both normal and fault conditions.

The conclusion of the chapter is that none of the design bases or limiting conditions is exceeded when the fuel is subjected to the full range of operational and fault conditions considered in Chapter 9.

28.6.8 Containment and Ventilation

Chapter 23 provides the evidence that the design of the containment and nuclear ventilation systems in the AP1000 plant is adequate to meet the safety claims placed upon these systems in other parts of the safety case, both for normal operations and under fault conditions.

The containment and ventilation systems largely support the primary safety functions of the containment of radioactive substances and heat transfer/residual heat removal, and provide environmental support to SSCs, which contribute to primary safety functions. Analysis of the containment and ventilation systems has therefore been carried out to review their requirements against the primary safety functions.

The chapter provides evidence that each SSC can meet the requirements placed on it by the safety case in terms of performance and reliability appropriate to its importance for safety as characterised by its safety classification. The evidence consists of design criteria, discussion of applicable codes and standards, and deterministic analysis, as appropriate.

The conclusion of the chapter is that the mechanical design fully meets the requirements of the safety case in that the individual SSCs assessed are designed, manufactured, installed, tested, and maintained according to the appropriate codes and standards and in a manner consistent with their safety importance as identified in the safety case and appropriate to their safety classification. The justification against these safety functions demonstrates that the risks have been reduced to a level that can be considered to be ALARP.

28.6.9 Engineering Substantiation Conclusions

The tolerance to faults and demonstration that risk is ALARP rely on claims made on the SSCs that make up the design and on assumptions regarding fuel design and reactor chemistry. The chapters that make up the engineering substantiation volume provide the arguments and evidence that substantiate the claims made on SSCs in the other parts of the safety case.

28.7 Radiological Releases Are Minimised in Normal and Abnormal Operating Conditions

The safety of pre-power operation, power operation and post-power operation activities for the AP1000 plant are based on risk reduction, dose minimisation, waste minimisation, and safe storage. Volume 4 addresses control of radiation in this context. The principle of ALARP is applied in addition in all of these cases.

28.7.1 Radiological Protection

Chapter 24 covers the protection of workers and members of the public against exposure to ionising radiation in normal operations and protection of essential workers following a major accident.

Radiation protection from external radiation under normal operating conditions, including routine maintenance, is achieved in the design by reducing the sources of radiation so far as is reasonably practicable (SFAIRP). Where sources cannot reasonably be reduced further, exposure to radiation is controlled by means of shielding and by controlling the duration of exposure.

The design of the AP1000 plant has taken account of utility requirements for reliability, safe operation and maintenance, and reduction in operator dose. Experience from the continuing improvements in operating plants has been incorporated into the design (e.g., materials selection, plant layout) and operating regime (e.g., reactivity control, water chemistry) to reduce radiation levels from the plant. In areas where exposure to external radiation are likely, suitable and sufficient shielding is provided to protect workers during normal operations, maintenance, and fault conditions. Features have been incorporated into the design that reduce the outage time for refuelling and, as a result, reduce the duration of worker exposure to radiation. Where applicable, remote inspection and maintenance systems have been developed to further reduce exposures during shutdown.

Protection from radioactive contamination is achieved by reducing the activity present in dispersible form, provision of suitable containment and ventilation, layout of areas, control of access, monitoring, and personal protective equipment.

In fault and accident conditions, the design allows the reactor to be brought to safe shutdown without any release of radioactivity and systems are in place to maintain the integrity of the containment systems for at least 72 hours without the need for standby systems. In the unlikely event that a release does occur, the MCR is provided with an uncontaminated supply of air from pressurised cylinders and shielding calculations demonstrate that the dose to workers in the MCR during this period will be limited. Pre-defined routes are provided to locations that need to be accessed in a major emergency.

The conclusion of this chapter is that everything has been done to ensure that risks from radiation in normal operation and risks to operators during accidents have been reduced to levels that are ALARP.

28.7.2 Accident Management

Chapter 25 complements the assessment in Chapter 24 in that it discusses protection of the public during fault and accident conditions.

By necessity, accident management arrangements will be site-specific, but the chapter addresses requirements for emergency response to a nuclear incident and emergency. It also

identifies the provisions available in the current AP1000 design to respond to a nuclear incident or an emergency, as well as identifies the requirement for contingency plans, which will be fully integrated with the environmental monitoring programme.

The chapter concludes that the AP1000 design facilitates the management of an incident or emergency by the provision of the MCR, technical support centre (TSC), RSR, and operational support centre (OSC).

28.7.3 Radioactive Waste Management

Chapter 26 provides evidence that Westinghouse has produced an integrated waste strategy to address the radioactive wastes and spent fuel produced by AP1000 plant, which is appropriate for the assessment of a generic design and contributes to the minimisation of radiation doses to the operators and public.

The design of the plant is such that the generation of radioactive wastes are minimised. Any wastes that are generated are contained, and cooled where necessary. As far as can be ascertained during the GDA process, all wastes generated during operation will be able to be packaged and disposed of offsite, with discharges that respect agreed annual limits.

28.7.4 Decommissioning

Chapter 27 identifies the principles that define the AP1000 plant decommissioning strategy.

The AP1000 plant has been designed so that it can be safely decommissioned, with steps being taken at the design stage to minimise the amount of waste generated during the process.

Assumptions have been made on the status of the plant at the end of operations based on the design and operational guidance set out in this document. A decommissioning plan, which meets UK regulatory requirements and international best practice, has been developed based on this strategy and assumptions regarding current available techniques. Dose management is assessed to be ALARP.

Waste volumes and activities have been minimised by design. It is recognised that a period of interim storage onsite may be required for some items before ultimate disposal is possible. The waste will be stored on-site in specifically designed facilities in a passively safe condition. The interim passively safe storage system will not compromise disposability.

28.7.5 Radiation Control Conclusions

Simplifications in the design mean that operator doses during normal operations and during fault conditions are significantly below regulatory and legal limits, and reduced to levels that are ALARP. Operator doses and routine releases to the environment from radioactive waste management onsite are minimised. Decommissioning activities are expected to produce less activated or contaminated material than for existing plants.

28.8 Summary

This PCSR demonstrates that the AP1000 design, construction, commissioning, operation, and ultimate decommissioning fully meet UK licensing requirements and fulfil the requirements of the SAPs (Reference 28.2). In particular, the PCSR demonstrates that normal operating limits are complied with, that risk and consequence targets are met, and that the risks arising from all modes of operation and all parts of the plant life cycle are ALARP.

The safety case presented in this PCSR that provides this demonstration is summarised by the five safety claims introduced in Chapter 2:

- Safety is managed throughout the plant life cycle.
- Safety is achieved through simple, passive design and defence in depth.
- Design and operation are tolerant to faults and risks are ALARP.
- Engineering solutions are fully substantiated.
- Radiological releases are minimised in normal and abnormal operating conditions.

The overall conclusions are that these claims are fully justified. In addition, it is concluded that:

- The use of passive systems and defence in depth makes the AP1000 plant extremely tolerant to faults as demonstrated by at-power internal events CDF of 1.7×10^{-7}/yr and an LRF of 1.7×10^{-8}/yr.

- For most fault conditions, the calculated doses and risks are significantly below the BSO of the relevant SAPs target. In the small number of cases where this is not so, the doses or risks are still significantly below the BSL.

- Risk reduction has been carried out systematically and comprehensively during every part of the design and safety assessment to the point that the risks from the AP1000 design and operation are ALARP.

28.9 References

28.1 "New Nuclear Reactors: Generic Design Assessment, Guidance to Requesting Parties, ONR-GDA-GD-001 Revision 2" Office for Nuclear Regulation, June 2016.

28.2 "Safety Assessment Principles for Nuclear Facilities, 2014 Edition" Rev. 0, Office for Nuclear Regulation, 2014.

28.3 Westinghouse Report UKP-GW-GL-737, Rev. 2, "Plant Life Cycle Safety Report," March 2011.

28.4 Westinghouse Report UKP-GW-GL-060, Rev. 10, "AP1000 Design Reference Point for UK GDA," January 2017.